Cisco Network Modules Hardware Installation Guide

For the Cisco 2600 Series, Cisco 2800 Series, Cisco 3600 Series, Cisco 3700 Series, and Cisco 3800 Series Routers, and the Cisco MWR 1941-DC Mobile Wireless Edge Router

Corporate 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: 408 526-4100

Text Part Number: OL-2485-20

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.

Cisco Network Modules Hardware Installation Guide

Preface

This preface describes the objectives and organization of this guide and explains how to find additional information on related products and services.

Audience

This publication is designed for people who have some experience installing networking equipment such as routers, hubs, servers, and switches. The person installing the device should be familiar with electronic circuitry and wiring practices and have experience as an electronic or electromechanical technician.

Document Organization

See Table 1-6 in Chapter 1, “Overview of Cisco Network Modules for Cisco Access Routers,” for a list of network modules supported by Cisco routers.

See Chapter 2, “Installing Cisco Network Modules in Cisco Access Routers,” for instructions on installing network modules in your router.

See Chapter 3 through Chapter 29 for information about connecting network modules to the network.

See the software configuration guides for Cisco 2600 series, Cisco 2800 series, Cisco 3600 series, Cisco 3700 series, and Cisco 3800 series routers for an overview of network module configuration procedures and information on configuring individual network module interfaces. To obtain this publication, see the “Obtaining Documentation” section on page viii.

See the *Cisco MWR 1941-DC Mobile Wireless Edge Router Software Configuration Guide* for an overview of network module configuration procedures and information on configuring individual network module interfaces on the Cisco MWR 1941-DC router. To obtain this publication, see the “Obtaining Documentation” section on page viii.

Document Conventions

This publication uses the following conventions to convey instructions and information.

Table 1 Document Conventions

Convention	Description
boldface font	Commands and keywords.
italic font	Variables for which you supply values.
[ ]	Keywords or arguments that appear within square brackets are optional.
{**x** | **y** | **z**}	A choice of required keywords appears in braces separated by vertical bars. You must select one.
`screen font`	Examples of information displayed on the screen.
`boldface screen font`	Examples of information you must enter.
< >	Nonprinting characters, for example passwords, appear in angle brackets in contexts where italic font is not available.
[ ]	Default responses to system prompts appear in square brackets.

Note Means *reader take note*. Notes contain helpful suggestions or references to additional information and material.

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

Tip Means *the following information can help you solve a problem*.

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

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. To see translations of the warnings that appear in this publication, refer to the translated safety warnings that accompanied this device.

Note: SAVE THESE INSTRUCTIONS

Note: This documentation is to be used in conjunction with the specific product installation guide that shipped with the product. Please refer to the Installation Guide, Configuration Guide, or other enclosed additional documentation for further details.

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. Voor een vertaling van de waarschuwingen die in deze publicatie verschijnen, dient u de vertaalde veiligheidswaarschuwingen te raadplegen die bij dit apparaat worden geleverd.

Opmerking BEWAAR DEZE INSTRUCTIES.

Opmerking Deze documentatie dient gebruikt te worden in combinatie met de installatiehandleiding voor het specifieke product die bij het product wordt geleverd. Raadpleeg de installatiehandleiding, configuratiehandleiding of andere verdere ingesloten documentatie voor meer informatie.

Varoitus **TÄRKEITÄ TURVALLISUUTEEN LIITTYVIÄ OHJEITA**

Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. Tässä asiakirjassa esitettyjen varoitusten käännökset löydät laitteen mukana toimitetuista ohjeista.

Huomautus SÄILYTÄ NÄMÄ OHJEET

Huomautus Tämä asiakirja on tarkoitettu käytettäväksi yhdessä tuotteen mukana tulleen asennusoppaan kanssa. Katso lisätietoja asennusoppaasta, kokoonpano-oppaasta ja muista mukana toimitetuista asiakirjoista.

Attention **IMPORTANTES INFORMATIONS DE SÉCURITÉ**

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions d'avertissements figurant dans cette publication, consultez les consignes de sécurité traduites qui accompagnent cet appareil.

Remarque CONSERVEZ CES INFORMATIONS

Remarque Cette documentation doit être utilisée avec le guide spécifique d'installation du produit qui accompagne ce dernier. Veuillez vous reporter au Guide d'installation, au Guide de configuration, ou à toute autre documentation jointe pour de plus amples renseignements.

Warnung **WICHTIGE SICHERHEITSANWEISUNGEN**

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewusst. Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise sind im Lieferumfang des Geräts enthalten.

Hinweis BEWAHREN SIE DIESE SICHERHEITSANWEISUNGEN AUF

Hinweis Dieses Handbuch ist zum Gebrauch in Verbindung mit dem Installationshandbuch für Ihr Gerät bestimmt, das dem Gerät beiliegt. Entnehmen Sie bitte alle weiteren Informationen dem Handbuch (Installations- oder Konfigurationshandbuch o. Ä.) für Ihr spezifisches Gerät.

Figyelem! **FONTOS BIZTONSÁGI ELÕÍRÁSOK**

Ez a figyelmezetõ jel veszélyre utal. Sérülésveszélyt rejtõ helyzetben van. Mielõtt bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplõ figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található.

Megjegyzés ÕRIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Megjegyzés Ezt a dokumentációt a készülékhez mellékelt üzembe helyezési útmutatóval együtt kell használni. További tudnivalók a mellékelt Üzembe helyezési útmutatóban (Installation Guide), Konfigurációs útmutatóban (Configuration Guide) vagy más dokumentumban találhatók.

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. Per le traduzioni delle avvertenze riportate in questo documento, vedere le avvertenze di sicurezza che accompagnano questo dispositivo.

Nota CONSERVARE QUESTE ISTRUZIONI

Nota La presente documentazione va usata congiuntamente alla guida di installazione specifica spedita con il prodotto. Per maggiori informazioni, consultare la Guida all'installazione, la Guida alla configurazione o altra documentazione acclusa.

Advarsel VIKTIGE SIKKERHETSINSTRUKSJONER

Dette varselssymbolet betyr fare. Du befinner deg i en situasjon som kan forårsake personskade. Før du utfører arbeid med utstyret, bør du være oppmerksom på farene som er forbundet med elektriske kretssystemer, og du bør være kjent med vanlig praksis for å unngå ulykker. For å se oversettelser av advarslene i denne publikasjonen, se de oversatte sikkerhetsvarslene som følger med denne enheten.

Merk TA VARE PÅ DISSE INSTRUKSJONENE

Merk Denne dokumentasjonen skal brukes i forbindelse med den spesifikke installasjonsveiledningen som fulgte med produktet. Vennligst se installasjonsveiledningen, konfigureringsveiledningen eller annen vedlagt tilleggsdokumentasjon for detaljer.

Aviso INSTRUÇÕES IMPORTANTES DE SEGURANÇA

Este símbolo de aviso significa perigo. O utilizador encontra-se numa situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha em atenção os perigos envolvidos no manuseamento de circuitos eléctricos e familiarize-se com as práticas habituais de prevenção de acidentes. Para ver traduções dos avisos incluídos nesta publicação, consulte os avisos de segurança traduzidos que acompanham este dispositivo.

Nota GUARDE ESTAS INSTRUÇÕES

Nota Esta documentação destina-se a ser utilizada em conjunto com o manual de instalação incluído com o produto específico. Consulte o manual de instalação, o manual de configuração ou outra documentação adicional inclusa, para obter mais informações.

¡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. Vea las traducciones de las advertencias que acompañan a este dispositivo.

Nota GUARDE ESTAS INSTRUCCIONES

Nota Esta documentación está pensada para ser utilizada con la guía de instalación del producto que lo acompaña. Si necesita más detalles, consulte la Guía de instalación, la Guía de configuración o cualquier documentación adicional adjunta.

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. Se översättningarna av de varningsmeddelanden som finns i denna publikation, och se de översatta säkerhetsvarningarna som medföljer denna anordning.

OBS! SPARA DESSA ANVISNINGAR

OBS! Denna dokumentation ska användas i samband med den specifika produktinstallationshandbok som medföljde produkten. Se installationshandboken, konfigurationshandboken eller annan bifogad ytterligare dokumentation för närmare detaljer.

Предупреждение ВАЖНЫЕ СВЕДЕНИЯ ПО БЕЗОПАСНОСТИ

Этот символ предупреждает о наличии опасности. При неправильных действиях возможно получение травм. Перед началом работы с любым оборудованием необходимо ознакомиться с ситуациями, в которых возможно поражение электротоком, и со стандартными действиями для предотвращения несчастных случаев. Переведенный текст предупреждений содержится в соответствующем документе, поставляемом вместе с устройством.

Примечание СОХРАНЯЙТЕ ЭТУ ИНСТРУКЦИЮ
Примечание Эта инструкция должна использоваться вместе с руководством по установке конкретного изделия, входящим в комплект поставки. Дополнительные сведения см. в руководстве по установке, руководстве по настройке и другой документации, поставляемой с изделием.

警告 有关安全的重要说明

这个警告符号指有危险。您所处的环境可能使身体受伤。操作设备前必须意识到电流的危险性，务必熟悉操作标准，以防发生事故。如果需要了解本说明中出现的警告符号的译文，请参阅本装置所附之安全警告译文。

注意 保存这些说明
注意 本文件应与本产品附带的具体安装说明一并阅读。如欲了解详情，请参阅《安装说明》、《配置说明》或所附的其他文件。

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、一般的な事故防止対策に留意してください。このマニュアルに記載されている警告の各国語版は、装置に付属の「Translated Safety Warnings」を参照してください。

注 これらの注意事項を保管しておいてください。
注 この資料は、製品に付属のインストレーション ガイドと併用してください。詳細は、インストレーション ガイド、コンフィギュレーション ガイド、または添付されているその他のマニュアルを参照してください。

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

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 library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

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

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

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

If you do not have a user ID or password, you can register at this URL:

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

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

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 do the following:

- 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 encryption key 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 to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: http://tools.cisco.com/RPF/register/register.do) Registered users can access the tool at this URL: http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

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 Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This 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.

Tip Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box

and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

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 Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- 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 channel product 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

- *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 where networking professionals 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

- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- 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

Overview of Cisco Network Modules for Cisco Access Routers

This chapter provides an overview of Cisco network modules used in Cisco access routers, and contains the following sections:

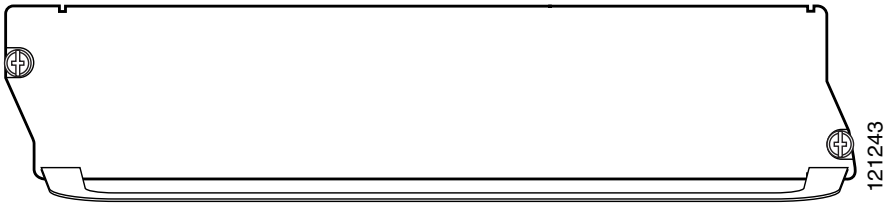
Introduction to Cisco Network Module Form Factors

Cisco network modules are available in the following four different form factors to provide greater modularity and functionality for users:

- Single-wide network modules, also called NM or NME (see Figure 1-1)
- Extended single-wide network modules, also called NME-X (see Figure 1-2)
- Double-wide network modules, also called NMD (see Figure 1-3)
- Extended double-wide network modules, also called NME-XD (see Figure 1-4)

Single-wide network modules are installed in fixed network module slots on Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, and Cisco MWR 1941-DC routers, and in configurable network module slots on Cisco 2811, Cisco 2821, Cisco 2851, and Cisco 3800 series routers. See Figure 1-1 for a sample single-wide network module.

Figure 1-1 Sample Single-Wide Network Module

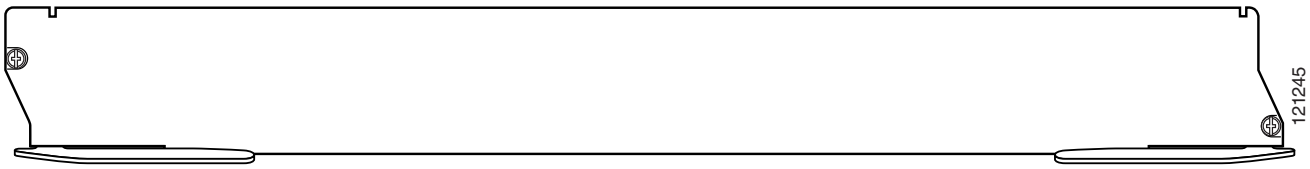


Extended single-wide network modules are installed in configurable network module slots on the Cisco 2821, Cisco 2851, and Cisco 3800 series routers. Extended single-wide network modules cannot be installed in Cisco 2600 series, Cisco 3600 series, Cisco 3700 series and Cisco MWR 1941-DC routers. See Figure 1-2 for a sample extended single-wide network module.

Figure 1-2 Sample Extended Single-Wide Network Module

Double-wide network modules require the removal of the right side panel for installation in the top slot of the Cisco 3725 router, because the bottom slot only supports single-wide modules. On the Cisco 3745 router, the double-wide network module occupies two single-wide slots and is supported by removing the midwall divider. On Cisco 2851 and Cisco 3800 series routers, network module slots must be set up properly before double-wide network modules can be installed. See Figure 1-3 for a sample double-wide network module.

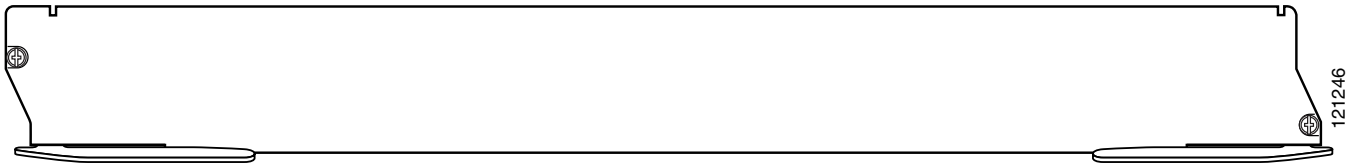
Figure 1-3 Sample Double-Wide Network Module



Tip For information on configuring network module slots to fit double-wide network modules, see the "Preparing Cisco Router Slots for Network Module Installation" section on page 2-8.

Extended double-wide network modules are supported only on the Cisco 2851 and Cisco 3800 series routers. Extended double-wide network modules occupy two extended single-wide network module slots, which must be set up properly before extended double-wide network modules can be installed. See Figure 1-4 for a sample extended double-wide network module.

Figure 1-4 Sample Extended Double-Wide Network Module



Tip For information on configuring network module slots to fit extended double-wide network modules, see the "Preparing Cisco Router Slots for Network Module Installation" section on page 2-8.

Note Extension modules, such as the EVM-HD-8FXS/DID, are equivalent to a single-wide network module. However, extension modules are not supported in all Cisco access router network module slots. See Table 1-1 for information on slots supporting extension modules.

Cisco Access Routers and Cisco Network Modules

The Cisco network modules described in this document are supported on the following Cisco routers:

- Cisco 2600 series, including the Cisco 2610, Cisco 2610XM, Cisco 2611, Cisco 2611XM, Cisco 2612, Cisco 2613, Cisco 2620, Cisco 2620XM, Cisco 2621, Cisco 2621XM, Cisco 2650, Cisco 2650XM, Cisco 2651, Cisco 2651XM, and Cisco 2691 routers

  Note References to the Cisco 2600XM routers apply to the following routers: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.

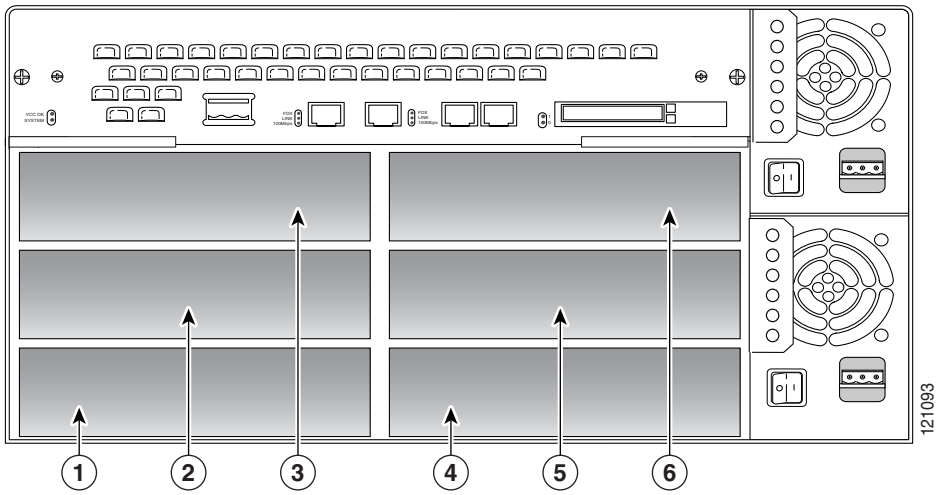
- Cisco 2811, Cisco 2821, and Cisco 2851 routers
- Cisco 3600 series, including the Cisco 3620, Cisco 3631, Cisco 3640, Cisco 3640A, Cisco 3661, and Cisco 3662 routers
- Cisco 3700 series, including the Cisco 3725 and Cisco 3745 routers
- Cisco 3800 series, including the Cisco 3825 and Cisco 3845 routers
- Cisco MWR 1941-DC routers

For information on these Cisco routers, see the hardware documentation described in the "Related Documents" section on page 1-30.

Network Module Slot Locations and Numbering on Cisco Access Routers

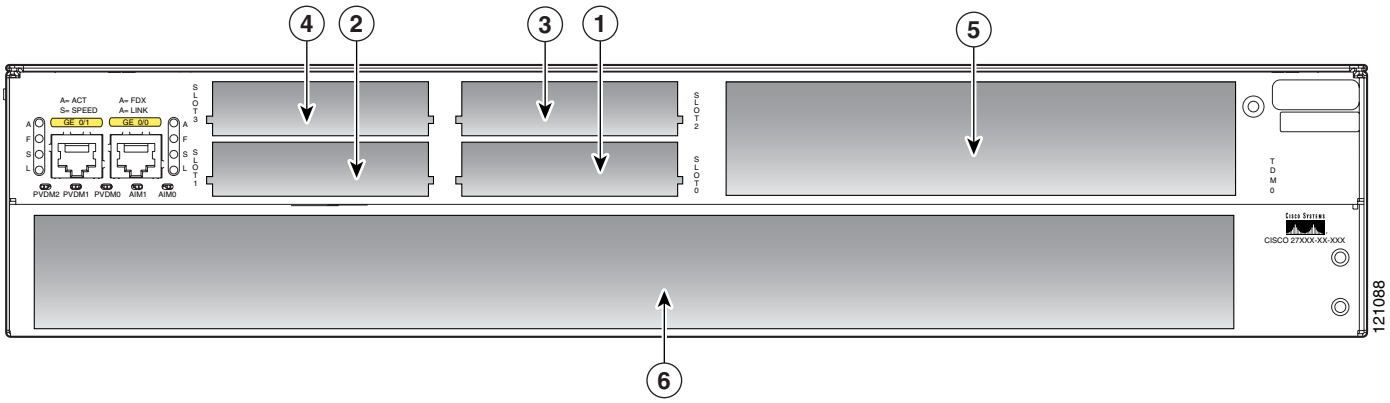
Most Cisco access router network module slots are numbered from right to left, bottom to top. However, some routers use different slot numbering schemes. See Figure 1-5 and Figure 1-6 for examples of network module slot numbering on Cisco access routers.

Figure 1-5 Cisco 3660 Router Rear View



1	Network module slot 2	**4**	Network module slot 1
2	Network module slot 4	**5**	Network module slot 3
3	Network module slot 6	**6**	Network module slot 5

Figure 1-6 Chassis Slot Locations in Cisco 2851 Routers



1	High-speed WAN interface card slot 0	**4**	High-speed WAN interface card slot 3
2	High-speed WAN interface card slot 1	**5**	Extension module slot
3	High-speed WAN interface card slot 2	**6**	Network module slot

Platform and Slot Limitations for Cisco Network Modules

Certain platforms have restrictions on the number of total network modules of a certain type that can be installed, and some slots do not support certain network modules.

See Table 1-1 for information on the type and quantity of network module slots available on Cisco access routers.

Table 1-1 Network Module Slots Available on Cisco Access Routers

Cisco Router	Number of Slots	Slot Type	Slot Numbering	Installation Notes and Limitations
Cisco 2600 series	1	Single-wide	Slot 1	Does not support extension modules.
Cisco 2811 routers	1	Single-wide	Slot 1	Does not support extension modules.
Cisco 2821 routers	1	Single-wide Extended single-wide	Slot 1	Extension modules are not supported in standard network module slots on this platform.
	1	Extension module	Slot 2	Extension module slots do not support other single-wide network modules.
Cisco 2851 routers	1	Single-wide Extended single-wide Double-wide Extended double-wide	Slot 1	Extension modules are not supported in standard network module slots on this platform.
	1	Extension module	Slot 2	Extension module slots do not support other single-wide network modules.
Cisco 3620 routers	2	Single-wide	Slot 0–slot 1	Does not support extension modules.
Cisco 3640 routers	4	Single-wide	Slot 0–slot 3	Does not support extension modules.
Cisco 3660 routers	6	Single-wide Double-wide	Slot 1–slot 6 (see Figure 1-5)	Slot 0 refers to the board carrying fixed interfaces at the top of the chassis.
Cisco 3725 routers	2	Single-wide	Slot 1–slot 2	Slot 2 accommodates double-wide network modules. **Tip** To install double-wide network modules, remove the slot divider. (See the "Removing Slot Dividers" section on page 2-12.)
Cisco 3745 routers	4	Single-wide	Slot 1–slot 4	Does not support extension modules.
	2	Double-wide	Slot 2, slot 4	Removing the slot divider changes slot numbering as follows: • Slot 1 and slot 2 become slot 2 • Slot 3 and slot 4 become slot 4 **Tip** To install double-wide network modules, remove the slot divider. (See the "Removing Slot Dividers" section on page 2-12.)

Table 1-1 Network Module Slots Available on Cisco Access Routers (continued)

Cisco Router	Number of Slots	Slot Type	Slot Numbering	Installation Notes and Limitations
Cisco 3825 routers	3	Single-wide Extended single-wide Extension voice	Slot 1–slot 3	To install double-wide network modules, remove the slot divider. (See the "Removing Slot Dividers" section on page 2-12.) Only one extension module can be installed per chassis.
	1	Double-wide Extended double-wide	Slot 2	To install double-wide network modules, remove the slot divider. (See the "Removing Slot Dividers" section on page 2-12.) Only one NM-36ESW network module bcan be installed per chassis.
Cisco 3845 routers	4	Single-wide Extended single-wide Extension voice	Slot 1–slot 4	Only two extension modules can be installed per chassis.
	2	Double-wide Extended double-wide	Slot 1, slot 3	Removing the slot divider changes slot numbering as follows: • Slot 1 and slot 2 becomes slot 1 • Slot 3 and slot 4 becomes slot 3 **Tip** To install double-wide or extended double-wide network modules, remove the slot divider. (See the "Removing Slot Dividers" section on page 2-12.). Only two NM-36ESW network modules can be installed per chassis.
Cisco MWR 1941-DC routers	1	Single-wide	Slot 1	Cisco MWR 1941-DC routers support single-wide network modules only.

Cisco IOS Software Releases and Cisco Network Modules

Cisco network modules are often supported on multiple Cisco IOS releases. Cisco IOS release information is documented in the product data sheet and in Feature Navigator II, which is located on the Cisco website at http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

To determine which Cisco IOS releases support your particular router and combination of cards and modules, go to the Software Advisor at http://www.cisco.com/pcgi-bin/Support/CompNav/Index.pl.

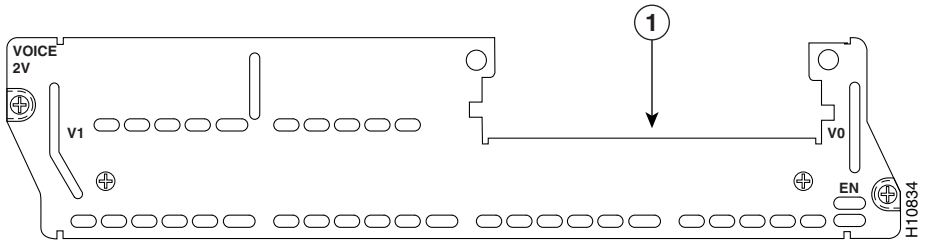
You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Cisco Interface Cards Supported on Cisco Network Modules

Some Cisco network modules have interface card slots to allow installation of Cisco interface cards. These network modules have either one or two interface card slots, supporting either voice or data interface cards. See Figure 1-7 and Figure 1-8 for sample 1- and 2-slot network modules.

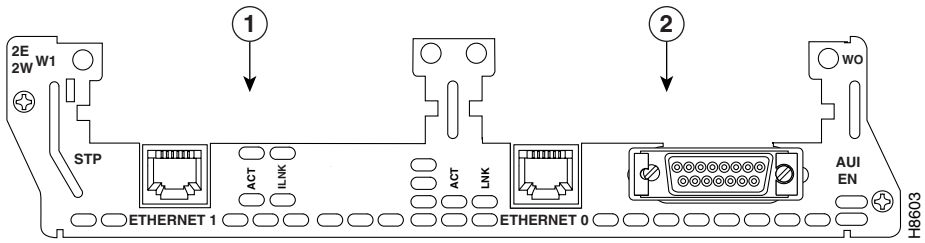
Note Some combination voice/data interface cards are supported on 1- or 2-slot network modules. However, interface card functionality is limited to either voice or data applications. See Table 1-2 for more information.

Figure 1-7 Sample 1-Slot Network Module



1	Interface card slot 0

Figure 1-8 Sample 2-Slot Network Module



1	Interface card slot 1	2	Interface card slot 0

For information on installing interface cards onto network modules, see the "Installing Cisco Interface Cards in 1- or 2-Slot Network Modules" section on page 2-24.

Note High-density WAN interface cards (HWICs) are not supported on 1- or 2-slot network modules.

Table 1-2 Interface Cards Supported on 1- or 2-Slot Network Modules

	Supported on					
Interface Card	**NM-2W NM-1FE2W NM-1FE2W-V2 NM-2FE2W NM-2FE2W-V2 NM-1FE1R2W NM-1FE1R2W-V2**	**NM-1V NM-2V**	**NM-HD-1V NM-HD-2V**	**NM-HD-2VE**	**NM-HDV NM-HDV2**	**NM-1A-OC3MM-1V NM-1A-OC3SMI-1V NM-1A-OC3SML-1V**
WIC-1T	Yes	No	No	No	No	No
WIC-2T	Yes	No	No	No	No	No
WIC-1B-S/T	Yes	No	No	No	No	No
WIC-1B-S/T-V3	Yes	No	No	No	No	No
WIC-1B-U	Yes	No	No	No	No	No
WIC-1B-U-V2	Yes	No	No	No	No	No
WIC-2A/S	Yes	No	No	No	No	No
WIC-1DSU-56K	Yes	No	No	No	No	No
WIC-1DSU-T1	Yes	No	No	No	No	No
WIC-1ADSL	Yes	No	No	No	No	No
WIC-1ADSL-I-DG	Yes	No	No	No	No	No
WIC-1SHDSL	Yes	No	No	No	No	No
WIC-1AM	Yes	No	No	No	No	No
WIC-2AM	Yes	No	No	No	No	No
WIC-1AM-V2	Yes	No	No	No	No	No
WIC-2AM-V2	Yes	No	No	No	No	No
WIC-1AM-V2	Yes	No	No	No	No	No
WIC-2AM-V2	Yes	No	No	No	No	No
VWIC-1MFT-G703	Data only	No	No	No	No	No
VWIC2-1MFT-G703	Data only	No	No	No	NM-HDV2 only	No
VWIC-2MFT-G.703	No	No	No	Yes	No	No
VWIC2-2MFT-G703	Data only	No	No	No	Yes	No
VWIC-1MFT-T1	Yes	No	No	Voice only	Yes	Yes
VWIC-1MFT-E1	No	No	No	Voice only	Yes	Yes
VWIC2-1MFT-T1/E1	Data only	No	No	Yes	Yes	No
VWIC-2MFT-T1	Data only	No	No	Voice only	Yes	Yes
VWIC-2MFT-E1	Data only	No	No	Voice only	Yes	Yes
VWIC2-2MFT-T1/E1	Data only	No	No	Yes	Yes	No
VWIC-2MFT-T1-DI	Data only	No	No	Voice only	Yes	Yes

Table 1-2 Interface Cards Supported on 1- or 2-Slot Network Modules (continued)

	Supported on					
Interface Card	**NM-2W NM-1FE2W NM-1FE2W-V2 NM-2FE2W NM-2FE2W-V2 NM-1FE1R2W NM-1FE1R2W-V2**	**NM-1V NM-2V**	**NM-HD-1V NM-HD-2V**	**NM-HD-2VE**	**NM-HDV NM-HDV2**	**NM-1A-OC3MM-1V NM-1A-OC3SMI-1V NM-1A-OC3SML-1V**
VWIC-2MFT-E1-DI	Data only	No	No	Voice only	Yes	Yes
VIC-2FXS	No	Yes	No	No	No	No
VIC2-2FXS	No	No	Yes	Yes	No	No
VIC-4FXS/DID	No	No	Yes[1]	Yes[1]	No	No
VIC-2FXO	No	Yes	No	No	No	No
VIC-2FXO-M1	No	Yes	No	No	No	No
VIC-2FXO-EU	No	Yes	No	No	No	No
VIC-2FXO-M2	No	Yes	No	No	No	No
VIC-2FXO-M3	No	Yes	No	No	No	No
VIC2-2FXO	No	No	Yes	Yes	No	No
VIC2-4FXO	No	No	Yes	Yes	No	No
VIC-2E/M	No	Yes	No	No	No	No
VIC2-2E/M	No	No	Yes	Yes	No	No
VIC-2BRI-S/T-TE	No	Yes	No	No	No	No
VIC-2BRI-NT-TE	No	Yes	No	No	No	No
VIC2-2BRI-NT/TE	No	No	Yes	Yes	No	No
VIC-2CAMA	No	Yes	No	No	No	No
VIC-2DID	No	Yes	Yes	Yes	No	No

1. Cisco 2600XM series, Cisco 2691, Cisco 2800 series, Cisco 3600 series, Cisco 3700 series, and Cisco 3800 series routers support direct inward dial (DID) on the 4-port FXS/DID cards in Cisco IOS Release 12.3(14)T and later.

For more information about Cisco interface cards, see the *Cisco Interface Cards Hardware Installation Guide*.

Cabling for Cisco Network Modules

The cables required to connect the network module to the network differ according to interface and connector type. See Table 1-3 for more information.

Note Cabling for 1- or 2-slot network modules is determined by the installed interface cards. See the *Cisco Interface Cards Hardware Installation Guide* for information.

Table 1-3 Cabling for Cisco Network Modules

Connection Type	Connector Type, Cable Color	Cable	Use with
Alarm Interface Connections			
To alarm interface patch panels or main distribution frame	50-pin D	Micro DB-50 SCSI transition	NM-AIC-64
Analog Dialup			
300 bps to 33.6 kbps analog dialup	RJ-11	RJ-11 straight-through	NM-8AM NM-8AM-V2 NM-16AM NM-16AM-V2
ATM			
ATM to ADSL	RJ-45, light green	RJ-45 UTP category 3, 4, 5 or higher	NM-1ATM-25
		RJ-45 STP category 1, 1A, 9, or 9A	
T3 ATM	BNC	BNC coaxial T3	NM-1A-T3 NM-1A-T3/E3
E3 ATM	BNC	BNC coaxial E3	NM-1A-E3 NM-1A-T3/E3
ATM, optical	Duplex or simplex SC	62.5-micron core with an optical loss of 0 to 9 dB **Note** Maximum path length of 2 km (1.24 miles), all cables, end to end	NM-1A-OC3-POM NM-1A-OC3MM NM-1A-OC3SMI NM-1A-OC3SML NM-1A-OC3MM-EP NM-1A-OC3SMI-EP NM-1A-OC3SML-EP NM-1A-OC3MM-1V NM-1A-OC3SMI-1V NM-1A-OC3SML-1V
		50-micron core with optical loss of 7 dB **Note** Maximum path length of 2 km (1.24 miles), all cables, end to end	
		9-micron core **Note** Maximum path length of 45 km (27.9 miles) for single-mode long (SML) reach and 15 km (9.3 miles) for single-mode intermediate (SMI) reach.	
Circuit Emulation over IP (CEoIP)			
T1/E1 CEoIP	RJ-48C	RJ-48 T1/E1 straight-through	NM-CEM-4TE1 **Note** To connect to a 75-ohm unbalanced E1 network, use CAB-ADP-75-120.
Serial CEoIP	60-pin D, blue	Cisco Smart serial 12-in-1—see Table 1-4 for part numbers	NM-CEM-4SER
		Cisco Smart serial extended 12-in-1—see Table 1-5 for part numbers	

Table 1-3 Cabling for Cisco Network Modules (continued)

Connection Type	Connector Type, Cable Color	Cable	Use with
Ethernet			
Ethernet	RJ-45, yellow	10BASE-T Category 5 or above UTP	NM-1E NM-4E NM-1E2W NM-2E2W NM-1E1R2W
	DB-15	Attachment unit interface (AUI) cable	
Fast Ethernet, copper	RJ-45	100BASE-T Category 5 or above UTP	NM-1FE-TX NM-1FE2W NM-1FE2W-V2 NM-2FE2W NM-2FE2W-V2 NM-1FE1R2W NM-1FE1R2W-V2 NM-1FE1CT1 NM-1FE2CT1 NM-1FE1CT1-CSU NM-1FE2CT1-CSU NM-1FE1CE1B NM-1FE1CE1U NM-1FE2CE1B NM-1FE2CE1U NM-16ESW NM-16ESW-1GIG NM-16ESW-PWR NM-16ESW-PWR-1GIG NM-CE-BP-20G-K9 NM-CE-BP-40G-K9 NM-CE-BP-80G-K9 NM-CE-BP-SCSI-K9 NM-CIDS-K9 NM-NAM NMD-36ESW NMD-36ESW-2GIG NMD-36ESW-PWR NMD-36ESW-PWR-2G NME-16ES-1G NME-16ES-1G-P NME-X-23ES-1G NME-X-23ES-1G-P NME-XD-24ES-1S-P NME-XD-48ES-2S-P
Fast Ethernet, optical	SC	100BASE-T MMF	NM-1FE-FX NM-1FE-FX-V2
	SC	100BASE-T SMF	NM-1FE-SMF

Table 1-3 Cabling for Cisco Network Modules (continued)

Connection Type	Connector Type, Cable Color	Cable	Use with
Gigabit Ethernet, copper	RJ-45	1000BASE-T Category 5 or above UTP	NM-16ESW NM-16ESW-1GIG NM-16ESW-PWR NM-16ESW-PWR-1GIG NM-1GE (through GBIC) NME-WAE-302-K9 NME-WAE-502-K9 NME-WAE-522-K9 NMD-36ESW NMD-36ESW-2GIG NMD-36ESW-PWR NMD-36ESW-PWR-2G NME-16ES-1G NME-16ES-1G-P NME-AIR-WLC8-K9 NME-AIR-WLC12-K9 NME-AON-K9 NME-NAC-K9 NME-NAM-80S NME-X-23ES-1G NME-X-23ES-1G-P NME-XD-24ES-1S-P NME-XD-48ES-2S-P
Gigabit Ethernet, optical	SC, yellow	10-micron SMF	NM-1GE (through GBIC) NME-16ES-1G NME-16ES-1G-P NME-X-23ES-1G NME-X-23ES-1G-P NME-XD-24ES-1S-P NME-XD-48ES-2S-P
	SC, orange	62.5-micron MMF	
ISDN Connections			
Channelized T1 PRI, without CSU	DB-15	DB-15 straight-through T1	NM-1FE1CT1 NM-1FE2CT1 NM-1CT1 NM-2CT1
Channelized T1 PRI, with CSU	RJ-48C, tan	RJ-48C to RJ-48C straight-through T1	NM-1FE1CT1-CSU NM-1FE2CT1-CSU NM-1CT1-CSU NM-2CT1-CSU
Channelized T1 PRI, with or without CSU	RJ-48S, tan	RJ-48S to RJ-48S straight-through T1	NM-1CE1T1-PRI NM-2CE1T1-PRI

Table 1-3 Cabling for Cisco Network Modules (continued)

Connection Type	Connector Type, Cable Color	Cable	Use with
Channelized E1 PRI, balanced	DB-15, tan	DB-15 to DB-15 120-ohm balanced E1	NM-1FE1CE1B NM-1FE2CE1B NM-1CE1B NM-2CE1B
	DB-15 to twin-ax, tan	DB-15 to twin-ax 75-ohm balanced E1	
	DB-15 to RJ-45, tan	DB-15 to RJ-45 120-ohm balanced E1	
	RJ-48S, tan	RJ-48S to RJ-48S straight-through 120-ohm balanced E1	NM-1CE1T1-PRI NM-2CE1T1-PRI
	RJ-48S to DB-15, tan	RJ-48S to DB-15 120-ohm balanced E1	
	RJ-48S to twin-ax	RJ-48S to twin-ax 120-ohm balanced E1	
Channelized E1 PRI, unbalanced	DB-15 to BNC, tan	DB-15 to BNC 75-ohm unbalanced E1	NM-1FE1CE1U NM-1FE2CE1U NM-1CE1U NM-2CE-1U
	RJ-48S to BNC, tan	RJ-48S to BNC 75-ohm unbalanced E1	NM-1CE1T1-PRI NM-2CE1T1-PRI
BRI S/T (external NT1)	RJ-45, orange	RJ-45 straight-through	NM-4B-S/T NM-8B-S/T
BRI U (built-in NT1)	RJ-45, red	RJ-45 straight-through	NM-4B-U NM-8B-U
Serial Connections			
Synchronous serial	60-pin D, blue	Serial transition cable (EIA/TIA-232, EIA/TIA-449, EIA/TIA-530 DTE, V.35, X.21, NRZ/NRZI)	NM-4T NM-4A/S NM-8A/S
Asynchronous serial	68-pin D to 25-pin D	DB-68 to DB-25 EIA/TIA-232 octal	NM-16A NM-32A
	68-pin D to RJ-45	DB-68 to RJ-45 EIA/TIA-232 octal	
Serial	60-pin D, blue	Cisco Smart serial 12-in-1—see Table 1-4 for part numbers	NM-16A/S
Serial surge protection		Cisco Product ID CAB-SS-SURGE	
Fractional DS3 or below, to DSU	50-pin D, blue	DB-50 HSSI DTE	NM-1HSSI
Fractional DS3 or below, to another router		DB-50 HSSI null modem	

Table 1-3 Cabling for Cisco Network Modules (continued)

Connection Type	Connector Type, Cable Color	Cable	Use with
Service Module Connections			
To external storage array	68-pin D	68-pin low-voltage differential (LVD) SCSI **Note** 36-, 91- or 108-inch (274 cm) cables can be used, depending on the distance between the network module and the external storage array.	NM-CE-BP-SCSI
Token Ring Connections			
Token Ring, shielded	DB-9	Token Ring lobe cable, shielded STP	NM-1E1R2W NM-1FE1R2W NM-1FE1R2W-V2
Token Ring, unshielded	RJ-45	Token Ring lobe cable, unshielded UTP	
WAN Connections			
T1/E1 WAN	RJ-48C/CA81A	RJ-48 T1/E1 straight-through	NM-4T1-IMA NM-8T1-IMA NM-4E1-IMA NM-8E1-IMA NM-HDV2-1T1/E1 NM-HDV2-2T1/E1
T3/DS3/E3 WAN	BNC connector	BNC T3/E3 coaxial	NM-1T3/E3 NM-1A-T3 NM-1A-E3 NM-1A-T3/E3
Wireless and Satellite Connections			
To antenna	BNC	BNC indoor IF coaxial	NM-WMDA
To satellite dish	F-connector	75-ohm F-connector shielded RG-6	NM-1VSAT-GILAT
Voice Connections			
Analog voice FXS/FXO	RJ-21	253PP10GYADI male-to-male (Graybar)	NM-HDA-4FXS
		253PC10GYADI male-to-female (Graybar)	
		AT125-SM patch panel (Graybar)	
		RJ-21 cable	EVM-HDA-8FXS/DID

Note A single fiber link should not mix 62.5- and 50-micron cable.

Table 1-4 Cisco 12-in-1 Smart Serial Interface Cable Part Numbers

Interface	DCE/DTE	Cisco Cable Part Number
EIA/TIA-232	Female DCE Male DTE	CAB-SS-232FC CAB-SS-232MT
EIA/TIA-449	Female DCE Male DTE	CAB-SS-449FC CAB-SS-449MT

Table 1-4 Cisco 12-in-1 Smart Serial Interface Cable Part Numbers (continued)

Interface	DCE/DTE	Cisco Cable Part Number
EIA-530	Male DTE	CAB-SS-530MT
EIA-530A	Male DTE	CAB-SS-530AMT
V.35	Female DCE Female DTE Male DCE Male DTE	CAB-SS-V35FC CAB-SS-V35FT CAB-SS-V35MC CAB-SS-V35MT
X.21	Female DCE Male DTE	CAB-SS-X21FC CAB-SS-X21MT

Table 1-5 Cisco Extended 12-in-1 Smart Serial Interface Cable Part Numbers

Interface	DCE/DTE	Cisco Cable Part Number
EIA/TIA-232	Female DCE Male DTE	CAB-SS-232FC-EXT CAB-SS-232MT-EXT
EIA/TIA-449	Female DCE Male DTE	CAB-SS-449FC-EXT CAB-SS-449MT-EXT
EIA-530	Female DCE Male DTE	CAB-SS-530FC-EXT CAB-SS-530MT-EXT
EIA-530A	Female DCE Male DTE	CAB-SS-530AFC-EXT CAB-SS-530AMT-EXT
V.35	Female DCE Female DTE Male DCE Male DTE	CAB-SS-V35FC-EXT CAB-SS-V35FT-EXT CAB-SS-V35MC-EXT CAB-SS-V35MT-EXT

Platform Support for Cisco Network Modules

Table 1-6 lists the platforms supported by each interface card. The interface cards are grouped by technology area:

- Alarm Monitoring and Control Network Modules
- Analog and ISDN Basic Rate Voice Network Modules
- Extension Modules
- Analog Dialup and Remote Access Network Modules
- Application and Service Modules
- ATM Network Modules
- Channelized T1/E1 and ISDN Network Modules
- Circuit Emulation over IP (CEoIP) Network Modules
- Compression Network Modules
- Digital Dialup and Remote Access Network Modules

- Digital Voice Network Modules
- Ethernet Switching Network Modules
- LAN Network Modules
- LAN and Interface Card Slot Combo Network Modules
- LAN and T1/E1 Combination Network Modules
- Serial Connectivity Network Modules
- Wireless and Satellite Network Modules

Table 1-6 Platform Support for Cisco Network Modules

Product Description	Cisco Product ID	Supported on Cisco Routers	See Section
Alarm Monitoring and Control Network Modules			
Alarm monitoring and control network module	NM-AIC-64	Cisco 2600 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3600 series Cisco 3700 series Cisco 3800 series Cisco MWR 1941-DC	Connecting Alarm Interface Controller Network Modules
Analog and ISDN Basic Rate Voice Network Modules			
1-slot 2-channel voice network module	NM-1V	Cisco 2600 series Cisco 3600 series Cisco 3700 series	Connecting Voice Network Modules
2-slot 4-channel voice network module	NM-2V	Cisco 2600 series Cisco 3600 series Cisco 3700 series	Connecting Voice Network Modules
1-slot IP communications voice/fax network module	NM-HD-1V	Cisco 2600 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3640 Cisco 3660 Cisco 3700 series Cisco 3800 series	Connecting Voice Network Modules
2-slot IP communications voice/fax network module	NM-HD-2V	Cisco 2600 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3640 Cisco 3660 Cisco 3700 series Cisco 3800 series	Connecting Voice Network Modules

Table 1-6 Platform Support for Cisco Network Modules (continued)

Product Description	Cisco Product ID	Supported on Cisco Routers	See Section
2-slot IP communications enhanced voice/fax network module	NM-HD-2VE	Cisco 2600 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3640 Cisco 3660 Cisco 3700 series Cisco 3800 series	Connecting Voice Network Modules
4-port FXS high-density analog (HDA) voice/fax network module	NM-HDA-4FXS	Cisco 2600 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3640 Cisco 3660 Cisco 3700 series Cisco 3800 series	Connecting High-Density Analog Telephony Network Modules
Extension Modules			
High-density extension module	EVM-HD-8FXS/DID	Cisco 2821 Cisco 2851 Cisco 3800 series	Connecting Cisco High-Density Extension Modules
Analog Dialup and Remote Access Network Modules			
8-port analog modem network module with v.92	NM-8AM	Cisco 2600 series Cisco 3600 series Cisco 3725 Cisco 3745	Connecting Analog Modem Network Modules
16-port analog modem network module with v.92	NM-16AM	Cisco 2600 series Cisco 3600 series Cisco 3725 Cisco 3745	Connecting Analog Modem Network Modules
8-port analog modem network module with v.92, version 2	NM-8AM-V2	Cisco 2600XM series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 2691 Cisco 3660 Cisco 3700 series Cisco 3800 series	Connecting Analog Modem Network Modules
16-port analog modem network module with v.92, version 2	NM-16AM-V2	Cisco 2600XM series Cisco 2691 Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3660 Cisco 3700 series Cisco 3800 series	Connecting Analog Modem Network Modules

Table 1-6 Platform Support for Cisco Network Modules (continued)

Product Description	Cisco Product ID	Supported on Cisco Routers	See Section
Application and Service Modules			
Cisco AON network module with 512 MB memory	NM-AON-K9	Cisco 2600XM series Cisco 2691 Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3700 series Cisco 3800 series	Connecting AON Network Modules
Cisco AON network module with 1 GB memory	NME-AON-K9	Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3700 series Cisco 3800 series	Connecting AON Network Modules
Cisco Application Performance Assurance enhanced network module	NME-APA-E2	Cisco 2811 Cisco 2821 Cisco 2851	Connecting Application Performance Assurance Enhanced Network Modules
Cisco Application Performance Assurance enhanced network module	NME-APA-E3	Cisco 3800 series	Connecting Application Performance Assurance Enhanced Network Modules
Cisco Content Engine network module for caching and content delivery, with 20-GB hard drive expansion module	NM-CE-BP-20G-K9	Cisco 2600 series Cisco 3640 Cisco 3660 Cisco 3700 series	Connecting Content Engine Network Modules for Caching and Content Delivery
Cisco Content Engine network module for caching and content delivery, with 40-GB hard drive expansion module	NM-CE-BP-40G-K9	Cisco 2600 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3640 Cisco 3660 Cisco 3700 series Cisco 3800 series	Connecting Content Engine Network Modules for Caching and Content Delivery
Cisco Content Engine network module for caching and content delivery, with 80-GB hard drive expansion module	NM-CE-BP-80G-K9	Cisco 2600 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3640 Cisco 3660 Cisco 3700 series Cisco 3800 series	Connecting Content Engine Network Modules for Caching and Content Delivery

Table 1-6 Platform Support for Cisco Network Modules (continued)

Product Description	Cisco Product ID	Supported on Cisco Routers	See Section
Cisco Content Engine network module for caching and content delivery, with SCSI connector expansion module **Note** Requires an external SCSI disk array such as the Cisco SA-6	NM-CE-BP-SCSI-K9	Cisco 2600 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3640 Cisco 3660 Cisco 3700 series Cisco 3800 series	Connecting Content Engine Network Modules for Caching and Content Delivery
Cisco Intrusion Detection System (IDS) network module	NM-CIDS-K9	Cisco 2600XM series Cisco 2691 Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3660 Cisco 3700 series Cisco 3800 series	Connecting Cisco Intrusion Detection System Network Modules
Cisco Unity Express voice-mail network module	NM-CUE	Cisco 2600XM series Cisco 2691 Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3700 series Cisco 3800 series	Connecting Cisco Unity Express Network Modules
Cisco Unity Express voice-mail enhanced network module	NME-CUE	Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3700 series Cisco 3800 series	Connecting Cisco Unity Express Enhanced Network Modules, page 24-1
Cisco Network Admission Control network module	NME-NAC-K9	Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3800 series	Connecting Cisco Network Admission Control Network Modules
Cisco Network Analysis Module network module	NM-NAM	Cisco 2600XM series Cisco 2691 Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3660 Cisco 3700 series Cisco 3800 series	Connecting Cisco Network Analysis Modules
Cisco Network Analysis Module enhanced network module	NME-NAM-80S	Cisco 3700 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3800 series	Connecting NAM Enhanced Network Modules

Table 1-6 Platform Support for Cisco Network Modules (continued)

Product Description	Cisco Product ID	Supported on Cisco Routers	See Section
Cisco Unified Messaging Gateway enhanced network module	NME-UMG	Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3800 series	Connecting Cisco Unified Messaging Gateway Enhanced Network Modules
Cisco Unified Messaging Gateway enhanced network module	NME-UMG-EC	Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3800 series	Connecting Cisco Unified Messaging Gateway Enhanced Network Modules
Cisco WAAS enhanced network module with 80 GB hard disk and 512 MB memory	NME-WAE-302-K9	Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3800 series	Connecting WAAS Enhanced Network Modules
Cisco WAAS enhanced network module with 120 GB hard disk and 1 GB memory	NME-WAE-502-K9	Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3800 series	Connecting WAAS Enhanced Network Modules
Cisco WAAS enhanced network module with 160 GB hard disk and 2 GB memory	NME-WAE-522-K9	Cisco 3800 series	Connecting WAAS Enhanced Network Modules
ATM Network Modules			
1-port ATM-25	NM-1ATM-25	Cisco 2600 series Cisco 3600 series	Connecting ATM Network Modules
1-port DS3 ATM network module	NM-1A-T3	Cisco 2600 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3600 series Cisco 3700 series Cisco 3800 series	Connecting ATM Network Modules
1-port E3 ATM network module	NM-1A-E3	Cisco 2600 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3600 series Cisco 3700 series Cisco 3800 series	Connecting ATM Network Modules
1-port ATM T3/E3 network module	NM-1A-T3/E3	Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3800 series	Connecting ATM Network Modules
1-port ATM OC-3c/STM1 pluggable optical module (POM) network module	NM-1A-OC3-POM	Cisco 3825 Cisco 3845	Connecting ATM Network Modules

Table 1-6 Platform Support for Cisco Network Modules (continued)

Product Description	Cisco Product ID	Supported on Cisco Routers	See Section
1-port ATM OC-3c/STM1 multimode network module	NM-1A-OC3MM	Cisco 2691 Cisco 3600 series Cisco 3725	Connecting ATM Network Modules
1-port ATM OC-3c/STM1 single-mode, intermediate-reach network module	NM-1A-OC3SMI	Cisco 2691 Cisco 3600 series Cisco 3725	Connecting ATM Network Modules
1-port ATM OC-3c/STM1 single-mode, long-reach network module	NM-1A-OC3SML	Cisco 2691 Cisco 3600 series Cisco 3725	Connecting ATM Network Modules
1-port ATM OC-3c/STM1 multimode network module with enhanced performance	NM-1A-OC3MM-EP	Cisco 3745	Connecting ATM Network Modules
1-port ATM OC-3c/STM1 single-mode, intermediate-reach network module with enhanced performance	NM-1A-OC3SMI-EP	Cisco 3745	Connecting ATM Network Modules
1-port ATM OC-3c/STM1 single-mode, long-reach network module with enhanced performance	NM-1A-OC3SML-EP	Cisco 3745	Connecting ATM Network Modules
1-port ATM OC-3c/STM1 multimode network module with 1 voice interface card slot	NM-1A-OC3MM-1V	Cisco 3600 series	Connecting ATM Network Modules
1-port ATM OC-3c/STM1 single-mode, intermediate-reach network module with 1 voice interface card slot	NM-1A-OC3SMI-1V	Cisco 3600 series	Connecting ATM Network Modules
1-port ATM OC-3c/STM1 single-mode, long-reach network module with 1 voice interface card slot	NM-1A-OC3SML-1V	Cisco 3600 series	Connecting ATM Network Modules
4-port T1 ATM network module with Inverse Multiplexing over ATM (IMA)	NM-4T1-IMA	Cisco 2600 series Cisco 3600 series Cisco 3700 series Cisco 3800 series	Connecting T1/E1 IMA Network Modules
4-port E1 ATM network module with IMA	NM-4E1-IMA	Cisco 2600 series Cisco 3600 series Cisco 3700 series Cisco 3800 series	Connecting T1/E1 IMA Network Modules
8-port T1 ATM network module with IMA	NM-8T1-IMA	Cisco 2600 series Cisco 3600 series Cisco 3700 series Cisco 3800 series	Connecting T1/E1 IMA Network Modules
8-port E1 ATM network module with IMA	NM-8E1-IMA	Cisco 2600 series Cisco 3600 series Cisco 3700 series Cisco 3800 series	Connecting T1/E1 IMA Network Modules

Table 1-6 Platform Support for Cisco Network Modules (continued)

Product Description	Cisco Product ID	Supported on Cisco Routers	See Section
Channelized T1/E1 and ISDN Network Modules			
1-port channelized T1/ISDN-PRI network module	NM-1CT1	Cisco 2600 series Cisco 3600 series Cisco 3700 series	Connecting ISDN PRI Network Modules
2-port channelized T1/ISDN-PRI network module	NM-2CT1	Cisco 2600 series Cisco 3600 series Cisco 3700 series	Connecting ISDN PRI Network Modules
1-port channelized T1/ISDN-PRI network module with CSU	NM-1CT1-CSU	Cisco 2600 series Cisco 3600 series Cisco 3700 series	Connecting ISDN PRI Network Modules
2-port channelized T1/ISDN-PRI network module with CSU	NM-2CT1-CSU	Cisco 2600 series Cisco 3600 series Cisco 3700 series	Connecting ISDN PRI Network Modules
1-port channelized E1/ISDN-PRI network module, unbalanced	NM-1CE1U	Cisco 2600 series Cisco 3600 series Cisco 3700 series	Connecting ISDN PRI Network Modules
2-port channelized E1/ISDN-PRI network module, unbalanced	NM-2CE1U	Cisco 2600 series Cisco 3600 series Cisco 3700 series	Connecting ISDN PRI Network Modules
1-port channelized E1/ISDN-PRI network module, balanced	NM-1CE1B	Cisco 2600 series Cisco 3600 series Cisco 3700 series	Connecting ISDN PRI Network Modules
2-port channelized E1/ISDN-PRI network module, balanced	NM-2CE1B	Cisco 2600 series Cisco 3600 series Cisco 3700 series	Connecting ISDN PRI Network Modules
1-port channelized T1/E1/ISDN-PRI network module with G.703	NM-1CE1T1-PRI	Cisco 2600XM series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 2691 Cisco 3631 Cisco 3660 Cisco 3700 series Cisco 3800 series	Connecting ISDN PRI Network Modules
2-port channelized T1/E1/ISDN-PRI network module with G.703	NM-2CE1T1-PRI	Cisco 2600XM series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 2691 Cisco 3631 Cisco 3660 Cisco 3700 series Cisco 3800 series	Connecting ISDN PRI Network Modules

Table 1-6 Platform Support for Cisco Network Modules (continued)

Product Description	Cisco Product ID	Supported on Cisco Routers	See Section
4-port ISDN BRI network module—S/T interface	NM-4B-S/T	Cisco 2600 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3600 series Cisco 3700 series Cisco 3800 series	Connecting ISDN BRI Network Modules
4-port ISDN BRI network module with integrated Network Termination 1 (NT1)—U interface	NM-4B-U	Cisco 2600 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3600 series Cisco 3700 series Cisco 3800 series	Connecting ISDN BRI Network Modules
8-port ISDN BRI network module—S/T interface	NM-8B-S/T	Cisco 2600 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3600 series Cisco 3700 series Cisco 3800 series	Connecting ISDN BRI Network Modules
8-port ISDN BRI network module with integrated NT1—U interface	NM-8B-U	Cisco 2600 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3600 series Cisco 3700 series Cisco 3800 series	Connecting ISDN BRI Network Modules
Circuit Emulation over IP (CEoIP) Network Modules			
4-port serial CEoIP network module	NM-CEM-4SER	Cisco 2600XM series Cisco 2691 Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3660 Cisco 3700 series Cisco 3800 series	Connecting Circuit Emulation Over IP Network Modules
4-port T1/E1 CEoIP network module	NM-CEM-4TE1	Cisco 2600XM series Cisco 2691 Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3660 Cisco 3700 series Cisco 3800 series	Connecting Circuit Emulation Over IP Network Modules
Compression Network Modules			

Table 1-6 Platform Support for Cisco Network Modules (continued)

Product Description	Cisco Product ID	Supported on Cisco Routers	See Section
Compression network module	NM-COMPR	Cisco 3600 series	Connecting Compression Network Modules
Digital Dialup and Remote Access Network Modules			
6-modem digital modem network module	NM-6DM	Cisco 3600 series Cisco 3700 series Cisco 3800 series	Connecting Digital Modem Network Modules
12-modem digital modem network module	NM-12DM	Cisco 3600 series Cisco 3700 series Cisco 3800 series	Connecting Digital Modem Network Modules
18-modem digital modem network module	NM-18DM	Cisco 3600 series Cisco 3700 series Cisco 3800 series	Connecting Digital Modem Network Modules
24-modem digital modem network module	NM-24DM	Cisco 3600 series Cisco 3700 series Cisco 3800 series	Connecting Digital Modem Network Modules
30-modem digital modem network module	NM-30DM	Cisco 3600 series Cisco 3700 series Cisco 3800 series	Connecting Digital Modem Network Modules
Digital Voice Network Modules			
High-density digital voice/fax network module	NM-HDV	Cisco 2600 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3600 series Cisco 3700 series Cisco 3800 series	Connecting Voice Network Modules
IP communications high-density digital voice/fax network module	NM-HDV2	Cisco 2600XM Cisco 2691 Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3700 series Cisco 3800 series	Connecting Voice Network Modules
1-port T1/E1 IP communications high-density digital voice/fax network module	NM-HDV2-1T1/E1	Cisco 2600 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3700 series Cisco 3800 series	Connecting Voice Network Modules

Table 1-6 Platform Support for Cisco Network Modules (continued)

Product Description	Cisco Product ID	Supported on Cisco Routers	See Section
2-port T1/E1 IP communications high-density digital voice/fax network module	NM-HDV2-2T1/E1	Cisco 2600 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3700 series Cisco 3800 series	Connecting Voice Network Modules
Ethernet Switching Network Modules			
16-port EtherSwitch network module	NM-16ESW	Cisco 2600 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3600 series Cisco 3700 series Cisco 3800 series Cisco MWR 1941-DC	Connecting Ethernet Switch Network Modules
16-port EtherSwitch network module with 1-port GE expansion module	NM-16ESW-1GIG	Cisco 2600 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3600 series Cisco 3700 series Cisco 3800 series Cisco MWR 1941-DC	Connecting Ethernet Switch Network Modules
16-port EtherSwitch network module with inline power expansion module	NM-16ESW-PWR	Cisco 2600 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3600 series Cisco 3700 series Cisco 3800 series	Connecting Ethernet Switch Network Modules
16-port EtherSwitch network module with both 1-port GE and inline power expansion modules	NM-16ESW-PWR-1GIG	Cisco 2600 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3600 series Cisco 3700 series Cisco 3800 series	Connecting Ethernet Switch Network Modules
36-port EtherSwitch high-density service module (HDSM)	NM-36-ESW	Cisco 2851 routers Cisco 3660 Cisco 3700 series Cisco 3800 series	Connecting Ethernet Switch Network Modules
36-port EtherSwitch high-density service module (HDSM) with 2 1-port GE expansion modules	NMD-36-ESW-2GIG	Cisco 2851 routers Cisco 3660 Cisco 3700 series Cisco 3800 series	Connecting Ethernet Switch Network Modules

Table 1-6 Platform Support for Cisco Network Modules (continued)

Product Description	Cisco Product ID	Supported on Cisco Routers	See Section
36-port EtherSwitch high-density service module (HDSM) with inline power expansion module	NMD-36-ESW-PWR	Cisco 2851 routers Cisco 3660 Cisco 3700 series Cisco 3800 series	Connecting Ethernet Switch Network Modules
36-port EtherSwitch high-density service module (HDSM) with 2 1-port GE and 1 inline power expansion modules	NMD-36-ESW-PWR-2G	Cisco 2851 routers Cisco 3660 Cisco 3700 series Cisco 3800 series	Connecting Ethernet Switch Network Modules
16 10/100 Ethernet ports, 1 10/100/1000 Ethernet port, no StackWise connector ports, single-wide, no Power over Ethernet (PoE) support	NME-16ES-1G	Cisco 2691 routers (without –48 V) Cisco 3700 series Cisco 2800 series Cisco 3800 series	Connecting Cisco EtherSwitch Service Modules
16 10/100 Ethernet ports, 1 10/100/1000 Ethernet port, no StackWise connector ports, single-wide, with PoE support	NME-16ES-1G-P	Cisco 2691 routers (without –48 V) Cisco 3700 series Cisco 2800 series Cisco 3800 series	Connecting Cisco EtherSwitch Service Modules
23 10/100 Ethernet ports, 1 10/100/1000 Ethernet port, no StackWise connector ports, extended single-wide, no PoE support	NME-X-23ES-1G	Cisco 2851 routers Cisco 3800 series	Connecting Cisco EtherSwitch Service Modules
23 10/100 Ethernet ports, 1 10/100/1000 Ethernet port, no StackWise connector ports, extended single-wide, with PoE support	NME-X-23ES-1G-P	Cisco 2851 routers Cisco 3800 series	Connecting Cisco EtherSwitch Service Modules
24 10/100 Ethernet ports, 1 small form-factor pluggable (SFP) port, 2 StackWise connector ports, extended double-wide, with PoE support	NME-XD-24ES-1S-P	Cisco 2821 routers Cisco 2851 routers Cisco 3800 series	Connecting Cisco EtherSwitch Service Modules
48 10/100 Ethernet ports, 2 SFP ports, no StackWise connector ports, extended double-wide, with PoE support	NME-XD-48ES-2S-P	Cisco 2851 routers Cisco 3800 series	Connecting Cisco EtherSwitch Service Modules
LAN Network Modules			
1-port Ethernet network module	NM-1E	Cisco 2600 series Cisco 3600 series	Connecting Ethernet, Fast Ethernet, and Token Ring Network Modules
4-port Ethernet network module	NM-4E	Cisco 2600 series Cisco 3600 series	Connecting Ethernet, Fast Ethernet, and Token Ring Network Modules
1-port Fast Ethernet network module (100BASE-TX interface)	NM-1FE-TX	Cisco 3600 series	Connecting Ethernet, Fast Ethernet, and Token Ring Network Modules

Table 1-6 Platform Support for Cisco Network Modules (continued)

Product Description	Cisco Product ID	Supported on Cisco Routers	See Section
1-port Fast Ethernet network module (100BASE-FX interface)	NM-1FE-FX	Cisco 2691 Cisco 3600 series Cisco 3700 series	Connecting Ethernet, Fast Ethernet, and Token Ring Network Modules
1-port Fast Ethernet network module (100BASE-FX interface), version 2	NM-1FE-FX-V2	Cisco 2691 Cisco 3700 series Cisco 3800 series	Connecting Ethernet, Fast Ethernet, and Token Ring Network Modules
1-port Fast Ethernet network module (100BASE-SMF)	NM-1FE-SMF	Cisco 3600 series **Note** Not supported on Cisco 3630 routers Cisco 3700 series	Connecting Ethernet, Fast Ethernet, and Token Ring Network Modules
1-port Gigabit Ethernet network module	NM-1GE	Cisco 2691 Cisco 3660 Cisco 3700 series Cisco 3800 series	Connecting Gigabit Ethernet Network Modules
LAN and Interface Card Slot Combo Network Modules			
2-slot network module (no LAN ports)	NM-2W	Cisco 2600 series Cisco 3600 series Cisco 3700 series Cisco 3800 series Cisco MWR 1941-DC	
2-slot network module with 1 Ethernet port	NM-1E2W	Cisco 3600 series	Connecting Ethernet, Fast Ethernet, and Token Ring Network Modules
2-slot network module with 2 Ethernet ports	NM-2E2W	Cisco 3600 series	Connecting Ethernet, Fast Ethernet, and Token Ring Network Modules
2-slot network module with 1 Ethernet port and 1 Token Ring port	NM-1E1R2W	Cisco 3600 series	Connecting Ethernet, Fast Ethernet, and Token Ring Network Modules
2-slot network module with 1 Fast Ethernet port	NM-1FE2W	Cisco 2691 Cisco 3600 series Cisco 3700 series Cisco 3800 series	Connecting Ethernet, Fast Ethernet, and Token Ring Network Modules
2-slot network module with 1 Fast Ethernet port, version 2	NM-1FE2W-V2	Cisco 2691 Cisco 3600 series Cisco 3700 series Cisco 3800 series	Connecting Ethernet, Fast Ethernet, and Token Ring Network Modules
2-slot network module with 2 Fast Ethernet ports	NM-2FE2W	Cisco 2691 Cisco 3600 series Cisco 3700 series Cisco 3800 series	Connecting Ethernet, Fast Ethernet, and Token Ring Network Modules

Table 1-6 Platform Support for Cisco Network Modules (continued)

Product Description	Cisco Product ID	Supported on Cisco Routers	See Section
2-slot network module with 2 Fast Ethernet ports, version 2	NM-2FE2W-V2	Cisco 2691 Cisco 3600 series Cisco 3700 series Cisco 3800 series	Connecting Ethernet, Fast Ethernet, and Token Ring Network Modules
2-slot network module with 1 Fast Ethernet port and 1 Token Ring port	NM-1FE1R2W	Cisco 2691 Cisco 3600 series Cisco 3700 series Cisco 3800 series	Connecting Ethernet, Fast Ethernet, and Token Ring Network Modules
LAN and T1/E1 Combination Network Modules			
1-port Fast Ethernet with 1-port channelized T1/ISDN-PRI network module, without CSU	NM-1FE1CT1	Cisco 3600 series	Connecting Fast Ethernet-PRI Network Modules
1-port Fast Ethernet with 1-port channelized T1/ISDN-PRI network module, with CSU	NM-1FE1CT1-CSU	Cisco 3600 series	Connecting Fast Ethernet-PRI Network Modules
1-port Fast Ethernet with 2-port channelized T1/ISDN-PRI network module, without CSU	NM-1FE2CT1	Cisco 3600 series	Connecting Fast Ethernet-PRI Network Modules
1-port Fast Ethernet with 2-port channelized T1/ISDN-PRI network module, with CSU	NM-1FE2CT1-CSU	Cisco 3600 series	Connecting Fast Ethernet-PRI Network Modules
1-port Fast Ethernet with 1-port E1/ISDN PRI, balanced	NM-1FE1CE1B	Cisco 3600 series	Connecting Fast Ethernet-PRI Network Modules
1-port Fast Ethernet with 1-port E1/ISDN PRI, unbalanced	NM-1FE1CE1U	Cisco 3600 series	Connecting Fast Ethernet-PRI Network Modules
1-port Fast Ethernet with 2-port E1/ISDN PRI, balanced	NM-1FE1CE1B	Cisco 3600 series	Connecting Fast Ethernet-PRI Network Modules
1-port Fast Ethernet with 2-port E1/ISDN PRI, unbalanced	NM-1FE2CE1U	Cisco 3600 series	Connecting Fast Ethernet-PRI Network Modules
Serial Connectivity Network Modules			
1-port High-Speed Serial interface (HSSI) network module	NM-1HSSI	Cisco 2691 Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3600 series Cisco 3700 series Cisco 3800 series	Connecting HSSI Network Modules

Table 1-6 Platform Support for Cisco Network Modules (continued)

Product Description	Cisco Product ID	Supported on Cisco Routers	See Section
1-port clear-channel T3/E3 network module	NM-1T3/E3	Cisco 2650XM Cisco 2651XM Cisco 2691 Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3660 Cisco 3700 series Cisco 3800 series Cisco MWR 1941-DC	Connecting T3/E3 Network Modules
4-port serial network module	NM-4T	Cisco 3600 series Cisco 3700 series Cisco 3800 series	Connecting Serial Network Modules
4-port asynchronous/synchronous serial network module	NM-4A/S	Cisco 2600 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3600 series Cisco 3700 series Cisco 3800 series Cisco MWR 1941-DC	Connecting Serial Network Modules
8-port asynchronous/synchronous serial network module	NM-8A/S	Cisco 2600 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3600 series Cisco 3700 series Cisco 3800 series Cisco MWR 1941-DC	Connecting Serial Network Modules
16-port asynchronous/synchronous serial network module	NM-16A/S	Cisco 2600 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3700 series Cisco 3800 series	Connecting Serial Network Modules
16-port asynchronous serial network module	NM-16A	Cisco 2600 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3600 series Cisco 3700 series Cisco 3800 series Cisco MWR 1941-DC	Connecting Serial Network Modules

Table 1-6 Platform Support for Cisco Network Modules (continued)

Product Description	Cisco Product ID	Supported on Cisco Routers	See Section
32-port asynchronous serial network module	NM-32A	Cisco 2600 series Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3600 series Cisco 3700 series Cisco 3800 series	Connecting Serial Network Modules
Wireless and Satellite Network Modules			
Cisco wireless multipoint subscriber unit network module	NM-WMDA	Cisco 2600 series Cisco 3600 series	Connecting Wireless Multipoint Network Modules
Cisco wireless LAN controller network module	NM-AIR-WLC6	Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3700 series Cisco 3800 series	Connecting Cisco Wireless LAN Controller Modules
Cisco wireless LAN controller enhanced network module	NME-AIR-WLC8-K9	Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3700 series Cisco 3800 series	Connecting Cisco Wireless LAN Controller Enhanced Network Modules
Cisco wireless LAN controller enhanced network module	NME-AIR-WLC12-K9	Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3700 series Cisco 3800 series	Connecting Cisco Wireless LAN Controller Enhanced Network Modules
Cisco IP VSAT satellite WAN network module	NM-1VSAT-GILAT	Cisco 2600XM series Cisco 2691 Cisco 2811 Cisco 2821 Cisco 2851 Cisco 3700 series Cisco 3800 series	Connecting Cisco IP VSAT Satellite WAN Network Modules

Related Documents

Cisco product documentation is available online at www.cisco.com (also known as Cisco.com) and is accessible through multiple navigation paths.

To access the documents and tools described in this section, you must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

To print a document in its original page format, access the online document, and click the PDF icon.

Tip Some authors provide a full-length "book" PDF, usually located above or below the links to the book chapter files on the main book index page. Use this book-length PDF to generate printed copies of the entire book.

Hardware Documentation

Cisco hardware documentation for Cisco access routers provides the following three categories of information:

- Hardware installation—Basic to advanced hardware installation procedures
- Hardware reference information and specifications—Dimensions, operating environment, cable pinouts
- Regulatory compliance and safety information—Safety warnings translated into multiple languages and statements of compliance with regulatory requirements from various countries around the world

Installation Documents

To find chassis installation instructions for any Cisco router, access the documents located at **Technical Support & Documentation > Product Support > Routers >** *Router series you are using* **> Install and Upgrade > Install and Upgrade Guides**.

To find installation instructions for Cisco network modules, access the *Cisco Network Modules Hardware Installation Guide*.

To find installation instructions for Cisco interface cards, access the *Cisco Interface Cards Hardware Installation Guide.*

Reference Documents

To find cabling specifications for Cisco modular access routers, access the *Cisco Modular Access Router Cable Specifications* located at **Technical Support & Documentation > Product Support > Routers >** *Router series you are using* **> Reference Guides > Technical References**.

Regulatory Compliance and Safety Information Documents

To find regulatory compliance and safety information for a Cisco router, access the documents located at **Technical Support & Documentation > Product Support > Routers >** *Router series you are using* **> Install and Upgrade > Install and Upgrade Guides**.

To find regulatory compliance and safety information for Cisco network modules and Cisco interface cards used on Cisco access routers, access the documents located at **Technical Support & Documentation > Product Support > Cisco Network Modules > Install and Upgrade > Install and Upgrade Guides**.

Cisco IOS Software Documentation

Cisco IOS software documentation provides the following categories of information:

- Software configuration—Basic to advanced software configuration procedures, sample configurations
- Software references—Command references, system message guides
- Software release information—Supported products, caveats
- Software release tools—Cisco Feature Navigator II, Cisco IOS Upgrade Planner, software downloads, security notices and advisories

Cisco IOS Software Configuration Documents

To find initial configuration instructions specific to the Cisco router you are using, access the documents located at **Technical Support & Documentation > Product Support > Routers >** *Router series you are using* **> Configure > Configuration Guides**.

To find configuration examples specific to the Cisco router you are using, access the documents located at **Technical Support & Documentation > Product Support > Routers >** *Router series you are using* **> Configure > Configuration Examples and TechNotes**.

To find advanced configuration instructions for a specific feature, access the documents located at **Technical Support & Documentation > Product Support > Cisco IOS Software >** *Cisco IOS release you are using* **> Configure > Feature Guides**.

Cisco IOS Software Reference Documents

To find command reference information for the Cisco IOS software release you are using, access the documents located at **Technical Support & Documentation > Product Support > Cisco IOS Software >** *Cisco IOS release you are using* **> Reference Guides > Command References**.

Timesaver You can also use the online Command Lookup tool, located at **Technical Support & Documentation > Tools & Resources > Command Lookup Tool**.

To find system message information for the Cisco IOS software release you are using, access the documents located at **Technical Support & Documentation > Product Support > Cisco IOS Software >** *Cisco IOS release you are using* **> Troubleshoot and Alerts > Error and System Messages**.

Cisco IOS Software Release Documents and Tools

To find Cisco IOS software release information for the Cisco IOS software release you are using, access the documents located at **Technical Support & Documentation > Product Support > Cisco IOS Software >** *Cisco IOS release you are using* **> General Information > Release Notes**.

To view Cisco IOS software features by release, or to compare two different Cisco IOS releases, access Cisco Feature Navigator II, located at **Products and Solutions > Cisco IOS Software > All Cisco IOS Software > Cisco Feature Navigator II**.

To download Cisco IOS software, or to locate license agreements and warranty information for a Cisco IOS software release, access the Software Center, located at **Technical Support & Documentation > Downloads**.

To plan for a Cisco IOS upgrade, access the Cisco IOS Upgrade Planner, located at **Technical Support & Documentation > Tools and Resources > Cisco IOS Upgrade Planner**.

To view Cisco IOS security advisories that might apply to your product, access the *Cisco Product Security Advisories and Notices* website located at http://www.cisco.com/warp/public/707/advisory.html.

Timesaver You can also sign up to receive e-mail alerts using the Product Alert Tool, located at **Technical Support & Documentation > Tools and Resources > Product Alert Tool**.

Where to Go Next

For network module installation information, go to Chapter 2, "Installing Cisco Network Modules in Cisco Access Routers."

For regulatory compliance and safety information, see the *Cisco Network Modules and Interface Cards Regulatory Compliance and Safety Information* document.

For hardware information about specific network modules, use Table 1-6 Platform Support for Cisco Network Modules in this document to locate the appropriate chapter.

CHAPTER 2

Installing Cisco Network Modules in Cisco Access Routers

This chapter provides information you should know before and during installation of Cisco network modules in Cisco access routers, and contains the following sections:

Recommended Practices for Cisco Network Modules

This section describes recommended practices for safe and effective installation of the hardware described in this document, and includes the following sections:

- Safety Recommendations
- Preventing Electrostatic Discharge Damage
- General Maintenance Guidelines for Cisco Network Modules

Safety warnings included in this section apply to all Cisco network modules used on Cisco access routers.

Note Recommendations and warnings for specific network modules are documented in the chapter specific to the network module.

Safety Recommendations

To prevent hazardous conditions, follow these safety recommendations while working with this equipment:

- Keep tools away from walk areas where you or others could fall over them.

- Do not wear loose clothing around the router. Fasten your tie or scarf and roll up your sleeves to prevent clothing from being caught in the chassis.
- Wear safety glasses when working under any conditions that might be hazardous to your eyes.
- Locate the emergency power-off switch in the room before you start working. If an electrical accident occurs, shut the power off.
- Before working on the router, turn off the power and unplug the power cord.
- Disconnect all power sources before doing the following:
  - Installing or removing a router chassis
  - Working near power supplies
- Do not work alone if potentially hazardous conditions exist.
- Always check that power is disconnected from a circuit.
- Remove possible hazards from your work area, such as damp floors, ungrounded power extension cables, or missing safety grounds.
- If an electrical accident occurs, proceed as follows:
  - Use caution; do not become a victim yourself.
  - Turn off power to the room using the emergency power-off switch.
  - If possible, send another person to get medical aid. Otherwise, determine the condition of the victim and then call for help.
  - Determine if the person needs rescue breathing or external cardiac compressions; then take appropriate action.

Preventing Electrostatic Discharge Damage

Electrostatic discharge can damage equipment and impair electrical circuitry. Electrostatic discharge occurs when electronic printed circuit cards, such as those used in Cisco network modules, are improperly handled and can result in complete or intermittent equipment failure. Always observe the following electrostatic discharge damage (ESD) prevention procedures when installing, removing, and replacing Cisco network modules, Cisco interface cards, Cisco expansion modules, or other electronic printed circuit cards:

- Make sure that the router chassis is electrically connected to earth ground.
- Wear an ESD-preventive wrist strap, and make sure that it makes good contact with your skin.
- Connect the wrist strap clip to an unpainted portion of the chassis frame to channel unwanted ESD voltages to ground.

Caution The wrist strap and clip must be used correctly to ensure proper ESD protection. Periodically confirm that the resistance value of the ESD-preventive wrist strap is between 1 and 10 megohms (Mohm).

- If no wrist strap is available, ground yourself by touching the metal part of the router chassis.

General Maintenance Guidelines for Cisco Network Modules

The following maintenance guidelines apply to Cisco network modules:

- Keep the router chassis area clear and dust-free during and after installation.
- If you remove the chassis cover for any reason, store it in a safe place.
- Do not perform any action that creates a hazard to people or makes equipment unsafe.
- Keep walk areas clear to prevent falls or damage to equipment.
- Follow installation and maintenance procedures as documented by Cisco Systems, Inc.

Safety Warnings for Cisco Network Modules

The following safety warning statements apply to all hardware procedures involving Cisco network modules for Cisco access routers. Translations of these warnings are available in the *Cisco Network Modules and Interface Cards Regulatory Compliance and Safety Information* document, which ships with all individual Cisco network module orders, and is also available online.

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

Warning **Two people are required to lift the chassis. Grasp the chassis underneath the lower edge and lift with both hands. To prevent injury, keep your back straight and lift with your legs, not your back. To prevent damage to the chassis and components, never attempt to lift the chassis with the handles on the power supplies or on the interface processors, or by the plastic panels on the front of the chassis. These handles were not designed to support the weight of the chassis.** Statement 194

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

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.** Statement 1040

The following warnings apply in Australia:

Warning **Do not touch the power supply when the power cord is connected. For systems with a power switch, line voltages are present within the power supply even when the power switch is OFF and the power cord is connected. For systems without a power switch, line voltages are present within the power supply when the power cord is connected.** Statement 4

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

Warning **This equipment is to be installed and maintained by service personnel only as defined by AS/NZS 3260 Clause 1.2.14.3 Service Personnel.** Statement 88

Warning **This equipment will be inoperable when mains power fails.** Statement 198

Warning **Incorrect connection of this or connected equipment to a general purpose outlet could result in a hazardous situation.** Statement 212

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

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

Warning **To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Both LAN and WAN ports may use RJ-45 connectors. Use caution when connecting cables.** Statement 1021

Warning **Hazardous network voltages are present in WAN ports regardless of whether power to the router is OFF or ON. To avoid electric shock, use caution when working near WAN ports. When detaching cables, detach the end away from the router first.** Statement 1026

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.** Statement 1040

Warning **Before opening the chassis, disconnect the telephone-network cables to avoid contact with telephone-network voltages.** Statement 1041

Warning **The telecommunications lines must be disconnected 1) before unplugging the main power connector and/or 2) while the housing is open.** Statement 1043

Installing Cisco Network Modules in Cisco Access Routers

This section describes installation tasks for Cisco network modules used on Cisco access routers, and contains the following subsections:

- Tools and Equipment Required During Cisco Network Module Installation
- Installing and Removing Blank Faceplates
  - Installing Blank Faceplates on Cisco Access Routers
  - Removing Blank Faceplates from Cisco Access Routers
- Preparing Cisco Router Slots for Network Module Installation
  - Installing Slot Dividers
  - Removing Slot Dividers
  - Installing Slot Adapters
  - Removing Slot Adapters
- Installing Single-Wide, Extended Single-Wide, and Extension Voice Network Modules in Cisco Access Routers
- Installing Double-Wide and Extended Double-Wide Network Modules in Cisco Access Routers

Note The following routers do not support online insertion and removal (OIR) of network modules:

- Cisco 2600 series
- Cisco 2811
- Cisco 2821
- Cisco 2851
- Cisco 3620
- Cisco 3640
- Cisco MWR 1941-DC

To avoid damaging the router, turn off electrical power and disconnect network cables before inserting or removing a network module into these routers.

Tools and Equipment Required During Cisco Network Module Installation

You will need the following tools and equipment while working with Cisco network modules:

- Number 1 Phillips screwdriver or a small flat-blade screwdriver
- ESD-preventive wrist strap
- (For routers using DC power) Tape to secure DC circuit breaker handle

Summary of Installation Tasks

When installing a network module in a Cisco access router, perform the following tasks:

Table 2-1 Network Module Hardware Installation Tasks for Cisco Access Routers

	For Cisco 2600 Series, Cisco 2811, Cisco 3600 Series (Except Cisco 3660 Routers), and Cisco MWR 1941-DC Routers	For Cisco 2821, Cisco 2851, Cisco 3700 Series, Cisco 3800 Series, and Cisco 3660 Routers
Step 1	Turn off power to the router.	Turn off power to the router.
Step 2	Remove blank faceplates from the slots you plan to use. (See the "Removing Blank Faceplates from Cisco Access Routers" section on page 2-8.)	Remove blank faceplates from the slots you plan to use. (See the "Removing Blank Faceplates from Cisco Access Routers" section on page 2-8.)
Step 3	Install the network module. (See the "Installing Single-Wide, Extended Single-Wide, and Extension Voice Network Modules in Cisco Access Routers" and "Installing Double-Wide and Extended Double-Wide Network Modules in Cisco Access Routers" sections.)	Prepare the slot for the network module form factor you are installing. (See the "Preparing Cisco Router Slots for Network Module Installation" section on page 2-8.)
Step 4	Install blank faceplates where appropriate. (See the "Installing Blank Faceplates on Cisco Access Routers" section on page 2-7.)	Install the network module. (See the "Installing Single-Wide, Extended Single-Wide, and Extension Voice Network Modules in Cisco Access Routers" section on page 2-15 and "Installing Double-Wide and Extended Double-Wide Network Modules in Cisco Access Routers" section on page 2-16 sections.)
Step 5	—	Install blank faceplates where appropriate. (See the "Installing Blank Faceplates on Cisco Access Routers" section on page 2-7.)

Installing and Removing Blank Faceplates

All empty chassis slots for network modules, extension voice modules, or interface cards must be covered with blank faceplates to ensure proper cooling airflow and to prevent electromagnetic interference.

Note Blank network module faceplates are for single-wide network module slots only.

To install a blank faceplate over a network module slot set up for an extended single-wide, double-wide, or extended double-wide network module, you must prepare the slot for single-wide network modules. See Table 2-3 and Table 2-4 for information on preparing network module slots for different network module form factors.

Table 2-2 Preparing to Install Blank Network Module Faceplates on Cisco Access Router Network Module Slots

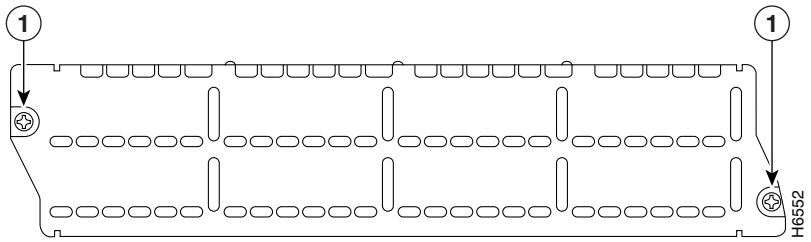
	On an Extended Single-Wide Slot	On a Double-Wide Slot	On an Extended Double-Wide Slot
Step 1	Install a slot adapter on the right side of the slot. (See the "Installing Slot Adapters" section on page 2-12.)	Install a slot divider in the slot. (See the "Installing Slot Dividers" section on page 2-10.)	Install a slot divider in the slot. (See the "Installing Slot Dividers" section on page 2-10.)
Step 2	Install the blank faceplate. (See the "Installing Blank Faceplates on Cisco Access Routers" section on page 2-7.)	Install a slot adapter in the right side of the left slot. (See the "Installing Slot Adapters" section on page 2-12.)	Install slot adapters in the right sides of both slots. (See the "Installing Slot Adapters" section on page 2-12.)
Step 3	—	Install one blank faceplate over each slot. (See the "Installing Blank Faceplates on Cisco Access Routers" section on page 2-7.)	Install one blank faceplate over each slot. (See the "Installing Blank Faceplates on Cisco Access Routers" section on page 2-7.)

Installing Blank Faceplates on Cisco Access Routers

To install a blank faceplate, perform the following steps:

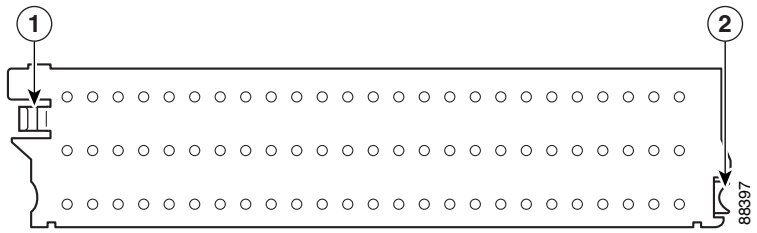
Step 1 Determine which type of blank network module faceplate you are using. (See Figure 2-1 and Figure 2-2.)

Figure 2-1 Blank Network Module Panel with Screws



1	Captive screws for securing blank faceplate

Figure 2-2 Blank Network Module Panel with Tabs



1	Snap-lock tab (use screwdriver to remove)	**2**	Tab

Step 2 Install the blank faceplate.

- (For blank faceplates with mounting screws) Align the captive screws with the screw holes on the chassis. Using either a number 1 Phillips screwdriver or a small flat-blade screwdriver, tighten the captive screws until the blank faceplate is flush with the chassis.
- (For blank faceplates with tabs) Align the blank faceplate tabs with the slots on the chassis. Press the blank faceplate against the chassis until the tabs pop into place. The blank faceplate is flush with the chassis when properly installed.

Step 3 Continue with hardware installation tasks.

Removing Blank Faceplates from Cisco Access Routers

To remove blank network module faceplates, perform the following steps:

Step 1 Determine which type of blank network module faceplate you are using. (See Figure 2-1 and Figure 2-2.)

Step 2 Remove the blank faceplate.

- (For blank faceplates with mounting screws) Using either a number 1 Phillips screwdriver or a small flat-blade screwdriver, unscrew the captive screws and remove the blank faceplate from the chassis slot you plan to use.
- (For blank faceplates with tabs) Using a small flat-blade screwdriver, release the snap-lock tab on the left side of the faceplate (see Figure 2-2). The faceplate pops out when the tab is released.

Tip Save blank faceplates for future use.

Step 3 Continue with hardware installation tasks.

Preparing Cisco Router Slots for Network Module Installation

Several Cisco access routers have flexible network module slots to support all four Cisco network module form factors. Before installing a network module, you must prepare the slot for the network module's particular form factor.

The following Cisco access routers may require network module slot preparation before installation of the network module:

- Cisco 2821 and 2851 routers
- Cisco 3660 routers (single-wide and double-wide network modules only)
- Cisco 3700 series routers (single-wide and double-wide network modules only)
- Cisco 3800 series routers

Tip For an introduction to Cisco network module form factors, see the "Introduction to Cisco Network Module Form Factors" section on page 1-1.

To prepare a network module slot for a single-wide or extended single-wide network module, perform the tasks listed in Table 2-3.

Table 2-3 Preparing Network Module Slots for Single-Wide and Extended Single-Wide Network Modules

	For Single-Wide Network Modules	For Extended Single-Wide Network Modules
Step 1	Remove the blank faceplates from the slots you plan to use. (See the "Removing Blank Faceplates from Cisco Access Routers" section on page 2-8.)	Remove the blank faceplates from the slots you plan to use. (See the "Removing Blank Faceplates from Cisco Access Routers" section on page 2-8.)
Step 2	Remove the slot adapters on the right side of the router slot. (See the "Removing Slot Adapters" section on page 2-14.)	Insert the slot divider. (See the "Installing Slot Dividers" section on page 2-10.)
Step 3	Insert the slot divider. (See the "Installing Slot Dividers" section on page 2-10.)	Install the network module. (See the "Installing Single-Wide, Extended Single-Wide, and Extension Voice Network Modules in Cisco Access Routers" section on page 2-15.)
Step 4	(For single-wide network modules only) Insert the slot adapter on the right side of the slot you plan to use. (See the "Installing Slot Adapters" section on page 2-12.)	—
Step 5	Install the network module. (See the "Installing Single-Wide, Extended Single-Wide, and Extension Voice Network Modules in Cisco Access Routers" section on page 2-15.)	—

Tip On Cisco 3800 series routers, extension voice modules can be installed in standard network module slots. When an extension module is installed in a standard network module slot, treat an extension voice module like a single-wide network module.

To prepare a network module slot for a double-wide or extended double-wide network module, perform the tasks listed in Table 2-4.

Table 2-4 Preparing Network Module Slots for Double-Wide and Extended Double-Wide Network Modules

	For Double-Wide Network Modules	For Extended Double-Wide Network Modules
Step 1	Remove blank faceplates from the slots you plan to use. (See the "Removing Blank Faceplates from Cisco Access Routers" section on page 2-8.)	Remove blank faceplates from the slots you plan to use. (See the "Removing Blank Faceplates from Cisco Access Routers" section on page 2-8.)
Step 2	Remove the slot adapters on the right side of each router slot. (See the "Removing Slot Adapters" section on page 2-14.)	Remove the slot adapter on the right side of the applicable router slot. (See the "Removing Slot Adapters" section on page 2-14.) **Timesaver** If the slot adapter is already installed against the right side wall of the router chassis, skip this step.
Step 3	Remove the slot divider. (See the "Removing Slot Dividers" section on page 2-12.)	Remove the slot divider. (See the "Removing Slot Dividers" section on page 2-12.)

Table 2-4 Preparing Network Module Slots for Double-Wide and Extended Double-Wide Network Modules (continued)

	For Double-Wide Network Modules	For Extended Double-Wide Network Modules
Step 4	(For double-wide network modules only) Insert 2 slot adapters on the right side of the router slot. (See the "Installing Slot Adapters" section on page 2-12.)	Install the network module. (See the "Installing Single-Wide, Extended Single-Wide, and Extension Voice Network Modules in Cisco Access Routers" section on page 2-15.)
Step 5	Install the network module. (See the "Installing Single-Wide, Extended Single-Wide, and Extension Voice Network Modules in Cisco Access Routers" section on page 2-15.)	—

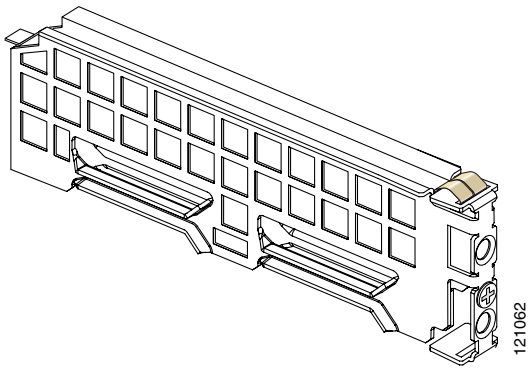
Installing Slot Dividers

Slot dividers (see Figure 2-3) are used to customize network module slots for different Cisco network module form factors. Slot dividers are used on the following Cisco access routers:

- Cisco 2851 routers
- Cisco 3660 routers
- Cisco 3745 routers
- Cisco 3800 series

Slot dividers are installed to permit use of extension voice modules (on Cisco 3800 series routers only), single-wide, and extended single-wide network modules in modular router slots. To determine whether you need to install or remove slot dividers on your Cisco access router, see Table 2-3 and Table 2-4.

Figure 2-3 Slot Divider for Network Module Slots (Sample Shows Divider for Cisco 2851 and 3800 Series)

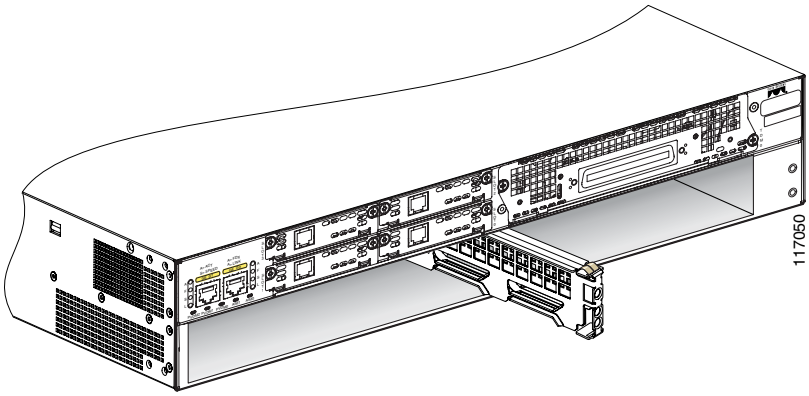


To install a slot divider, perform the following steps:

Step 1 Remove any installed network modules, blank faceplates, and slot adapters from the router slot you plan to use.

Step 2 Insert the top rails of the slot divider between the two guide rails in the top of the network module slot. (See Figure 2-4.)

Figure 2-4 Inserting a Slot Divider into a Network Module Slot



Step 3 Push the slot divider in until it is fully seated.

Step 4 Tighten the retention screw on the front of the slot divider with a number 1 Phillips screwdriver. (See Figure 2-5.) When the slot divider is fully inserted, its front surface is flush with the panel of the router. (See Figure 2-5.)

Figure 2-5 Tightening the Slot Divider in a Network Module Slot

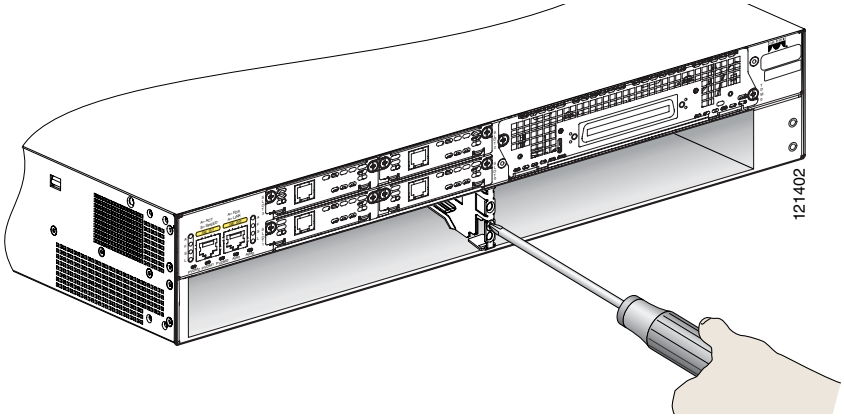
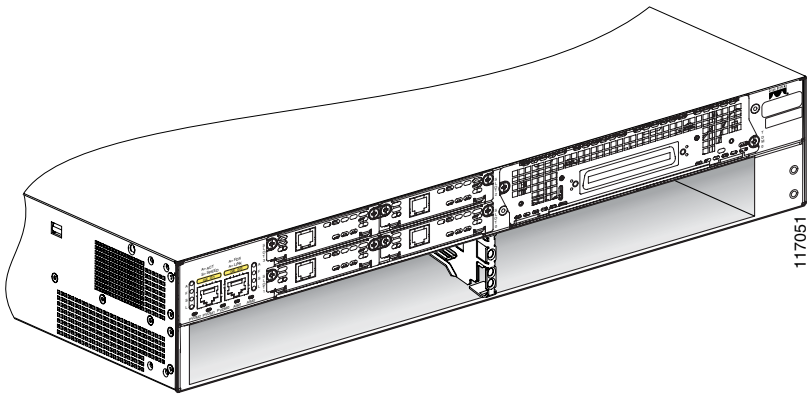


Figure 2-6 Slot Divider Installed in a Network Module Slot



Step 5 Proceed with hardware configuration tasks as listed in Table 2-3 and Table 2-4.

Removing Slot Dividers

Slot dividers are removed to permit use of double-wide and extended double-wide network modules in modular router slots. To determine whether you need to install or remove slot dividers on your Cisco access router, see Table 2-3 and Table 2-4.

To remove slot dividers from network module slots, perform the following steps:

Step 1 Remove any installed network modules, blank faceplates, and slot adapters from the router slot you plan to use.

Step 2 Loosen the retention screw on the front of the slot divider.

Step 3 Pull the slot divider straight out of the network module slot.

Step 4 Proceed with hardware configuration tasks as listed in Table 2-3 and Table 2-4.

Installing Slot Adapters

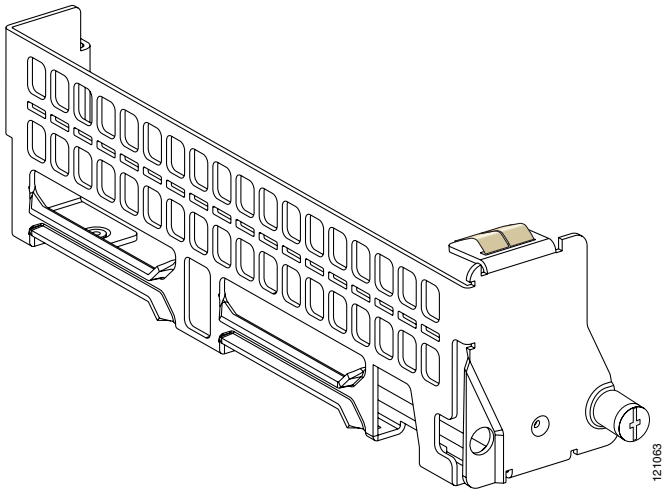
Slot adapters (see Figure 2-7) are used to customize network module slots for different Cisco network module form factors. Slot adapters are used on the following Cisco access routers:

- Cisco 2821
- Cisco 2851
- Cisco 3800 series

Slot adapters permit installation of extension voice modules (on Cisco 3800 series routers only), single-wide, and extended single-wide network modules in modular router slots.

To determine whether you need to install or remove slot adapters on your Cisco access router, see Table 2-3 and Table 2-4.

Figure 2-7 Sample Slot Adapter for Network Module Slots in Cisco Access Routers

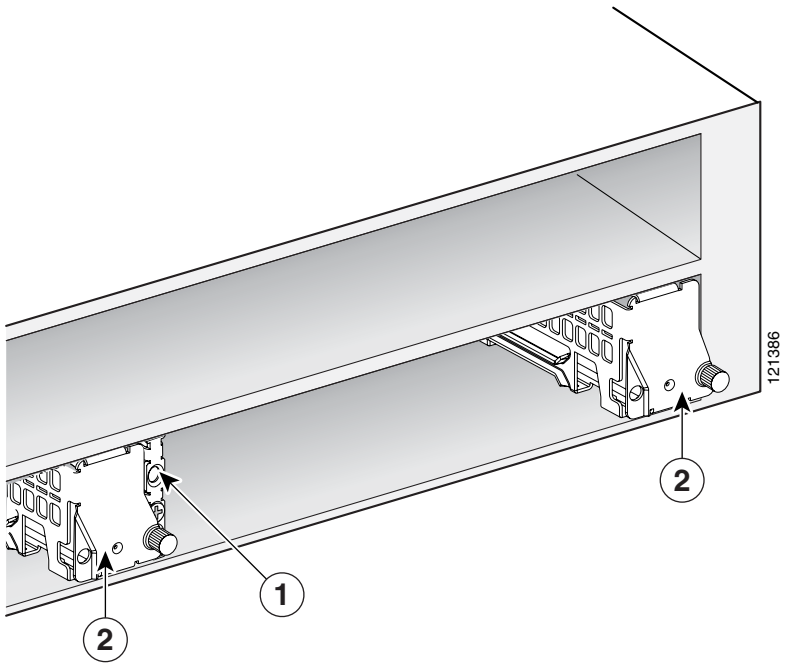


To install a slot adapter, perform the following steps:

Step 1 Remove any installed network modules from the router slot you plan to use.

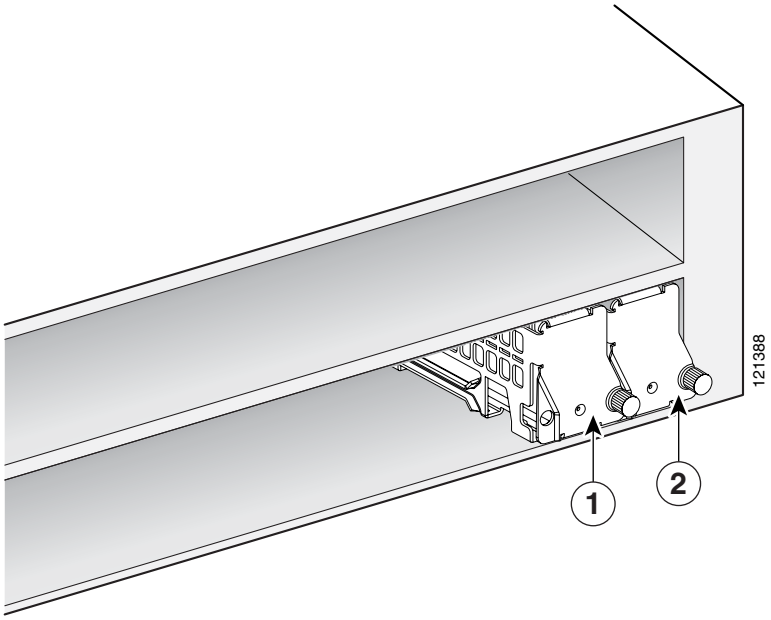
Step 2 Determine the location for slot adapter installation. (See Figure 2-8 and Figure 2-9.) The extended single-wide network modules use a slot divider instead of a slot adapter. (See Figure 2-6.)

Figure 2-8 Slot Divider and Adapters Locations for Standard Single-Wide Network Modules (Generic Router)



1	Slot divider	**2**	Slot adapters

Figure 2-9 Slot Adapter Locations for Double-Wide Network Modules (Generic Router)



1	Slot adapter	**2**	Slot adapter

Step 3 Install other hardware if necessary. (See Table 2-3 and Table 2-4.)

Step 4 Orient the slot adapter so the tab on the rear of the slot adapter aligns with the slot on the router backplane.

Note When correctly aligned, the captive screw on the slot adapter aligns with a threaded hole in the chassis, slot divider, or adjacent slot adapter, depending on your current hardware setup.

Step 5 Slide the slot adapter into the slot.

Step 6 Using a number 1 Phillips or small flat-head screwdriver, tighten the captive screw to secure the slot adapter.

Tip The slot adapter can be secured to the router chassis, to a slot divider, or to another slot adapter, depending on its installation location. See Figure 2-8 for possible variations.

Step 7 Proceed with hardware configuration tasks as listed in Table 2-3 and Table 2-4.

Removing Slot Adapters

Slot adapters are removed to permit use of double-wide and extended double-wide network modules in modular router slots. To determine whether you need to install or remove slot adapters on your Cisco access router, see Table 2-3 and Table 2-4.

To remove slot adapters from network module slots, perform the following steps:

Step 1 Remove any installed network modules and blank faceplates from the router slot you plan to use.

Step 2 Using a number 1 Phillips or small flat-head screwdriver, loosen the captive screw on the slot adapter. (See Figure 2-7.)

Step 3 Slide the slot adapter from the slot.

Step 4 Proceed with hardware configuration tasks as listed in Table 2-3 and Table 2-4.

Installing Single-Wide, Extended Single-Wide, and Extension Voice Network Modules in Cisco Access Routers

Network modules can be installed either before or after mounting the router, whichever is more convenient. To install a network module, follow these steps:

Step 1 Turn off electrical power to the router. Leave the power cable plugged in to channel ESD voltages to ground.

(For the Cisco MWR 1941-DC router) Turn off power by turning the DC power source circuit breaker to OFF. Tape the circuit breaker in the OFF position. To channel ESD voltages to ground, do not remove the wire from the ground lug.

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 7

Step 2 Remove all network cables, including telephone cables, from the rear panel of the router.

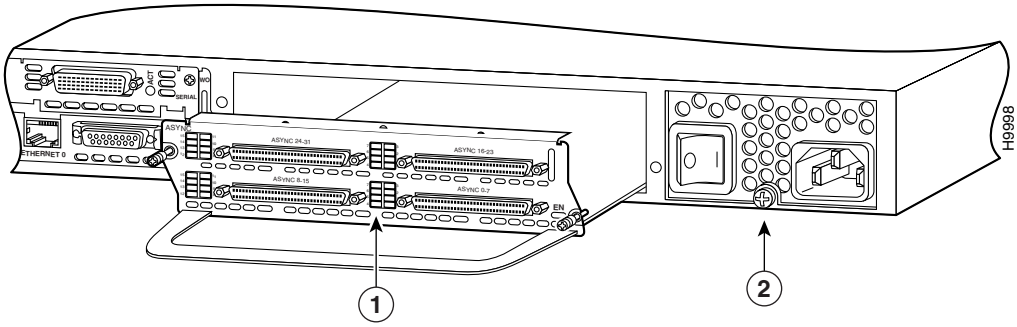
Step 3 Remove the blank faceplates installed over the slot you intend to use. (See the "Installing and Removing Blank Faceplates" section on page 2-6.)

Tip Save blank faceplates for future use.

Step 4 (For certain Cisco routers) Prepare the slot for the network module form factor you are installing. (See the "Preparing Cisco Router Slots for Network Module Installation" section on page 2-8.)

Step 5 Align the network module with the guides in the chassis walls or slot divider and slide it gently into the slot. (See Figure 2-10.)

Figure 2-10 Installing Single-Wide and Extended Single-Wide Network Modules in Cisco Access Routers



1	Single-wide network module	**2**	Router chassis

Step 6 Using the network module handle, push the module into place until you feel the edge connector seat securely into the connector on the router backplane. The network module faceplate should contact the chassis rear panel.

Step 7 Using a number 1 Phillips or flat-blade screwdriver, tighten the captive mounting screws on the module faceplate.

Step 8 Proceed with connecting the network module to the network and power up the router.

Tip See the "Where to Go Next" section on page 2-27 for information on locating additional hardware documentation.

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

Installing Double-Wide and Extended Double-Wide Network Modules in Cisco Access Routers

Network modules can be installed either before or after mounting the router, whichever is more convenient. To install a double-wide or extended double-wide network module, perform these steps:

Step 1 Turn off electrical power to the router. Leave the power cable plugged in to channel ESD voltages to ground.

Step 2 Remove all network cables, including telephone cables, from the rear panel of the router.

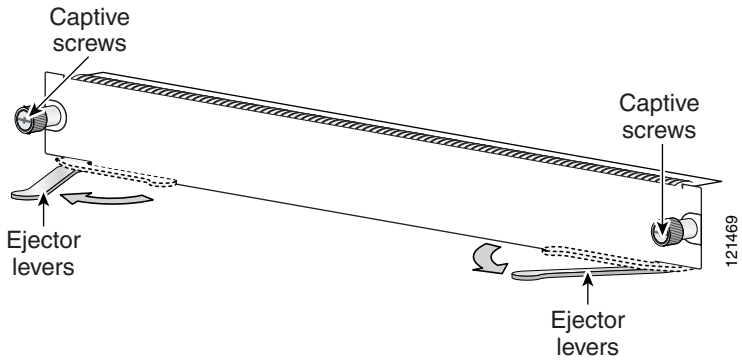
Step 3 Remove the blank faceplates installed over the slot you intend to use. (See the "Installing and Removing Blank Faceplates" section on page 2-6.)

Tip Save blank faceplates for future use.

Step 4 (For certain Cisco routers) Prepare the slot for the network module form factor you are installing. (See the "Preparing Cisco Router Slots for Network Module Installation" section on page 2-8.)

Step 5 Confirm that network module levers are in the open position away from the network module faceplate. (See Figure 2-11.)

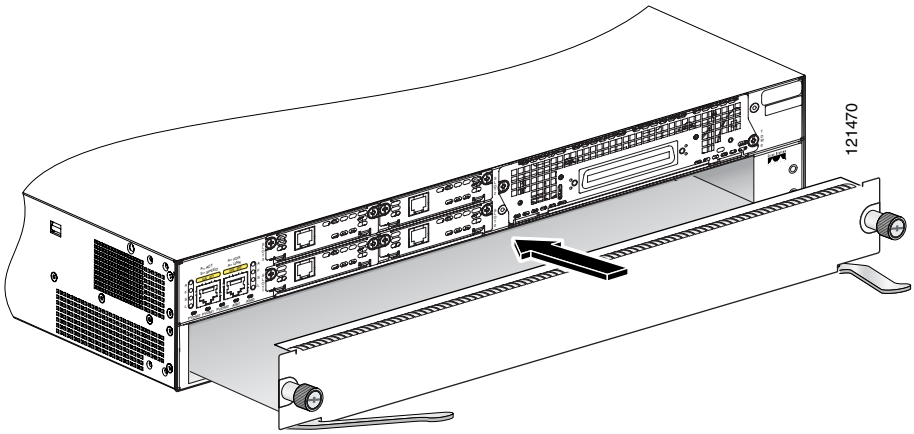
Figure 2-11 Open and Closed Positions for Double-Wide and Extended Double-Wide Network Module Ejector Levers



Timesaver If the network module ejector levers are not in the open position during installation, the network module does not seat properly and connections between the network module and the router backplane are not made. Install the network module with the ejector levers in the open position.

Step 6 Align the network module with the guides in the chassis walls and slide it gently into the slot (see Figure 2-12). Once seated, the ejector levers close halfway.

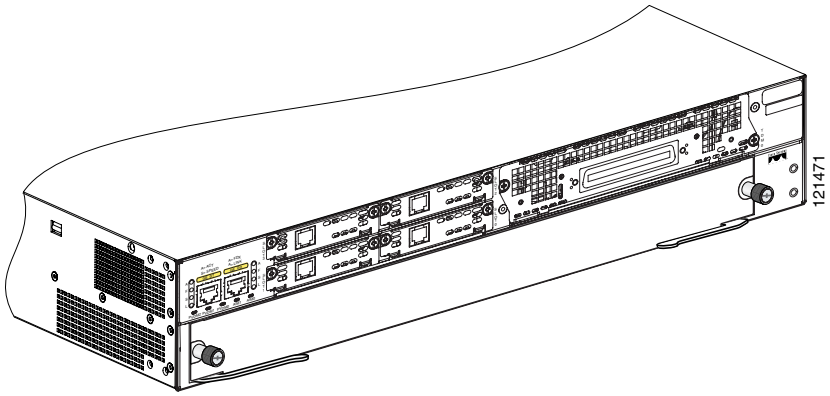
Figure 2-12 Installing Double-Wide and Extended Double-Wide Network Modules in Cisco Access Routers



Caution The double-wide and extended double-wide network modules can be heavy. Avoid touching the network module board to support the module. Handle the network module by the faceplate only to avoid damage to board components.

Step 7 Push the ejector levers so they make contact with the network module faceplate to finish seating the network module and lock the network module into place in the router slot. (See Figure 2-13.)

Figure 2-13 Seating a Double-Wide or Extended Double-Wide Network Module



Step 8 Proceed with connecting the network module to the network and power up the router.

Tip See the "Where to Go Next" section on page 2-27 for information on locating additional hardware documentation.

Removing or Replacing Cisco Network Modules for Cisco Access Routers

This section describes removal and replacement procedures for Cisco network modules used in Cisco access routers, and contains the following subsections:

- Removing or Replacing Single-Wide, Extended Single-Wide, and Extension Voice Network Modules from Cisco Access Routers
- Removing or Replacing Double-Wide and Extended Double-Wide Network Modules in Cisco Access Routers
- Replacing Network Modules in Cisco Access Routers with Online Insertion and Removal Support
- Removing or Replacing Application and Service Network Modules

Removing or Replacing Single-Wide, Extended Single-Wide, and Extension Voice Network Modules from Cisco Access Routers

To remove or replace a single-wide, extended single-wide, or extension voice network module from a Cisco access router, perform these steps:

Step 1 Turn off power to the router.

- (For routers without OIR support) Turn off electrical power to the router. Leave the power cable plugged in to channel ESD voltages to ground.
- (For the Cisco MWR 1941-DC router) Turn off power by turning the DC power source circuit breaker to OFF. Tape the circuit breaker in the OFF position. To channel ESD voltages to ground, do not remove the wire from the ground lug.

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 7

Step 2 Unplug all network interface cables from the rear panel of the router.

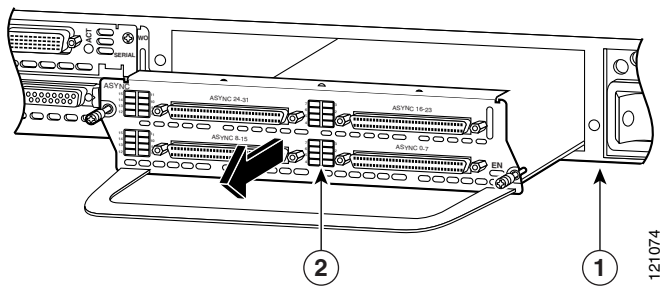
Timesaver To make it easier to work with network cables, label the cables or prepare a network cabling diagram before removing network interface cables from the network module.

Step 3 Using a number 1 Phillips or flat-blade screwdriver, loosen the captive mounting screws on the module faceplate.

Step 4 Using the module handle, pull the network module from the router slot.

Caution To avoid damaging the network module, always handle the network module by the handle or faceplate. Do not touch the circuit board.

Figure 2-14 Removing Single-Wide and Extended Single-Wide Network Modules from Cisco Access Routers



1	Router chassis	2	Single-wide network module

Step 5 Install the appropriate item.

- (If you are replacing the module) Install a replacement module using the procedures described in the "Installing Cisco Network Modules in Cisco Access Routers" section on page 2-5
- (If you are not replacing the module) Install a blank faceplate over the empty slots to ensure proper airflow. (See the "Installing and Removing Blank Faceplates" section on page 2-6.)

Tip See the "Where to Go Next" section on page 2-27 for information on locating additional hardware documentation.

Removing or Replacing Double-Wide and Extended Double-Wide Network Modules in Cisco Access Routers

To remove or replace a double-wide or extended double-wide network module, perform these steps:

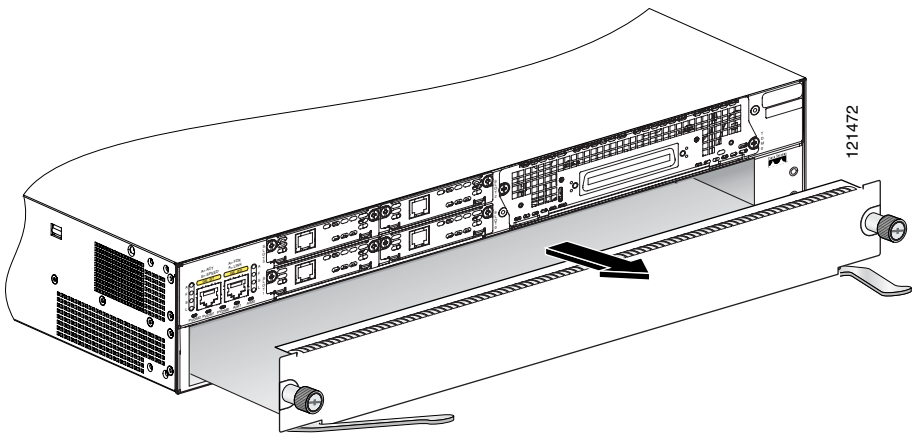
Step 1 Turn off electrical power to the router. Leave the power cable plugged in to channel ESD voltages to ground.

Step 2 Unplug all network interface cables from the network module.

Timesaver To make it easier to work with network cables, label the cables or prepare a network cabling diagram before removing network interface cables from the network module.

Step 3 Using your thumbs, open the levers on the network module faceplate. (See Figure 2-15.) When the ejector levers open, they unseat the network module from the router. The network module faceplate moves away from the router rear panel.

Figure 2-15 Removing Double-Wide and Extended Double-Wide Network Modules from Cisco Access Routers



Step 4 Using your fingers, grasp the edges of the network module faceplate, near the bottom where the board attaches. Pull the network module from the router slot.

Caution The double-wide and extended double-wide network modules can be heavy. Avoid touching the network module board to support the module. Handle the network module by the faceplate only to avoid damage to board components.

Step 5 Install the appropriate item.

- (If you are replacing the module) Install a replacement module using the procedures described in the "Installing Cisco Network Modules in Cisco Access Routers" section on page 2-5
- (If you are not replacing the module) Install blank faceplates over the empty slot to ensure proper airflow. (See the "Installing and Removing Blank Faceplates" section on page 2-6.)

Tip See the "Where to Go Next" section on page 2-27 for information on locating additional hardware documentation.

Replacing Network Modules in Cisco Access Routers with Online Insertion and Removal Support

Online insertion and removal (OIR) provides uninterrupted network operation, maintains routing information, and ensures session preservation. The following Cisco access routers support OIR for similar network modules:

- Cisco 3660 routers
- Cisco 3745 routers
- Cisco 3845 routers

Caution These Cisco access routers support OIR with similar network modules only. If you remove a network module, install the same model network module in its place. For 1- or 2-slot network modules, you must install the same network module and interface card combination.

Caution Do not perform OIR on interface cards in 1- or 2-slot network modules. To avoid damage to the interface card and to the network module, turn off electrical power and disconnect network cables before inserting an interface card into a network module slot.

OIR procedures require some interaction with Cisco IOS software. For more information on Cisco IOS software-related tasks, see documents listed in the "Where to Go Next" section on page 2-27.

Tip Not all Cisco network modules and Cisco interface cards support OIR. Check the hardware documentation specific to your network module or interface card to confirm OIR support before starting OIR procedures.

To replace a network module with OIR support from a Cisco access router, perform the following steps:

Step 1 Initiate a console session with your Cisco access router.

Step 2 Enter interface configuration mode and shut down each interface on the network module you plan to remove. (See Example 2-1.)

Example 2-1 Shutting Down Interfaces on Cisco Network Modules

```
Router(config)# interface fastethernet 1/0
Router(config-if)# shutdown
```

Tip To see information for all interfaces available on the network module, use the **show interfaces** command.

Step 3 Repeat Step 2 for each interface on the network module.

Step 4 Unplug all cables from the network module.

Timesaver To make it easier to work with network cables, label the cables or prepare a network cabling diagram before removing network interface cables from the network module.

Step 5 Remove the network module as described in the "Removing or Replacing Single-Wide, Extended Single-Wide, and Extension Voice Network Modules from Cisco Access Routers" and "Removing or Replacing Double-Wide and Extended Double-Wide Network Modules in Cisco Access Routers" sections.

Step 6 Install a replacement network module. If you are not planning to install another network module at this time, install a blank faceplate over the network module slot. (See the "Installing Blank Faceplates on Cisco Access Routers" section on page 2-7.)

Step 7 Connect the cables removed from the previous network module.

Step 8 Confirm that the network module LEDs come on, and that the Active/Ready LEDs on the front panel of the router also come on. For further information on network module LEDs, see the chapter describing your specific network module.

Step 9 Initiate a console session with your Cisco access router.

Step 10 Enter interface configuration mode and activate each interface on the network module, as shown in Example 2-2.

Example 2-2 Activating Interfaces on Cisco Network Modules

```
Router(config)# interface fastethernet 1/0
Router(config-if)# no shutdown
```

Step 11 Repeat Step 10 for every interface on the network module.

Removing or Replacing Application and Service Network Modules

Application and service network modules use hard disks and require special software procedures prior to removal or replacement.

Caution Online removal of disks without proper shutdown can result in file system corruption and might render the disk unusable. The operating system on the applications or services network module must be shut down in an orderly fashion before the network module can be removed.

To perform online removal of a Cisco application and service network module and insertion of a replacement, follow these steps with the router in privileged EXEC mode:

Step 1 Initiate an application and service network module console session using the following command:

```
Router# service-module service-engine slot/port session

Trying 10.10.10.1, 2129 ... Open

SE-netmodule> enable
Password:
SE-netmodule#

SE-netmodule con now available

Press RETURN to get started!

SE-netmodule> enable
Password:
SE-netmodule#
```

Timesaver Cisco application and service network modules use a blank password. Press **Enter** at the password prompt.

Step 2 Save the running configuration for the network module by entering the following command from the **SE-netmodule** prompt:

```
SE-netmodule# copy running-config ftp:

Address or name or remote host? username/password/remote host
Destination filename? filename
```

Step 3 Exit the network module console session by pressing **Ctrl-Shift-6**, followed by **x**.

Step 4 On the router, clear the network module console session with the following command:

```
Router# service-module service-engine slot/port session clear
```

Step 5 Perform a graceful halt of the network module disk drive with the following command:

```
Router# service-module service-engine slot/port shutdown
```

Step 6 Remove the network module, using the procedure described in the "Removing or Replacing Single-Wide, Extended Single-Wide, and Extension Voice Network Modules from Cisco Access Routers" section on page 2-19.

Step 7 Install the replacement network module, using the procedure described in the "Installing Cisco Network Modules in Cisco Access Routers" section on page 2-5.

Step 8 Check that the network module LEDs come on and that the Active/Ready LEDs on the router front panel also come on. This inspection ensures that connections are secure and that the new unit is operational.

Step 9 Initiate a network module console session with the following command:

```
Router# service-module service-engine slot/port session

Trying 10.10.10.1, 2129 ... Open

SE-netmodule con now available

Press RETURN to get started!

SE-netmodule> enable
SE-netmodule#
```

Step 10 Restore the running configuration for the network module with the following command from the SE-netmodule prompt:

```
SE-netmodule# copy ftp: running-config

Address or name or remote host? username/password/remote host
Source filename? filename
```

Step 11 Exit the network module console session by pressing **Ctrl-Shift-6**, followed by **x**.

Step 12 On the router, clear the console session using the following command:

```
Router# service-module service-engine slot/port session clear
```

Installing Cisco Interface Cards in 1- or 2-Slot Network Modules

Some network modules have one or two interface card slots, which support a variety of voice and data interface cards. (See Table 1-2 on page 1-8 for more information.)

Note Do not install an ISDN BRI WAN interface card or an ISDN BRI network module in the same chassis as an ISDN PRI network module unless you are using Cisco IOS Release 11.3(3)T or later.

Note Do not install newer BRI WAN interface cards in the same network module as older BRI WAN interface cards. To identify newer BRI WAN interface cards, examine the B-channel LEDs. Newer BRI WAN interface cards have B-channel LEDs that are arranged horizontally. Older BRI WAN interface cards have B-channel LEDs that are arranged vertically.

To install an interface card in a 1- or 2-slot network module, perform the following steps:

Step 1 Turn off electrical power to the router. Leave the power cable plugged in to channel ESD voltages to ground.

The following warning applies to routers that use a DC power supply:

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 7

Warning **To avoid electric shock, do not insert a WAN or voice interface card into a 2-slot module while power is on or network cables are connected.** Statement 68

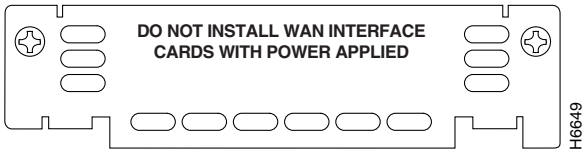
Caution Do not perform OIR on interface cards in 1- or 2-slot network modules. To avoid damage to the interface card and to the network module, turn off electrical power and disconnect network cables before inserting an interface card into a network module slot.

Step 2 Remove all network cables, including telephone cables, from the rear panel of the router.

Timesaver To make it easier to work with network cables, label the cables or prepare a network cabling diagram before removing network interface cables from the network module.

Step 3 Using a number 1 Phillips or flat-blade screwdriver, loosen the screws on the blank interface card faceplate. (See Figure 2-16.) Remove the blank faceplate.

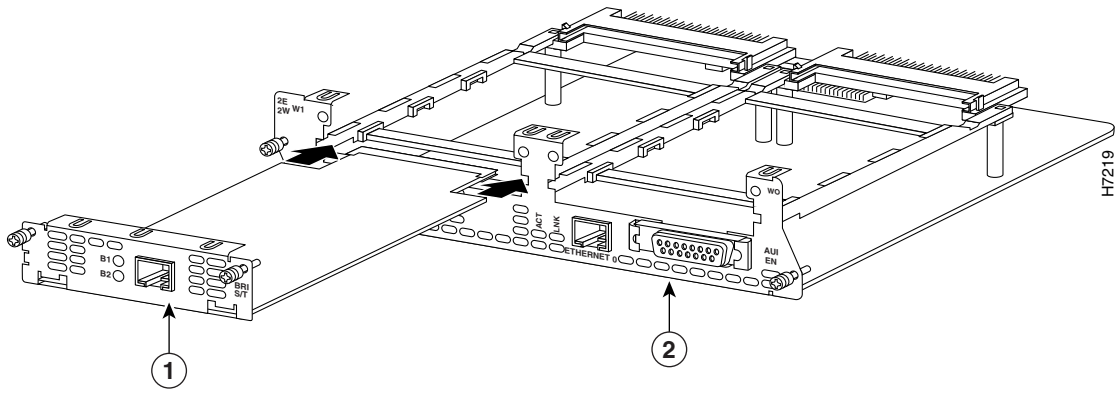
Figure 2-16 Blank Interface Card Faceplate



Tip Save blank interface card faceplates for future use.

Step 4 Align the interface card with the guides in the slot on the network module and slide it gently into place until the edge connector is seated into the connector on the module. (See Figure 2-17.)

Figure 2-17 Installing an Interface Card in a Network Module (Typical)



1	Interface card	**2**	2-slot network module

Step 5 Using a number 1 Phillips or flat-blade screwdriver, tighten the captive mounting screws into the holes on the network module faceplate.

Step 6 Reinstall the network interface cables and power up the router.

The following warning applies to routers that use a DC power supply:

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

Installing Other Accessories on Cisco Network Modules

Some Cisco network modules support a variety of additional modules, such as gigabit interface converters (GBICs) and small form-factor pluggable modules (SFPs).

Installing and Removing GBICs

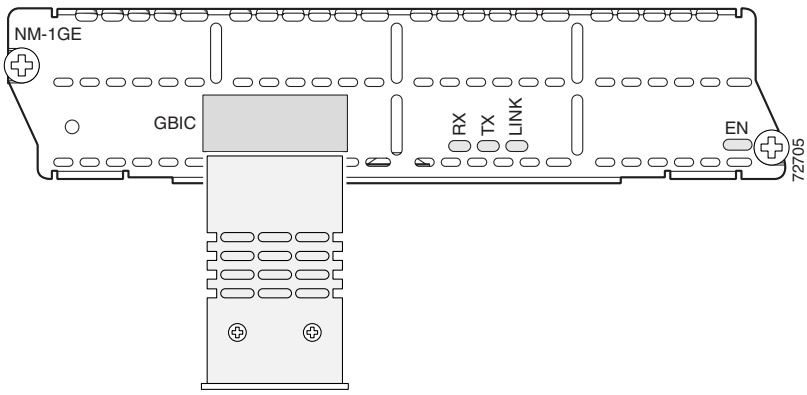
To install a GBIC, perform the following steps:

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

Step 1 (For optical GBICs) Confirm insertion of plugs into the SC connectors on the GBIC to prevent laser emissions.

Step 2 Hold down the clips on the side of the GBIC while inserting the GBIC into the GBIC slot in the network module faceplate. (See Figure 2-18.)

Figure 2-18 Installing a GBIC into a Network Module



Step 3 Release the side clips on the GBIC to lock the GBIC in place.

Step 4 Confirm that the GBIC is seated.

Caution Do not remove the optical port plugs used on the GBIC until you are ready to connect cabling to the network module.

Step 5 (For optical GBICs) Remove the plugs from the SC connectors on the GBIC.

Timesaver If installing the GBIC in a loose network module, install the network module (see the "Installing Cisco Network Modules in Cisco Access Routers" section on page 2-5) before connecting the network module to the network.

To remove a GBIC, perform the following steps:

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

Step 1 Disconnect the GBIC from the network.

Step 2 (For optical GBICs) Insert plugs into the SC connectors on the GBIC to prevent laser emissions.

Step 3 Hold down the clips on the side of the GBIC and remove the GBIC from the network module.

Step 4 Replace the GBIC with a similar model, or continue with network module removal.

Tip Gigabit Ethernet network modules can be removed with the GBIC installed.

Where to Go Next

For an introduction to Cisco network modules, go to Chapter 1, "Overview of Cisco Network Modules for Cisco Access Routers."

For regulatory compliance and safety information, see the *Cisco Network Modules and Interface Cards Regulatory Compliance and Safety Information* document.

CHAPTER 3

Connecting Ethernet, Fast Ethernet, and Token Ring Network Modules

This chapter describes how to connect Ethernet, Fast Ethernet, and Token Ring network modules for Cisco access routers. It contains the following sections:

Tip To determine whether your router supports a specific network module, see Table 1-6 on page 1-16.

Ethernet Network Modules

Ethernet connections are provided on 1- and 4-port Ethernet modules, and on 1-port Ethernet, 2-port Ethernet, and 1-port Ethernet 1-port Token Ring 2-WAN card slot modules.

1- and 4-Port Ethernet Modules

The following network modules provide Ethernet interfaces:

- 1-port Ethernet network module (NM-1E) (see Figure 3-1)
- 4-port Ethernet network module (NM-4E) (see Figure 3-2)

Figure 3-1 1-Port Ethernet Network Module

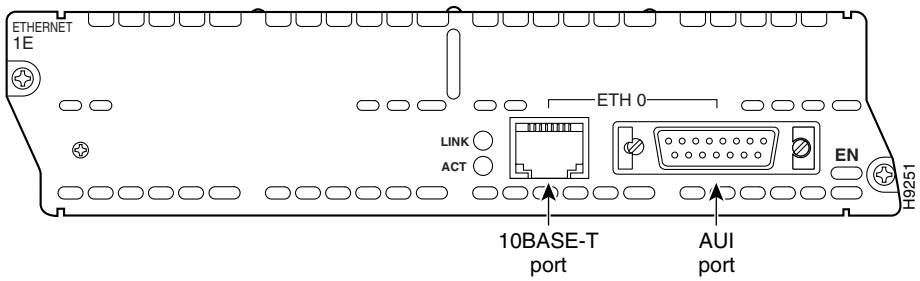
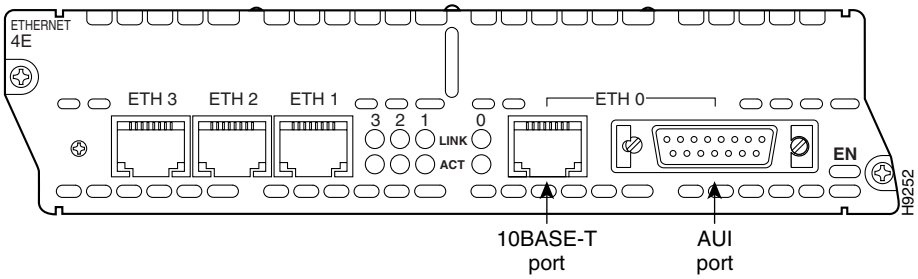


Figure 3-2 4-Port Ethernet Network Module



Ethernet 2-WAN Card Slot Modules

The following 2-slot network modules provide one or two Ethernet interfaces, plus two slots for optional WAN interface cards:

- 1-Ethernet 2-WAN card slot network module (NM-1E2W) (see Figure 3-3)
- 2-Ethernet 2-WAN card slot network module (NM-2E2W) (see Figure 3-4)
- 1-Ethernet 1-Token Ring 2-WAN card slot network module (NM-1E1R2W) (see Figure 3-5)

Figure 3-3 1-Ethernet 2-WAN Card Slot Network Module

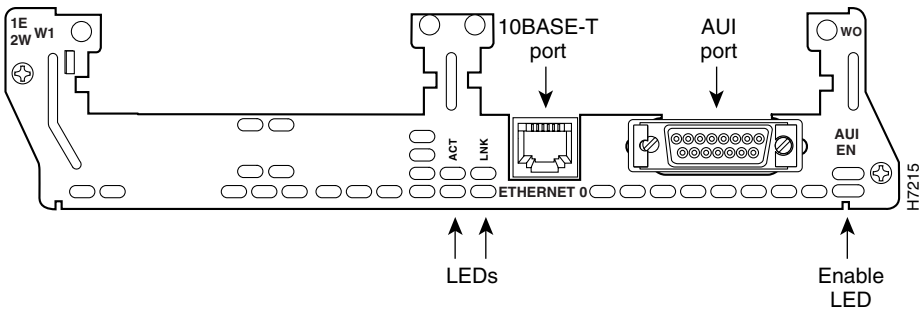


Figure 3-4 2-Ethernet 2-WAN Card Slot Network Module

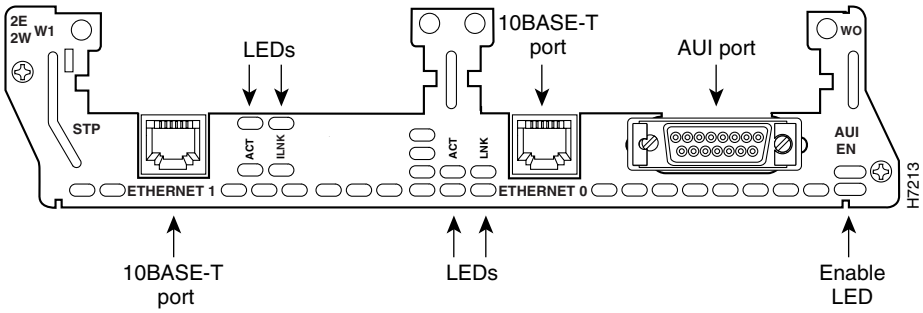
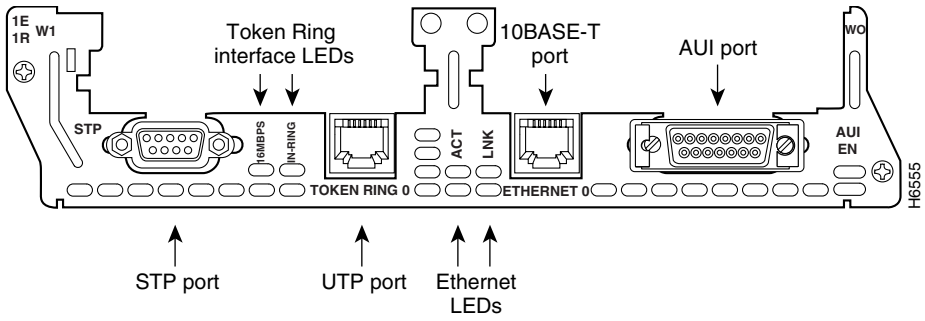


Figure 3-5 1-Ethernet 1-Token Ring 2-WAN Card Slot Network Module



Ethernet Connectors

The 1-port Ethernet network module, the 1-Ethernet 2-slot network module, and the 1-Ethernet 1-Token Ring 2-slot network module each provide a single Ethernet port. This port uses either the attachment unit interface (AUI) DB-15 connector on the right side of the module or the 10BASE-T (RJ-45) connector next to it. Only one of these connectors can be active at a time. The active port is identified in software by port type (Ethernet), slot number on the module, and port number 0.

All modules detect the type of network connection automatically, and you do not need to choose the media type in software. If cables are plugged into both ports, the 10BASE-T connection is chosen.

The 4-port Ethernet network module has ports for four Ethernet connections (0, 1, 2, and 3). Port 0 offers a choice of an AUI or 10BASE-T interface. Ethernet ports 1, 2, and 3 use 10BASE-T connectors only. These ports do not provide an AUI connector.

The 2-Ethernet 2-slot network module has ports for two Ethernet connections. Port 0 offers a choice of AUI or 10BASE-T. Port 1 uses 10BASE-T only.

Connecting Ethernet Ports

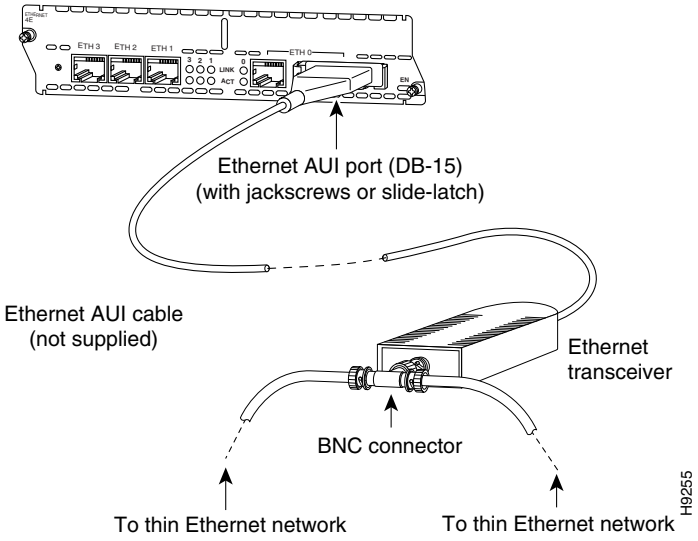
If an Ethernet port offers both an AUI connector and a 10BASE-T connector, you can use either connector, but not both at the same time.

AUI Connections

Use an Ethernet AUI cable to connect an AUI port to an Ethernet transceiver. These ports are color-coded yellow. The female end of the AUI cable mates with the slide-latch connector of the transceiver cable. Figure 3-6 shows a thin Ethernet transceiver as an example, but you can use any type of Ethernet transceiver.

If the transceiver cable has thumbscrew connectors, you can connect it directly to the AUI port by replacing the AUI port slide latch with a jackscrew (provided in a separate bag).

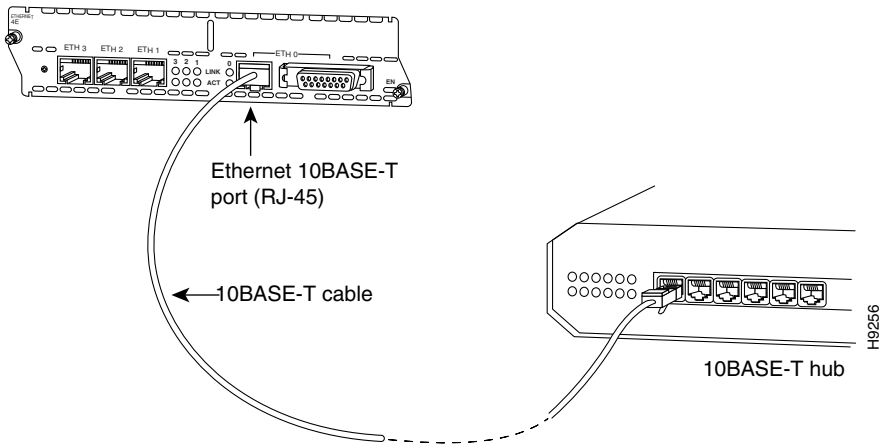
Figure 3-6 Connecting an Ethernet AUI Port to a Transceiver



10BASE-T Connections

Use an Ethernet 10BASE-T cable to connect a 10BASE-T port to a hub or other network device. These ports are color-coded yellow. Figure 3-7 shows the 10BASE-T port on an Ethernet network module connected to a hub.

Figure 3-7 Connecting an Ethernet 10BASE-T Port to a Hub



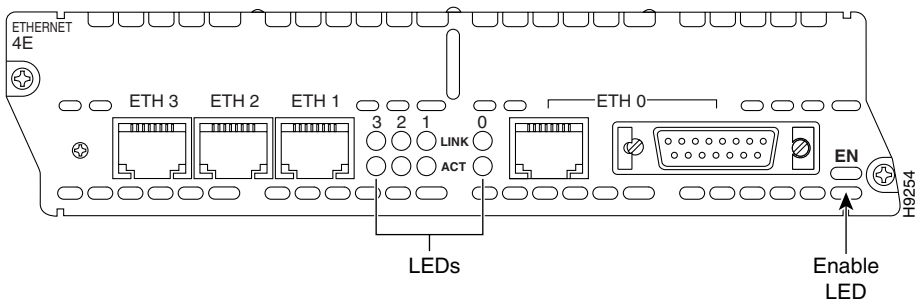
Ethernet LEDs

This section describes Ethernet module LEDs. Figure 3-8 shows 4-port Ethernet network module LEDs as an example.

All network modules have an enable (EN) LED. This LED indicates that the module has passed its self-tests and is available to the router.

Each Ethernet port has two LEDs. The activity (ACT) LED indicates that the router is sending or receiving Ethernet transmissions. The link (LINK) LED indicates that the Ethernet port is receiving the link integrity signal from the hub (10BASE-T only).

Figure 3-8 Ethernet Network Module LEDs (Typical)



Fast Ethernet Network Modules

Fast Ethernet connections are provided on 1-port Fast Ethernet modules, and on 1-port Fast Ethernet, 2-port Fast Ethernet, and 1-port Fast Ethernet 1-port Token Ring 2-WAN card slot modules.

Note The Fast Ethernet-PRI modules described in Chapter 4, "Connecting Fast Ethernet-PRI Network Modules," also provide a Fast Ethernet interface. See that chapter for further information.

1-Port Fast Ethernet Modules

The following network modules provide Fast Ethernet interfaces:

- 1-port Fast Ethernet network module with TX connector, Cisco product number NM-1FE-TX. (See Figure 3-9.) This module provides an RJ-45 connector for direct connection to 100BASE-T Ethernet networks.
- 1-port Fast Ethernet network module with FX connector, Cisco product number NM-1FE-FX. (See Figure 3-10.) This module provides a duplex SC-type fiber-optic port for direct connection to 100BASE-FX Ethernet networks.

Figure 3-9 1-Port Fast Ethernet Network Module (TX Connector)

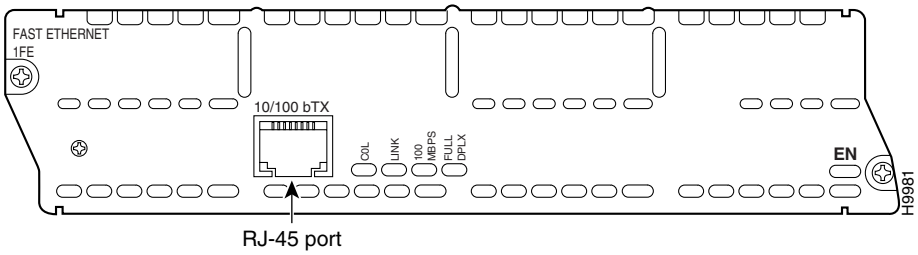
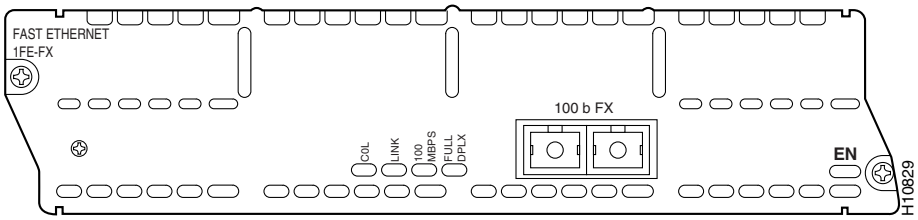


Figure 3-10 1-Port Fast Ethernet Network Module (FX Connector)



Fast Ethernet 2-WAN Card Slot Modules

The following 2-slot network modules provide one or two 100BASE-T Fast Ethernet interfaces, plus two slots for optional WAN interface cards:

- 1-Fast Ethernet 2-WAN card slot network module (NM-1FE2W and NM-1FE2W-V2). See Figure 3-11 for a sample faceplate.
- 2-Fast Ethernet 2-WAN card slot network module (NM-2FE2W and NM-2FE2W-V2). See Figure 3-12 for a sample faceplate.
- 1-Fast Ethernet 1-Token Ring 2-WAN card slot network module (NM-1FE1R2W and NM-1FE1R2W-V2). See Figure 3-13 for a sample faceplate.

Caution To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the 1-Fast Ethernet 2-WAN card slot network modules (NM-1FE2W-V2), the 2-Fast Ethernet 2-WAN card slot network modules (NM-2FE2W-V2), and the 1-Fast Ethernet 1-Token Ring 2-WAN card slot network modules (NM-1FE1R2W-V2) only to intrabuilding or nonexposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

Figure 3-11 1-Fast Ethernet 2-WAN Card Slot Network Module

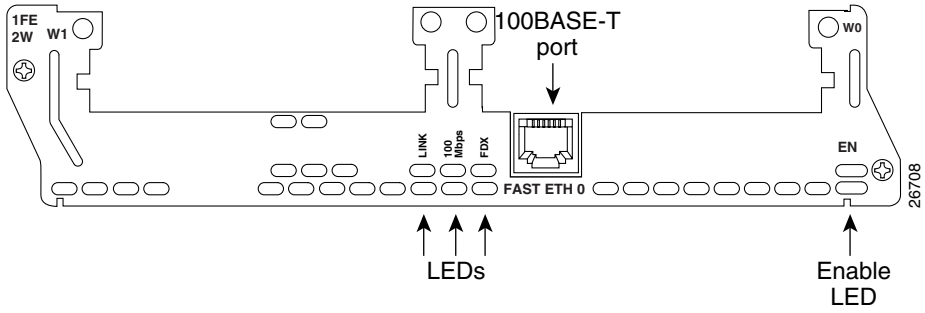


Figure 3-12 2-Fast Ethernet 2-WAN Card Slot Network Module

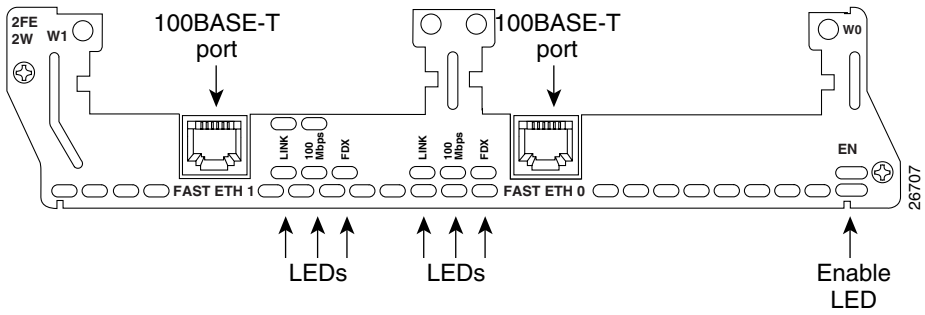
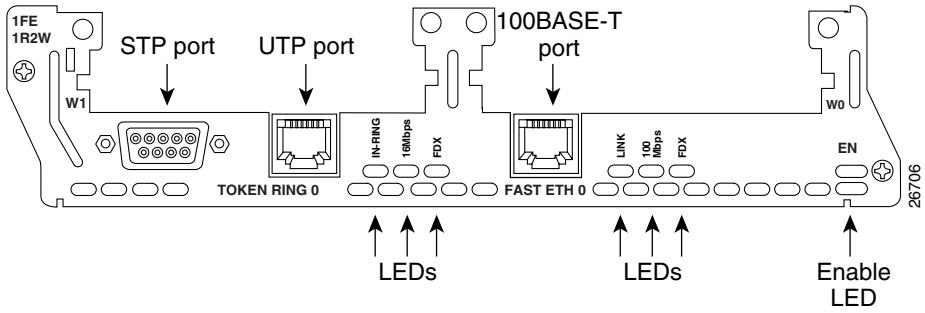


Figure 3-13 1-Fast Ethernet 1-Token Ring 2-WAN Card Slot Network Module



Connecting Fast Ethernet Ports

Use the following sections for 100BASE-T or 100BASE-FX connections.

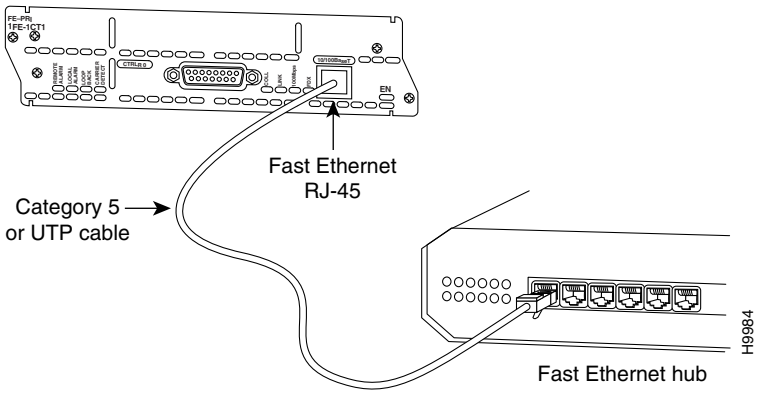
100BASE-T Connections

Use a two-pair Category 5 or unshielded twisted-pair (UTP) straight-through RJ-45 cable to connect a Fast Ethernet RJ-45 port to a switch, hub, repeater, server, or other network device. Figure 3-14 shows an RJ-45 port connected to a hub.

Note RJ-45 cables are not available from Cisco Systems. These cables are widely available and must be Category 5 cables.

Caution To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the 1-Fast Ethernet 2-WAN card slot network modules (NM-1FE2W-V2), the 2-Fast Ethernet 2-WAN card slot network modules (NM-2FE2W-V2), and the 1-Fast Ethernet 1-Token Ring 2-WAN card slot network modules (NM-1FE1R2W-V2) only to intrabuilding or nonexposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

Figure 3-14 Connecting a Fast Ethernet RJ-45 Port to a Hub



100BASE-FX Connections

Attach a multimode fiber-optic cable with SC-type connectors directly to the port on the Fast Ethernet network module (remove the protective plug from the port if it is present). Use either one duplex SC connector (see Figure 3-15 and Figure 3-17) or two simplex SC connectors (see Figure 3-16 and Figure 3-18). Attach the other end of the cable to a repeater, hub, or wall outlet. Be sure to observe the correct relationship between the receive (RX) and transmit (TX) ports on the network module and the cable.

Note Multimode SC-type fiber-optic cables are widely available commercially. Cisco Systems does not supply these cables.

Caution To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the 1-Fast Ethernet 2-WAN card slot network modules (NM-1FE2W-V2), the 2-Fast Ethernet 2-WAN card slot network modules (NM-2FE2W-V2), and the 1-Fast Ethernet 1-Token Ring 2-WAN card slot network modules (NM-1FE1R2W-V2) only to intra-building or non-exposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

Figure 3-15 Duplex SC Connector

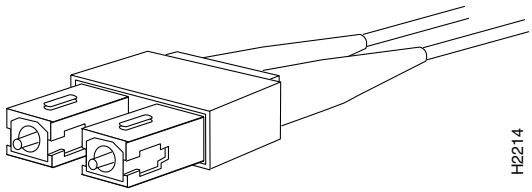


Figure 3-16 Simplex SC Connector

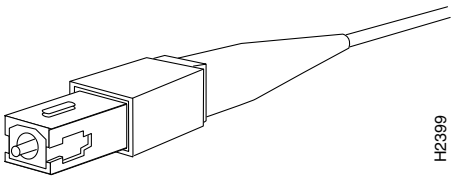


Figure 3-17 Connecting a Fast Ethernet FX Port to a Repeater or Hub (Duplex Connector)

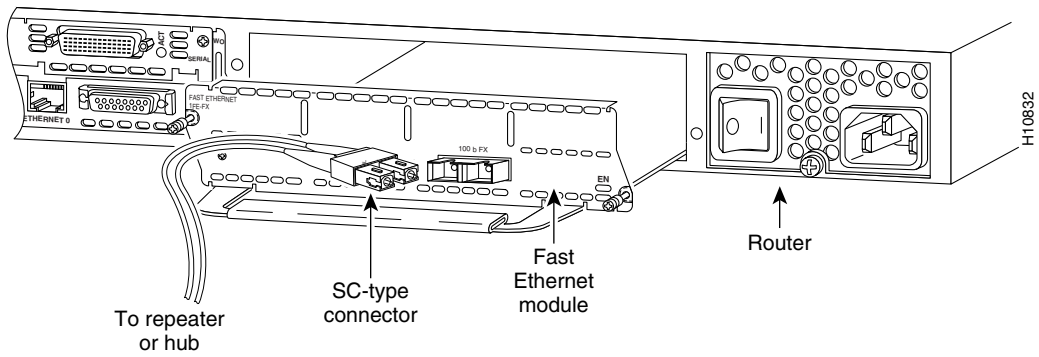
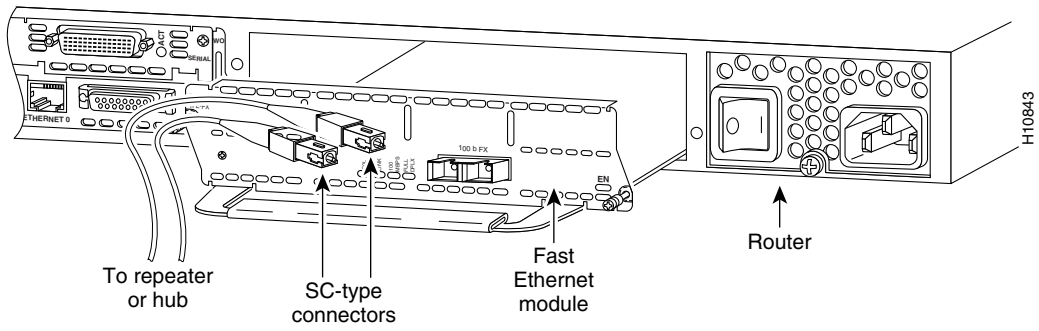


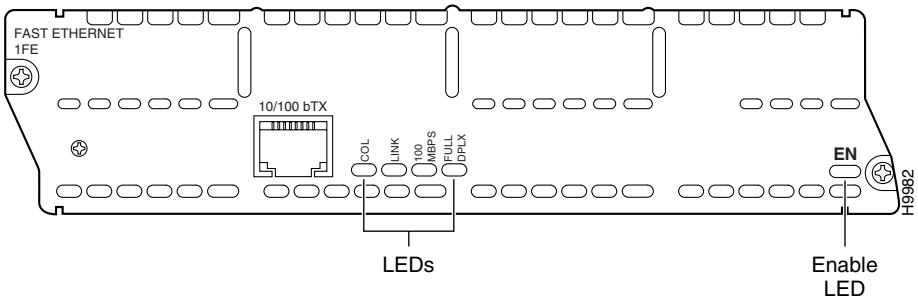
Figure 3-18 Connecting a Fast Ethernet FX Port to a Repeater or Hub (Simplex Connectors)



Fast Ethernet LEDs

This section describes Fast Ethernet module LEDs. Figure 3-19 shows 1-port Fast Ethernet network module LEDs as an example.

Figure 3-19 1-Port Fast Ethernet Network Module LEDs



All network modules have an enable (EN) LED. The enable LED indicates that the module has passed its self-tests and is available to the router.

Fast Ethernet network modules have the additional LEDs shown in Table 3-1.

Table 3-1 Fast Ethernet Network Module LEDs

LED	Meaning
COL	Collision activity is occurring on the network.
LINK	A link has been established with the station at the other end of the cable.
100MBPS	Speed of the interface is 100 Mbps.
FULL DPLX	Interface is in full-duplex mode.

Token Ring Network Modules

The following network modules provide Token Ring interfaces:

- 1-port Ethernet 1-port Token Ring 2-WAN card slot module (NM-1E1R2W) (see Figure 3-20)
- 1-port Fast Ethernet 1-port Token Ring 2-WAN card slot module (NM-1FE2R2W) (see Figure 3-21)

Figure 3-20 1-Ethernet 1-Token Ring 2-WAN Card Slot Network Module

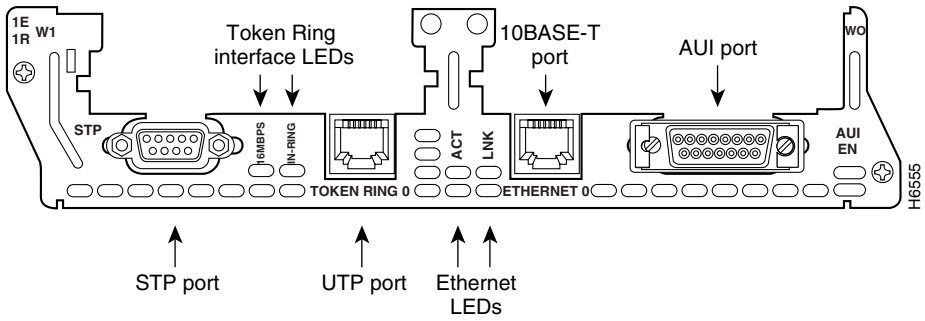
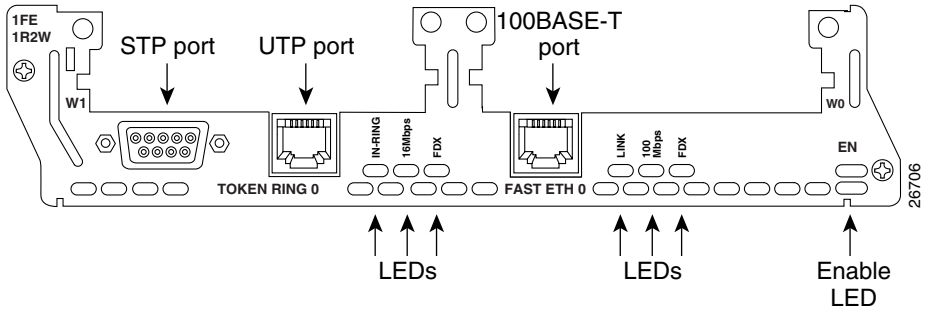


Figure 3-21 1-Fast Ethernet 1-Token Ring 2-WAN Card Slot Network Module



Connecting Token Ring Ports

The 1-Ethernet 1-Token Ring 2-WAN card slot network module and the 1-Fast Ethernet 1-Token Ring 2-WAN card slot network module each have one DB-9 connector for an STP Token Ring connection and one RJ-45 connector for a UTP Token Ring connection. Only one connector can be active at a time.

To connect the module to a Token Ring network, attach one end of a shielded Token Ring lobe cable to the DB-9 connector on the network module (see Figure 3-22), or attach one end of an unshielded Token Ring lobe cable to the UTP connector on the network module (see Figure 3-23). Attach the other end of the cable to the Token Ring media attachment unit (MAU). The network module automatically detects which connector is in use.

Figure 3-22 Connecting a Token Ring STP Port (DB-9) to a MAU

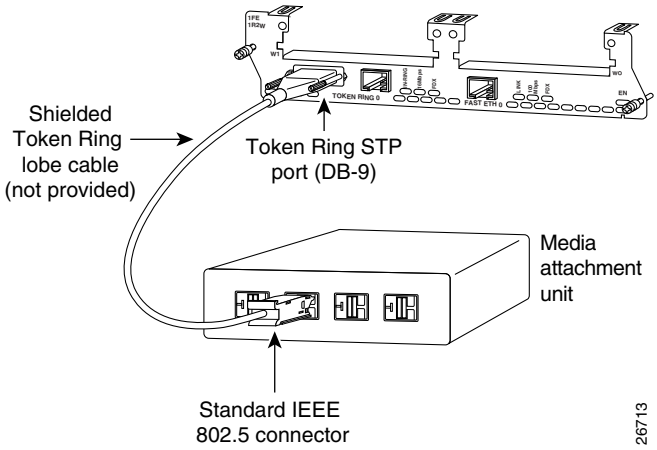
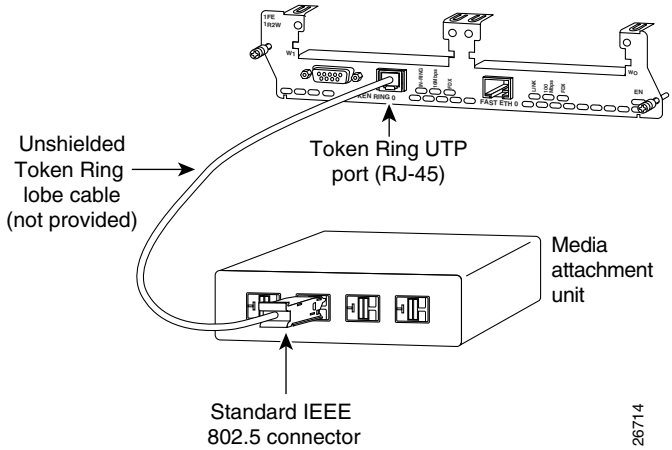


Figure 3-23 Connecting a Token Ring UTP Port (RJ-45) to an MAU



Token Ring LEDs

All network modules have an enable (EN) LED. The enable LED indicates that the module has passed its self-tests and is available to the router.

The 1-Ethernet 1-Token Ring 2-WAN card slot network module and the 1-Fast Ethernet 1-Token Ring 2-WAN card slot network module both have the following Token Ring LEDs:

- The 16MBPS LED indicates a ring speed of 16 Mbps. If it is off, the ring speed is 4 Mbps.
- The IN-RING LED indicates that the Token Ring interface is inserted into the ring. If it is off, the interface is not inserted into the ring.

The 1-Fast Ethernet 1-Token Ring 2-slot network module also has the FDX LED, which indicates full-duplex mode.

Timesaver When the IN-RING LED is off, you can unplug the Token Ring cable without causing a problem on the ring.

CHAPTER 4

Connecting Fast Ethernet-PRI Network Modules

This chapter describes how to connect Fast Ethernet-Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) network modules and contains the following sections:

Note Unless specifically identified, references to Fast Ethernet-PRI network modules in this chapter include all these network modules.

Tip To determine whether your router supports a specific network module, see Table 1-6 on page 1-16.

1-Port Fast Ethernet and 1- or 2-Port Channelized T1/ISDN PRI Network Modules

This section provides information about the following network modules:

- 1-port Fast Ethernet 1-port channelized T1/ISDN PRI network module (NM-1FE1CT1) (see Figure 4-1)
- 1-port Fast Ethernet 2-port channelized T1/ISDN PRI network module (NM-1FE2CT1) (see Figure 4-2)

Figure 4-1 1-Port Fast Ethernet 1-Port Channelized T1 Network Module

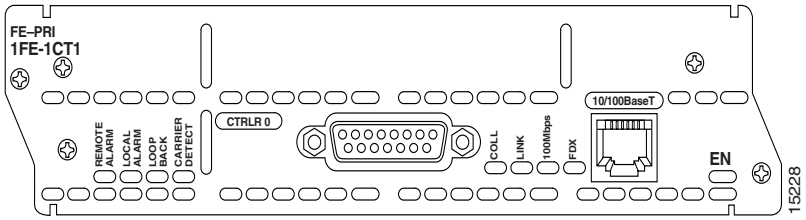
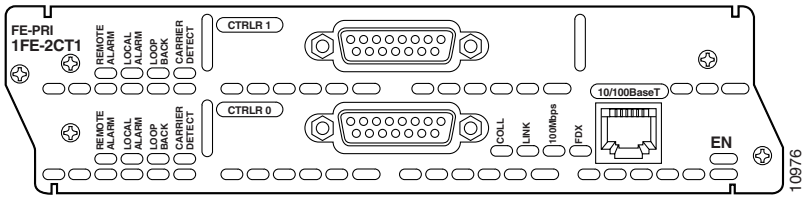


Figure 4-2 1-Port Fast Ethernet 2-Port Channelized T1 Network Module



Connecting Fast Ethernet Channelized T1 Modules

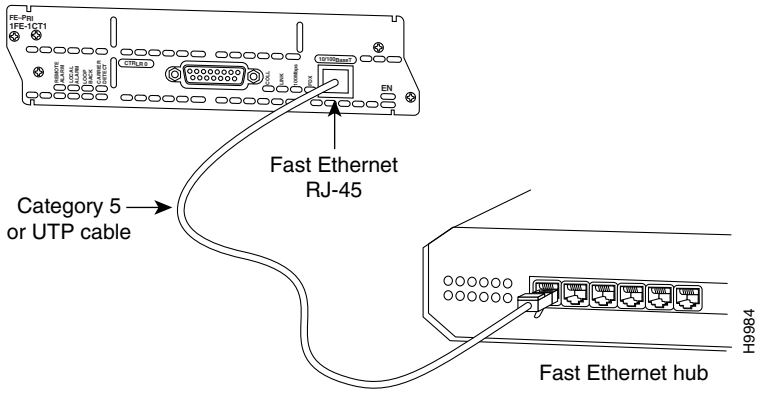
Use the following sections for Fast Ethernet and PRI connections.

Fast Ethernet Port

Use a straight-through two-pair Category 5 unshielded twisted-pair (UTP) cable to connect the RJ-45 port on the Fast Ethernet-PRI network module to a switch, hub, repeater, server, or other network device. These ports are color-coded yellow. Figure 4-3 shows the RJ-45 port connected to a hub.

Note RJ-45 cables are not available from Cisco Systems. These cables are widely available and must be Category 5 cables.

Figure 4-3 Connecting a Fast Ethernet RJ-45 Port to a Hub

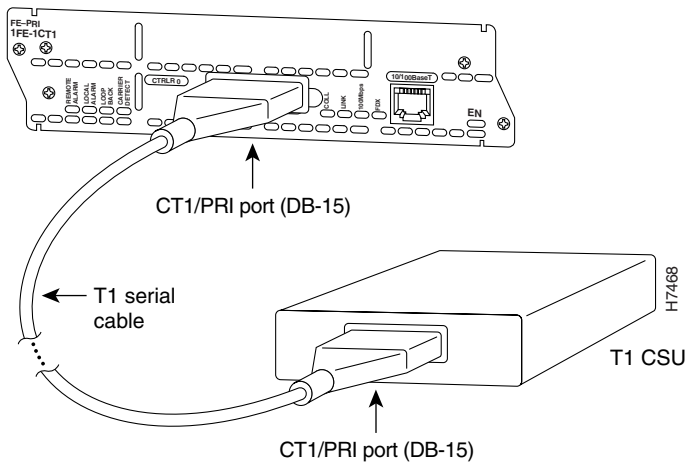


PRI Ports

This section describes how to connect channelized T1 and channelized E1 ISDN PRI ports to the network. These ports are color-coded tan.

Use a DB-15-to-DB-15 T1 serial cable to connect a CT1/PRI port to a T1 channel service unit (CSU). (See Figure 4-4.)

Figure 4-4 Connecting a CT1/PRI Port to a T1 CSU



1-Port Fast Ethernet and 1- or 2-Port Channelized T1/ISDN PRI with CSU Network Modules

This section provides information about the following network modules:

- 1-port Fast Ethernet 1-port channelized T1/ISDN PRI with CSU network module (NM-1FE1CT1-CSU) (see Figure 4-5)

- 1-port Fast Ethernet 2-port channelized T1/ISDN PRI with CSU network module (NM-1FE2CT1-CSU) (see Figure 4-6)

Figure 4-5 1-Port Fast Ethernet 1-Port Channelized T1 with CSU Network Module

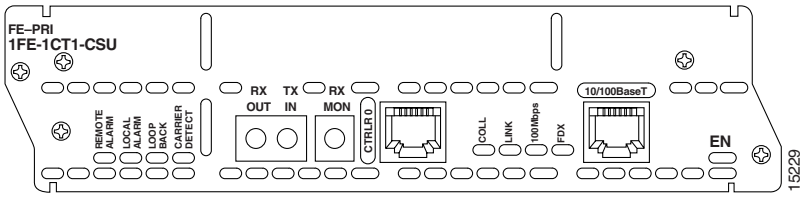
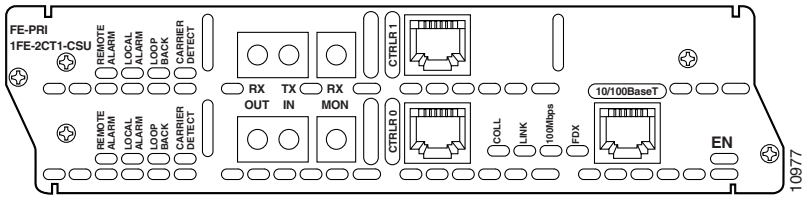


Figure 4-6 1-Port Fast Ethernet 2-Port Channelized T1 with CSU Network Module



Connecting Fast Ethernet Channelized T1 with CSU Modules

Use the following sections for connections to the Fast Ethernet or CT1/PRI-CSU ports.

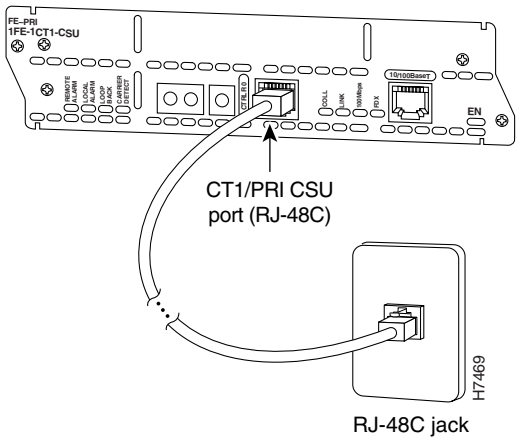
Fast Ethernet Port

To connect the Fast Ethernet port, see the "Fast Ethernet Port" section on page 4-2.

CT1/PRI-CSU Port

To connect the CT1/PRI-CSU PRI ports, use a straight-through RJ-48C-to-RJ-48C cable to connect a PRI port to an RJ-48C jack. (See Figure 4-7.) These ports are color-coded tan.

Figure 4-7 Connecting a CT1/PRI-CSU Port to an RJ-48C Jack



1-Port Fast Ethernet and 1- or 2-Port Channelized E1/ISDN PRI Balanced or Unbalanced Network Modules

This section provides information about the following network modules:

- 1-port Fast Ethernet 1-port channelized E1/ISDN PRI balanced (120-ohm) network module (NM-1FE1CE1B) (see Figure 4-8)
- 1-port Fast Ethernet 1-port channelized E1/ISDN PRI unbalanced (75-ohm) network module (NM-1FE1CE1U) (see Figure 4-8)
- 1-port Fast Ethernet 2-port channelized E1/ISDN PRI balanced (120-ohm) network module (NM-1FE2CE1B) (see Figure 4-9)
- 1-port Fast Ethernet 2-port channelized E1/ISDN PRI unbalanced (75-ohm) network module (NM-1FE2CE1U) (see Figure 4-9)

Figure 4-8 1-Port Fast Ethernet 1-Port Channelized E1 Network Module

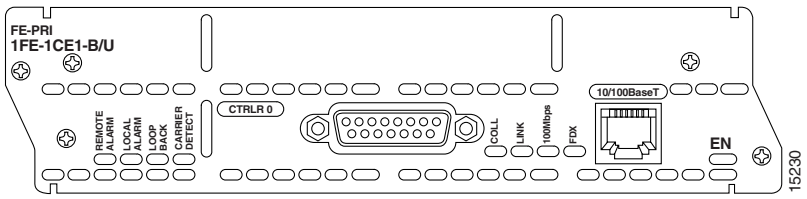
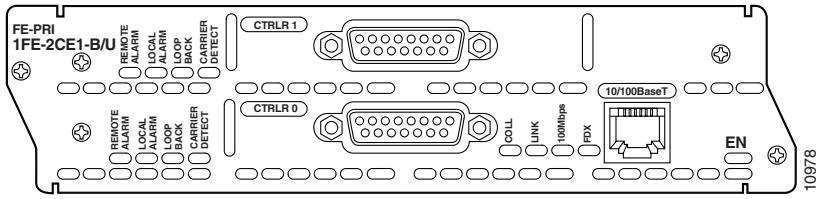


Figure 4-9 1-Port Fast Ethernet 2-Port Channelized E1 Network Module



Connecting Fast Ethernet Channelized E1 Modules

Use the following sections to connect to the Fast Ethernet or CE1-PRI-B ports.

Fast Ethernet Port

To connect the Fast Ethernet port, see the "Fast Ethernet Port" section on page 4-2.

CE1/PRI-B Port

Use the appropriate cable to connect a CE1/PRI-B (120-ohm) port to an E1 CSU. (See Figure 4-10, Figure 4-11, and Figure 4-12, showing DB-15, twinax, and RJ-45 CSUs respectively.) These ports are color-coded tan.

Figure 4-10 Connecting a CE1/PRI-B Port to an E1 CSU (DB-15-to-DB-15 Connectors)

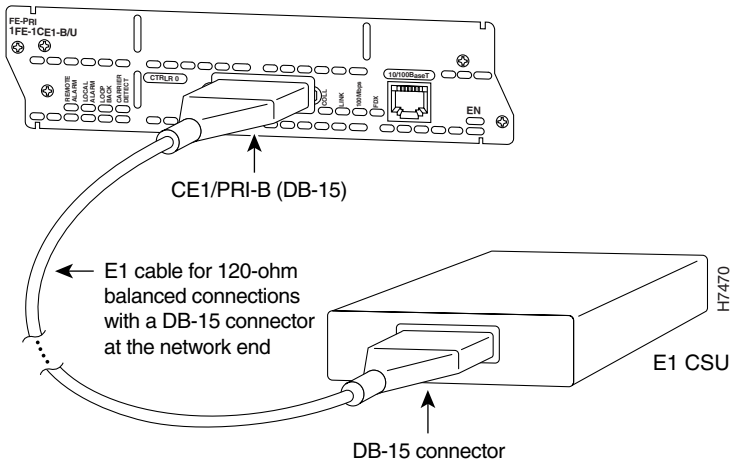


Figure 4-11 Connecting a CE1/PRI-B Port to an E1 CSU (DB-15-to-Twinax Connectors)

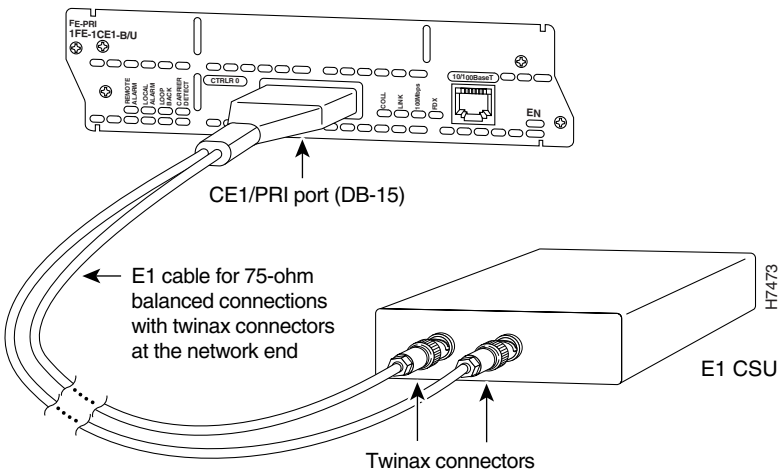
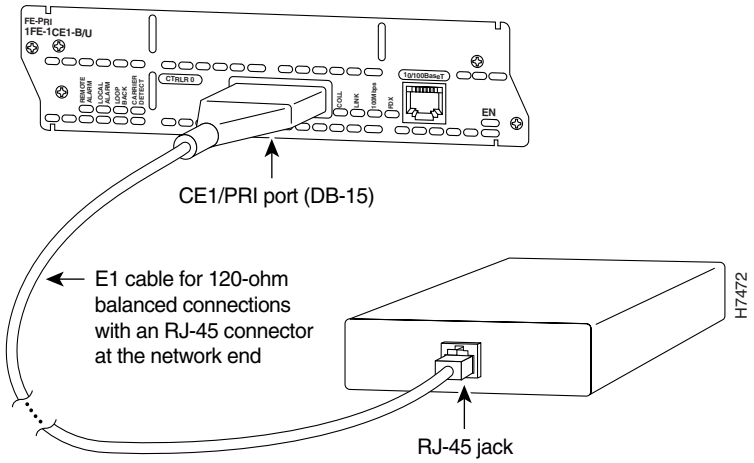


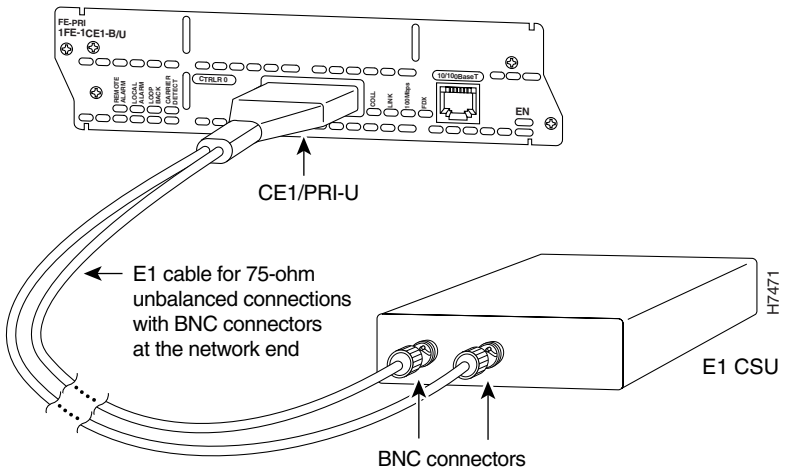
Figure 4-12 Connecting a CE1/PRI-B Port to an E1 CSU (DB-15-to-RJ-45 Connectors)



CE1/PRI-U Port

Use the appropriate cable to connect a CE1/PRI-U (75-ohm) port to an E1 CSU. Figure 4-13 shows a CSU with BNC connectors. These ports are color-coded tan.

Figure 4-13 Connecting a CE1/PRI-U Module to an E1 CSU (DB-15-to-BNC Connectors)

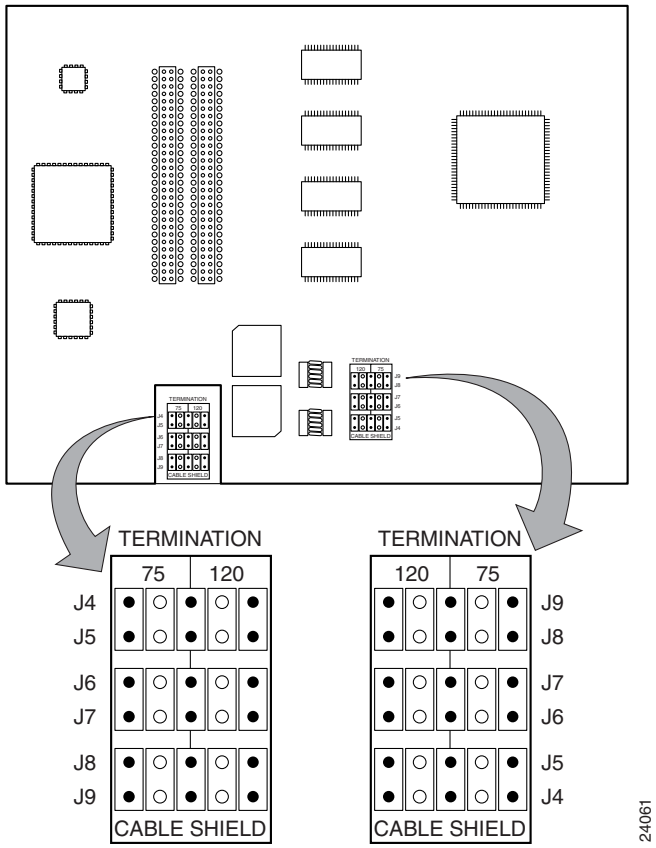


Setting Interfaces to Balanced or Unbalanced Termination

This section describes how to configure an E1 network module for balanced or unbalanced termination. The module consists of two circuit boards, or cards. A terminal block and a set of five jumpers are provided on each card to configure termination. Figure 4-14 shows these terminal blocks.

Caution To avoid damaging electrostatic discharge (ESD)-sensitive components, observe all ESD precautions when handling the circuit boards.

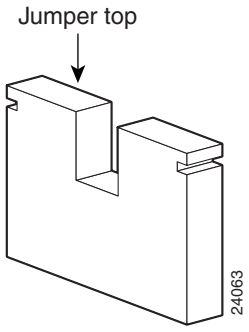
Figure 4-14 Terminal Block Locations



Note The position of the jumpers is different on the two terminal blocks. See Figure 4-14 and the silk screening on the network module to ensure the correct jumper position.

Figure 4-15 shows a typical jumper.

Figure 4-15 Jumper



Configuring Unbalanced Mode

To configure the network module for unbalanced mode, follow these steps:

Step 1 Turn off electrical power to the router. However, to channel ESD voltages to ground, do not unplug the power cable. Remove all network interface cables, including telephone cables, from the rear panel.

The following warning applies to routers that use a DC power supply:

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 7

Step 2 Loosen the module captive mounting screws, using a Phillips or flat-blade screwdriver.

Step 3 Hold the captive screws between two fingers, and pull the network module toward you until it slides free of the chassis.

Step 4 Set the network module on an ESD-preventive mat.

Step 5 Using needlenose pliers, set jumpers J5 through J9 on the top terminal block to the 75-ohm position. Set jumpers J4 through J8 on the bottom terminal block to the same 75-ohm position. (See Figure 4-16.)

Figure 4-16 Jumper Insertion

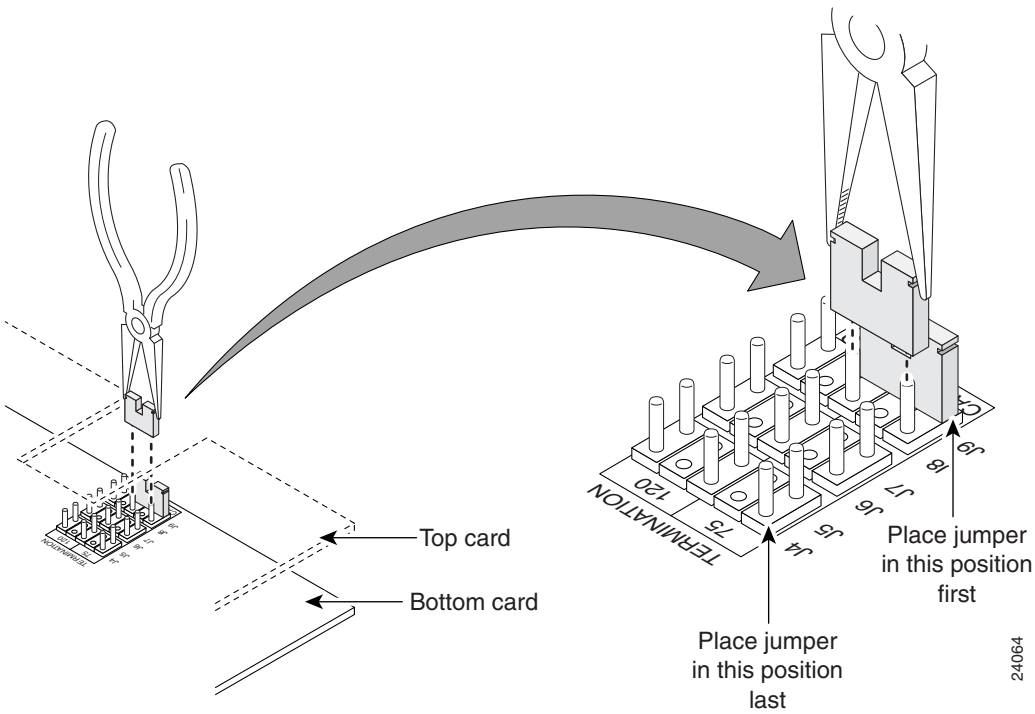
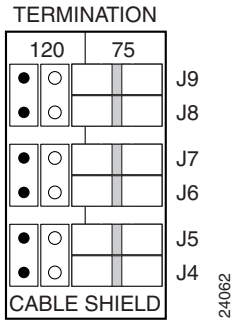


Figure 4-17 shows the top terminal block set to unbalanced (75-ohm) position.

Figure 4-17 Jumpers in Unbalanced 75-Ohm Position (Top Card)



Step 6 Align the network module with the guides in the chassis and slide it gently into the slot.

Step 7 Push the module into place until you feel its edge connector mate securely with the connector on the motherboard.

Step 8 Fasten the module captive mounting screws into the holes in the chassis, using the Phillips or flat-blade screwdriver.

Step 9 If the router was previously running, reinstall the network interface cables and turn on power to the router.

The following warning applies to routers that use a DC power supply:

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

Configuring Balanced Mode

To configure the network module for balanced mode, follow these steps:

Step 1 Turn off electrical power to the router. However, to channel ESD voltages to ground, do not unplug the power cable. Remove all network interface cables, including telephone cables, from the rear panel.

The following warning applies to routers that use a DC power supply:

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 7

Step 2 Loosen the module captive mounting screws, using a Phillips or flat-blade screwdriver.

Step 3 Hold the captive screws between two fingers, and pull the network module toward you until it slides free of the chassis.

Step 4 Set the network module on an ESD-preventive mat.

Step 5 Using needlenose pliers, set jumpers J5 through J9 on the top terminal block to the 120-ohm position. Set jumpers J4 through J8 on the bottom terminal block to the same 120-ohm position. (See Figure 4-16.)

Step 6 Align the network module with the guides in the chassis and slide it gently into the slot.

Step 7 Push the module into place until you feel its edge connector mate securely with the connector on the motherboard.

Step 8 Fasten the module captive mounting screws into the holes in the chassis, using the Phillips or flat-blade screwdriver.

Step 9 If the router was previously running, reinstall the network interface cables and turn on power to the router.

The following warning applies to routers that use a DC power supply:

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

Fast Ethernet-PRI Module LEDs

All network modules have an enable (EN) LED. This LED indicates that the module has passed its self-tests and is available to the router.

All Fast Ethernet-PRI modules have four LEDS for the Fast Ethernet port, and four additional LEDs for each PRI port. Figure 4-18 shows LEDs for the 1-port Fast Ethernet 2-port channelized E1/ISDN PRI balanced (120-ohm) network module as an example.

Figure 4-18 Fast Ethernet and ISDN PRI LEDs

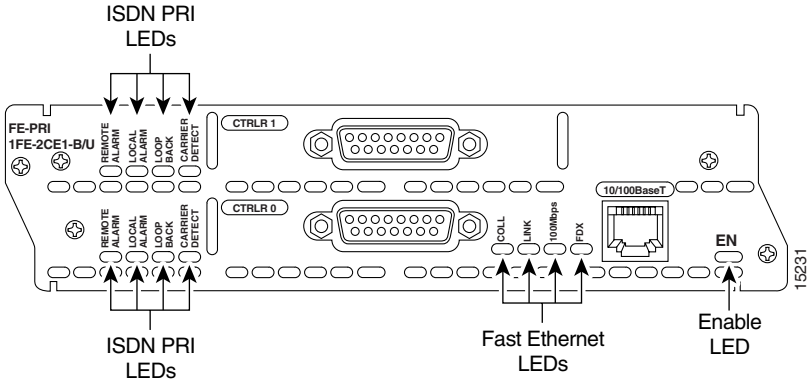


Table 4-1 describes Fast Ethernet LEDs. Table 4-2 describes ISDN PRI LEDs.

Table 4-1 Fast Ethernet LEDs

LED	Color	Meaning
COLL	Yellow	Collision activity is occurring on the network.
LINK	Green	A link has been established with the station at the other end of the cable.

Table 4-1 Fast Ethernet LEDs (continued)

LED	Color	Meaning
100MBPS	Green	Speed of the interface is 100 Mbps.
FDX	Green	Interface is in full-duplex mode.

Table 4-2 ISDN PRI LEDs

LED	Color	Meaning
REMOTE ALARM	Yellow	A remote source is indicating an error at its end of the connection.
LOCAL ALARM	Yellow	Incoming signal shows loss of signal, loss of frame, or excessive errors.
LOOPBACK	Yellow	Line or local loopback state is set or detected.
CARRIER DETECT	Green	DS-1 carrier to the network is detected.

CHAPTER 5

Connecting Serial Network Modules

This chapter describes how to connect serial network modules for Cisco modular routers and contains the following sections:

Tip To determine whether your router supports a specific network module, see Table 1-6 on page 1-16.

About Serial Connections

Serial connections can be provided by either WAN interface cards or network modules. For more information about WAN interface cards, see the *Cisco Interface Cards Hardware Installation Guide*. To obtain this publication, see the "Obtaining Documentation" section on page viii.

Before you connect a device to a serial port, you need to know the following:

- Type of device—data terminal equipment (DTE) or data communications equipment (DCE)—you are connecting to
- Type of connector, male or female, needed to connect to the device
- Signaling standard required by the device

About DTE and DCE Devices

A device that communicates over a synchronous serial interface is either a DTE or a DCE device. A DCE device provides a clock signal between the device and the router. A DTE device does not provide a clock signal. DTE devices usually connect to DCE devices. The documentation that accompanied the device should tell you whether it is DTE or DCE. (Some devices have a jumper to select DTE or DCE mode.) If you cannot find this information in your documentation, see Table 5-1 to help you determine the proper device type.

Table 5-1 Identifying the Device Type

Device Type	Typical Connector	Typical Devices
DTE	Male[1]	Terminal PC
DCE	Female[2]	Modem CSU/DSU Multiplexer

1. If pins protrude from the base of the connector, the connector is male.
2. If the connector has holes to accept pins, the connector is female.

Note Serial ports configured as synchronous DTE require external clocking from a channel service unit/data service unit (CSU/DSU) WAN interface card or other DCE device.

About Serial Cables Used with Cisco 2600 Series, Cisco 3600 Series, Cisco 3700 Series, and Cisco MWR 1941-DC Routers

Cisco Systems offers 10 types of serial cables (also called *serial adapter cables* or *transition cables*) as listed in Table 5-2.

Table 5-2 Serial Cables and Cisco Smart Serial Cables

Standard Serial Cables	Cisco Smart Serial Cables
EIA/TIA-232 serial cable	EIA/TIA-232 Smart Serial cable
EIA/TIA-449 serial cable	EIA/TIA-449 Smart Serial cable
V.35 serial cable	V.35 Smart Serial cable
X.21 serial cable	X.21 Smart Serial cable
EIA/TIA-530 serial cable	EIA/TIA-530 Smart Serial cable EIA/TIA-530A Smart Serial cable

The documentation for the device you plan to connect to the serial port should indicate which interface is used. You can then order a serial transition cable of the correct type.

Tip A cable providing surge protection (CAB-SS-SURGE) is also available from Cisco Systems for use with the NM-16A/S network module. See the "12-in-1 Smart Serial Cables" section on page 5-4 for instructions on connecting the surge protector cable.

A standard serial cable uses a universal 60-pin plug at the network module or WAN interface card end. The Smart Serial cable uses a 12-in-1 Smart Serial connector designed by Cisco. The network end of each cable provides the physical connectors most commonly used for the interface. For example, the network end of the EIA/TIA-232 serial cable is a DB-25 connector, the most widely used EIA/TIA-232 connector.

All serial interface types except EIA/TIA-530 and EIA/TIA-530A are available in DTE or DCE format: DTE with a plug connector at the network end, and DCE with a receptacle at the network end. V.35 is available in either mode, with either gender at the network end. EIA/TIA-530 and EIA/TIA-530A are available in DTE only.

Serial cables are not provided with the network module. For ordering information, see the "Obtaining Technical Assistance" section on page xi.

Although manufacturing your own serial cables is not recommended (because of the small size of the pins on the DB-60 serial connector), cable pinouts are provided in the online document *Cisco Modular Access Router Cable Specifications.* For further information, see the "Obtaining Documentation" section on page viii.

About Data Rates and Distance Limitations

All serial signals are subject to distance limits, beyond which the signal degrades significantly or is completely lost. Generally, the slower the data rate, the greater the distance.

Table 5-3 lists recommended maximum speeds and distances for each serial interface type. If you understand and compensate for potential electrical problems, you may get good results at speeds and distances greater than those listed. For instance, the recommended maximum rate for V.35 is 2 Mbps, but 4 Mbps is commonly used.

Table 5-3 Serial Interface Recommended Maximum Speeds and Distances

	EIA/TIA-232 Distance		**EIA/TIA-449, -530, -530A, V.35, and X.21 Distance**	
Data Rate, bps	**Feet**	**Meters**	**Feet**	**Meters**
2400	200	60	4100	1250
4800	100	30	2050	625
9600	50	15	1025	312
19200	25	8	500	150
38400	12	4	250	75
56000	9	3	100	30
1544000 (T1)	—	—	50	15

Balanced drivers allow EIA/TIA-449 signals to travel greater distances than EIA/TIA-232 signals. The recommended distance limits for EIA/TIA-449 shown in Table 5-3 are also valid for V.35, X.21, and EIA/TIA-530. Typically, EIA/TIA-449 and EIA/TIA-530 support 2-Mbps rates, and V.35 can support 4-Mbps rates.

Asynchronous and Synchronous Serial Module Data Rates

The following data-rate limitations apply to the slow-speed serial interfaces found on asynchronous and synchronous serial modules:

- The maximum data rate on the slow-speed asynchronous interface is 115.2 kbps. The traffic throughput rate allowed is the full 115.2 kbps, with 10 percent of traffic in the opposite direction.
- The maximum data rate for the slow-speed synchronous interface is 128 kbps full duplex.

Connecting Asynchronous Network Modules to Asynchronous Devices

An asynchronous network module provides two or four 68-pin receptacles. Each receptacle connects to asynchronous devices by means of an octal cable that has a 68-pin plug at the module end and eight connectors at the network end, one for each of the eight EIA/TIA-232 serial ports. Depending on the type of cable, the network end consists of either RJ-45 connectors or male DB-25 connectors. RJ-45-to-DB-25 adapters are also available.

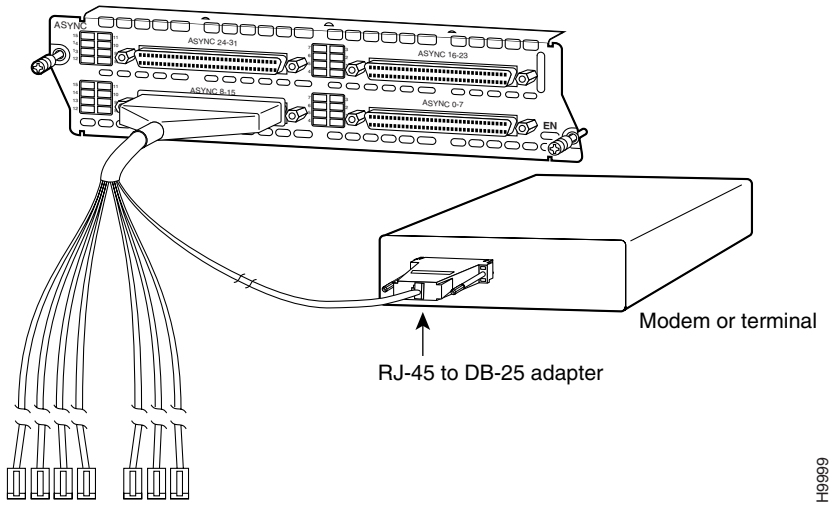
Ports are numbered from right to left and from bottom to top, as labeled on the module rear panel. (See the "Asynchronous Network Module Interface Numbering" section on page 5-6.)

Octal Cables

Octal cables are not provided with the network module. For ordering information, see the "Obtaining Technical Assistance" section on page xi.

Use an octal cable, and adapters if necessary, to connect each of the module's 68-pin receptacles to one or more asynchronous modems, terminals, or other devices. (See Figure 5-1.)

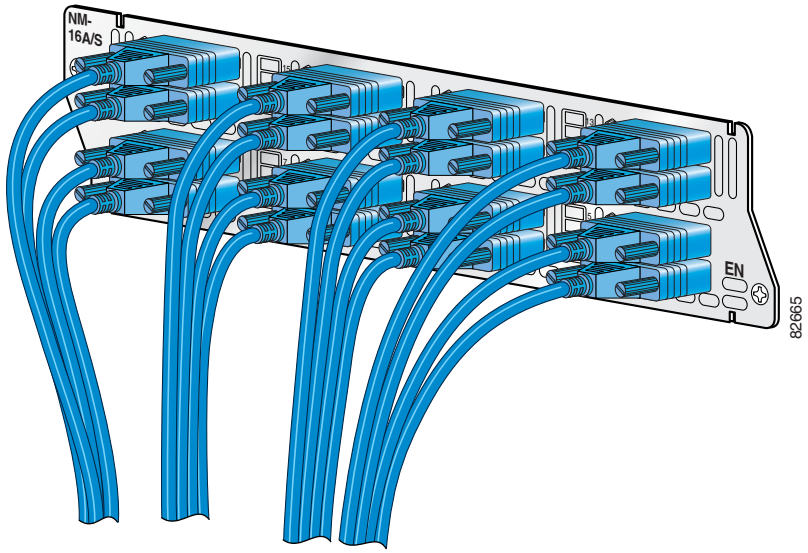
Figure 5-1 Connecting an Asynchronous Network Module to an Asynchronous Device



12-in-1 Smart Serial Cables

The Cisco NM-16A/S network module uses sixteen 12-in-1 Smart Serial cables. The cables connect the network module to a patch panel or one or more asynchronous modems, terminals, or other devices. (See Figure 5-2.)

Figure 5-2 Connecting the NM-16A/S Network Module



The surge protection cable (CAB-SS-SURGE) is installed between the network module and the 12-in-1 Smart Serial cable. (See Figure 5-3.)

Figure 5-3 Connecting the Cisco Surge Protector Cable (CAB-SS-SURGE) to the NM-16A/S Network Module

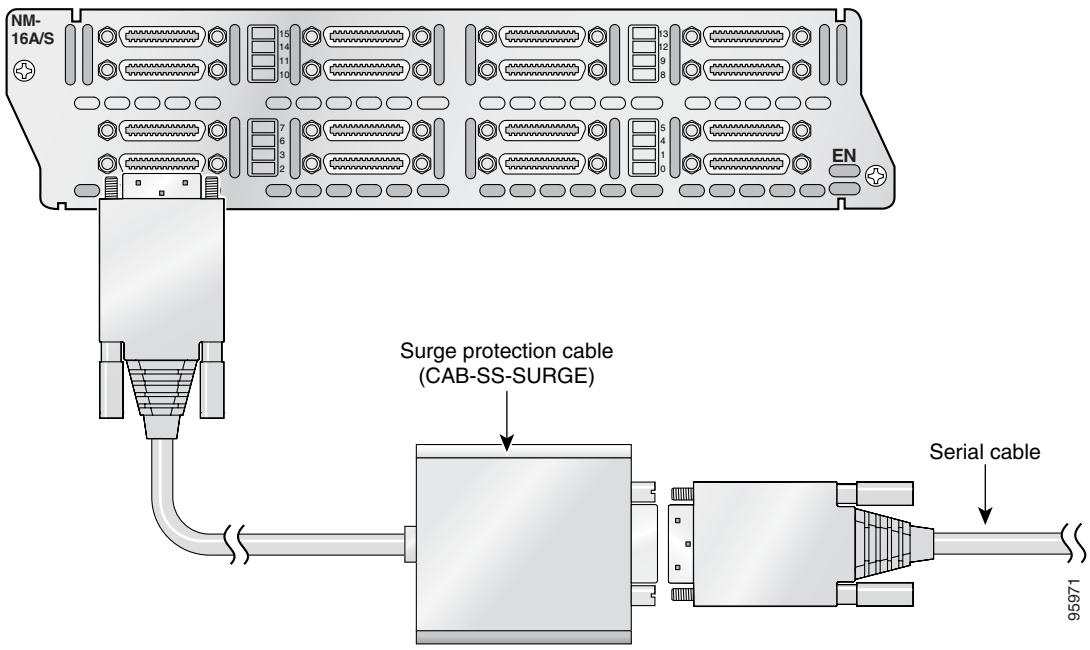
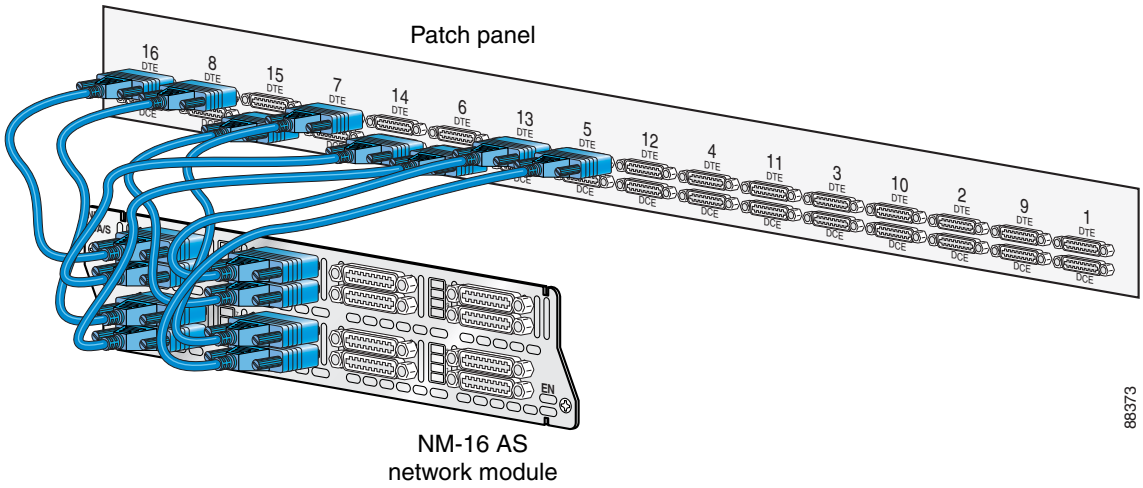


Figure 5-4 shows the 12-in-1 Smart Serial cables going from the Cisco NM-16A/S network module to a patch panel installed above the network module in a standard telco rack. The numbers next to the connectors on the patch panel correspond to the port number (or connector) on the other side of the patch panel.

Figure 5-4 Cabling the Cisco NM-16AS Network Module to a Patch Panel



Asynchronous Network Module Interface Numbering

Certain Cisco IOS configuration commands identify asynchronous ports by an interface number (or a line number, which is the same as the interface number). The interface number of a port on an asynchronous network module is related to the slot number where the module is installed and the unit number of the port in the module.

Cisco 3600 Series and Cisco MWR 1941-DC Router 16- and 32-Port Interface Numbering

Cisco 3600 series and Cisco MWR 1941-DC router slot numbering is explained in the "Network Module Slot Locations and Numbering on Cisco Access Routers" section on page 1-3.

Ports on the 16- and 32-port asynchronous network modules correspond to the outputs of the octal cables that connect the module to the network. These ports are numbered in the same pattern as slot numbers, beginning at 0 at the lower right and continuing from right to left and (in the 32-port module) from bottom to top. In the 16-port module, the right connector provides ports 0 to 7, and the left connector provides ports 8 to 15, as labeled on the module rear panel. In the 32-port module, the connectors in the bottom row provide ports 0 to 7 and 8 to 15, and the connectors in the top row provide ports 16 to 23 and 24 to 31.

The interface number of a port is determined using the following formula:

interface-number = (32 x *slot-number*) + *unit-number* + 1

For example, asynchronous port 12 in slot 1 corresponds to interface number (32 x 1) + 12 + 1 = 45. This is also the line number for the port. Port 12 in slot 1 is always assigned interface number 45, regardless of whether the module in slot 0 is a 16-port asynchronous module, a

32-port asynchronous module, or some other type of module—or even whether there is a network module in slot 0 at all. If you move the module in slot 1 to a different slot, however, its interface numbers change.

Note The Cisco MWR 1941-DC router has one network module slot (slot 1).

Table 5-4 shows the range of interface numbers available for each type of asynchronous network module in each Cisco 3600 series router slot. (Interface 0 is automatically assigned to the console.)

Table 5-4 Cisco 3600 Series 16- and 32-Port Asynchronous Network Module Interface Numbering

Slot Number	Interface Numbers (16-Port Module)	Interface Numbers (32-Port Module)
0	1–16	1–32
1	33–48	33–64
2	65–80	65–96
3	97–112	97–128
4	129–144	129–160
5	161–176	161–192
6	193–208	193–224

Cisco 2600 Series and Cisco MWR 1941-DC Router Serial Interface Numbering

Interface numbering for Cisco 2600 series and Cisco MWR 1941-DC routers differ from Cisco 3600 series interface numbering in the following ways:

- WAN interface card slot numbers always appear as slot 0, even if the interface card is installed in the slot labeled W1.
- WAN interface cards are numbered dynamically, starting with the first card installed. For example:
  - If slot W0 is empty and slot W1 contains a 1-port serial WAN interface card, the interface number is serial 0/0.
  - If slot W0 contains a 2-port serial WAN interface card and slot W1 contains a 1-port serial interface card, serial 0/0 and 0/1 reside in slot W0 and serial 0/2 resides in slot W1.

Port Interface Numbering

Note The Cisco MWR 1941-DC router requires Cisco IOS Release 12.2(15)MC1a and later for 4- and 8-port asynchronous/synchronous and 16- and 32-port asynchronous modules network module support.

4- and 8-Port

The 4-port and 8-port asynchronous/synchronous network modules, when configured for asynchronous operation under releases earlier than Cisco IOS Release 11.2(7)P, use a different interface numbering algorithm:

interface-number = (16 x *slot-number*) + *unit-number* + 1

16- and 32-Port

Table 5-5 shows the numbers available under this numbering scheme. These interface numbers create potential conflicts with the numbers assigned to 16- and 32-port asynchronous modules; that is, it would be possible for a 16- or 32-port asynchronous module in one slot to overlap the interface numbers of a 4- or 8-port asynchronous and synchronous module in another slot.

Table 5-5 4-, 8-, and 16-Port Serial Network Module Interface Numbering

Slot Number	Interface Numbers (4-Port Module)	Interface Numbers (8-Port Module)	Interface Numbers (16-Port Module)
0	1–4	1–8	1–16
1	17–20	17–24	17–24
2[1]	33–36	33–40	33–40
3[1]	49–52	49–56	49–64
4	N/A	N/A	65–80
5	N/A	N/A	81–96

1. Cisco 3640 and Cisco 3660 routers only.

To prevent this conflict, Cisco IOS Release 11.2(7)P, which is required to operate 16- and 32-port asynchronous network modules, checks when the router boots for the presence of 4- and 8-port asynchronous/synchronous network modules configured as asynchronous. If the software finds any of these network modules, it rewrites the starting configuration in nonvolatile random access memory (NVRAM), if necessary, to adopt the new line numbering scheme for these modules, as shown in Table 5-6 on page 5-8.

Table 5-6 New 4- and 8-Port Serial Network Module Interface Numbering

Slot Number	Interface Numbers (4-Port Module)	Interface Numbers (8-Port Module)
0	1–4	1–8
1	33–36	33–40

Table 5-6 New 4- and 8-Port Serial Network Module Interface Numbering (continued)

Slot Number	Interface Numbers (4-Port Module)	Interface Numbers (8-Port Module)
2[1]	65–68	65–72
3[1]	97–100	97–104

1. Cisco 3640 and Cisco 3660 routers only.

When an automatic configuration update is performed, the following message appears:

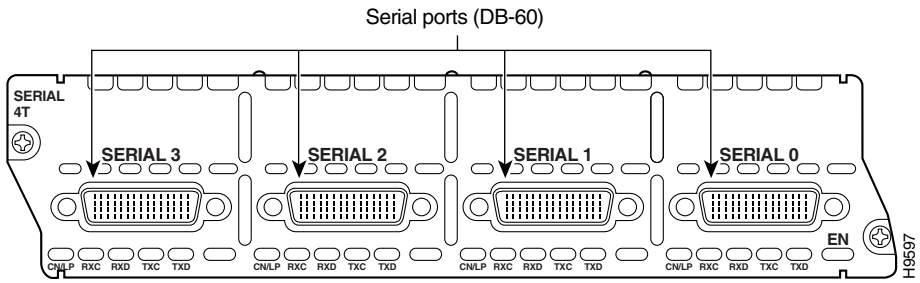
```
Line number convention changed from 16 lines/slot to 32 lines/slot.
```

4-Port Serial Network Module

This section provides information about the 4-port serial network module (Cisco product number NM-4T). (See Figure 5-5.) With the appropriate serial transition cable, each port on this module can provide an EIA/TIA-232, EIA/TIA-449, V.35, X.21, EIA/TIA-530 DTE, or nonreturn to zero/nonreturn to zero inverted (NRZ/NRZI) serial interface. The module provides a synchronous data rate of 8 MB per second on port 0, 4 MB per second each on port 0 and port 2, or 2 MB on all four ports simultaneously.

Note Half-duplex and binary-synchronous communications are not supported on the 4-port serial network module.

Figure 5-5 4-Port Serial Network Module

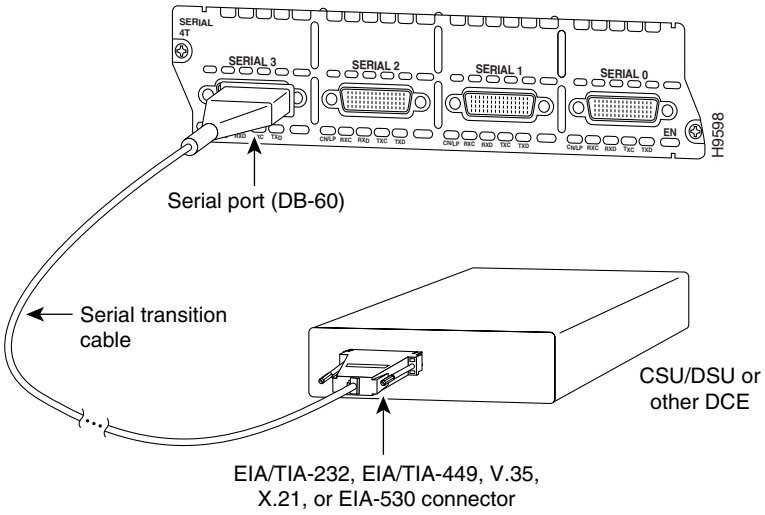


Connecting the 4-Port Serial Module to a Network

The 4-port serial network module provides four universal, high-density, 60-pin receptacles. The serial cable attached to each receptacle determines the port's electrical interface type and mode, DTE or DCE.

After you install a 4-port serial module, use the appropriate serial cable to connect each of the DB-60 serial ports to a synchronous modem, channel service unit/data service unit (CSU/DSU), or other DCE equipment. (See Figure 5-6.)

Figure 5-6 Connecting a 4-Port Serial Module to a CSU/DSU



4-Port Serial Network Module LEDs

All network modules have an enable (EN) LED. This LED indicates that the module has passed its self-tests and is available to the router.

Each port on the 4-port serial network module also has the additional LEDs shown in Figure 5-7 and described in Table 5-7.

Figure 5-7 4-Port Serial Network Module LEDs

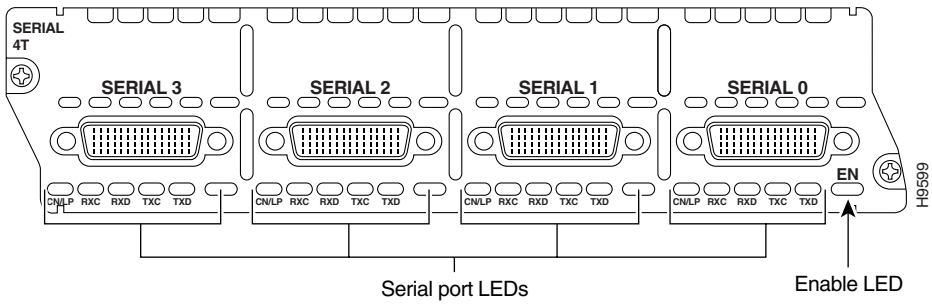


Table 5-7 4-Port Serial Network Module LEDs

LED	Meaning
CN/LP	In connect mode when green, in loopback mode when yellow
RXC	Receive clock
RXD	Receive activity
TXC	Transmit clock
TXD	Transmit activity

16- and 32-Port Asynchronous Serial Network Modules

This section provides information about the following network modules:

- 16-port asynchronous network module (NM-16A) (see Figure 5-8)
- 32-port asynchronous network module (NM-32A) (see Figure 5-9)

When used with corresponding octal cables, these modules provide 16 or 32 EIA/TIA-232 data terminal equipment (DTE) serial interfaces. Speeds up to 134.4 kbps are supported.

Figure 5-8 16-Port Asynchronous Network Module

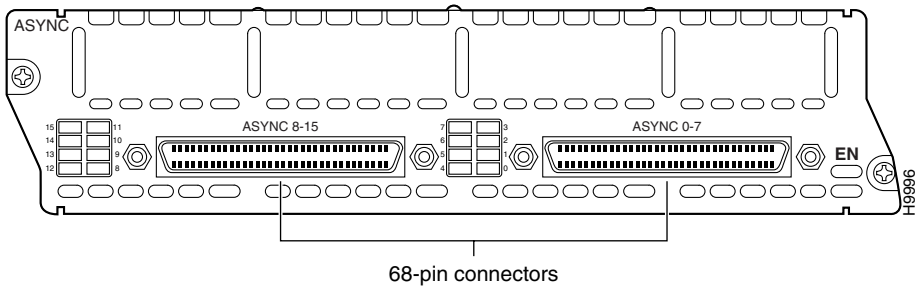
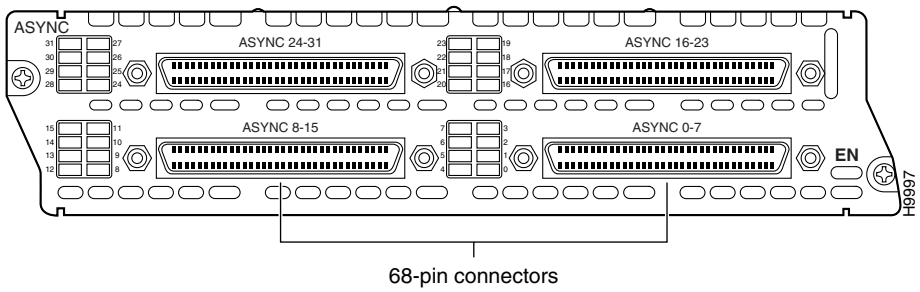


Figure 5-9 32-Port Asynchronous Network Module



Asynchronous Network Module LEDs

All network modules have an enable (EN) LED. This LED indicates that the module has passed its self-tests and is available to the router.

Each port on an asynchronous network module also has a green status LED to indicate that the port is connected to the network. These LEDs are grouped in blocks of eight to the left of each module and are labeled with the port numbers. (See Figure 5-10 and Figure 5-11.)

Figure 5-10 16-Port Asynchronous Network Module LEDs

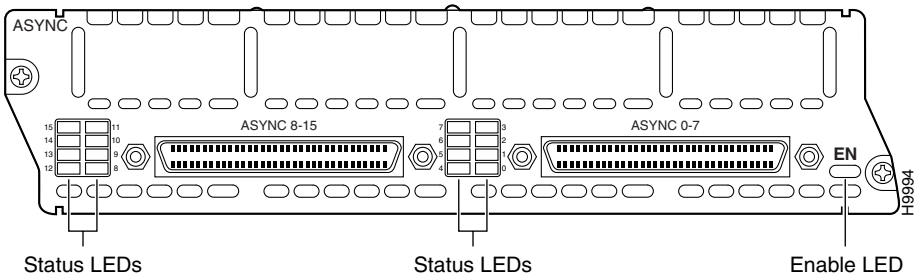
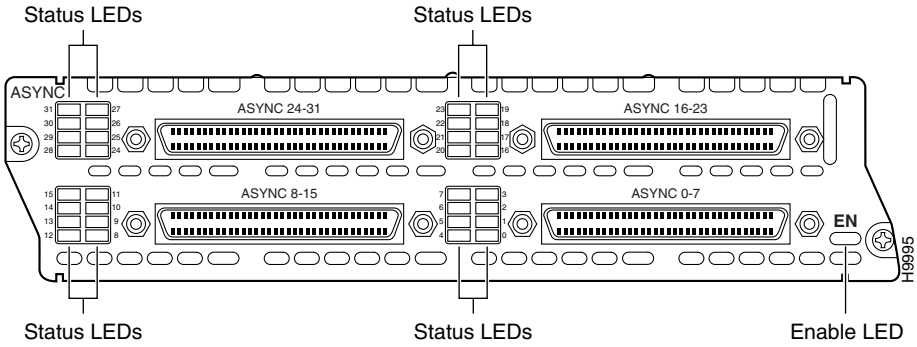


Figure 5-11 32-Port Asynchronous Network Module LEDs



4-, 8-, and 16-Port Asynchronous/Synchronous Serial Network Modules

This section provides information about the following network modules for Cisco modular routers:

- 4-port asynchronous/synchronous serial network module (NM-4A/S) (see Figure 5-12).
- 8-port asynchronous/synchronous serial network module (NM-8A/S) (see Figure 5-13).
- 16-port asynchronous/synchronous serial network module (NM-16A/S) (see Figure 5-14).

Note The Cisco NM-16A/S network module uses a Cisco patented 12-in-1 Smart Serial cable.

With the appropriate serial transition cable, the ports on these modules can provide an EIA/TIA-232, EIA/TIA-449, V.35, X.21, EIA/TIA-530 DTE, or NRZ/NRZI serial interface. The NM-16 A/S network module can provide an EIA/TIA-530A DTE interface.

Caution To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the 8-port A/S serial network modules (NM-8A/S) and 16-port A/S serial network modules (NM-16A/S) only to intrabuilding or nonexposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

Figure 5-12 4-Port Asynchronous/Synchronous Serial Network Module

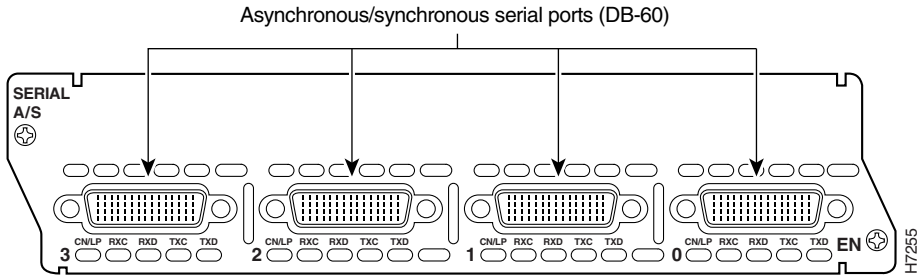


Figure 5-13 8-Port Asynchronous/Synchronous Serial Network Module

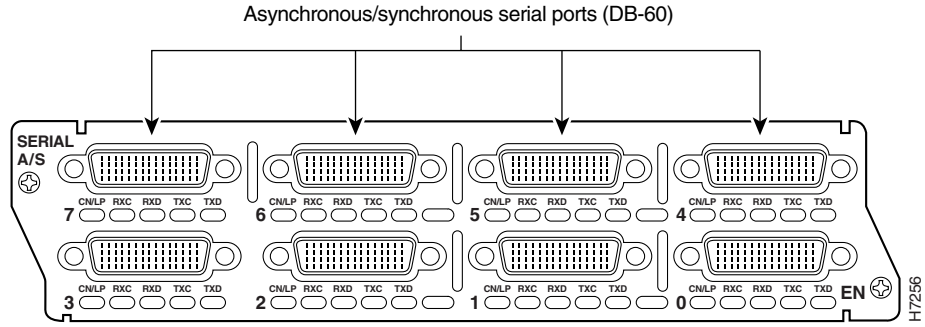
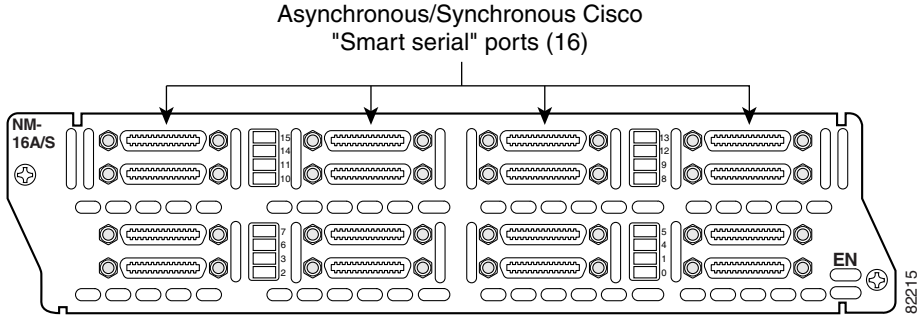


Figure 5-14 16-Port Asynchronous/Synchronous Serial Network Module



Asynchronous/Synchronous Serial Module LEDs

Figure 5-15 shows LEDs for the 4-port asynchronous/synchronous serial network module. Figure 5-16 shows LEDs for the 8-port asynchronous/synchronous serial network module. Figure 5-17 shows the LEDs for the 16-port asynchronous/synchronous serial network module.

Figure 5-15 4-Port Asynchronous/Synchronous Serial Network Module LEDs

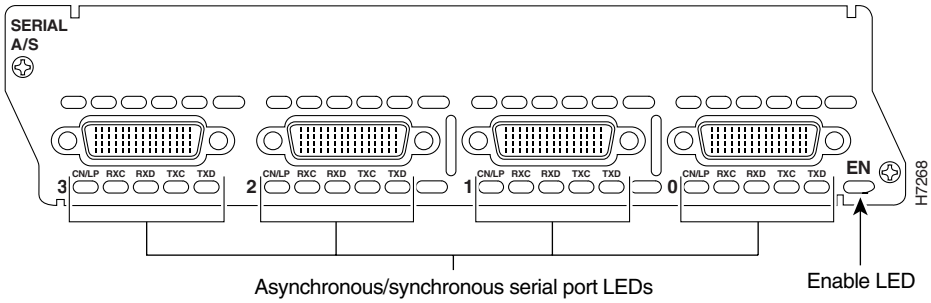
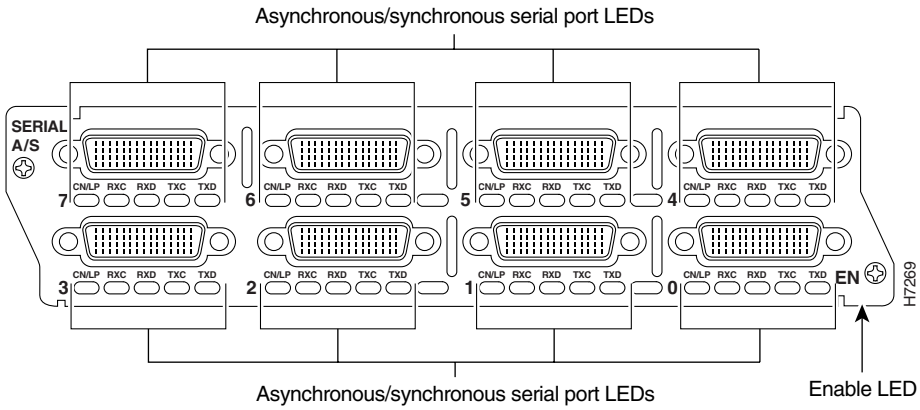


Figure 5-16 8-Port Asynchronous/Synchronous Serial Network Module LEDs



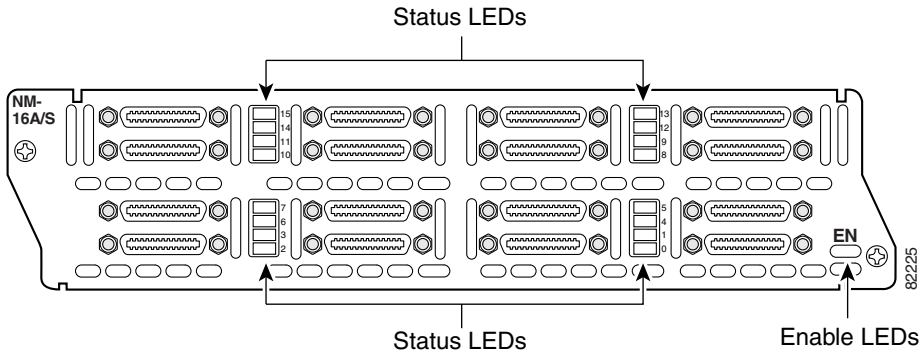
All network modules have an enable (EN) LED. This LED indicates that the module has passed its self-tests and is available to the router.

Each port on an asynchronous/synchronous serial network module also has the additional LEDs shown in Table 5-8.

Table 5-8 4- and 8-Port Asynchronous/Synchronous Serial Network Module LEDs

LED	Meaning
CN/LP	In connect mode when green, in loopback mode when yellow
RXC	Receive clock
RXD	Receive activity
TXC	Transmit clock
TXD	Transmit activity

Figure 5-17 16-Port Asynchronous/Synchronous Serial Network Module LEDs



The NM-16 A/S network module has LEDs that indicate the status of the port. When the LED is green, the physical port is in the up state. When the LED is yellow, the port is in loopback mode. (See Table 5-9.)

Table 5-9 16-port Asynchronous Status LEDs and Enabled LEDs

Mode	LED Color	Meaning
DCE	Green	Data terminal ready (DTR) and request to send (RTS) are present.
DTE	Green	Data set ready (DSR), data carrier detect (DCD), and clear to send (STC) are present.
Loopback	Yellow	The port is in loopback mode

CHAPTER 6

Connecting ISDN BRI Network Modules

This chapter describes how to connect Integrated Services Digital Network (ISDN) Basic Rate Interface (BRI) network modules for Cisco modular routers and contains the following sections:

Unless specifically identified, references to BRI modules in this chapter include all ISDN BRI network modules.

Note Do not install an ISDN BRI network module in the same chassis as an ISDN Primary Rate Interface (PRI) network module unless you are using Cisco IOS Release 11.3(3)T or later. Earlier Cisco IOS releases do not support this configuration.

Tip To determine whether your router supports a specific network module, see Table 1-6 on page 1-16.

4- and 8-Port ISDN BRI S/T Network Modules

This section provides information about the following network modules for Cisco modular routers:

- 4-port ISDN BRI network module (NM-4B-S/T or CPANM-4B-S/T) (see Figure 6-1). This module connects to an ISDN WAN through an external Network Termination 1 (NT1) device (also known as an *S/T interface*). It is also referred to as the *4-port BRI S/T network module*.
- 8-port ISDN BRI network module (NM-8B-S/T or CPANM-8B-S/T) (see Figure 6-2). This module connects to an ISDN WAN through an external NT1 device (also known as an *S/T interface*). It is also referred to as the *8-port BRI S/T network module*.

Figure 6-1 4-Port ISDN BRI Network Module (S/T Interface)

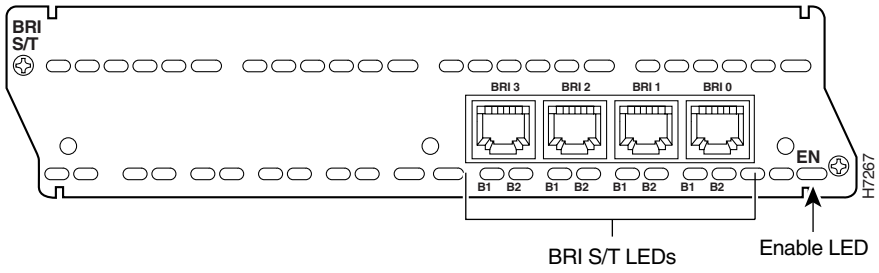
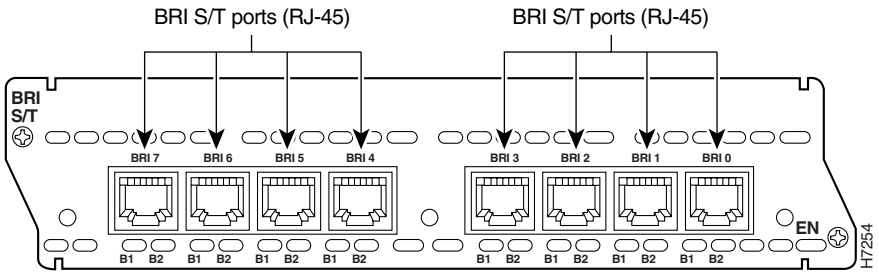


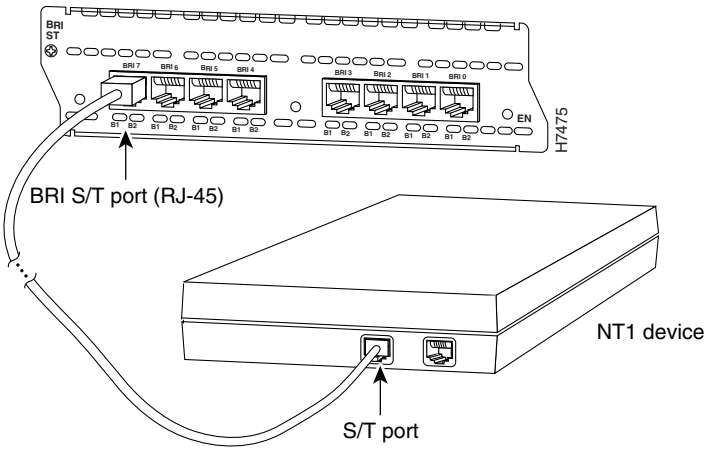
Figure 6-2 8-Port ISDN BRI Network Module (S/T Interface)



Connecting BRI S/T Modules to a Network

To connect a BRI S/T network module to a network, use a straight-through RJ-45-to-RJ-45 cable to connect the ISDN BRI port to an NT1. (See Figure 6-3.) These ports are color-coded orange.

Figure 6-3 Connecting an ISDN BRI S/T Network Module to an NT1



BRI S/T Module LEDs

Figure 6-4 shows LEDs for the 4-port BRI S/T network module. Figure 6-5 shows LEDs for the 8-port BRI S/T network module.

Figure 6-4 4-Port ISDN BRI S/T Network Module LEDs

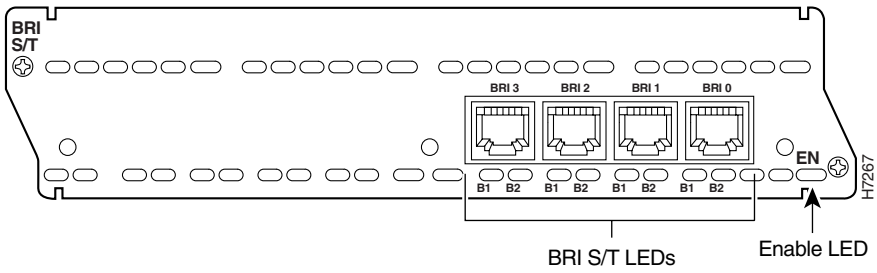
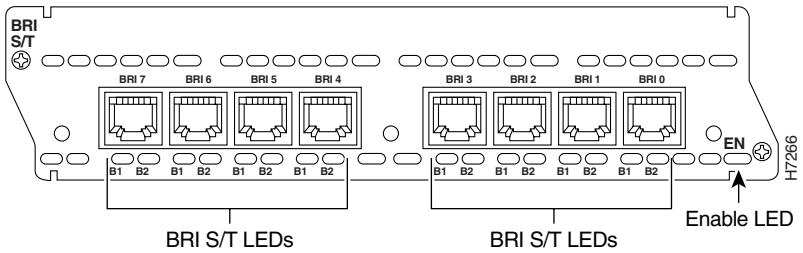


Figure 6-5 8-Port ISDN BRI S/T Network Module LEDs



All network modules have an enable (EN) LED. This LED indicates that the module has passed its self-tests and is available to the router.

In addition, BRI S/T modules have two LEDs for each port. These LEDs indicate call activity on the two ISDN BRI B channels, as described in Table 6-1.

Table 6-1 BRI S/T Network Module LEDs

LED	Meaning
B1	Call active on B1 channel
B2	Call active on B2 channel

4- and 8-Port ISDN BRI U Network Modules

This section provides information about the following network modules for Cisco modular routers:

- 4-port ISDN BRI with NT1 network module (NM-4B-U or CPANM-4B-U) (see Figure 6-6). This module connects to an ISDN WAN using a built-in NT1 device (also known as a *U interface*). It is also referred to as the *4-port BRI U network module*.
- 8-port ISDN BRI with NT1 network module (NM-8B-U or CPANM-8B-U) (see Figure 6-7). This module connects to an ISDN WAN using a built-in NT1 device (also known as a *U interface*). It is also referred to as the *8-port BRI U network module*.

Figure 6-6 4-Port ISDN BRI with NT1 Network Module (U Interface)

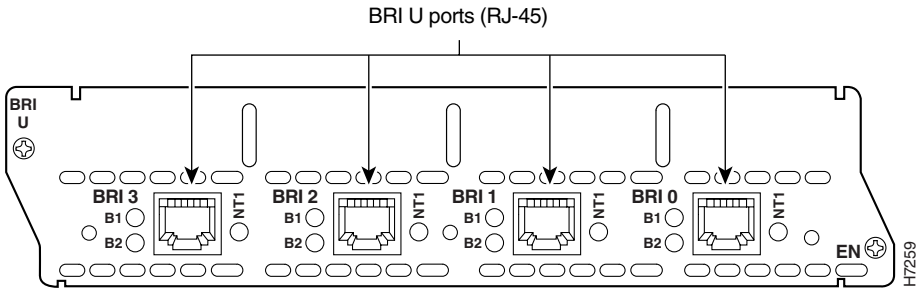
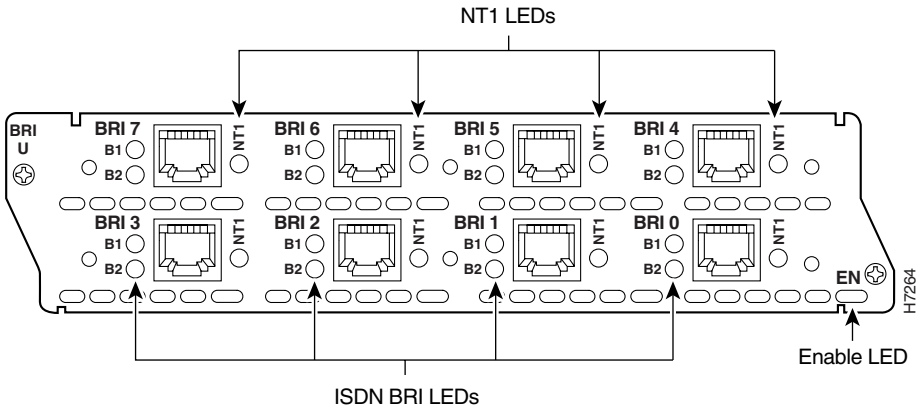


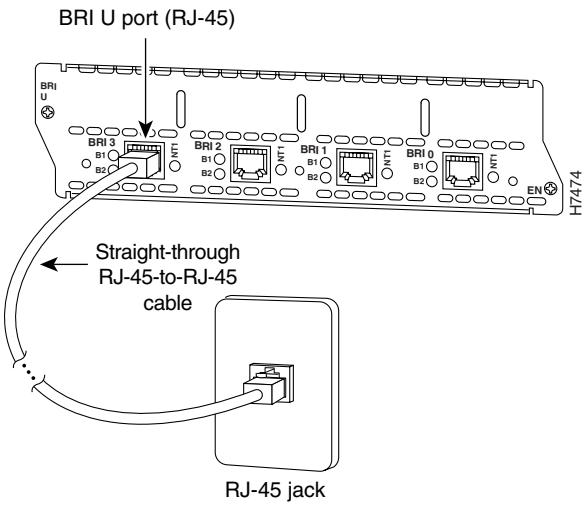
Figure 6-7 8-Port ISDN BRI with NT1 Network Module (U Interface)



Connecting BRI U Modules to a Network

To connect a BRI U module to a network, use a straight-through RJ-45-to-RJ-45 cable to connect the ISDN BRI port to an RJ-45 jack. (See Figure 6-8.) These ports are color-coded red.

Figure 6-8 Connecting a BRI U Network Module to an RJ-45 ISDN Jack



BRI U Module LEDs

Figure 6-9 shows LEDs for the 4-port BRI U network module. Figure 6-10 shows LEDs for the 8-port BRI U network module.

Figure 6-9 4-Port ISDN BRI U Network Module LEDs

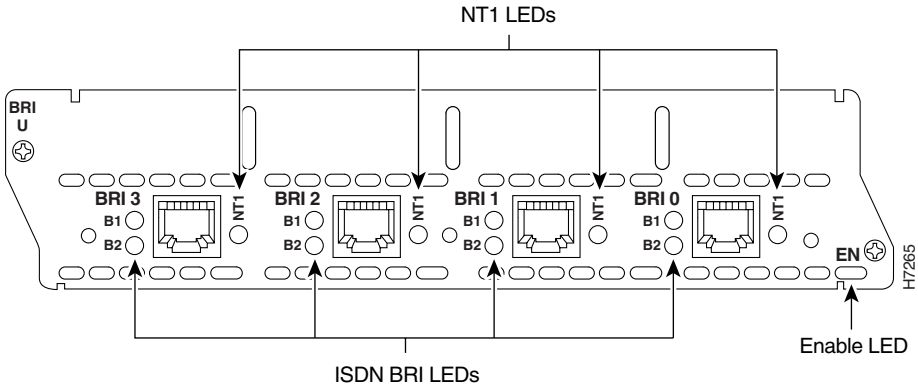
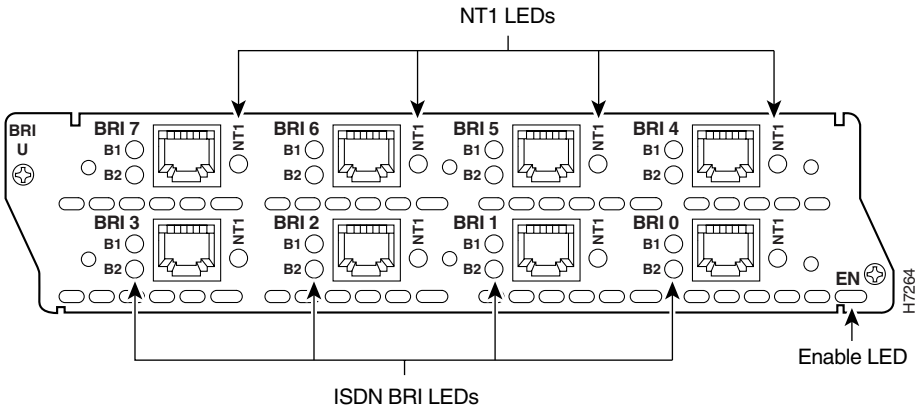


Figure 6-10 8-Port ISDN BRI U Network Module LEDs



All network modules have an enable (EN) LED. This LED indicates that the module has passed its self-tests and is available to the router.

In addition, BRI U modules have three LEDs for each port. Two of these LEDs indicate call activity on the two ISDN BRI B channels, as described in Table 6-2. The third LED, labeled NT1, indicates synchronization status of the NT1.

Table 6-2 BRI U Network Modules LEDs

LED	Meaning
B1	Activity on B1 channel
B2	Activity on B2 channel
NT1	Synchronous status of NT1

Upgrading ISDN BRI Network Modules

If your Cisco 3600 series router contains an ISDN BRI network module (product numbers NM-4B-S/T, NM-4B-U, NM-8B-S/T, or NM-8B-U) and a digital modem network module (product numbers NM-6DM, NM-12DM, NM-18DM, NM-24DM, or NM-30DM), your ISDN BRI network module may need to be upgraded to the minimum revision shown in Table 6-3.

Earlier revisions of the ISDN BRI network module cannot send modem calls to the digital modem network module.

Table 6-3 ISDN BRI Network Module Upgrade Revisions

Module	Minimum Revision
NM-4B-S/T	800-01236-03
NM-4B-U	800-01238-06
NM-8B-S/T	800-01237-03
NM-8B-U	800-01239-06

If your BRI module is the wrong revision, you see a message similar to this one when the router boots:

```
The BRI network module in slot 0 is incompatible with the digital modems installed in the
router.
```

To determine the revision level, you can examine the network module itself (outside the router) or use the Cisco IOS **show diag** command. The label on the module board should show a part number beginning with 800-, corresponding to Table 6-3. A BRI S/T module whose part number ends with -01 or -02 needs to be upgraded, as does a BRI U module whose part number is lower than -06.

The output of the **show diag** command looks similar to the following:

```
Port adapter is analyzed
Port adapter insertion time unknown
Hardware revision 1.0           Board revision A0
Serial number     4152626       Part number    800-01236-01
Test history      0x0           RMA number     00-00-00
   EEPROM format version 1
   EEPROM contents (hex):
   0x20: 01 26 01 00 00 3F 5D 32 50 04 CC 01 00 00 00 00
   0x30: 50 00 00 00 96 11 04 17 FF FF FF FF FF FF FF FF
```

To order network module upgrades, see the “Obtaining Technical Assistance” section on page xi.

CHAPTER 7

Connecting ISDN PRI Network Modules

This chapter describes how to connect Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) network modules for Cisco modular routers and contains the following sections:

Note Unless specifically identified, references to PRI modules in this chapter include all these network modules.

Note Cisco Fast Ethernet-PRI network modules also provide a PRI interface. See Chapter 4, "Connecting Fast Ethernet-PRI Network Modules," for further information.

Note Do not install an ISDN BRI network module in the same chassis as an ISDN PRI network module, unless you are using Cisco IOS Release 11.3(3)T or later. Earlier Cisco IOS releases do not support this configuration.

Tip To determine whether your router supports a specific network module, see Table 1-6 on page 1-16.

CT1/PRI modules are available with or without a built-in channel service unit (CSU), and with one or two ports. CT1/PRI modules connect to an external CSU; CT1/PRI-CSU modules connect directly to the network. Each T1 module provides up to 24 virtual channels per T1 port. Each channel can be configured individually as a serial interface.

CT1/PRI and CT1/PRI-CSU modules receive and transmit data bidirectionally, at the T1 rate of 1.544 Mbps.

Channelized T1/E1 PRI Network Modules with G.703

This section provides information about the following network modules:

- 1-port T1/E1 channelized PRI network module with G.703 (NM-1CE1T1-PRI) (see Figure 7-1)
- 2-port T1/E1 channelized PRI network module with G.703 (NM-2CE1T1-PRI) (see Figure 7-2)

Cisco T1/E1 channelized PRI network modules with G.703 provide connection of one or two primary rate ISDN lines. T1 or E1 interfaces are configurable through Cisco IOS command-line interface (CLI) commands. Each port supports 100/120-ohm balanced and 75-ohm unbalanced termination, and features RJ-48C connectors and cable accessories allowing for DB-15, BNC, and other connector types. An onboard advanced integration module (AIM) connector allows for future universal port AIM support.

Caution To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the 1-port T1/E1 channelized PRI network modules with G.703 (NM-1CE1T1-PRI) and 2-port T1/E1 channelized PRI network modules with G.703 (NM-2CE1T1-PRI) only to intrabuilding or nonexposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

Cisco T1/E1 channelized PRI network modules with G.703 (NM-1CE1T1-PRI and NM-2CE1T1-PRI) replace the following network modules (also described in this chapter):

- NM-1CE1B
- NM-1CE1U
- NM-1CT1
- NM-1CT1-CSU
- NM-2CE1B
- NM-2CE1U
- NM-2CT1
- NM-2CT1-CSU

For information on Cisco modular access routers supporting Cisco channelized T1/E1 PRI network modules with G.703, see Table 7-1.

Table 7-1 Modular Access Routers Supporting Cisco Channelized T1/E1 PRI Network Modules with G.703

Modular Access Router	NM-1CE1T1-PRI	NM-2CE1T1-PRI
Cisco 26*xx*	No	No
Cisco 26*xx*XM	Yes	Yes
Cisco 2691	Yes	Yes
Cisco 3620	No	No
Cisco 3631	Yes	Yes
Cisco 3640	No	No

Table 7-1 Modular Access Routers Supporting Cisco Channelized T1/E1 PRI Network Modules with G.703

Modular Access Router	NM-1CE1T1-PRI	NM-2CE1T1-PRI
Cisco 3660	Yes	Yes
Cisco 37*xx*	Yes	Yes

Figure 7-1 and Figure 7-2 show the faceplates for the 1-port and 2-port channelized T1/E1 PRI network modules with G.703.

Figure 7-1 1-Port Channelized T1/E1 PRI Network Module with G.703

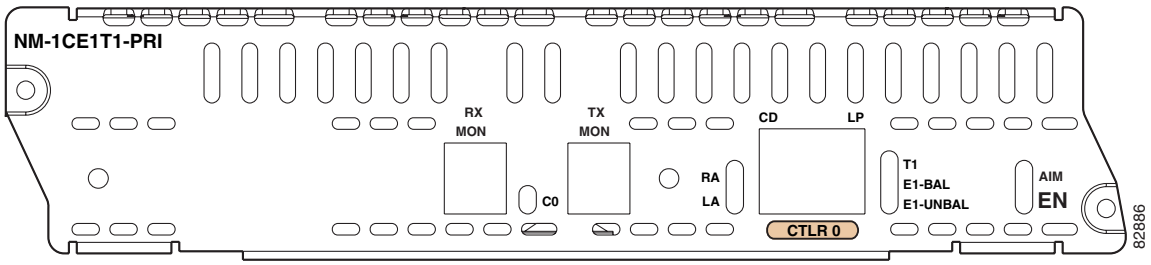
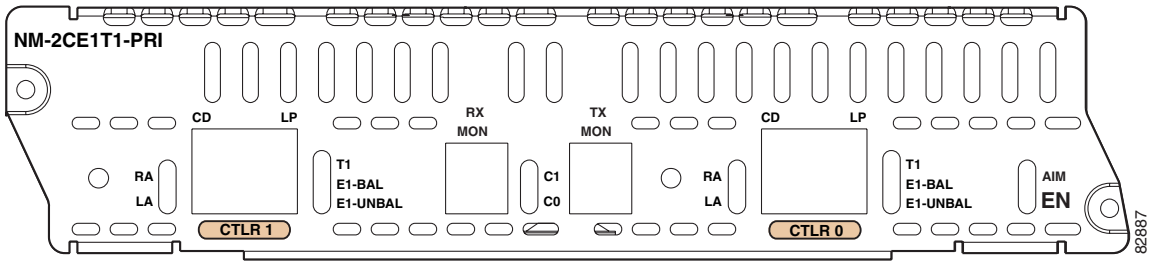


Figure 7-2 2-Port Channelized T1/E1 PRI Network Module with G.703



Enabling Wetting Current on Channelized T1/E1 PRI Network Modules with G.703

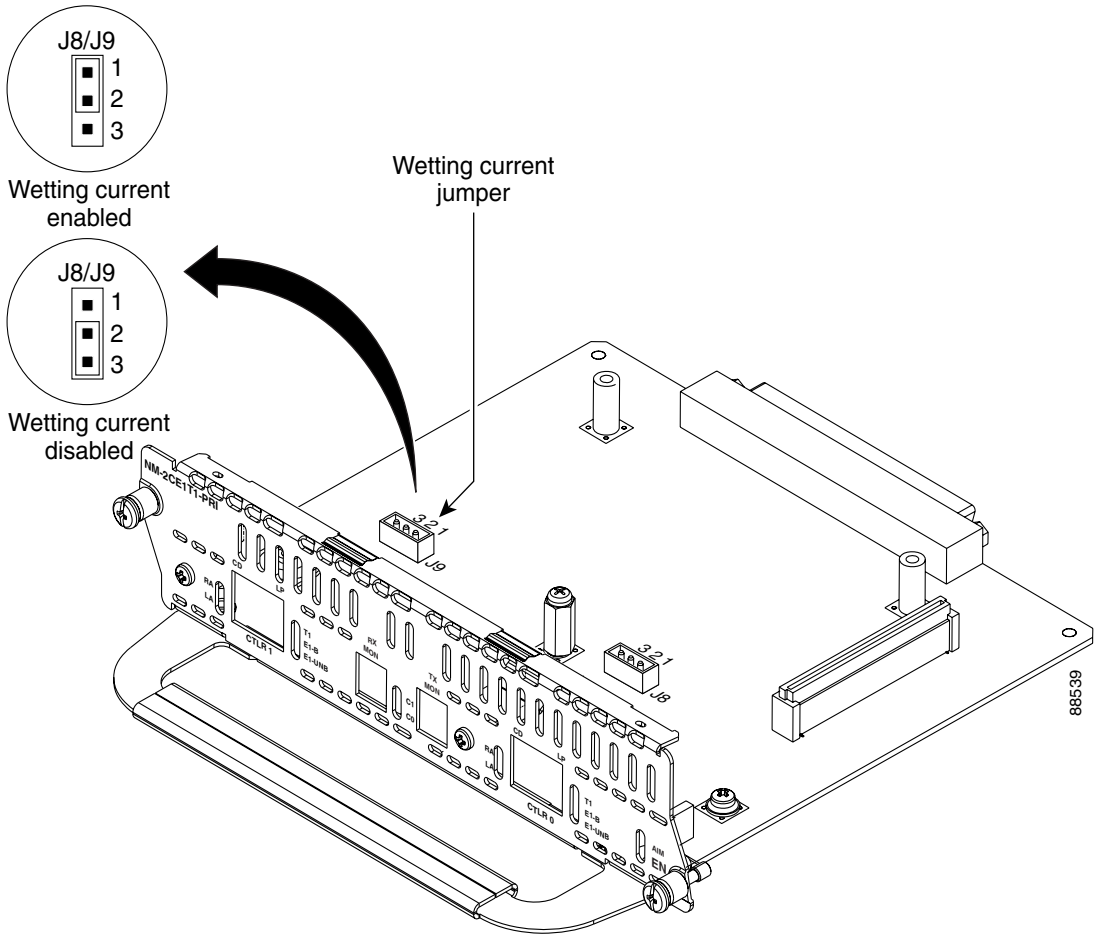
Wetting current is a small amount of electrical current (60 to 140 milliamps) sent from the central office to the card to prevent the corrosion of electrical contacts in the module network connection.

The wetting current feature can be enabled or disabled by the end user. It is controlled by the location of a jumper on the J8 (CTLR 0) and J9 (CTLR 1) connectors on the network module. (See Figure 7-3.)

To enable the wetting current feature, connect pins 1 and 2 on the J8 and J9 connectors with the jumper. To disable the wetting current feature, either remove the jumper completely, or use the jumper to connect pins 2 and 3 on the J8 and J9 connectors.

The card is shipped with the jumper connecting pins 2 and 3 on the J8 and J9 connectors, disabling the wetting current feature.

Figure 7-3 Wetting Current Jumper Locations on Channelized T1/E1 PRI Network Modules with G.703



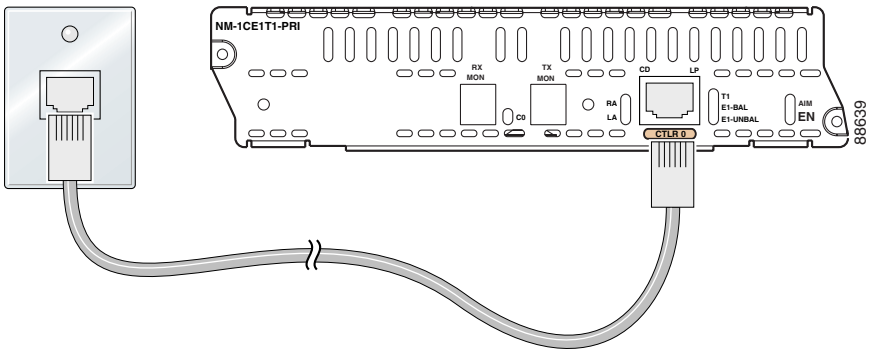
Connecting Channelized T1/E1 PRI Network Modules with G.703 to a Network

Warning **For connections outside the building where the equipment is installed, the following ports must be connected through an approved network termination unit with integral circuit protection: T1** Statement 1044

Figure 7-4 shows a connection between a channelized T1/E1 PRI network module with G.703 and a networking device.

Caution To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the 1-port T1/E1 channelized PRI network modules with G.703 (NM-1CE1T1-PRI) and 2-port T1/E1 channelized PRI network modules with G.703 (NM-2CE1T1-PRI) only to intrabuilding or nonexposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

Figure 7-4 Connecting a Channelized T1/E1 PRI Network Module with G.703 to a Networking Device



Channelized T1/ISDN PRI Network Modules

This section provides information about the following network modules for Cisco modular routers:

- 1-port channelized T1/ISDN PRI network module (NM-1CT1 or CPANM-1CT1) (see Figure 7-5). This module is also referred to as the *1-port CT1/PRI network module*.
- 2-port channelized T1/ISDN PRI network module (NM-2CT1 or CPANM-2CT1) (see Figure 7-6). This module is also referred to as the *2-port CT1/PRI network module*.

Figure 7-5 1-Port Channelized T1/ISDN PRI Network Module

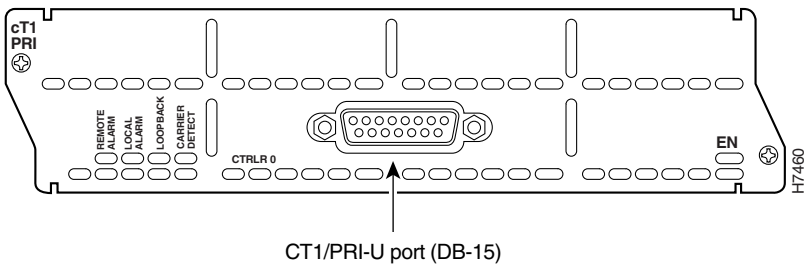
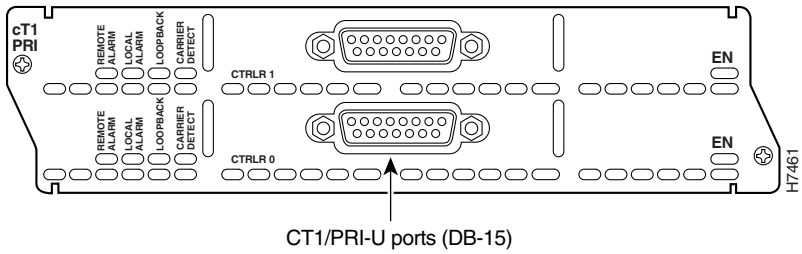


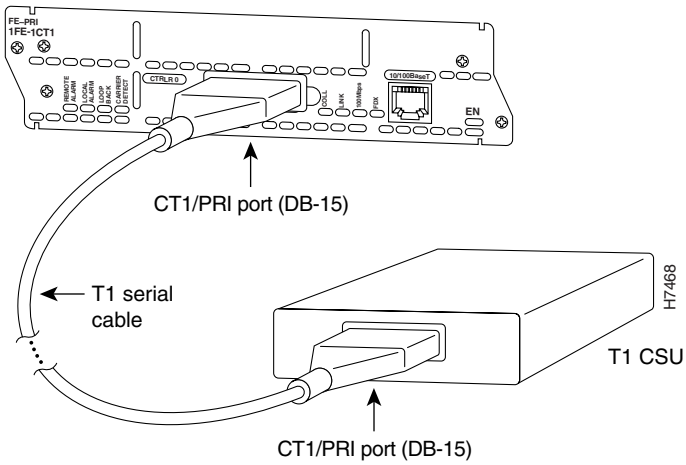
Figure 7-6 2-Port Channelized T1/ISDN PRI Network Module



Connecting CT1/PRI Modules to the Network

To connect a CT1/PRI module to the network, use a DB-15-to-DB-15 T1 serial cable to connect the CT1/PRI port to a T1 channel service unit (CSU). (See Figure 7-7.) These ports are color-coded tan.

Figure 7-7 Connecting a CT1/PRI Module to a T1 CSU



Channelized T1/ISDN PRI with CSU Network Modules

This section provides information about the following network modules for Cisco modular routers:

- 1-port channelized T1/ISDN PRI with CSU network module (NM-1CT1-CSU or CPANM-1CT1-CSU) (see Figure 7-8). This module is also referred to as the *1-port CT1/PRI CSU network module*.
- 2-port channelized T1/ISDN PRI with CSU network module (NM-2CT1-CSU or CPANM-2CT1-CSU) (see Figure 7-9). This module is also referred to as the *2-port CT1/PRI CSU network module*.

Figure 7-8 1-Port Channelized T1/ISDN PRI with CSU Network Module

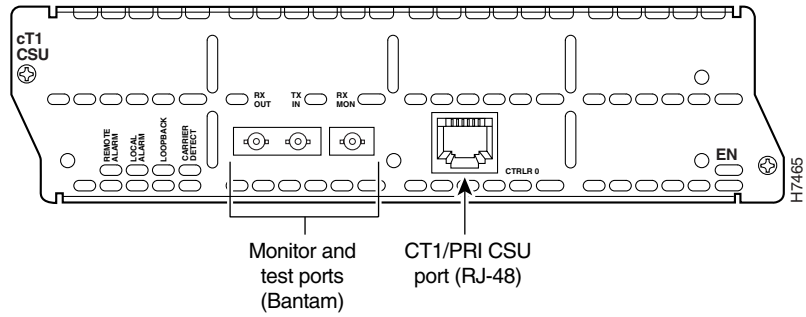
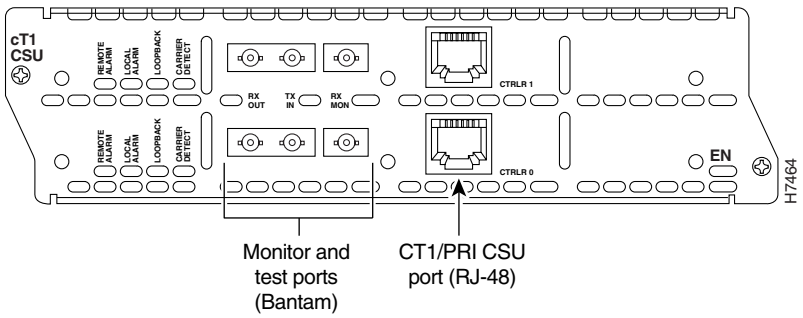


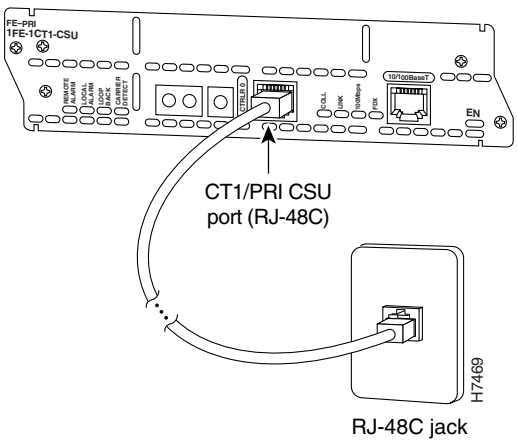
Figure 7-9 2-Port Channelized T1/ISDN PRI with CSU Network Module



Connecting CT1/PRI CSU Modules to the Network

To connect a CT1/PRI CSU module to the network, use a straight-through RJ-48C-to-RJ-48C cable to connect the RJ-48C port to an RJ-48C jack (see Figure 7-10). These ports are color-coded tan.

Figure 7-10 Connecting a CT1/PRI CSU Module to an RJ-48C Jack



Channelized E1/ISDN PRI Balanced (120-Ohm) Network Modules

This section provides information about the following network modules for Cisco modular routers:

- 1-port channelized E1/ISDN PRI balanced (120-ohm) network module (NM-1CE1B or CPANM-1CE1B) (see Figure 7-11). This module is also referred to as the *1-port CE1/PRI-B network module*.
- 2-port channelized E1/ISDN PRI balanced (120-ohm) network module (NM-2CE1B or CPANM-2CE1B) (see Figure 7-12). This module is also referred to as the *2-port CE1/PRI-B network module*.

Figure 7-11 1-Port Channelized E1/ISDN PRI Network Module (Balanced)

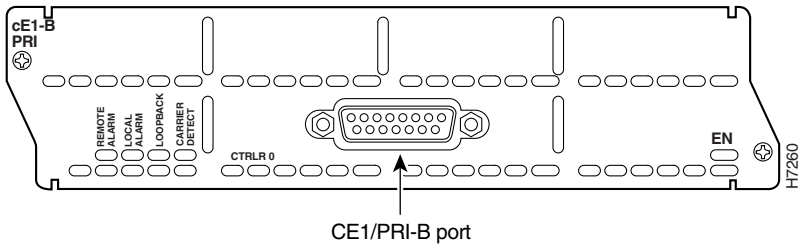
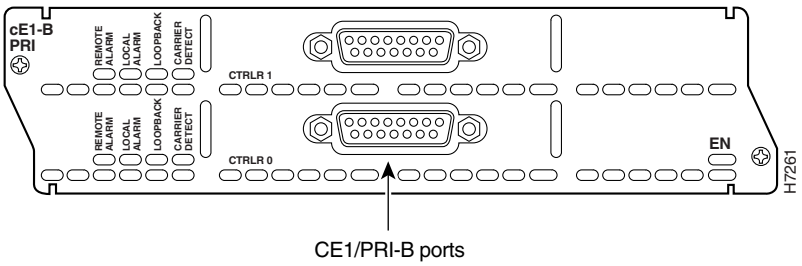


Figure 7-12 2-Port Channelized E1/ISDN PRI Network Module (Balanced)



CE1/PRI modules are available with one or two E1 ports and with balanced or unbalanced interfaces. These modules receive and transmit data bidirectionally at the E1 rate of 2.048 Mbps, and provide up to 30 virtual channels per E1 port. Each channel can be configured individually as a serial interface.

CE1/PRI Module Jumper Settings

Jumpers on CE1/PRI modules can be used to connect or disconnect receive shield to ground. (See Table 7-2.) The default setting for balanced, 120-ohm CE1/PRI-B modules disconnects receive shield to ground. The default setting for unbalanced, 75-ohm CE1/PRI-U modules connects receive shield to ground. If you are experiencing ground loop problems with E1 cabling, you may want to try changing the jumper settings for the module.

Table 7-2 CE1/PRI Module Jumpers

CE1/PRI Module Type	Default Setting	Function
Balanced, 120-ohm	2 and 3	Disconnects receive shield from ground
Unbalanced, 75-ohm	1 and 2	Connects receive shield to ground

Connecting CE1/PRI-B Modules to the Network

To connect a CE1/PRI-B (120-ohm) module to the network, use the appropriate cable to connect the CE1/PRI-B port to an E1 CSU. (See Figure 7-13, Figure 7-14, and Figure 7-15, showing DB-15, twinax, and RJ-45 CSUs, respectively.) These ports are color-coded tan.

Figure 7-13 Connecting a 120-ohm CE1/PRI-B Module to an E1 CSU (DB-15-to-DB-15 Connectors)

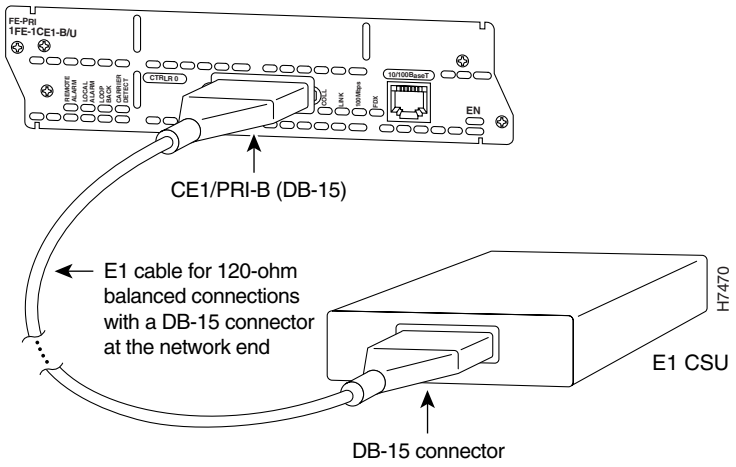


Figure 7-14 Connecting a 120-ohm CE1/PRI-B Module to an E1 CSU (DB-15-to-Twinax Connectors)

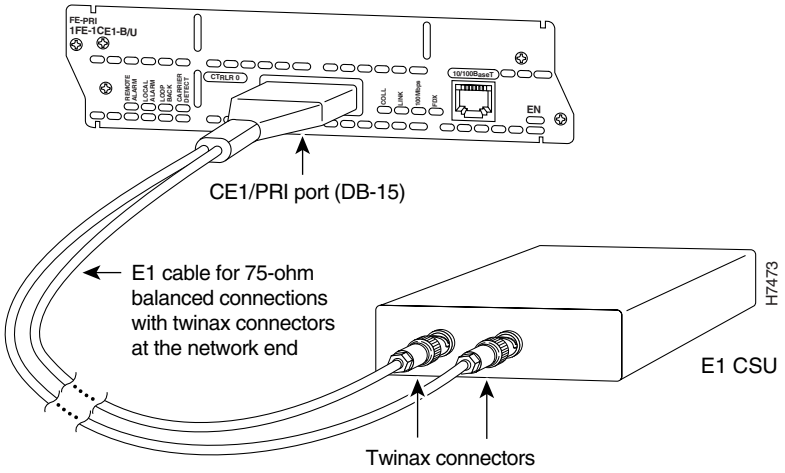
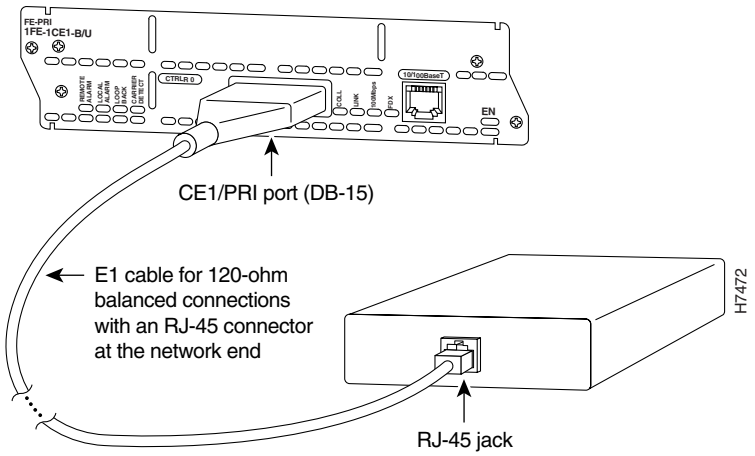


Figure 7-15 Connecting a 120-ohm CE1/PRI-B Module to an E1 CSU (DB-15-to-RJ-45 Connectors)



Channelized E1/ISDN PRI Unbalanced (75-Ohm) Network Modules

This section provides information about the following network modules for Cisco modular routers:

- 1-port channelized E1/ISDN PRI unbalanced (75-ohm) network module (NM-1CE1U or CPANM-1CE1U) (see Figure 7-16). This module is also referred to as the *1-port CE1/PRI-U network module*.
- 2-port channelized E1/ISDN PRI unbalanced (75-ohm) network module (NM-2CE1U or CPANM-2CE1U) (see Figure 7-17). This module is also referred to as the *2-port CE1/PRI-U network module*.

Figure 7-16 1-Port Channelized E1/ISDN PRI Network Module (Unbalanced)

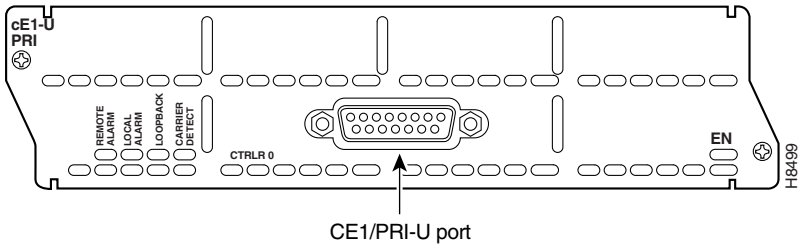
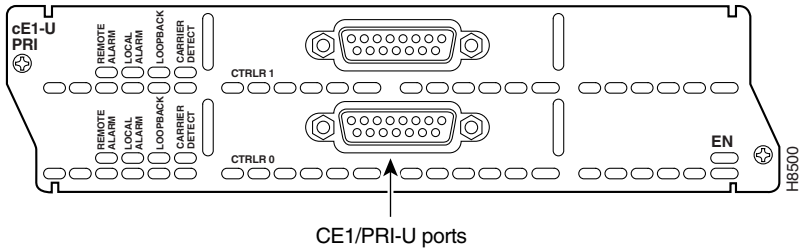


Figure 7-17 2-Port Channelized E1/ISDN PRI Network Module (Unbalanced)



CE1/PRI Module Jumper Settings

Jumpers on CE1/PRI modules can be used to connect or disconnect receive shield to ground (see Table 7-3). The default setting for balanced, 120-ohm CE1/PRI-B modules disconnects receive shield to ground. The default setting for unbalanced, 75-ohm CE1/PRI-U modules connects receive shield to ground. If you are experiencing ground loop problems with E1 cabling, you may want to try changing the jumper settings for the module.

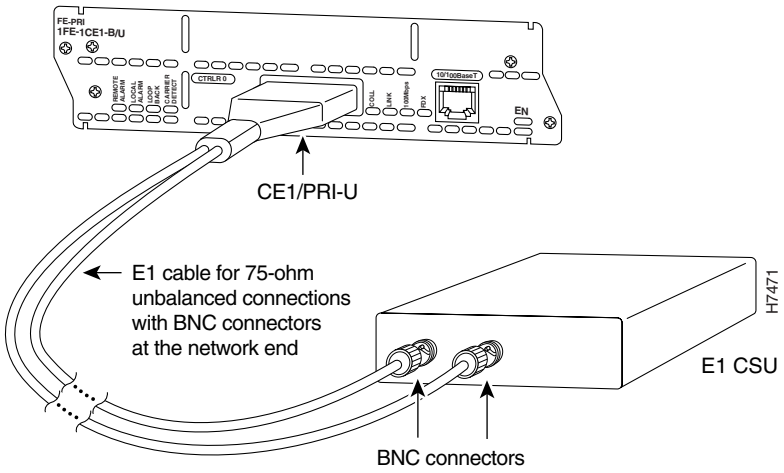
Table 7-3 CE1/PRI Module Jumpers

CE1/PRI Module Type	Default Setting	Function
Balanced, 120-ohm	2 and 3	Disconnects receive shield from ground
Unbalanced, 75-ohm	1 and 2	Connects receive shield to ground

Connecting CE1/PRI-U Modules to the Network

To connect a CE1/PRI-U (75-ohm) module to the network, use the appropriate cable to connect the CE1/PRI-U port to an E1 CSU (see Figure 7-18). These ports are color-coded tan. The illustration shows a CSU with BNC connectors.

Figure 7-18 Connecting a CE1/PRI-U Module to an E1 CSU (DB-15-to-BNC Connectors)



PRI Module LEDs

All network modules have an enable (EN) LED. This LED indicates that the module has passed its self-tests and is available to the router.

All PRI modules display four additional LEDs for each port. These LEDs are described in Table 7-4.

Table 7-4 ISDN PRI Network Module LEDs

LED	Meaning
RA	Local alarm at remote end of connection
LA	Loss of signal, loss of frame, or unavailability because of excessive errors
LP	Loopback mode
CD	Carrier received on telco link

Channelized T1/E1 PRI Network Module with G.703 LEDs

Figure 7-19 and Figure 7-20 show channelized T1/E1 PRI network module with G.703 LEDs. See Table 7-5 for LED definitions.

For LEDs found on all PRI network modules, see Table 7-4.

Figure 7-19 1-Port Channelized T1/E1 PRI Network Module with G.703 LEDs

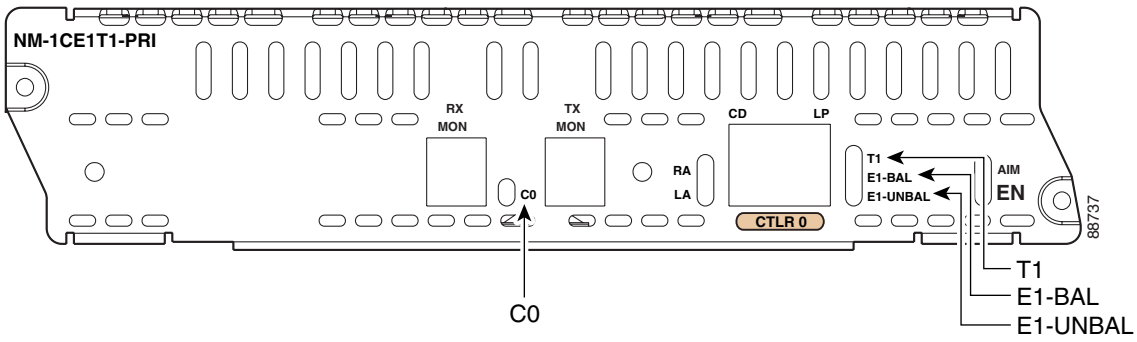


Figure 7-20 2-Port Channelized T1/E1 PRI Network Module with G.703 LEDs

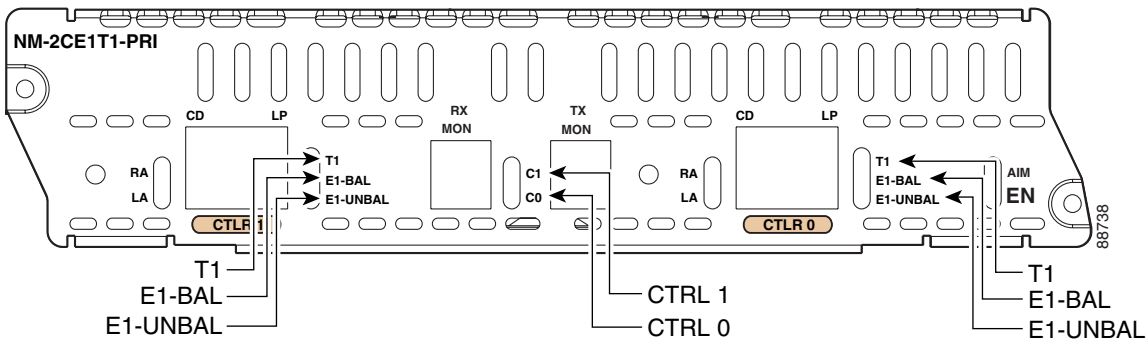


Table 7-5 Channelized T1/E1 PRI Network Module with G.703 LEDs

LED	Color	Meaning
T1	Green	Interface is configured for balanced T1.
E1-BAL	Green	Interface is configured for balanced E1.
E1-UNBAL	Green	Interface is configured for unbalanced E1.
C0	Green	Port 0 is connected to the bantam monitor connector.
C1	Green	Port 1 is connected to the bantam monitor connector.
AIM	Green	An advanced integration module (AIM) is installed on the network module.

CT1/PRI Network Module LEDs

Figure 7-21 and Figure 7-22 show CT1/PRI network module LEDs.

Figure 7-21 1-Port CT1/PRI Network Module LEDs

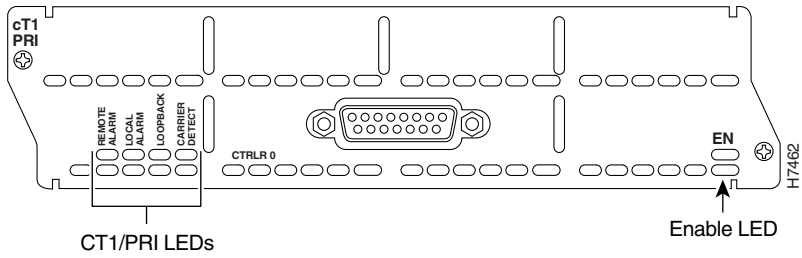
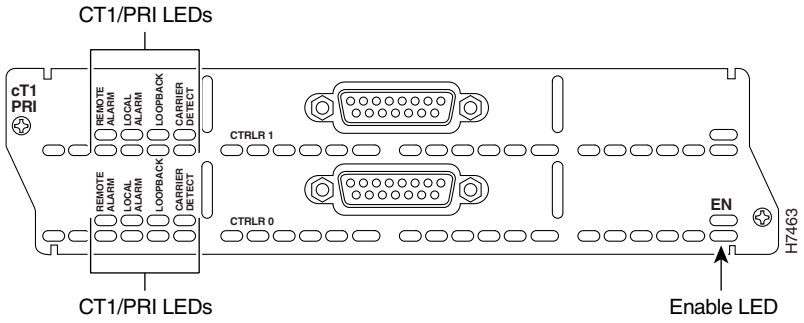


Figure 7-22 2-Port CT1/PRI Network Module LEDs



CT1/PRI CSU Network Module LEDs

Figure 7-23 and Figure 7-24 show CT1/PRI CSU module LEDs.

Figure 7-23 1-Port CT1/PRI CSU Network Module LEDs

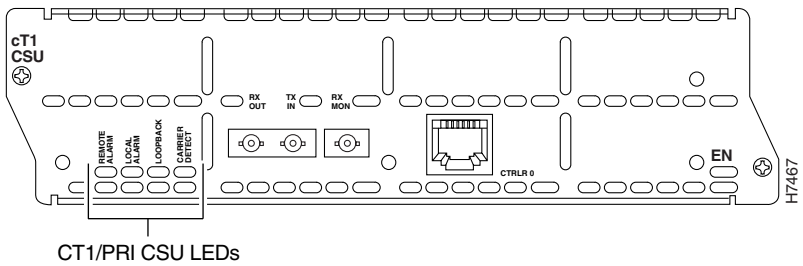
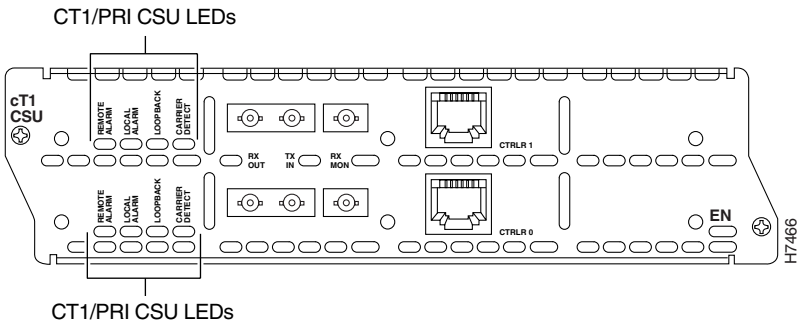


Figure 7-24 2-Port CT1/PRI CSU Network Module LEDs



CE1/PRI Network Module LEDs

Figure 7-25 and Figure 7-26 show CE1/PRI module LEDs. These LEDs are the same for balanced and unbalanced modules.

Figure 7-25 1-Port CE1/PRI Network Module LEDs

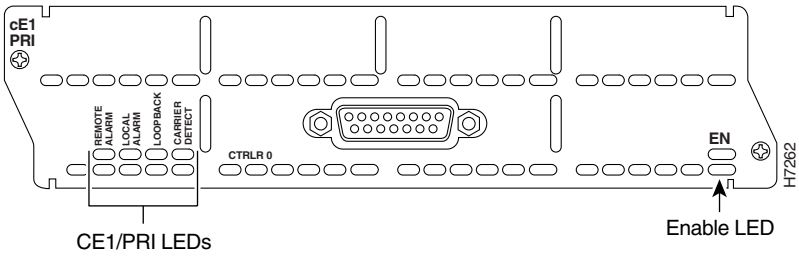
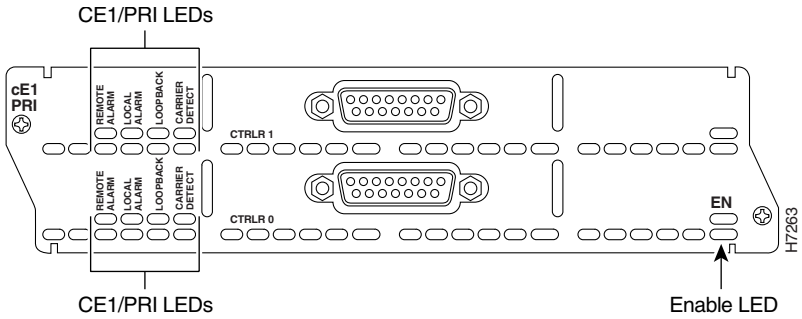


Figure 7-26 2-Port CE1/PRI Network Module LEDs



Online Insertion and Removal with a Cisco PRI Network Module (Cisco 3660 and Cisco 3745 Only)

Some Cisco modular access routers allow you to replace network modules without switching off the router or affecting the operation of other interfaces. This feature is called online insertion and removal (OIR). OIR of network modules provides uninterrupted operation to network users, maintains routing information, and ensures session preservation.

Note All Cisco PRI network modules have OIR support, but OIR is supported only on Cisco 3660 and Cisco 3745 platforms.

Caution Cisco routers support OIR with similar modules only. If you remove a network module, install another module exactly like it in its place. If you remove a network module with an installed interface card, expansion module, or AIM, the replacement module should have the same hardware installed.

For a description of informational and error messages that may appear on the console during this procedure, refer to the hardware installation guide for your type of router.

Upgrading ISDN PRI Network Modules

If your Cisco 3600 series router contains a legacy ISDN PRI network module and a digital modem network module (product numbers NM-6DM, NM-12DM, NM-18DM, NM-24DM, or NM-30DM), your ISDN PRI network module may need to be upgraded to revision level -03 or higher. Earlier revisions of ISDN PRI network modules cannot send modem calls to the digital modem network module.

Note Channelized T1/E1 PRI network modules with G.703 provide full support for Cisco digital modem network modules.

If your PRI module is the wrong revision, you see a message similar to the following message when the router boots:

```
The PRI network module in slot 0 is incompatible with the digital modems installed in the
router.
```

To determine the revision level, you can examine the network module itself (outside the router) or use the Cisco IOS **show diag** command. The label on the module board should show a part number beginning with 800- and ending with the revision level.

The output of the **show diag** command looks similar to the following:

```
Port adapter is analyzed
Port adapter insertion time unknown
Hardware revision 1.0           Board revision A0
Serial number     4152626       Part number    800-01236-01
Test history      0x0           RMA number     00-00-00
EEPROM format version 1
EEPROM contents (hex):
   0x20: 01 26 01 00 00 3F 5D 32 50 04 CC 01 00 00 00 00
   0x30: 50 00 00 00 96 11 04 17 FF FF FF FF FF FF FF FF
```

CHAPTER 8

Connecting Voice Network Modules

The voice functionality built into Cisco IOS software enables modular access routers to carry voice traffic, such as telephone calls and faxes, as Voice over IP (VoIP) simultaneously with data traffic over LANs, MANs, and WANs. Voice network modules convert telephone voice signals into a form that can be transmitted over an IP network.

Voice network modules convert telephone voice signals into a form that can be transmitted over an IP network. These modules have one or two slots for installing supported interface cards (see Table 1-1 on page 1-5 and Table 1-2 on page 1-8). Voice interface cards (VICs) or voice/WAN interface cards (VWICs) installed in the voice network module provide physical connections to the telephony equipment or network, and are connected using the appropriate cables. See the *Cisco Interface Cards Hardware Installation Guide* for more information.

You can install one voice interface card in a 1-slot voice network module, and two voice interface cards in a 2-slot module. For information on installing voice interface cards into a network module, see the "Installing Cisco Interface Cards in 1- or 2-Slot Network Modules" section on page 2-24.

This chapter contains the following sections:

Tip To determine whether your router supports a specific network module, see Table 1-6 on page 1-16.

2- and 4-Channel Voice Network Modules

This section describes the following modules:

- 1-slot 2-channel voice network module (NM-1V) (see Figure 8-1)
- 2-slot 4-channel voice network module (NM-2V) (see Figure 8-2)

For information on the Cisco interface cards supported on these voice network modules, see Table 1-2 on page 1-8.

Figure 8-1 1-Slot 2-Channel Voice Network Module (NM-1V)

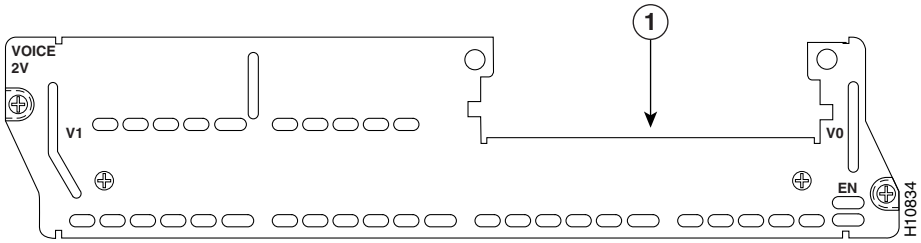
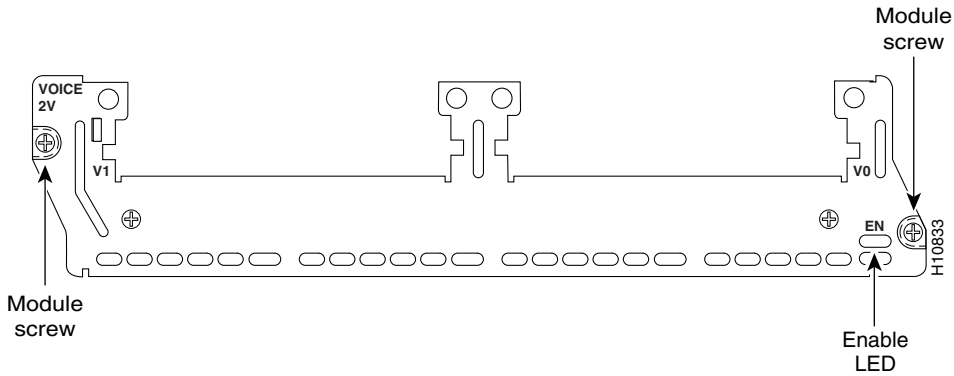


Figure 8-2 2-Slot 4-Channel Voice Network Module (NM-2V)



4-, 8-, and 48-Channel High-Density Voice Network Modules

This section describes the following modules:

- 1-slot 4-channel high-density voice network module with one digital signal processor (DSP) (NM-HD-1V) (see Figure 8-3)
- 2-slot 8-channel high-density voice network module with one DSP (NM-HD-2V) (see Figure 8-4)
- 2-slot 48-channel high-density enhanced network module with 3 DSPs, supporting up to 8 analog or 48 digital channels (NM-HD-2VE) (see Figure 8-5)

Caution To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the 2-slot 48-channel high-density enhanced network module (NM-HD-2VE) only to intrabuilding or nonexposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

Note For the NM-HD-1V, NM-HD-2V, and NM-DS-2VE network modules, DSPs are on-board and are not field-replaceable units (FRUs).

Note The NM-HD-1V, NM-HD-2V, and NM-HD-2VE network modules replace the NM-1V and NM-2V network modules. The NM-1V and NM-2V network modules are still available for use on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

For information on the Cisco interface cards supported on these voice network modules, see Table 1-2 on page 1-8.

Figure 8-3 1-Slot 4-Channel High-Density Network Module (NM-HD-1V)

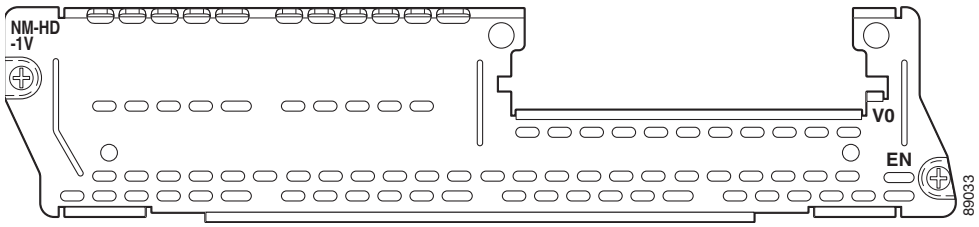


Figure 8-4 2-Slot 8-Channel High-Density Voice Network Module (NM-HD-2V)

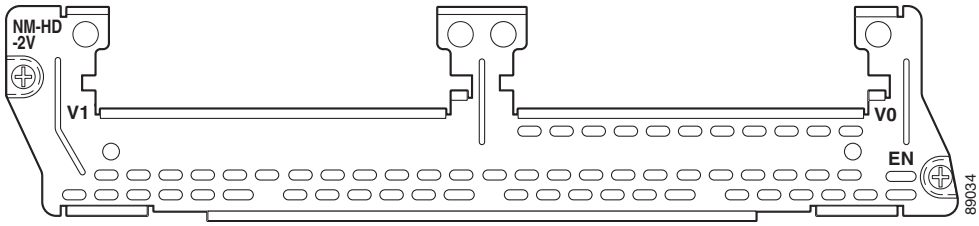
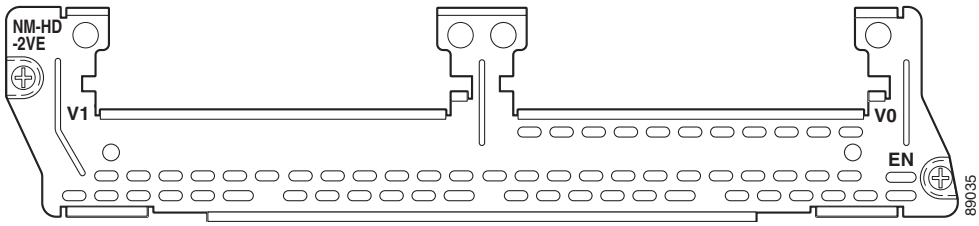


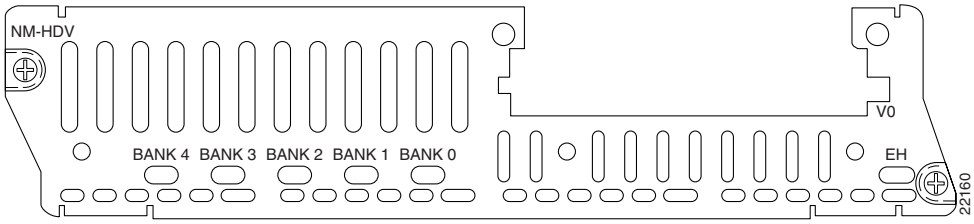
Figure 8-5 2-Slot 48-Channel High-Density Voice Network Module (NM-HD-2VE)



60-Channel High-Density Voice Network Module

This section describes the 60-channel high-density voice (HDV) network module, shown in Figure 8-6. When used in conjunction with T1/E1 multiflex trunk interface cards and packet voice digital signal processor modules (PVDMs), this module is also called a *digital T1/E1 packet voice trunk network module*.

Figure 8-6 60-Channel High-Density Voice Network Module (NM-HDV)



The 60-channel HDV network module converts voice and fax into IP packets or frames that can be transmitted as VoIP over a variety of transport technologies (channelized T1/E1, Frame Relay, Asynchronous Transfer Mode (ATM), and others). The number of channels supported depends on the number of PVDMs installed:

- Up to 6 channels per PVDM (30 channels for cards with 5 PVDMs) for high-complexity vocoders that support the following compression algorithms: G.711, G.726, G.729, G.723.1, G.728, and Fax Relay
- Up to 12 channels per PVDM (60 channels for cards with 5 PVDMs) for medium-complexity vocoders that support the following compression algorithms: G.711, G.726, G.729a, and Fax Relay

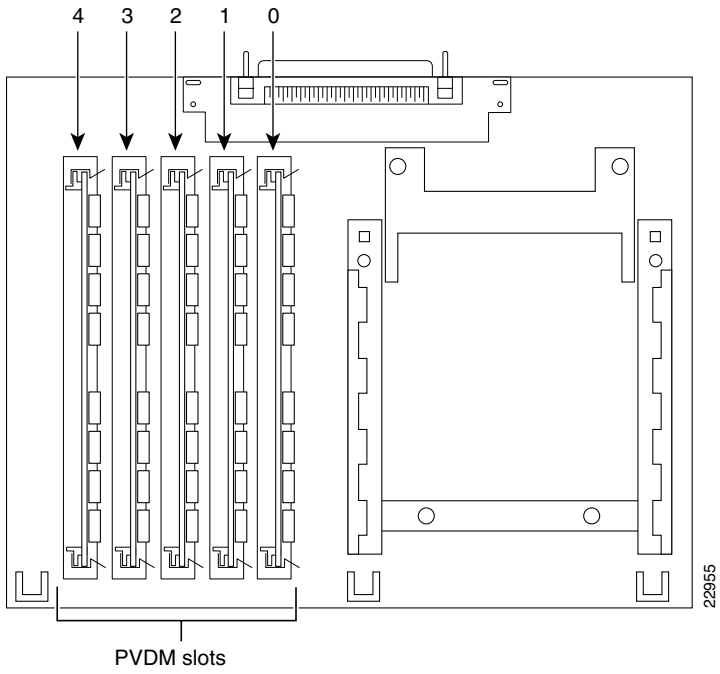
Both a 60-channel HDV network module and a voice interface card (VIC) are required to connect to the public switched telephone network (PSTN) or a PBX. One VIC (providing one or two T1/E1 line interfaces) can be installed in the HDV network module. Currently, only the 1- and 2-port T1/E1 multiflex trunk interface cards (VWIC-1MFT-T1, VWIC-2MFT-T1, and VWIC-2MFT-T1-DI) are supported using channel-associated signaling (CAS). In Cisco 3620 and Cisco 3640 routers, at least one other network module or WAN interface card (WIC) must be installed in the router to provide the connection to the IP LAN or WAN. In Cisco 3660 routers, a network module is required for WAN access or a direct connection is required for LAN access. In Cisco 2600 series routers, a WIC is required for WAN access or a direct connection is required for LAN access.

Packet Voice DSP Modules

The HDV network module contains five 72-pin SIMM sockets or banks for packet voice DSP modules (PVDMs), numbered 0 through 4. (See Figure 8-7.) Each socket can be filled with a single 72-pin PVDM. The PVDMs must be installed starting from slot 0.

Note PVDM and PVDM2 modules are not interchangeable. Use PVDM modules with the NM-HDV network module only, and use PVDM2 modules with the NM-HDV2 network module only.

Figure 8-7 PVDM Slot Locations

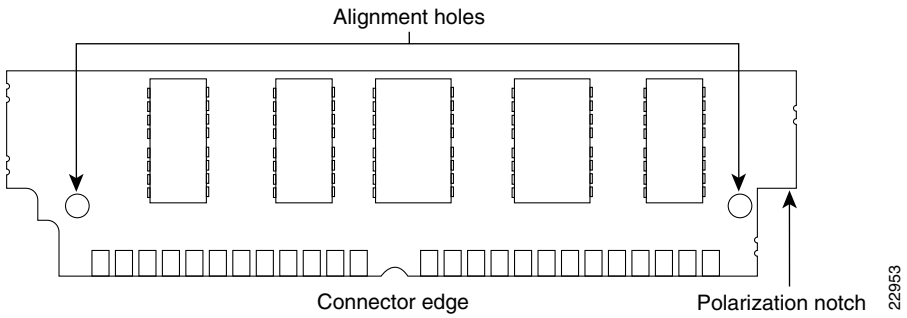


PVDM Orientation

PVDMs are manufactured with a polarization notch to ensure proper orientation and alignment holes to ensure proper positioning. Figure 8-8 shows the polarization notch and alignment holes on a PVDM card. PVDM cards are installed with the connector edge down, the polarization notch near the front of the chassis, and the component side facing the right side of the chassis.

Caution To avoid damaging ESD-sensitive components, observe all ESD precautions. To avoid damaging the HDV network module, avoid using excessive force when you remove or replace PVDMs.

Figure 8-8 PVDM Orientation



Removing PVDMs

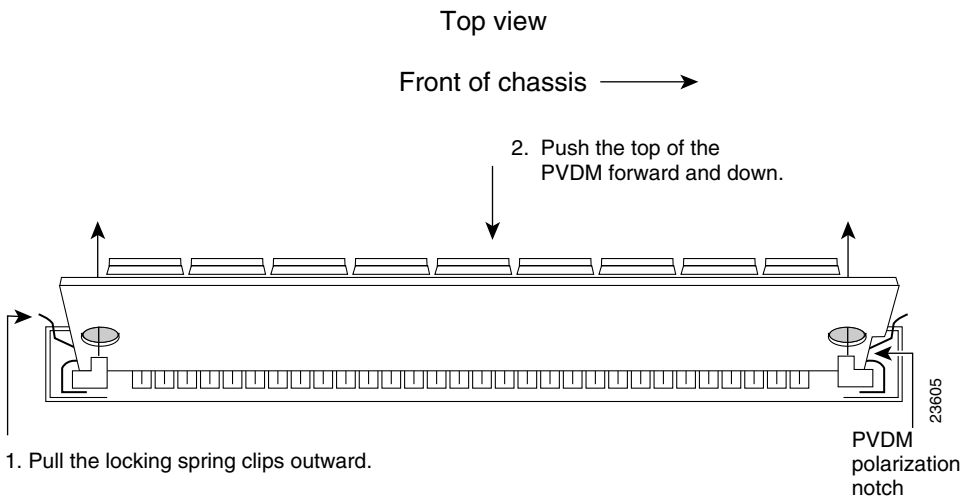
To remove PVDMs, follow these steps:

Step 1 Find the PVDM sockets on the HDV network module. (See Figure 8-7.)

Caution Handle PVDMs by the card edges only. PVDMs are ESD-sensitive components and can be damaged by mishandling.

Step 2 Remove one PVDM at a time, beginning with the PVDM in bank 4. To lift the PVDM out of its socket, pull the locking spring clips on both sides outward and tilt the PVDM toward the right side of the chassis, free of the clips. (See Figure 8-9.)

Figure 8-9 Removing PVDMs



Step 3 Hold the PVDM by the edges with your thumb and index finger and lift it out of the socket. Place the removed PVDM in an antistatic bag to protect it from ESD damage.

Step 4 Repeat Step 2 and Step 3 for each PVDM.

Installing PVDMs

To install PVDMs, follow these steps:

Step 1 Find the PVDM sockets on the HDV network module. (See Figure 8-7.)

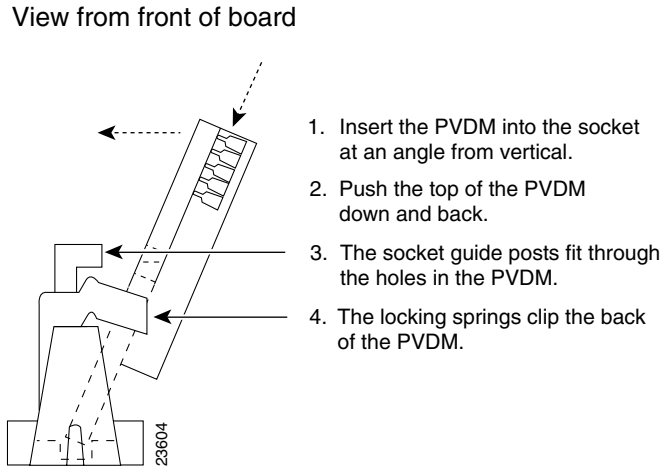
Caution Handle PVDMs by the card edges only. PVDMs are ESD-sensitive components and can be damaged by mishandling.

Step 2 Hold the PVDM with the polarization notch on the right, near the front of the chassis, and the component side away from you, with the connector edge at the bottom. (See Figure 8-8.)

Step 3 Beginning with bank 0, insert the PVDM into the connector slot at an angle, tilted toward the right side of the chassis. Align the PVDM in a vertical position (see Figure 8-10) by using the minimum amount of force required. When the PVDM is properly seated, the socket guide posts fit through the alignment holes, and the connector springs click into place.

Step 4 Ensure that each PVDM is straight and that the alignment holes (as shown in Figure 8-9) line up with the plastic guides on the socket.

Figure 8-10 Installing PVDMs



Caution It is normal to feel some resistance, but do not use excessive force on the PVDM and do not touch the surface components.

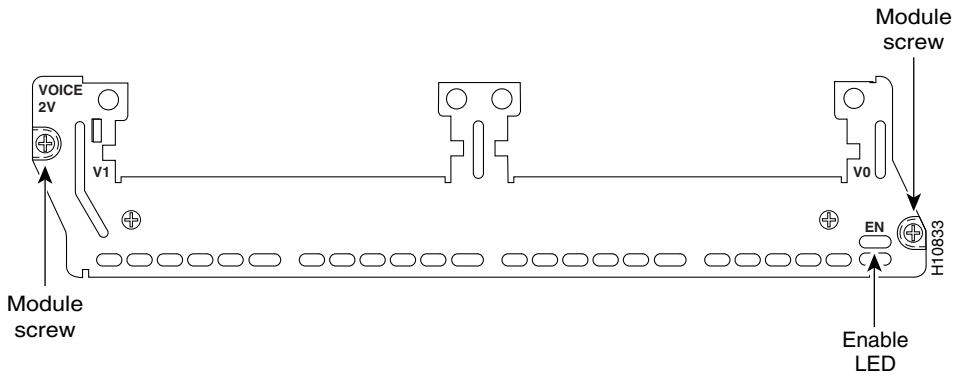
Step 5 Repeat Step 2 through Step 4 for each PVDM.

Voice Network Module LEDs

All network modules have an enable (EN) LED. This LED indicates that the module has passed its self-tests and is available to the router. The following network modules have no additional LEDs. (See Figure 8-11 for a sample faceplate.)

- NM-1V
- NM-2V
- NM-HD-1V
- NM-HD-2V
- NM-HD-2VE

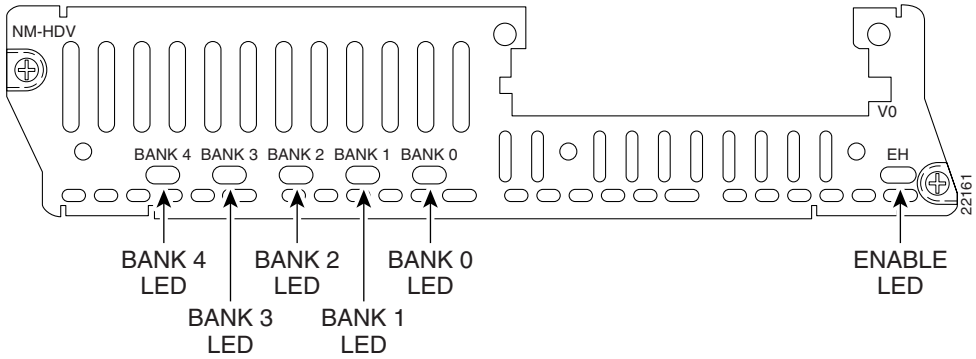
Figure 8-11 Voice Network Module LED



HDV Network Module LEDs

High-density network modules have an enable (EN) LED, and five LEDs for the PVDM banks, numbered 0 through 4. The enable LED indicates that the module has passed its self-tests and is available to the router. The BANK 0 through BANK 4 LEDs indicate the current operating condition of the PVDMs installed on the card. (See Figure 8-12.) If the BANK LEDs do not come on after initial installation and configuration, check that the PVDMs are properly seated in their slots.

Figure 8-12 HDV Network Module LEDs



IP Communications High-Density Digital Voice or Fax Network Module

This section describes the IP communications high-density digital voice or fax (NM-HDV2) network module. This module is available in three base-board stock-keeping units (SKUs):

- NM-HDV2, with no built-in T1/E1 ports, shown in Figure 8-13
- NM-HDV2-1T1/E1, with one built-in T1/E1 port, shown in Figure 8-14
- NM-HDV2-2T1/E1, with two built-in T1/E1 ports, shown in Figure 8-15

These three base-board SKUs also include a single VIC or VWIC slot for Foreign Exchange Station (FXS), Foreign Exchange Office (FXO) or centralized automated message accounting trunk protocol (CAMA), receive and transmit (E&M), Direct Inward Dial (DID), Basic Rate Interface (BRI), or E1/T1 interface cards.

Figure 8-13 NM-HDV2

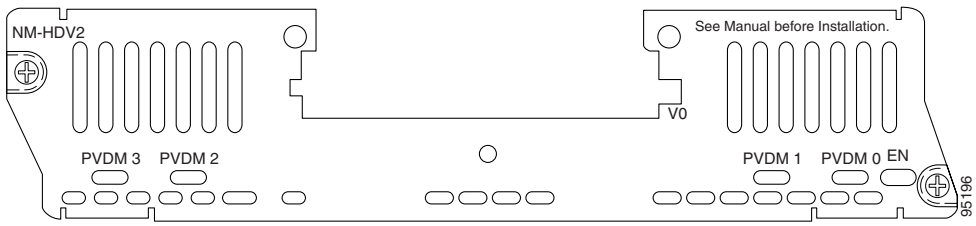


Figure 8-14 NM-HDV2-1T1/E1

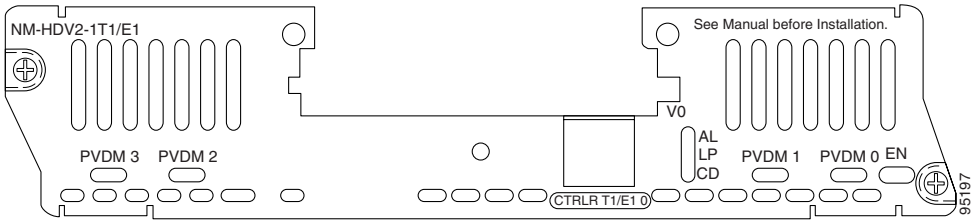
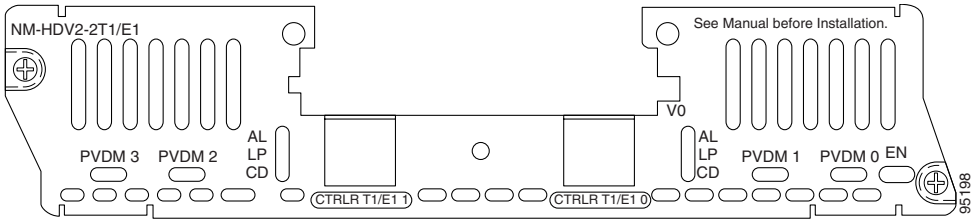


Figure 8-15 NM-HDV2-2T1/E1



The NM-HDV2 network module converts voice and fax into IP packets or frames that can be transmitted as VoIP over a variety of transport technologies (channelized T1, Frame Relay, Asynchronous Transfer Mode [ATM], and others).

Packet Fax or Voice DSP Modules

The packet fax or voice digital signal processor (DSP) module (PVDM2) is available in five stock-keeping units (SKUs):

Table 8-1 PVDM2 Module SKUs

Module Name	Description
PVDM2-8	8-channel packet fax or voice DSP module
PVDM2-16	16-channel packet fax or voice DSP module
PVDM2-32	32-channel packet fax or voice DSP module
PVDM2-48	48-channel packet fax or voice DSP module
PVDM2-64	64-channel packet fax or voice DSP module

You can install up to four PVDM2 modules on all of the NM-HDV2 SKUs. The number of channels supported depends on the number and density-type of PVDM2 modules installed.

Table 8-2 Channels Per PVDM2 Module Type

Module Name	Max Channels for High Complexity[1]	Max Channels for Medium Complexity[2]	Range of Channels for Flexi Complexity[3]
PVDM2-8	4	4	4-8
PVDM2-16	6	8	6-16

Table 8-2 Channels Per PVDM2 Module Type

Module Name	Max Channels for High Complexity[1]	Max Channels for Medium Complexity[2]	Range of Channels for Flexi Complexity[3]
PVDM2-32	12	16	12-32
PVDM2-48	18	24	18-48
PVDM2-64	24	32	24-64

1. High-complexity vocoders supported: G.711, G.726, G.729, G.723.1, G.728, and Fax Relay.
2. Medium-complexity vocoders supported: G.711, G.726, G.729a, and Fax Relay.
3. Flexi vocoders supported: G.711, G.726, G.729, G.723.1, G.728, and Fax Relay (number of channels depends on codec selected).

Note PVDM and PVDM2 modules are not interchangeable. Use PVDM modules with the NM-HDV network module only, and use PVDM2 modules with the NM-HDV2 network module only.

When used with PVDM2 modules and either the built-in T1/E1 ports or the T1/E1 voice or WAN interface cards (VWIC), the NM-HDV2 network module provides the interface to the PBX, the PSTN, or WAN. The following VWICs are supported:

- VWIC-1MFT-T1
- VWIC-2MFT-T1
- VWIC-2MFT-T1-DI
- VWIC-1MFT-E1
- VWIC-2MFT-E1
- VWIC-2MFT-E1-DI
- VWIC-1MFT-G703
- VWIC-2MFT-G703

When used with PVDM2 modules and next-generation analog or BRI voice interface cards (VIC2), the NM-HDV2 network module provides the interface to telephony equipment (PBX, key systems, telephones, and fax machines) and to the PSTN. The following VICs are supported:

- VIC-2DID
- VIC-1J1
- VIC-4FXS/DID (DID feature not supported)
- VIC2-2FXO
- VIC2-4FXO
- VIC2-2FXS
- VIC2-2E/M
- VIC2-2BRI-NT/TE

Configuring E1 Ports for Normal or Wetting Current Mode

On the NM-HDV2-1T1/E1 and NM-HDV2-2T1/E1 network modules there is a jumper block for each built-in T1/E1 port that controls whether the port supports normal or wetting current mode. Wetting current is a small amount of electrical current (60 to 140 milliamps) sent from the central office to the card to prevent the corrosion of electrical contacts in the module's network connection. Depending on how your E1 line is provisioned, you might have to change the jumper setting on the network module to allow proper operation.

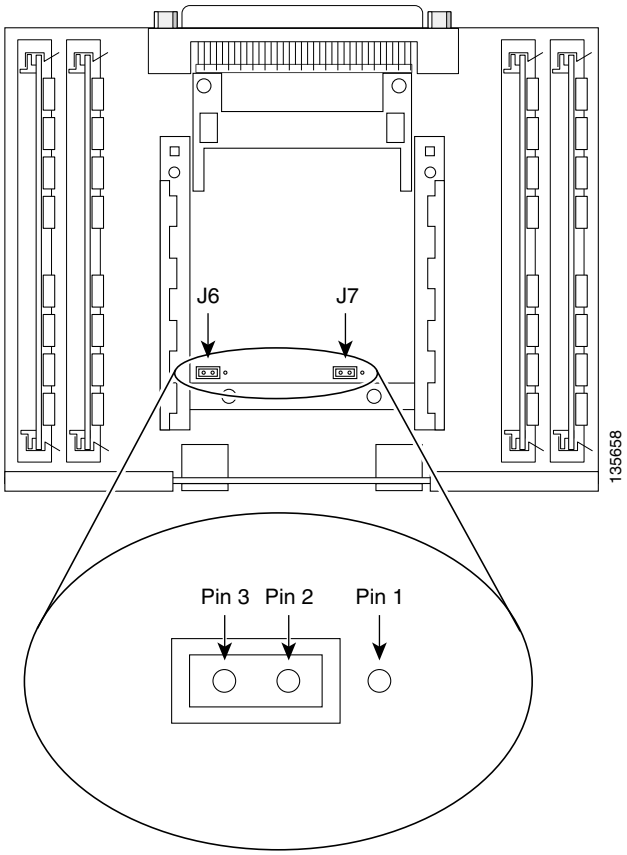
The jumper blocks are identified on the printed circuit board of the NM-HDV2-1T1/E1 and NM-HDV2-2T1/E1 network modules as J6 and J7. (See Figure 8-16.) J6 is the jumper block for T1/E1 controller 1 and J7 is the jumper block for T1/E1 controller 0. The pins on each jumper block are numbered 1 to 3 from right to left.

- To configure an E1 port for normal mode, set the jumper to pins 2 and 3.
- To configure an E1 port for wetting current mode, set the jumper to pins 1 and 2.

Figure 8-16 shows the jumper block configured for normal mode, with the jumper set to pins 2 and 3.

Tip If you are unsure whether your E1 line is configured for normal or wetting current mode, check with your provider. You can also use the **show controllers E1** command to look for line code violations and path code violations. These errors can indicate that the jumper is not set correctly.

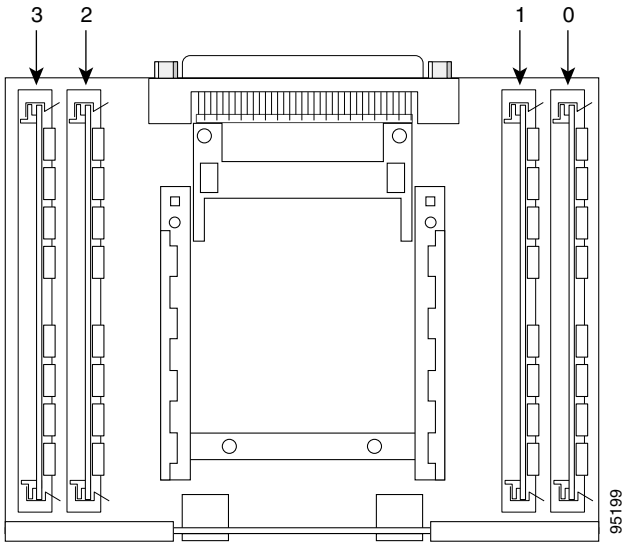
Figure 8-16 NM-HDV2-2T1/E1 Jumpers Configured for Normal Mode



Installing PVDM2 Modules

The NM-HDV2 network modules contain four 80-pin SIMM sockets for PVDM2 modules, numbered 0 through 3. (See Figure 8-17.) Each socket can be filled with a single 80-pin PVDM2 module.

Figure 8-17 PVDM2 Module Slot Locations

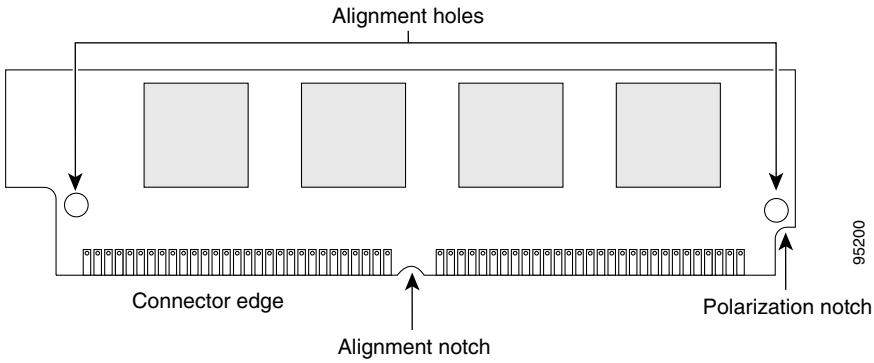


PVDM2 Module Orientation

PVDM2 modules are manufactured with a polarization notch to ensure proper orientation, and alignment holes to ensure proper positioning. Figure 8-18 shows the polarization notch and alignment holes on a PVDM2 module. PVDM2 modules are installed with the connector edge down, the polarization notch near the back of the chassis.

Caution To avoid damaging ESD-sensitive components, observe all ESD precautions. To avoid damaging the NM-HDV2 network module, avoid using excessive force when you remove or replace PVDM2 modules.

Figure 8-18 PVDM2 Module Orientation



Removing PVDM2 Modules

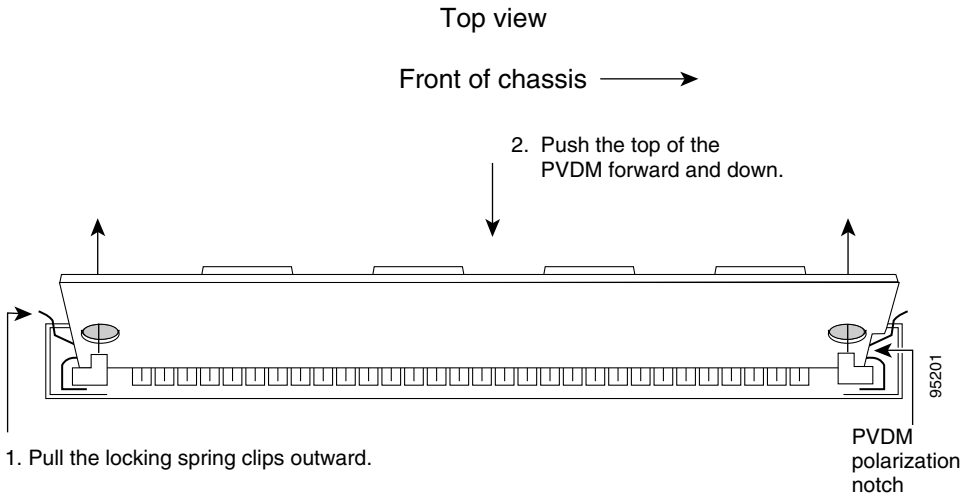
To remove PVDM2 modules, follow these steps:

Step 1 Find the PVDM2 sockets on the NM-HDV2 network module. (See Figure 8-17.)

Caution Handle PVDM2 modules by the card edges only. PVDM2 modules are ESD-sensitive components and can be damaged by mishandling.

Step 2 Remove one PVDM2 module at a time. To make your job easier, if you have a PVDM2 module in both socket 0 and socket 1, remove PVDM 1 before removing PVDM 0. Similarly, remove PVDM 3 before removing PVDM 2. To lift the PVDM2 module out of its socket, pull the locking spring clips on both sides outward and tilt the PVDM2 module toward the left side of the chassis, free of the clips. (See Figure 8-19.)

Figure 8-19 Removing PVDM2 Modules



Step 3 Hold the PVDM2 module by the edges with your thumb and index finger and lift it out of the socket. Place the removed PVDM2 module in an antistatic bag to protect it from ESD damage.

Step 4 Repeat Step 2 and Step 3 for each PVDM2 module.

Installing PVDM2 Modules

To install PVDM2 modules, follow these steps:

Step 1 Find the PVDM2 sockets on the NM-HDV2 network module. (See Figure 8-17.)

Caution Handle PVDM2 modules by the card edges only. PVDM2 modules are ESD-sensitive components and can be damaged by mishandling.

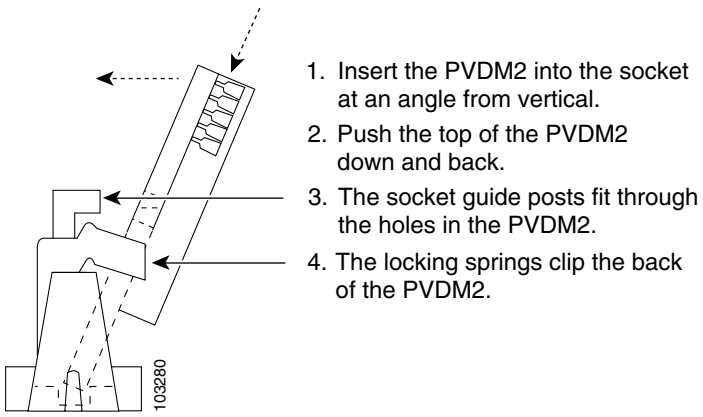
Step 2 Hold the PVDM2 module with the polarization notch on the right, near the back of the chassis, with the connector edge at the bottom. (See Figure 8-18.)

Step 3 Again, to make your job easier, begin with socket 0, then socket 1, or socket 2, then socket 3. Insert the PVDM2 module into the connector slot at an angle, tilted toward the left side of the chassis. Align the PVDM2 module in a vertical position (see Figure 8-20), by using the minimum amount of force required. When the PVDM2 module is properly seated, the socket guide posts fit through the alignment holes, and the connector springs click into place.

Step 4 Ensure that each PVDM2 module is straight and that the alignment holes (as shown in Figure 8-19) line up with the plastic guides on the socket.

Note Be sure to align the alignment notch in the bottom of the PVDM2 module with the rib in the 80-pin socket.

Figure 8-20 Installing PVDM2 Modules



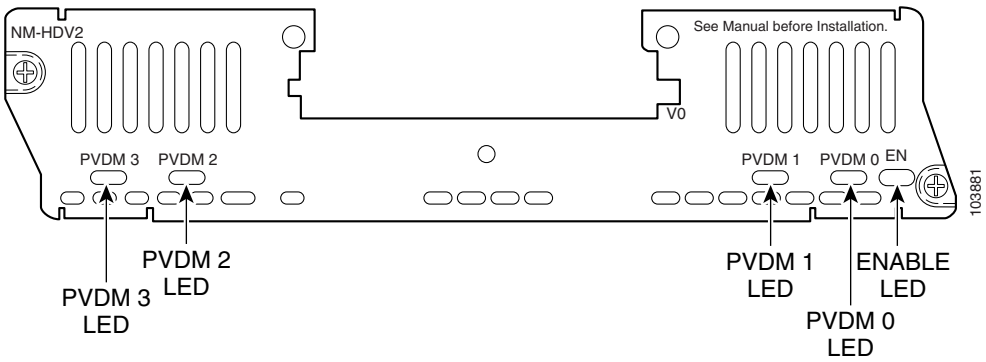
Caution It is normal to feel some resistance, but do not use excessive force on the PVDM2 module, and do not touch the surface components.

Step 5 Repeat Step 2 through Step 4 for each PVDM2 module.

NM-HDV2 Network Module LEDs

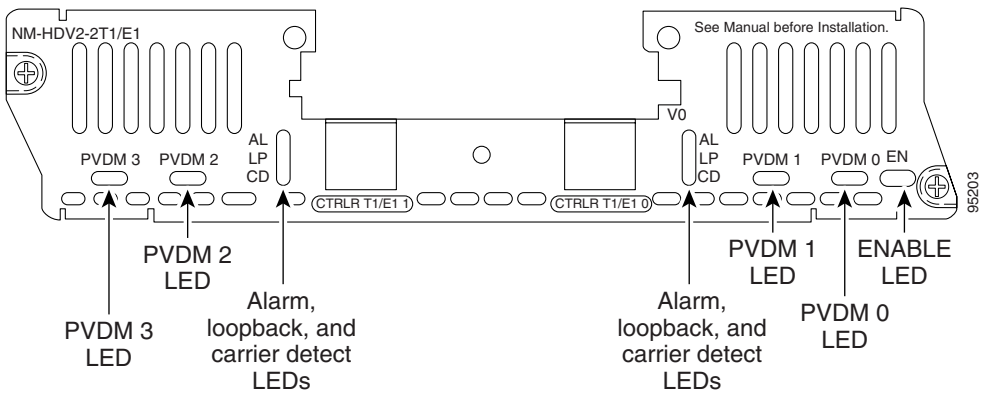
IP communications high-density digital voice or fax (NM-HDV2) network modules have an enable (EN) LED, and four LEDs for the PVDM2 modules, numbered 0 through 3. The enable LED indicates that the module has passed its self-tests and is available to the router. The PVDM 0 through PVDM 3 LEDs indicate the current operating condition of the PVDM2 modules installed on the card. (See Figure 8-21.) If the PVDM LEDs are not green after initial installation and configuration, check that the PVDM2 modules are properly seated in their slots.

Figure 8-21 NM-HDV2 Network Module LEDs



The NM-HDV2-1T1/E1 and NM-HDV2-2T1/E1 network modules have LEDs monitoring the alarm (AL), loopback (LP), and carrier detection (CD) conditions of the built-in T1/E1 ports. (See Figure 8-22.)

Figure 8-22 NM-HDV2-2T1/E1 LEDs



Connecting Digital Modem Network Modules

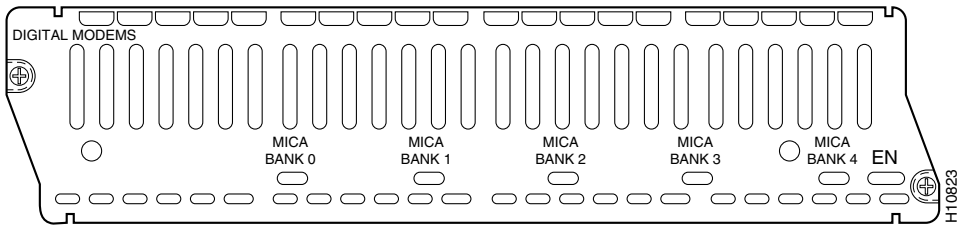
This chapter describes how to connect 6-, 12-, 18-, 24-, and 30-port digital modem network modules (NM-6DM, NM-12DM, NM-18DM, NM-24DM, and NM-30DM) for Cisco modular routers and contains the following sections:

Tip To determine whether your router supports a specific network module, see Table 1-6 on page 1-16.

Digital Network Modem Network Modules Overview

These modules (see Figure 9-1) contain 6, 12, 18, 24, or 30 V.34+ digital modems for a direct digital connection to an Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) or Basic Rate Interface (BRI) channel, allowing you to mix digital and analog calls to provide remote access to a LAN.

Figure 9-1 Digital Modem Network Module



Digital modem network modules do not provide network interfaces of their own, but instead handle analog calls passing through other router interfaces. In addition to the digital modem module, the router must contain a PRI or BRI interface to connect to the ISDN channel, and another interface, such as Ethernet, to provide connectivity to the LAN. The PRI or BRI module concurrently handles digital ISDN data connections and remote voice-channel (analog) modem connections, allowing a dynamic mix of digital and modem connections. The digital modem module acts as a pool of available modems that can be used for both incoming and outgoing calls.

The digital modems support all standard data rates from 300 bps through 33.6 kbps (V.34 bis); V.42 bis and MNP 5 data compression; and V.42, LAPM, and MNP 4 error correction.

Each digital modem module contains from one to five banks of 6-port modem ISDN channel aggregation (MICA) modules. You can add modems to a module, in groups of six, by installing additional MICA modules (Cisco product number MICA-6MOD), up to a maximum of 30 modems.

Hardware and Software Requirements

In addition to the digital modem module, the router must contain a PRI or BRI network interface to connect to the ISDN channel, and another interface, such as Ethernet or Fast Ethernet, to provide connectivity to the LAN.

A PRI network module (NM-1CT1, NM-2CT1, NM-1CT1-CSU, NM-2CT1-CSU, NM-1CE1B, NM-2CE1B, NM-1CE1U, or NM-2CE1U) used with a digital modem module must be revision level -03 or higher. A BRI S/T network module (NM-4B-S/T or NM-8B-S/T) must be revision level -03 or higher, and a BRI U module (NM-4B-U or NM-8B-U) must be revision level -06 or higher. Earlier revisions of these network modules cannot send modem calls to the digital modem module.

If the PRI or BRI module is the wrong revision, you see a message similar to this one when the router boots:

```
The T1 or E1 network module in slot 0 is incompatible with the digital modems installed in
the router.
```

To determine the revision level, you can examine the network module itself (outside the router), or use the Cisco IOS **show diag** command. The label on the module board should show a part number beginning with 800- and ending with the revision level. The output of the **show diag** command looks similar to the following:

```
Slot 3:
        Port adapter is analyzed
        Port adapter insertion time unknown
        Hardware revision 1.0           Board revision A0
        Serial number     4152626       Part number    800-01228-01
        Test history      0x0           RMA number     00-00-00
        EEPROM format version 1
        EEPROM contents (hex):
          0x20: 01 26 01 00 00 3F 5D 32 50 04 CC 01 00 00 00 00
          0x30: 50 00 00 00 96 11 04 17 FF FF FF FF FF FF FF FF
```

To order network module upgrades, see the "Obtaining Technical Assistance" section on page xi.

Interface Numbering

Individual digital modem ports are not physically distinct, but Cisco IOS software identifies each modem uniquely through its slot number and port number. Slot numbering is explained in the "Network Module Slot Locations and Numbering on Cisco Access Routers" section on page 1-3.

Each digital modem module can hold up to five banks of MICA modules, numbered 0 to 4 from left to right (as viewed from the rear of the router). Each MICA module holds six modems, which are assigned modem numbers 0 to 5.

Each modem in a digital modem module is also assigned a port number in the range 0 to 29. Modems in the left MICA module (as viewed from the rear of the router), bank 0, are assigned port numbers 0 to 5. Additional MICA modules, if present, are assigned port numbers as follows:

port-number = (6 x *bank-number*) + *modem-number*

For example, the third modem (modem 2) in the second MICA module from the left (bank 1) is assigned port number (6 x 1) + 2 = 8.

Some Cisco IOS commands identify ports by interface number (or line number or TTY number, which is the same as the interface number) rather than slot and port number. The interface number of a modem port is related to its slot and port number in the following way:

interface-number = (32 x *slot-number*) + *port-number* + 1

This can also be expressed as:

interface-number = (32 x *slot-number*) + ((6 x *bank-number*) + *modem-number*) + 1

For example, if the module containing the modem in the last example is placed in slot 2, the modem is assigned interface number (32 x 2) + ((6 x 1) + 2) + 1 = (32 x 2) + 8 + 1 = 73. This is also the line and TTY number for the port. The modem in this position is always assigned interface 73, whether or not there are other MICA modules in the digital modem network module or other digital modem network modules in the router chassis. If you move the MICA module to a different position in the digital modem network module, however, or move the digital modem network module to a different slot in the router chassis, the interface number changes.

Table 9-1 shows the range of interface numbers available in each router slot. Interface 0 is automatically assigned to the console.

Table 9-1 Digital Modem Network Module Interface Numbering

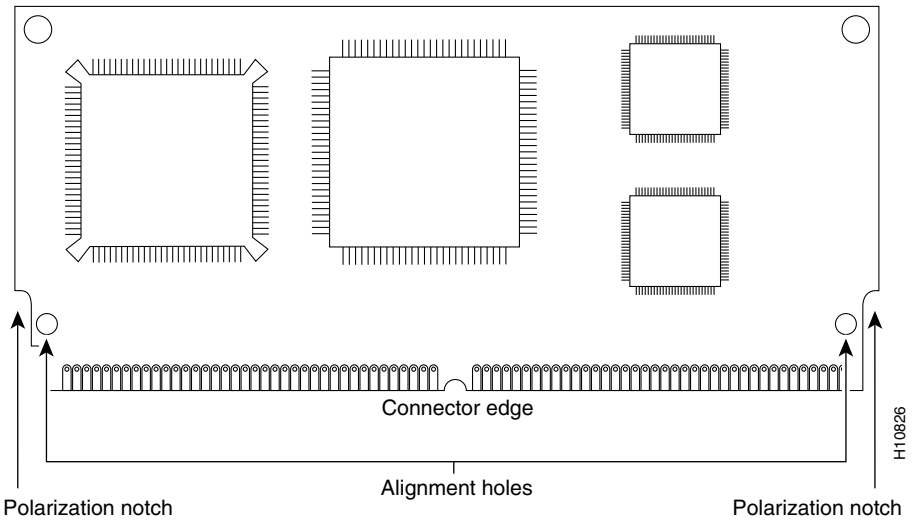
Slot Number	Interface Numbers
0	1–30
1	33–62
2	65–94
3	97–126
4	129–158
5	161–190
6	193–222

Adding 6-Port MICA Modules to a Digital Modem Network Module

You can add modems to a digital modem network module, in groups of six, by installing additional 6-port MICA modules, up to a maximum of five MICA modules (30 modems).

MICA modules are manufactured with a polarization notch to ensure proper orientation, and alignment holes that fit over guide posts to ensure proper positioning. (See Figure 9-2.)

Figure 9-2 6-Port MICA Module



Caution To avoid damaging electrostatic discharge (ESD)-sensitive components, observe all ESD precautions when handling MICA modules. To avoid damaging the network module or the MICA module, avoid excessive force when you remove or replace MICA modules.

To remove, replace, or install a MICA module, you must first remove the digital modem module from the router chassis.

Removing the Digital Modem Network Module

Caution Digital modem network modules do not currently support online insertion and removal (hot swap) of network modules. To avoid damaging the module, you must turn off electrical power and disconnect network cables before you remove it from the chassis slot.

To remove a digital modem network module, follow these steps:

Step 1 Turn off electrical power to the router. However, to channel ESD voltages to ground, do not unplug the power cable. Remove all network interface cables, including telephone cables, from the rear panel.

The following warning applies to routers that use a DC power supply:

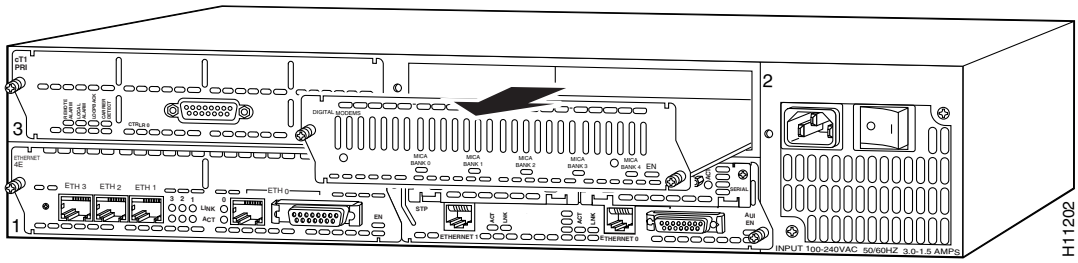
Warning **Before performing any of the following procedures, ensure that power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.** Statement 7

Step 2 Loosen the modules captive mounting screws, using a Phillips or flat-blade screwdriver.

Step 3 Hold the captive screws between two fingers, and pull the network module toward you until it slides free of the chassis. (See Figure 9-3.)

Step 4 Set the network module on an ESD-preventive mat.

Figure 9-3 Removing a Digital Modem Network Module from a Router



Removing 6-Port MICA Modules

To remove a MICA module from the digital modem network module, follow these steps:

Step 1 Orient the digital modem network module so that the faceplate is on the right.

Caution Handle MICA modules by the card edges only. MICA modules are ESD-sensitive components and can be damaged by mishandling.

Step 2 Remove one MICA module at a time, beginning with the one farthest from you.

Step 3 To lift the MICA module out of its socket, pull the spring clips on both sides outward (see Figure 9-4) and tilt the MICA module away from you until it is free of the clips (see Figure 9-5).

Step 4 Hold the MICA module by the edges with your thumb and index finger and lift it out of the socket (see Figure 9-6). Place the removed MICA module in an antistatic bag to protect it from ESD damage.

Step 5 Repeat Step 2 through Step 4 for any remaining MICA modules that you want to remove.

Figure 9-4 Releasing the Mounting Clips

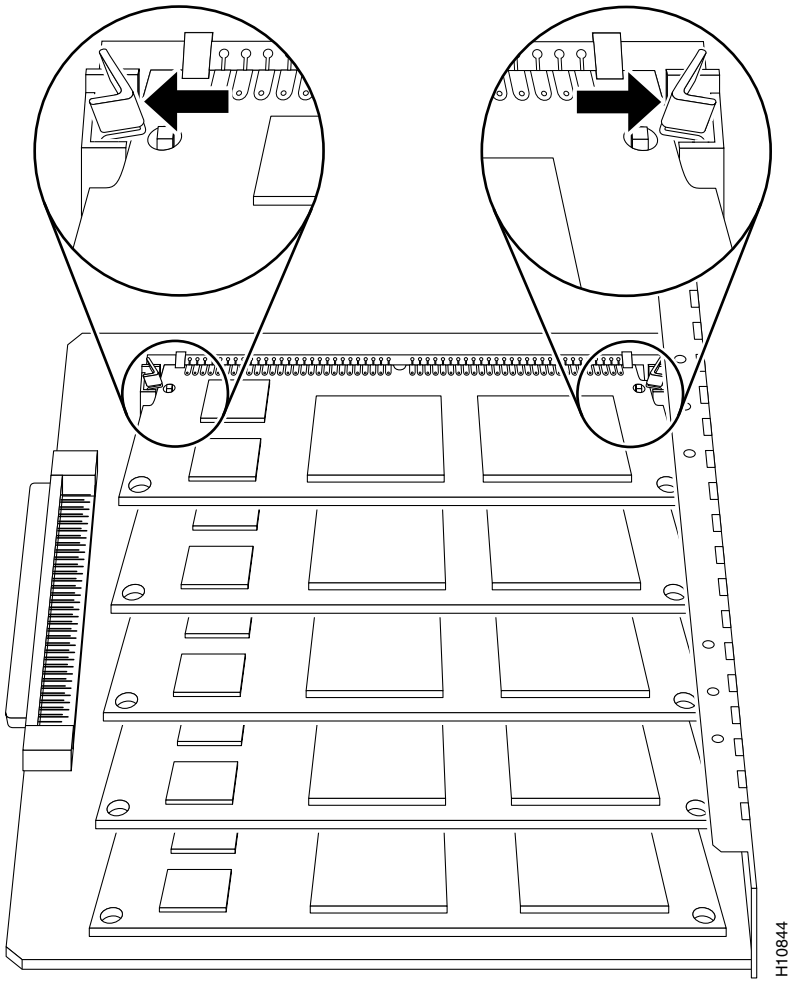


Figure 9-5 Tilting a 6-Port MICA Module Free of the Mounting Clips

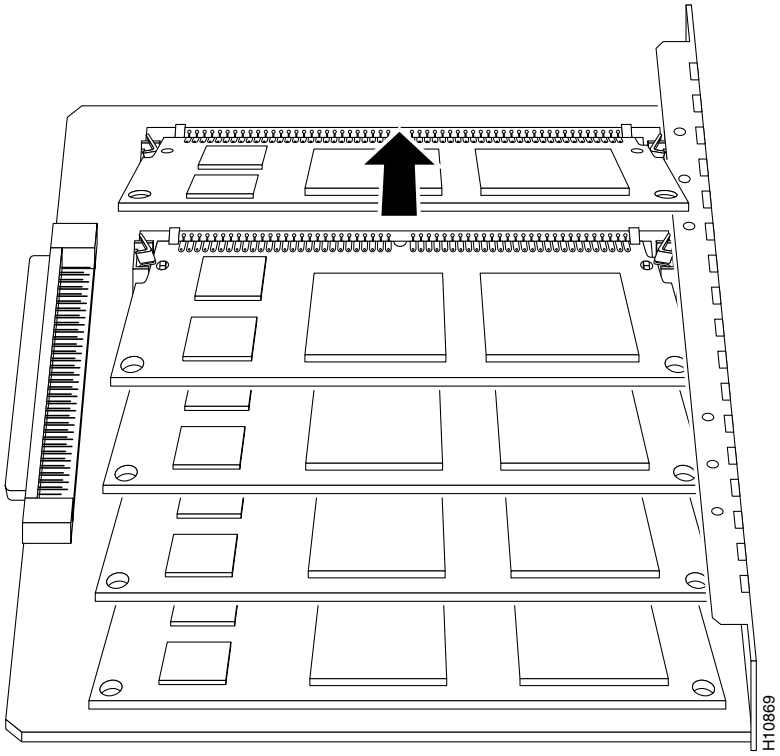
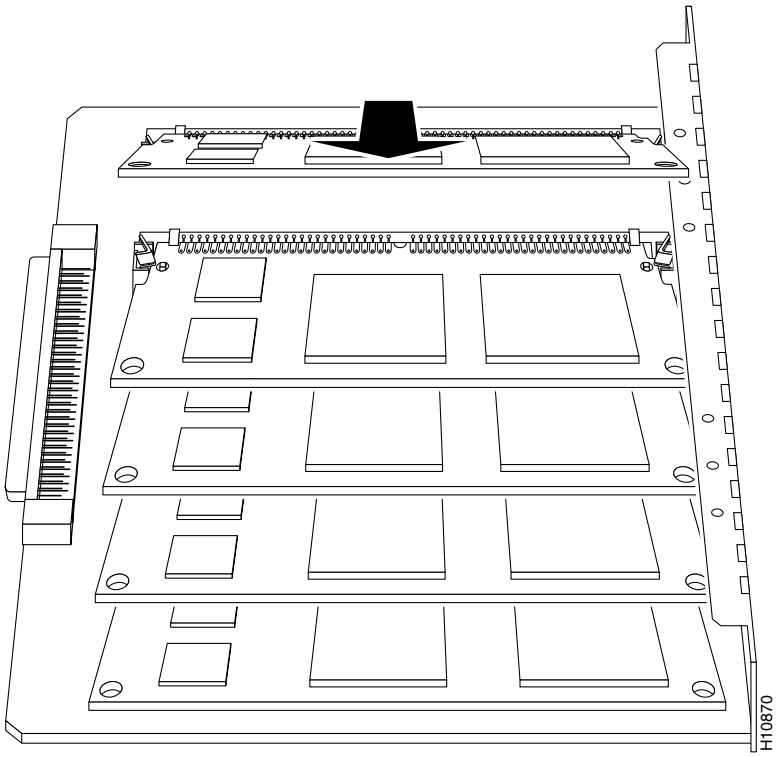


Figure 9-6 Lifting a 6-Port MICA Module Out of the Socket



Installing 6-Port MICA Modules

To install new or replacement MICA modules, follow these steps:

Step 1 Orient the digital modem network module so that the faceplate is on the right.

Caution Handle MICA modules by the card edges only. MICA modules are ESD-sensitive components and can be damaged by mishandling.

Step 2 Hold the MICA module with the connector edge at the bottom and the polarization notch at the right.

Step 3 Tilting the MICA module toward you at about a 45-degree angle, insert it into a socket, beginning with the empty socket closest to you. (See Figure 9-7.) Rock it downward, using the minimum amount of force required. (See Figure 9-8.) When the MICA module is properly seated, the socket guide posts fit through the alignment holes, and the spring clips click into place.

Step 4 Ensure that the MICA module is straight and that the alignment holes line up with the plastic guides on the socket. It is normal to feel some resistance, but do not use excessive force on the MICA module, and do not touch the surface components.

Step 5 Repeat Step 2 through Step 4 for any additional MICA modules.

Figure 9-7 Inserting a 6-Port MICA Module into a Socket

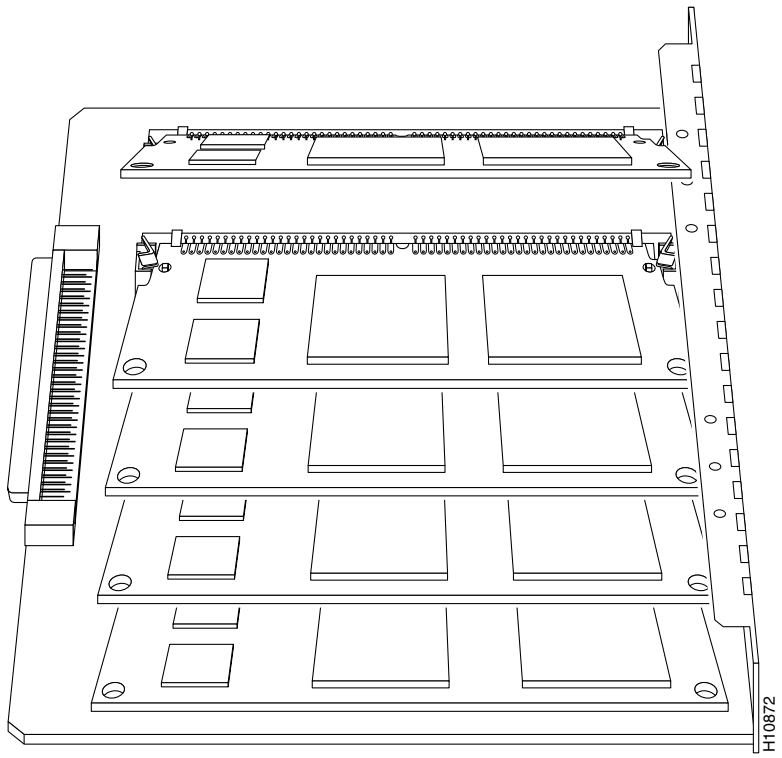
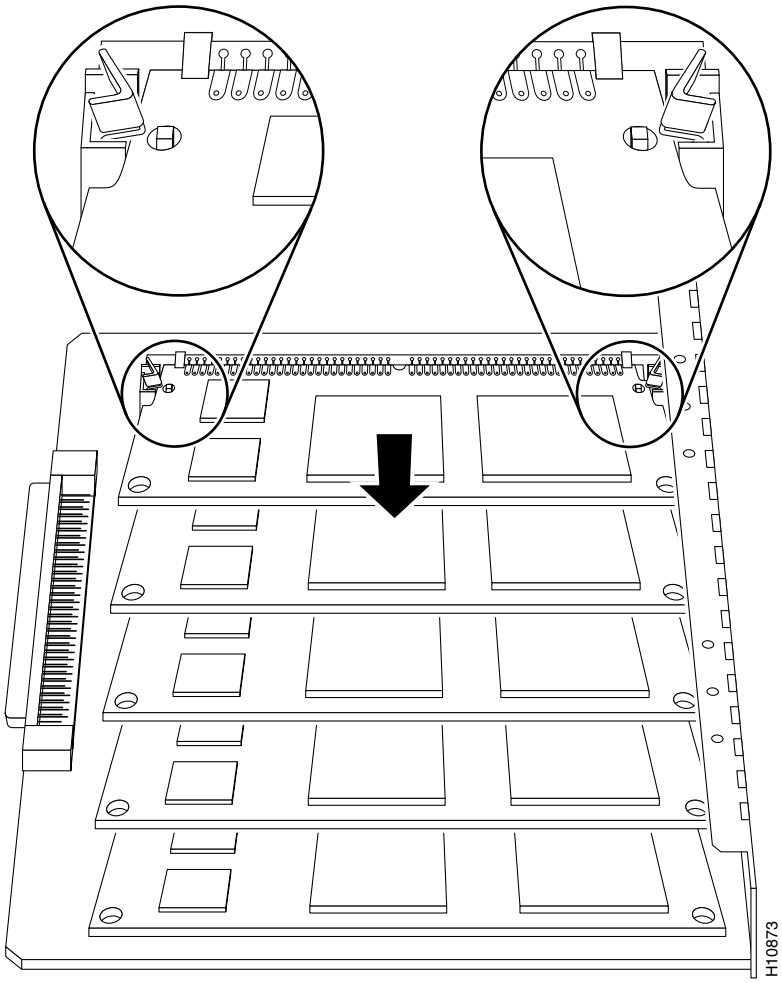


Figure 9-8 Rocking a 6-Port MICA Module Downward



Reinstalling the Digital Modem Network Module

When you finish installing MICA modules, replace the digital modem network module in the router chassis, following these steps:

Step 1 Align the network module with the guides in the chassis and slide it gently into the slot.

Step 2 Push the module into place until you feel its edge connector mate securely with the connector on the motherboard.

Step 3 Fasten the module captive mounting screws into the holes in the chassis, using the Phillips or flat-blade screwdriver.

Step 4 If the router was previously running, reinstall the network interface cables and turn on power to the router.

The following warning applies to routers that use a DC power supply:

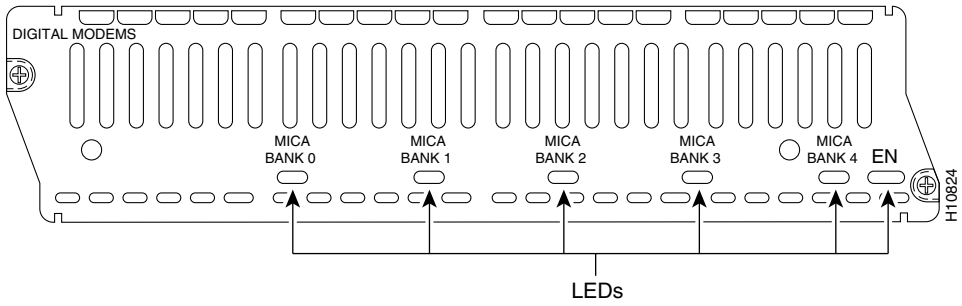
Warning **After wiring the DC power supply, remove the tape from the circuit breaker switch handle and reinstate power by moving the handle of the circuit breaker to the ON position.** Statement 8

Digital Modem Module LEDs

All network modules have an enable (EN) LED. (See Figure 9-9.) This LED indicates that the module has passed its self-tests and is available to the router.

Digital modem modules have five additional LEDs, one for each MICA module bank. The LEDs blink during initialization. After the enable LED comes on, the MICA module LEDs indicate that the corresponding MICA module is functioning. If a MICA module fails its diagnostics, or if no MICA module is installed in a position, its LED remains off.

Figure 9-9 Digital Modem Network Module LEDs



CHAPTER 10

Connecting Analog Modem Network Modules

This chapter describes 8- and 16-port analog modem network modules for Cisco modular routers. It contains the following sections:

Tip To determine whether your router supports a specific network module, see Table 1-6 on page 1-16.

8- and 16-Port Analog Modem Network Modules

The following analog modem network modules originate or terminate analog telephone transmissions through RJ-11 modular jacks:

- 8-port analog modem network module (NM-8AM) (see Figure 10-1)
- 16-port analog modem network module (NM-16AM) (see Figure 10-2)

Figure 10-1 8-Port Analog Modem Network Module

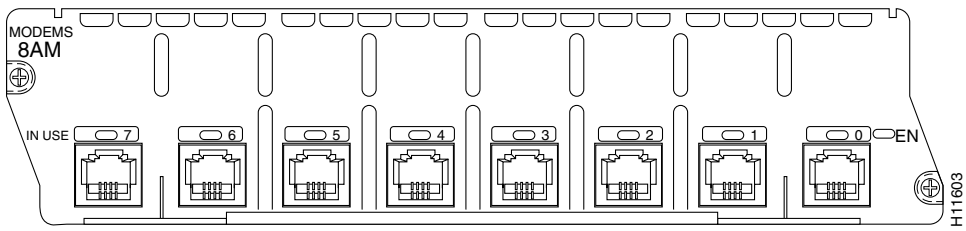
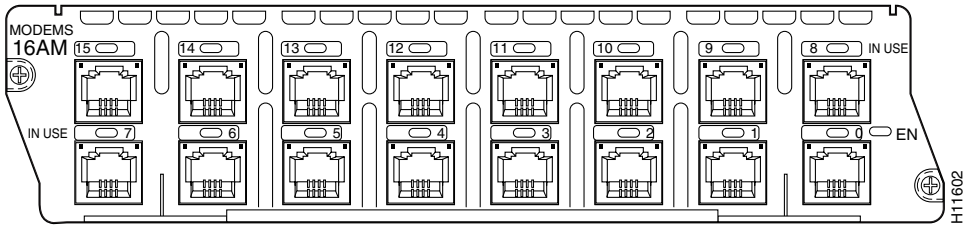


Figure 10-2 16-Port Analog Modem Network Module



The following warning applies in Australia:

Warning **This equipment will be inoperable when main power fails.**

The following warning applies in New Zealand:

Warning **This equipment does not fully meet Telecom's impedance requirements. Performance limitations may occur when used in conjunction with some parts of the network. Telecom will accept no responsibility should difficulties arise in such circumstances.**

Network Protocols Supported

The analog modems described in this chapter support the following protocols:

- All standard data rates from 300 bps to 33.6 kbps (V.34*bis*)
- V.42*bis* and Microcom Network Protocol (MNP) 5 data compression
- V.42, Link Access Procedure for Modems (LAPM), and MNP 2 to 4 error correction
- MNP 10 for high performance under all line conditions
- MNP 10EC for high performance in analog cellular environments

8- and 16-Port Analog Modem Network Modules, Version 2

The following analog modem network modules originate or terminate analog telephone transmissions through RJ-11 modular jacks:

- 8-port analog modem network module (NM-8AM-V2) (see Figure 10-3)
- 16-port analog modem network module (NM-16AM-V2) (see Figure 10-4)

Caution To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the 16-port analog modem network module (NM-16AM-V2) only to intra-building or non-exposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

Figure 10-3 8-Port Analog Modem Network Module (NM-8AM-V2)

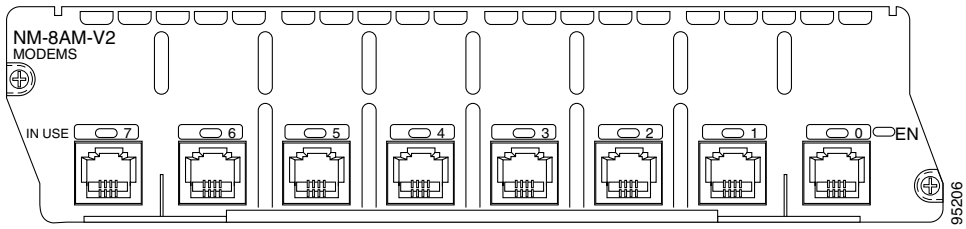
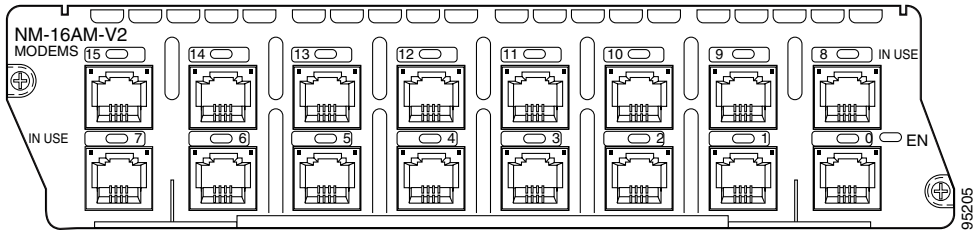


Figure 10-4 16-Port Analog Modem Network Module (NM-16AM-V2)



The following warning applies in Australia:

Warning **This equipment will be inoperable when main power fails.**

The following warning applies in New Zealand:

Warning **This equipment does not fully meet Telecom's impedance requirements. Performance limitations may occur when used in conjunction with some parts of the network. Telecom will accept no responsibility should difficulties arise in such circumstances.**

Network Protocols Supported

The analog modems described in this chapter support these protocols:

- Standardized modem protocols
  - ITU-T V.90
  - V.92 Quick Connect
  - ITU-T V.34bis
  - ITU-T V.34
  - ITU-T V.34+ up to 33,600 bps
  - ITU-T V.32*bis*
  - ITU-T V.32
  - ITU-T V.32 turbo up to 19,200 bps
  - ITU-T V.22*bis* (with V.54 loopback)
  - ITU-T V.22 A/B

  - ITU-T V.23 at 75 and 1200 bps
  - ITU-T V.21 at 300 bps
  - BELL 103 and 212a
- Standardized fax protocols
  - ITU-T V.17
  - ITU-T V.29
  - ITU-T V.27ter
  - ITU-T V.21 channel 2
  - EIA 578 Class 2
  - Group 3 fax class 1 and class 2
- Standardized modem error correction and compression
  - MNP 2 – 4
  - ITU-T V.42 Link Access Procedure for Modems (LAPM)
  - Microcom Network Protocol (MNP) 5
  - V.42bis (with 4-K dictionaries)
  - ITU-T V.44

Interface Numbering

Cisco IOS software identifies each modem uniquely by its slot number and port number.

Some Cisco IOS configuration commands identify asynchronous ports by an interface number (or a line number, which is the same as the interface number). The interface number of a port on an 8- or 16-port analog modem network module is related to the slot number where the module is installed and the number of the port in the module.

Ports in the 8- and 16-port analog modem network modules are numbered in the same pattern as slot numbers, beginning at 0 at the lower right and continuing from right to left and (in the 16-port module) from bottom to top.

The interface number of a port is determined in the following way:

interface-number = (32 x *slot-number*) + *port-number* + 1

For example, modem port 12 in slot 1 corresponds to interface number (32 x 1) + 12 + 1 = 45. This is also the line number for the port. Port 12 in slot 1 is always assigned interface number 45, regardless of whether the module in slot 0 is an 8-port analog modem network module, a 16-port analog modem module, or some other kind of module entirely, or even whether there is a network module in slot 0 at all. If you move the module from slot 1 to a different slot, however, its interface numbers change.

Table 10-1 shows the range of interface numbers available for each type of analog modem network module in each router slot. (Interface 0 is automatically assigned to the console.)

Table 10-1 16- and 32-Port Analog Module Interface Numbering

Slot Number	Interface Numbers (8-Port Module)	Interface Numbers (16-Port Module)
0	1–8	1–16
1	33–40	33–48

Table 10-1 16- and 32-Port Analog Module Interface Numbering

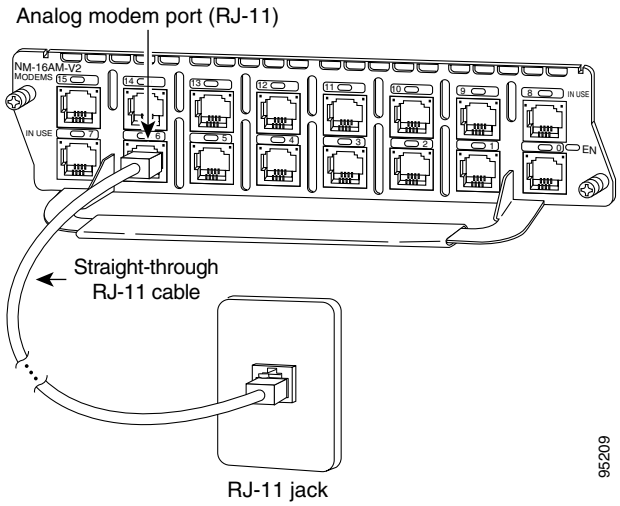
Slot Number	Interface Numbers (8-Port Module)	Interface Numbers (16-Port Module)
2	65–72	65–80
3	97–104	97–112
4	129–136	129–144
5	161–168	161–176
6	193–200	193–208

Connecting the Modules to the Telephone Network

Each analog modem network module provides 8 or 16 RJ-11 jacks for standard modular cables. These ports are color-coded pink. Cables are not provided with the network module.

To establish an analog connection, use a straight-through RJ-11 modular cable to connect the jack to a wall telephone outlet. (See Figure 10-5.)

Figure 10-5 Connecting an Analog Modem Network Module



Analog Modem Network Module LEDs

All network modules have an enable (EN) LED. This LED indicates that the module has passed its self-tests and is available.

Each modem in the module has an in use (IN USE) LED that lights when the modem is off-hook. (See Figure 10-6 and Figure 10-7.)

Figure 10-6 8-Port Analog Modem Network Module LEDs

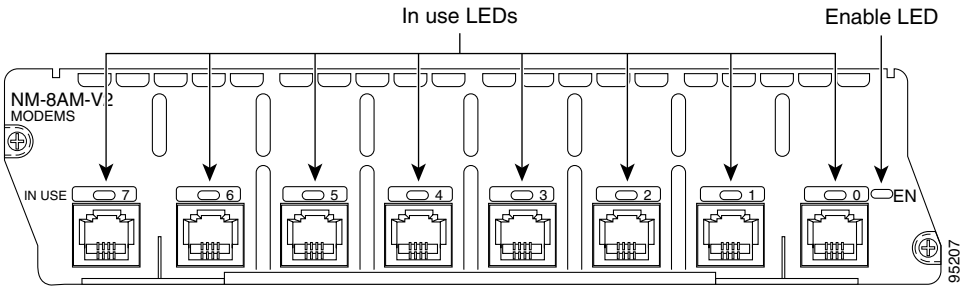
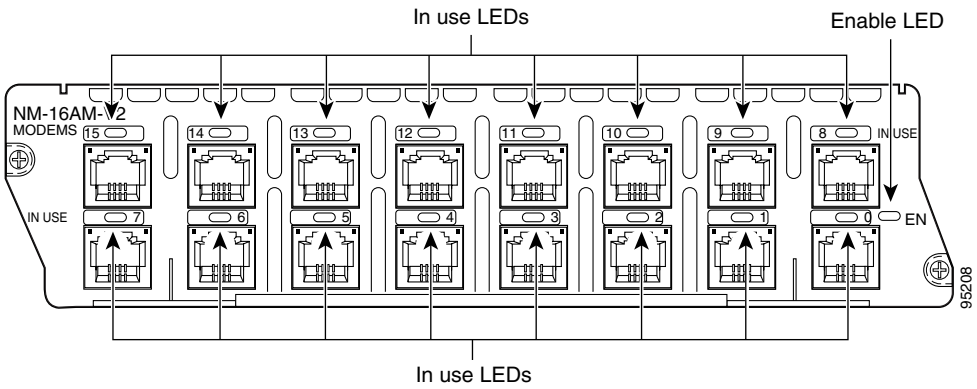


Figure 10-7 16-Port Analog Modem Network Module LEDs



CHAPTER 11

Connecting ATM Network Modules

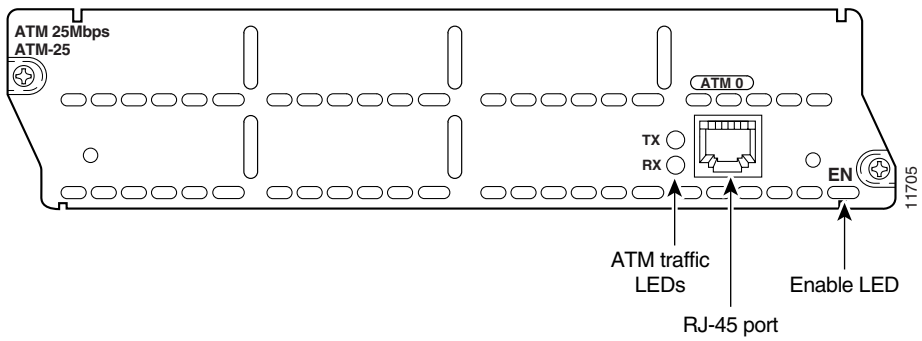
This chapter describes how to connect Asynchronous Transfer Mode (ATM) network modules for Cisco modular routers and contains the following sections:

Tip To determine whether your router supports a specific network module, see Table 1-6 on page 1-16.

ATM-25 Network Module

The ATM-25 network module (see Figure 11-1) provides ATM traffic shaping for use with asymmetric digital subscriber line (ADSL) uplink speeds, and protocol support for permanent virtual circuit (PVC) environments. The network module provides full support for multiprotocol encapsulation over ATM Adaptive Layer 5 (RFC 1483), classic IP over ATM encapsulation (RFC 1577), and Point-to-Point Protocol (PPP) over ATM.

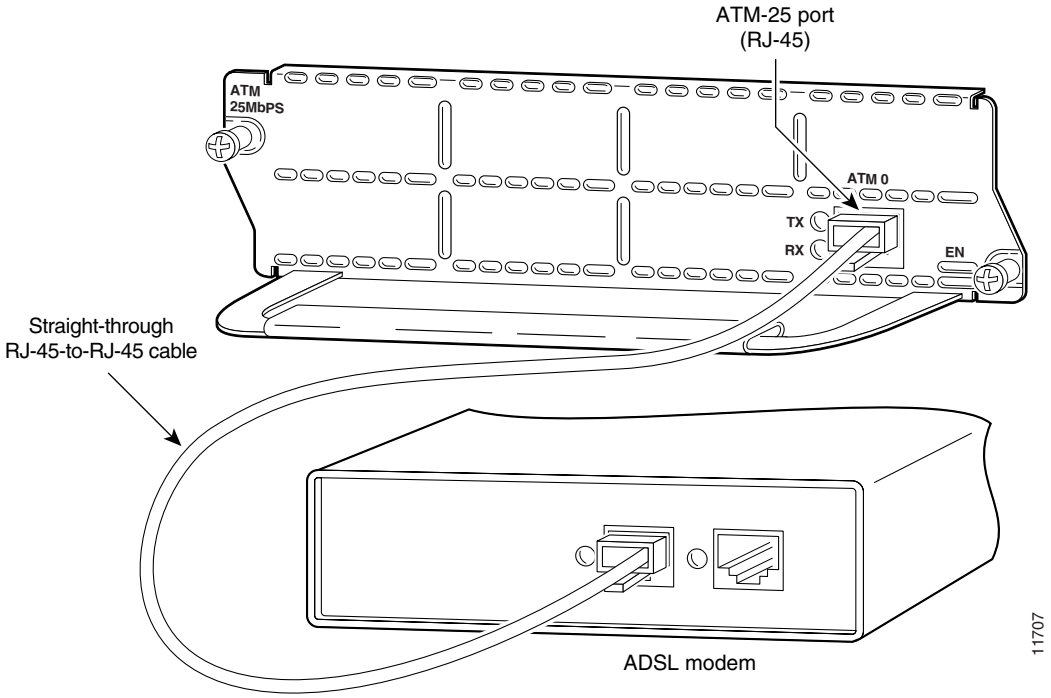
Figure 11-1 ATM-25 Network Module



Connecting ATM-25 Ports to the Network

The ATM-25 port is a standard RJ-45 jack, color-coded light green. Use a straight-through modular RJ-45 UTP Category 3, 4, or 5 cable or STP Category 1, 1A, 9, or 9A cable to connect the port to an external ADSL modem. See Figure 11-2.

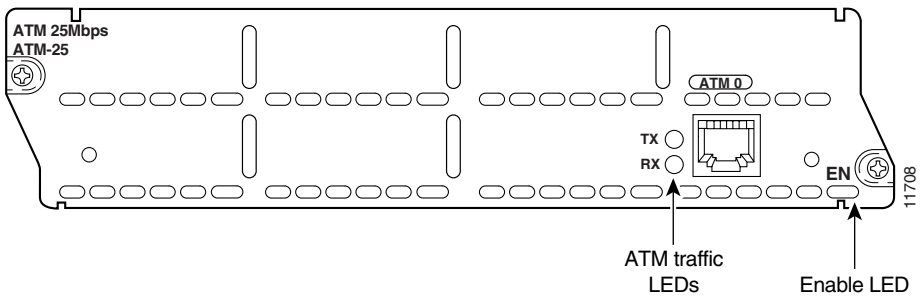
Figure 11-2 Connecting the ATM-25 Module to an ADSL Modem



ATM-25 Network Module LEDs

Figure 11-3 shows ATM-25 network module LEDs.

Figure 11-3 ATM-25 Network Module LEDs



All network modules have an enable (EN) LED. The enable LED indicates that the module has passed its self-tests and is available to the router. The ATM-25 network module has the additional LEDs shown in Table 11-1.

Table 11-1 ATM-25 Network Module LEDs

LED	Meaning
RX	Module is receiving ATM traffic
TX	Module is transmitting ATM traffic

ATM T3 and E3 Network Modules

ATM T3 and E3 network modules provide T3 and E3 ATM connectivity for high-bandwidth data applications. There are three versions of these network modules: the ATM T3 Network Module, the ATM E3 Network Module, and the ATM T3/E3 Network Module. See Figure 11-4, Figure 11-5 and Figure 11-6. These network modules offer full support for multiprotocol encapsulation over ATM Adaptive Layer 5 (RFC 1483), classic IP over ATM encapsulation (RFC 1577), Point-to-Point Protocol (PPP) over ATM, and LAN Emulation (LANE). Up to 1024 virtual circuits (VCs) are supported on the ATM T3/E3 network modules.

Figure 11-4 ATM Network Module with T3 Interface

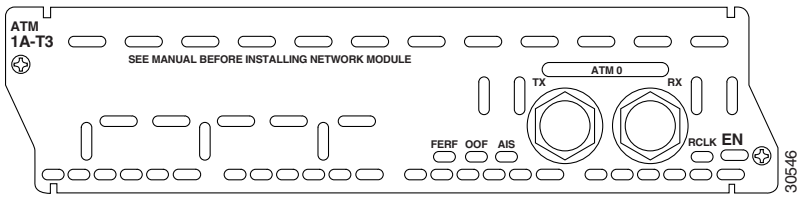


Figure 11-5 ATM Network Module with E3 Interface

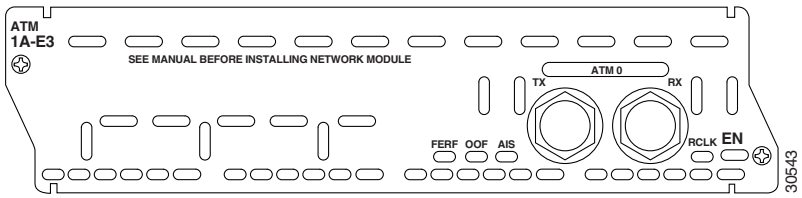
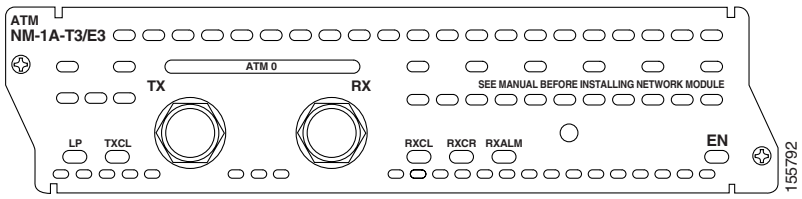


Figure 11-6 ATM Network Module with one T3/E3 Interface



Note The ATM T3 network module has a sensitive receiver. If you use a short T3 cable, it is possible to saturate the receiver, leading to bit errors. If this occurs, we recommend one of the following:

- Reduce the transmit level of the device attached to the T3 network module. Many devices have a line build-out (LBO) configuration setting for this purpose.
- Insert a 4-dB attenuator on the receive side of the T3 network module.

Connecting ATM T3 and E3 Ports to the Network

Use a coaxial cable to connect the module BNC port to a T3 or E3 network.

ATM T3 Network Module and ATM E3 Network Module LEDs

The ATM T3 network module and the ATM E3 network module have the LEDs shown in Table 11-2.

Table 11-2 ATM T3 Network Module and ATM E3 Network module LEDs

LED	Color	Meaning
EN	Green	Module has passed its self-tests and is available to the router.
RCLK	Green	Receive clock has been detected.
FERF	Yellow	Far-end receive failure.
OOF	Yellow	Out of frame.
AIS	Yellow	Alarm indication signal.

ATM T3/E3 Network Module LEDs

Table 11-3 shows the LEDs for the combined ATM T3/E3 network module.

Table 11-3 ATM T3/E3 Network Module LEDs

LED	Color	Meaning
TXCL	Green	Cell transmitted.
RXCL	Green	Cell received.
RXALM	Yellow	Alarm indication signal.
RXCR	Green	Carrier present.
Loopback LED	Green	Loopback

ATM OC-3 Network Modules

ATM OC-3 network modules provide full 155-Mbps ATM connectivity, including STS-3c and STM-1 framing, for high-bandwidth data applications and voice-data integration applications. Characteristics and installation of these modules are described in the following sections.

OC-3 Network Modules for Cisco 3600 and Cisco 3700 Series Routers

This section describes the following OC-3 (Optical Carrier level 3) network modules for most Cisco 3600 and Cisco 3700 series routers.

Note ATM OC-3 network modules are not supported by the Cisco 3631 router.

The following modules are supported on the Cisco 3600 series routers and the Cisco 3725 router:

- NM-1A-OC3MM provides a multimode (MM) fiber uplink port. See Figure 11-7.
- NM-1A-OC3SMI provides a single-mode intermediate-reach (SMI) fiber uplink port. See Figure 11-8.
- NM-1A-OC3SML provides a single-mode long-reach (SML) fiber uplink port. See Figure 11-9.

The following modules are supported on the Cisco 3745 router:

- NM-1A-OC3MM-EP provides an MM fiber uplink port with enhanced performance. See Figure 11-7 for a similar faceplate.
- NM-1A-OC3SMI-EP provides an SMI fiber uplink port with enhanced performance. See Figure 11-8 for a similar faceplate.
- NM-1A-OC3SML-EP provides an SML fiber uplink port with enhanced performance. See Figure 11-9 for a similar faceplate.

The following modules are supported on the Cisco 3600 series routers:

- NM-1A-OC3MM-1V provides an MM fiber uplink port and circuit emulation service. See Figure 11-10.
- NM-1A-OC3SMI-1V provides an SMI fiber uplink port and circuit emulation service. See Figure 11-11.
- NM-1A-OC3SML-1V provides an SML fiber uplink port and circuit emulation service. See Figure 11-12.

Circuit emulation service allows the network module to carry voice traffic, such as telephone calls and faxes, over an ATM network simultaneously with data traffic.

If you are using the ATM OC-3/STM-1 circuit emulation service network module, you need both the network module and a 1- or 2-port T1 or E1 multiflex trunk interface card (VWIC-1MFT-T1, VWIC-1MFT-E1, VWIC-2MFT-T1, VWIC-2MFT-E1, VWIC-2MFT-T1-DI, or VWIC-2MFT-E1-DI) for a voice connection. You can install one multiflex trunk interface card (providing up to two voice

ports) in the ATM OC-3/STM-1 circuit emulation service network module. If a multiflex trunk interface card is not installed, the ATM OC-3/STM-1 circuit emulation service network module continues to perform data-routing functions.

To install a multiflex trunk interface card in a network module, see the *Cisco Interface Cards Hardware Installation Guide*. To obtain this publication, see the "Obtaining Documentation" section on page viii.

Note 1- or 2-port T1 or E1 multiflex trunk interface cards that support G.703 (VWIC-1MFT-G703, VWIC-2MFT-G703) are not supported in ATM OC-3/STM-1 circuit emulation service network modules.

Figure 11-7 ATM OC-3 Multimode Fiber Network Module

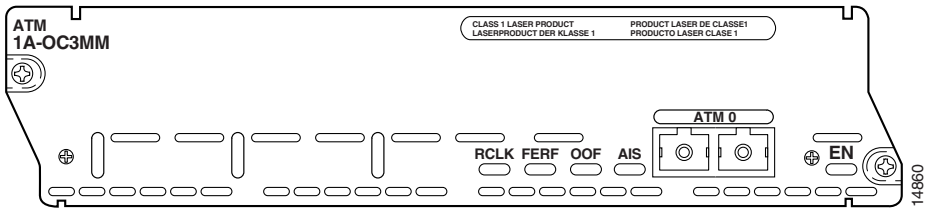


Figure 11-8 ATM OC-3 Single-Mode Intermediate-Reach Fiber Network Module

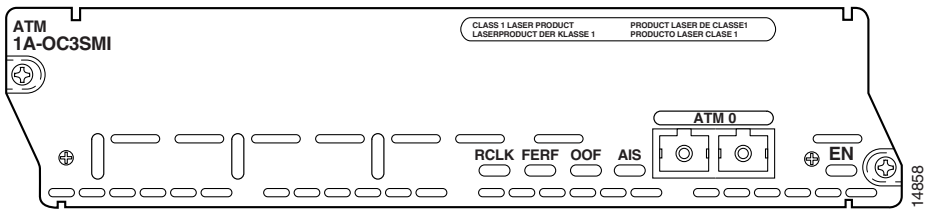


Figure 11-9 ATM OC-3 Single-Mode Long-Reach Fiber Network Module

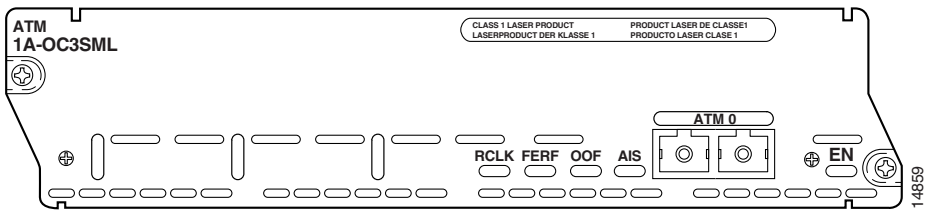


Figure 11-10 ATM OC-3/STM-1 Circuit Emulation Service Multimode Fiber Network Module

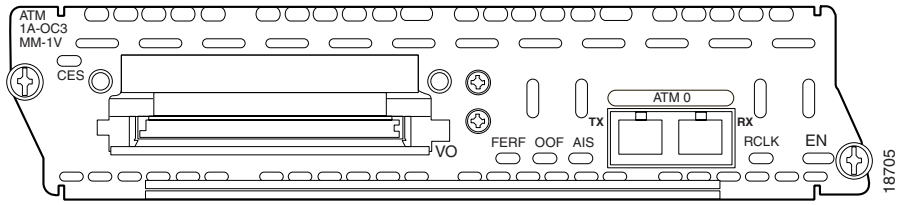


Figure 11-11 ATM OC-3/STM-1 Circuit Emulation Service Single-Mode Intermediate-Reach Fiber Network Module

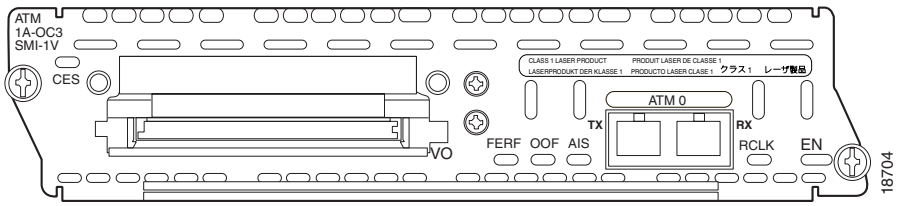
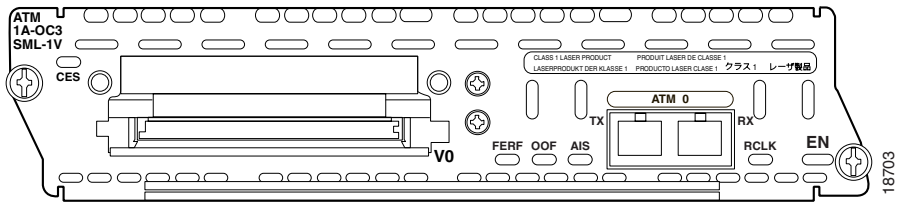


Figure 11-12 ATM OC-3/STM-1 Circuit Emulation Service Single-Mode Long-Reach Fiber Network Module



ATM OC-3 Network Module LEDs

Figure 11-13 and Figure 11-14 show ATM OC-3 network module LEDs. Table 11-4 describes their functions.

Figure 11-13 ATM OC-3 Network Module LEDs

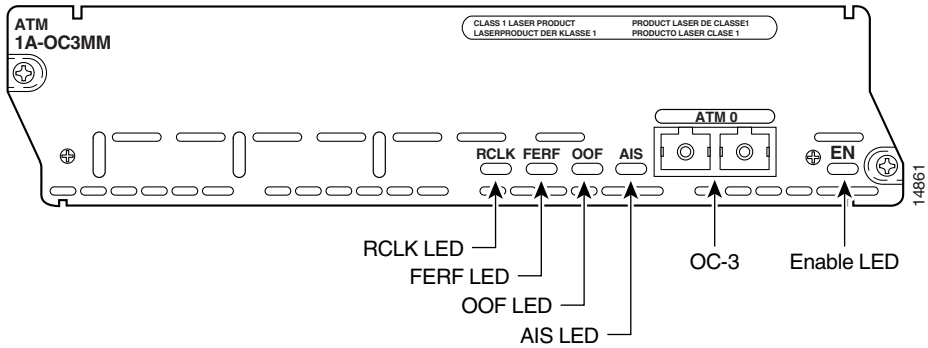


Figure 11-14 ATM OC-3/STM-1 Circuit Emulation Service Network Module LEDs

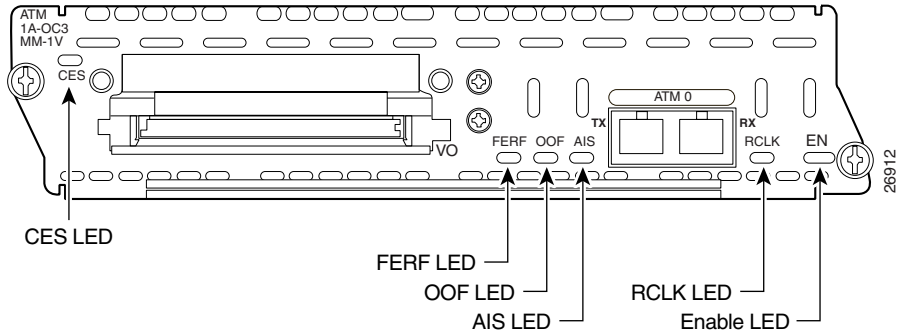


Table 11-4 ATM OC-3 Network Module LEDs

LED	Color	Meaning
EN	Green	Module has passed its self-tests and is available to the router.
RCLK	Green	Receive clock has been detected.
FERF	Yellow	Far-end receive failure.
OOF	Yellow	Out of frame.
AIS	Yellow	Alarm indication signal.
CES	Green	An active CES connection is established (ATM OC-3/STM-1 circuit emulation service network module only).

Hardware Compatibility with Cisco 3620 Routers

Cisco 3620 routers require a minimum PCMCIA controller revision level to recognize ATM OC-3 network modules; otherwise, an error message appears. Cisco 3620 routers installed in the field before April 1999 contain a Revision C PCMCIA controller, which is not compatible with these modules. Starting in April 1999, all Cisco 3620 routers shipped from the factory include Revision E PCMCIA controllers, which are fully compatible with all three ATM OC-3 network modules.

You can identify the version of PCMCIA controller in your Cisco 3620 router by entering the **show pci hardware** command in privileged EXEC mode, or by examining the part number on the motherboard. Supported versions are shown in Table 11-5.

Table 11-5 Cisco 3620 Router Versions for ATM OC-3 Network Modules

	Does Not Support ATM OC-3	Supports ATM OC-3
PCMCIA controller	0x22, 0xE2	0x20, 0xE0
Motherboard	73-1850-10 and older	73-1850-11 or newer

The output of the **show pci hardware** command looks similar to this:

```
Router# show pci hardware
```

```
CLPD6729 registers:
    (0x00) Chip Revision = 0x82
    (0x1E) Misc Control 2 = 0x08
    (0x1F) Chip Information = 0xE2
```

If you have incompatible hardware, contact the Cisco Systems Technical Assistance Center (TAC) at 800 553-24HR or 408 526-7209, or send e-mail to tac@cisco.com to request a free replacement Cisco 3620 router.

CES Cross-Connection on the Cisco 3660 Router

The Cisco 3660 router can deliver traditional PCM-encoded 64-kbps circuit-based voice over the ATM OC-3 CES network module. To use this functionality, the multiservice interchange card (MIX) must be installed on the Cisco 3660 router. T1/E voice channels on NM-xFE2W and NM-HDV network modules can be transported across the MIX module to ATM OC-3 network modules (NM-1A-OC3XX-1V) over an ATM network. PVC-based (permanent virtual circuit) CES allows service providers to quickly deliver local or long distance voice, while SVC (switched virtual circuit) capabilities ensure that these services are optimized for maximum profitability.

To install the MIX card, see the *Installing the Multiservice Interchange Card in Cisco 3660 Routers* document. To configure CES, see the *OC-3/STM-1 ATM Circuit Emulation Service Network Module* document.

Connecting ATM OC-3 Ports to the Network

To connect an ATM OC-3 network module to the network, insert a fiber-optic cable with one duplex SC connector (see Figure 11-15) or two simplex SC connectors (see Figure 11-16) into the ATM interface.

Note Some network modules are shipped with a dust plug to protect this interface. Pull to remove it.

Figure 11-15 Duplex SC Connector

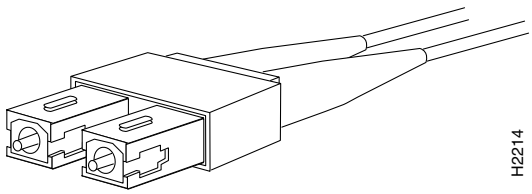
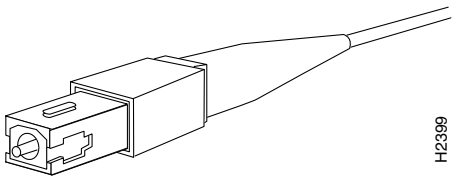


Figure 11-16 Simplex SC Connector



Note Cisco Systems does not sell these fiber-optic cables, but they are available from many cable vendors. Cables should perform to the specifications listed in Table 11-6.

Table 11-6 Fiber-Optic Cable Specifications

Standard	Maximum Path Length	Cabling
ISO/IEC 9314-3	1.24 miles (2 km) all cables in a connection, end to end	62.5-micron core with an optical loss of 0 to 9 dB, or 50-micron core with an optical loss of 7 dB
IEC 793-2	27.9 miles (45 km) for SML and 9.3 miles (15 km) for SMI	9-micron core
ANSI/TIA/EIA-492 CAAA	27.9 miles (45 km) for SML and 9.3 miles (15 km) for SMI	9-micron core

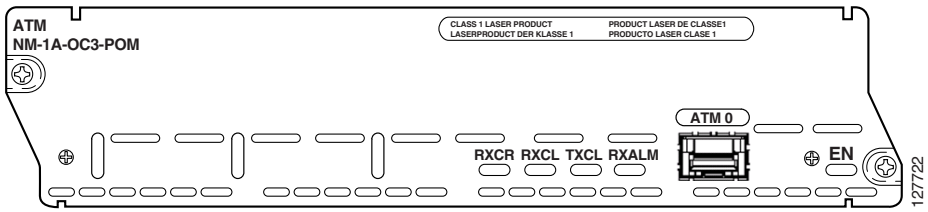
Note A single fiber link should not mix 62.5- and 50-micron cable.

ATM-OC3-POM Network Module for Cisco 3800 Series Routers

The NM-1A-OC3-POM network module provides a high-performance fiber uplink port for Cisco 3800 series integrated services routers. See Figure 11-17. Supported platforms are:

- Cisco 3825 integrated services router
- Cisco 3845 integrated services router

Figure 11-17 ATM OC3-POM Network Module



The ATM interface is the small form-factor pluggable (SFP) optical port labeled ATM 0. See Figure 11-17. The optical interface is provided by an SFP module that is inserted into the SFP port. Fiber-optic cables to the network are attached to the SFP module.

The network module has three modes of operation. The mode of operation is determined by the SFP module that is used.

Caution Only SFP modules provided by Cisco should be used in the network module. SFP modules that are not provided by Cisco have not been evaluated for reliability or user safety.

The modes of operation and usable SFP modules are:

- Multimode (MM)
  - POM-OC3-MM

  - SFP-OC3-MM
- Single-mode intermediate reach (SMI)
  - POM-OC3-SMIR
  - SFP-OC3-IR1
- Single-mode long reach (SML)
  - POM-OC3-SMLR
  - SFP-OC3-LR1

ATM-OC3-POM Network Module LEDs

Table 11-7 describes the functions of the LEDs on the ATM-OC3-POM network module shown in Figure 11-17.

Table 11-7 ATM-OC3-POM Network Module LEDs

LED	Color	Meaning
RXCR	Green	Lit when carrier signal into the network module is present.
RXCL	Green	Blinks to indicate packet reception.
TXCL	Green	Blinks to indicate packet transmission.
RXALM	Yellow	Alarm indication signal.
EN	Green	Module has passed its self-tests and is available to the router.

Connecting ATM-OC3-POM Ports to the Network

The following sections describe how to remove and install SFP modules, and how to connect the ports on a module to the network.

Handling an SFP Module

Before handling an SFP module, observe the following guidelines:

- SFP modules are static-sensitive. To prevent electrostatic discharge (ESD) damage, follow your normal board- and component-handling procedures.
- SFP modules are dust-sensitive. When storing an SFP module or when a fiber-optics cable is not plugged into the connector, always keep plugs in SFP module optical bores.

Note The most common source of contaminants in the optical bores is debris picked up on the ferrules of the optical connectors. Use alcohol swabs or lint-free absorbent wipes to clean the ferrules of the optical connector.

Removing an SFP Module

The following procedure describes removing an SFP module from the network module.

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.** Statement 1040

Caution You can remove and install SFP modules with power on to the system; however, we strongly recommend that you do not remove or install an SFP module with optical fiber cables attached.

To remove an SFP module, perform the following steps:

Step 1 Attach an ESD wrist strap to your wrist and to the ESD connection socket on the chassis or to a bare metal surface on the chassis or frame.

Step 2 Disconnect the network fiber cable from the SFP module connector.

Step 3 Remove the SFP module from the slot.

a. Using your thumb and forefinger, grip the colored latching band on the front of the SFP module.

b. Gently push the latching band back toward the SFP port. You may hear a click or feel the SFP module disengage from the holding latch.

Note Not all SFP modules have the same kind of latching mechanism.

c. While still holding the latching band, pull the SFP module forward and out of the slot.

Step 4 Set the SFP module aside on an antistatic surface.

Installing an SFP Module

Use the following procedure to install an SFP module:

Step 1 Attach an ESD-preventive wrist strap to your wrist and between yourself and an unpainted chassis surface.

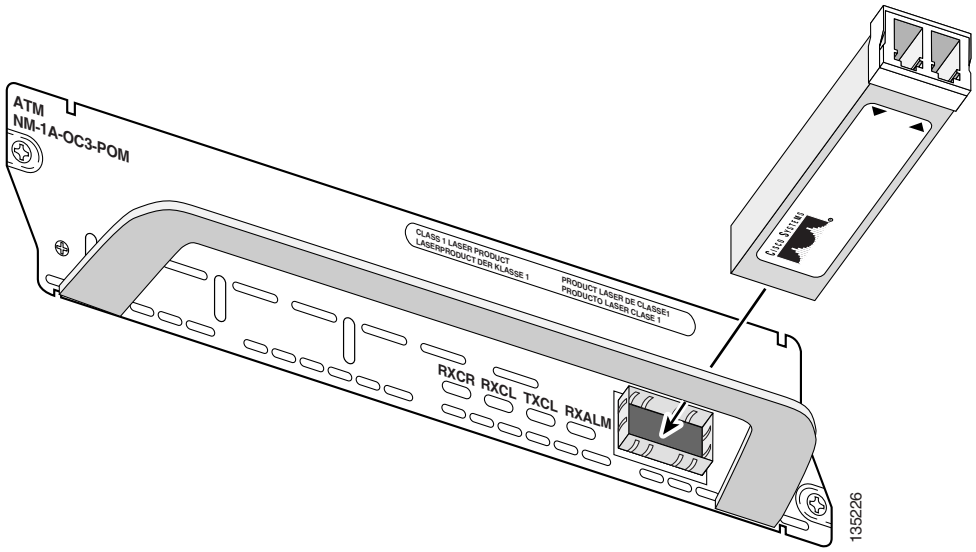
Step 2 Verify that you have the correct SFP module for your installation.

- Check the part number and distance information on the SFP module label.
- Alternatively, if the distance information is not on the label, use the **show contr pos x/y** command to display the information after the SFP module is installed.

Step 3 Align the SFP module with the slot so that the label is facing away from the handle.

Step 4 Holding the module at the latching band (with your thumb and forefinger), insert the SFP module into the slot on the SFP port. See Figure 11-18.

Figure 11-18 Installing an SFP Module



Step 5 Push the module back into the slot until the latch engages. When fully inserted, only the band around the front of the SFP module should be visible.

Step 6 Remove the plug from the SFP module optical bores and save the plug for future use.

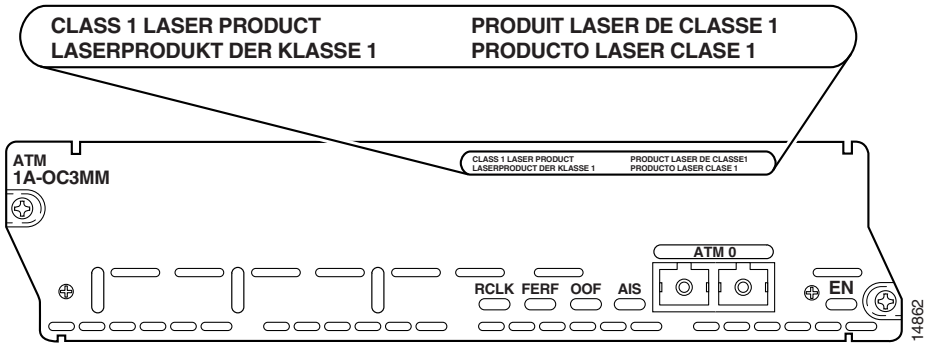
Step 7 Attach the network interface fiber-optic cable, as described in the "Connecting ATM OC-3 Ports to the Network" section on page 11-9.

Laser Safety Guidelines

ATM OC-3 network modules use a small laser to generate the fiber-optic signal. Keep the transmit port covered whenever a cable is not connected to it.

The module faceplate carries a Class 1 laser warning label. See Figure 11-19.

Figure 11-19 Class 1 Laser Warning Label



Warning **Because invisible laser radiation may be emitted from the aperture of the port when no fiber cable is connected, avoid exposure to laser radiation and do not stare into open apertures.** Statement 240

Fiber-Optic Transmission Specifications

This section describes Synchronous Optical Network (SONET) specifications for fiber-optic transmissions, defines the power budget, and helps you estimate your power margin for multimode and single-mode transmissions. This section contains the following information:

- SONET Distance Limitations
- Power Budget and Power Margin
- Link Loss
- Estimating the Power Margin
- Single-Mode Transmission

SONET Distance Limitations

The SONET specification for fiber-optic transmission defines two types of fiber, single-mode and multimode. Single-mode fiber allows only one bundle of light rays to propagate through the fiber, whereas multimode fiber allows multiple bundles entering at different angles. Because different bundles (referred to as modes) travel different distances, depending on the entry angle, they arrive at the destination at different times (modal dispersion). Single-mode fiber is capable of higher bandwidth and greater cable run distances than multimode fiber.

Table 11-8 lists typical maximum distances for single-mode and multimode transmissions, as defined by SONET. Use the calculations described in this section to determine the actual maximum for your network. If the distance between two connected stations exceeds this limit, transmission can become unreliable.

Table 11-8 Typical SONET Maximum Fiber-Optic Transmission Distances

Transceiver Type	Maximum Distance Between Stations
MM	1.5 miles (2 km)
SMI	9 miles (15 km)
SML	28 miles (40 km)

Power Budget and Power Margin

Proper operation of an optical data link depends on modulated light reaching the receiver with enough power to be demodulated. The power budget (PB) is the difference between transmitter power (PT) and receiver sensitivity (PR). For instance, if transmitter power is –20 dB and receiver sensitivity is –30 dB, the power budget is 10 dB:

PB = PT – PR

PB = –20 dB – (–30 dB)

PB = 10 dB

The SONET specification requires that the signal meet the worst-case requirements listed in Table 11-9.

Table 11-9 SONET Signal Requirements

	MM	SMI	SML
Transmitter power	–20 dBm	–15 dBm	–5 dBm
Receiver sensitivity	–30 dBm	–31 dBm	–34 dBm
Power budget	10 dBm	16 dBm	29 dBm

The difference between the power budget and the link loss (LL) is called the power margin (PM). If the power margin is zero or positive, the link should work. If it is negative, the signal may not arrive with enough power to operate the receiver.

Link Loss

Power loss over a fiber-optic link arises from the following causes:

- Passive components—Attenuation caused by cables, cable splices, and connectors is common to both multimode and single-mode transmission. Attenuation is significantly lower for optical fiber than for other media.
- Chromatic dispersion—The signal spreads in time because of differing speeds of the different wavelengths of light.
- Modal dispersion—In multimode fiber, the signal spreads in time because of the different propagation modes.
- Higher-order mode loss (HOL)—This loss results from light radiated into the fiber cladding.
- Clock recovery at the receiver—This recovery consumes a small amount of power.

The power lost over the data link is the sum of all these losses. Table 11-10 gives an estimate of the amount of loss attributable to each cause.

Table 11-10 Link Loss Causes and Amounts

Cause	Amount of Loss
Fiber attenuation	SM: 0.5 dB/km MM: 1 dB/km
Splice	0.5 dB
Connector	0.5 dB
Modal and chromatic dispersion	Depends on fiber and wavelength[1]
Higher-order mode losses	0.5 dB
Clock recovery	1 dB

1. Dispersion is usually negligible for single-mode fiber. For multimode fiber, the product of bandwidth and distance should be less than 500 MHz-km.

Estimating the Power Margin

The following example calculates a multimode power margin based on these values:

- Power budget 10 dB (SONET worst-case specification for multimode fiber)
- Link length 3 km
- Four connectors
- Three splices
- Higher-order loss (HOL)
- Clock recovery

The power margin is:

PM = PB – LL

= 10 dB – [3 km x (1.0 dB/km) + 4 x (0.5 dB) + 3 x (0.5 dB) + 0.5 dB + 1 dB] = 2 dB

The positive result means this link should have enough power for transmission. The product of bandwidth and distance is 155 MHz x 3 km = 465 MHz-km; this is within the dispersion limit of 500 MHz-km.

Single-Mode Transmission

Single-mode transmission is useful for longer distances, because there is a single transmission path within the fiber and modal dispersion does not occur.

The maximum receive power for SML is –10 dBm, and the maximum transmit power is 0 dBm. The SML receiver can be overloaded when using short lengths of fiber. Overloading the receiver does not damage it, but can cause unreliable operation. To prevent overloading an SML receiver, insert a minimum 10-dB attenuator on the link between any SML transmitter and the receiver.

The SMI receiver cannot be overloaded by the SMI transmitter and does not require a minimum fiber cable length or loss.

The following example of a single-mode power margin assumes these values:

- Power budget 16 dB (SONET worst-case specification for SMI)
- Two buildings 8 kilometers apart
- Connections through a patch panel in an intervening building with a total of 12 connectors

  PM = PB – LL

  = 16 dB – 8 km x (0.5 dB/km) – 12 x (0.5 dB)

  = 6 dB

The positive value means this link should have enough power for transmission.

CHAPTER 12

Connecting T1/E1 IMA Network Modules

This chapter describes how to connect 4- and 8-port T1 and E1 IMA (inverse multiplexing for ATM) network modules for Cisco modular routers and contains the following sections:

Tip To determine whether your router supports a specific network module, see Table 1-6 on page 1-16.

IMA Network Modules

This section provides information about the following network modules for Cisco modular routers:

- 4-port T1 IMA network module (NM-4T1-IMA) (see Figure 12-1)
- 8-port T1 IMA network module (NM-8T1-IMA) (see Figure 12-2)
- 4-port E1 IMA network module (NM-4E1-IMA) (see Figure 12-3)
- 8-port E1 IMA network module (NM-8E1-IMA) (see Figure 12-4)

Each port provides 1.544 Mbps/2.048 Mbps connectivity. The IMA aggregation of multiple T1/E1 links increases bandwidth inexpensively to allow WAN uplinks at speeds ranging up to those of a T3/E3 link.

Figure 12-1 4-Channel IMA T1 Network Module

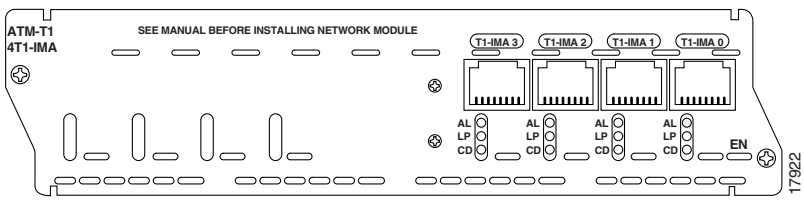


Figure 12-2 8-Channel IMA T1 Network Module

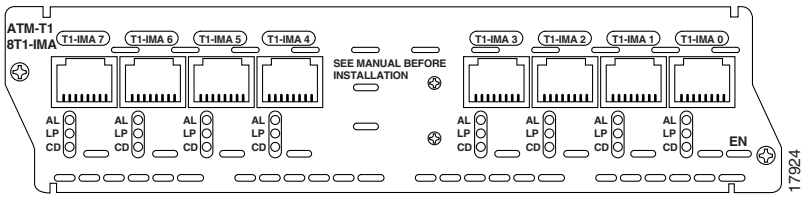


Figure 12-3 4-Channel IMA E1 Network Module

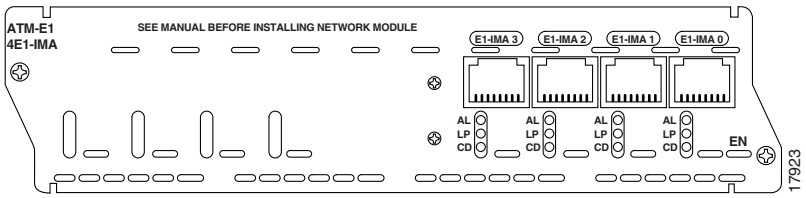
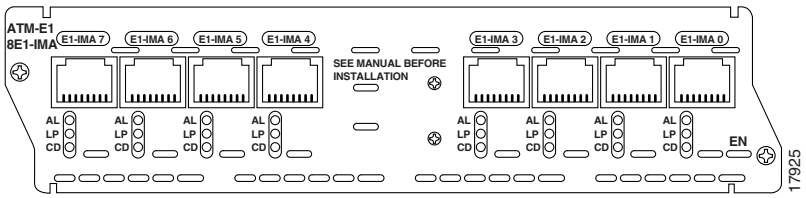


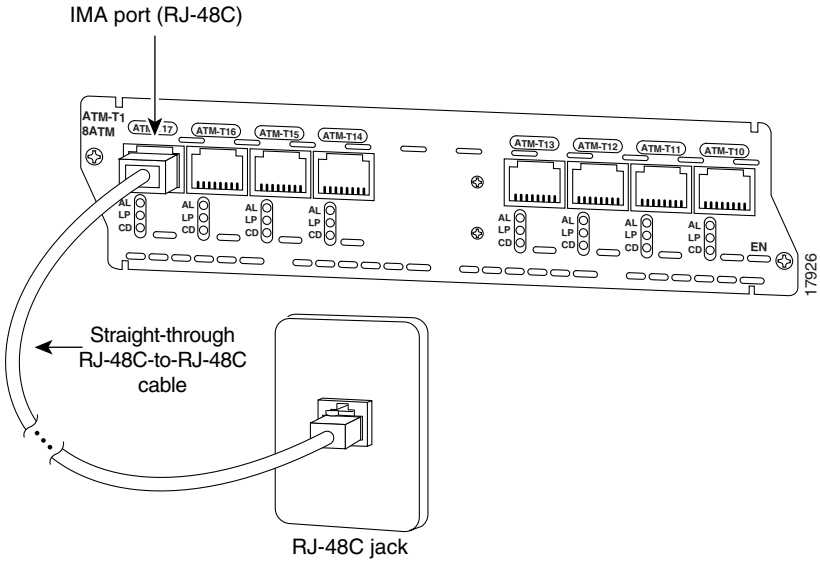
Figure 12-4 8-Channel IMA E1 Network Module



Connecting T1/E1 IMA Ports to the Network

To connect a T1/E1 IMA network module to a network, use a straight-through RJ-48C-to-RJ-48C cable to connect the T1 or E1 port to an RJ-48C wall jack. (See Figure 12-5.)

Figure 12-5 Connecting a T1/E1 IMA Network Module to an RJ-48C Wall Jack



IMA Network Module Interface Numbering

An individual (ungrouped) interface on the IMA network module is numbered by interface type and slot and port number, for example atm 0/2.

An interface that is part of an IMA group loses its individual port number, but adopts the IMA group number, for example atm 0/ima2.

Up to four groups can be created (numbered 0 through 3).

T1/E1 IMA Network Module LEDs

All network modules have an enable (EN) LED. The enable LED indicates that the module has passed its self-tests and is available to the router. T1/E1 IMA network modules have the additional LEDs shown in Figure 12-6 and described in Table 12-1.

Figure 12-6 T1/E1 IMA Network Module LEDs

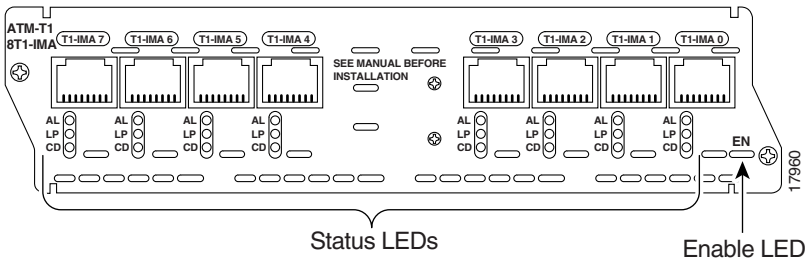


Table 12-1 T1/E1 IMA Network Module LEDs

LED	Color	Meaning
AL	Yellow	Alarm indicating loss of signal, loss of frame, or unavailability because of excessive errors.
LP	Yellow	Controller local loopback.
CD	Green	Carrier received on telco link.

CHAPTER 13

Connecting HSSI Network Modules

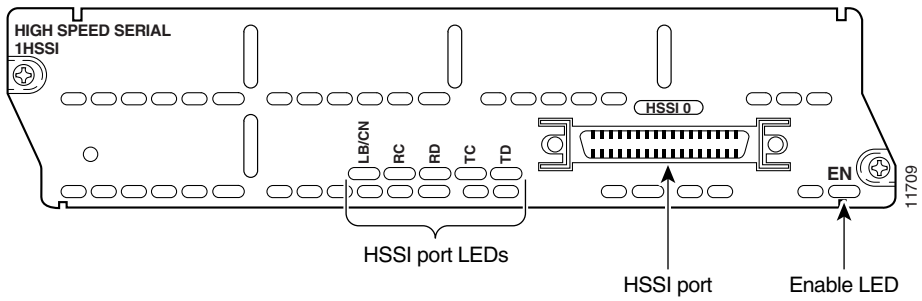
This chapter describes the 1-port High-Speed Serial Interface (HSSI) network module for Cisco 3600 series and Cisco 3700 series routers and contains the following sections:

Tip To determine whether your router supports a specific network module, see Table 1-6 on page 1-16.

HSSI Network Modules

The 1-port High-Speed Serial Interface (HSSI) network module (see Figure 13-1) provides connectivity for fractional DS3 rate links and slower.

Figure 13-1 HSSI Network Module



Connecting HSSI Modules to the Network

The HSSI module contains a 50-pin receptacle, color-coded blue. You can connect this port to a network in either of two ways:

- To an external data service unit (DSU), using a HSSI data terminal equipment (DTE) cable for operation in DTE mode (see Figure 13-2). The HSSI port is configured to operate in this mode by default.

- To another router for back-to-back operation, using a HSSI null modem cable. (See Figure 13-3.) Both routers must be at the same site. Back-to-back operation allows you to verify operation of the HSSI port or link routers directly to build a larger node. Both routers must be configured to use a 51.84-MHz internal clock.

Figure 13-2 Connecting the 1-Port HSSI Module to an External DSU

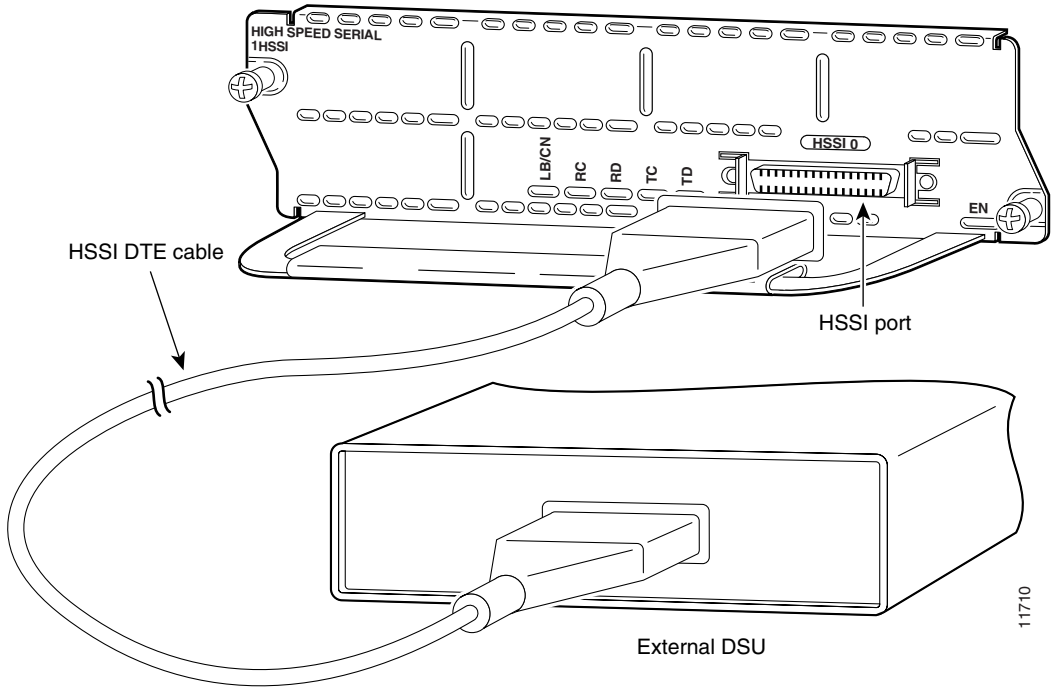
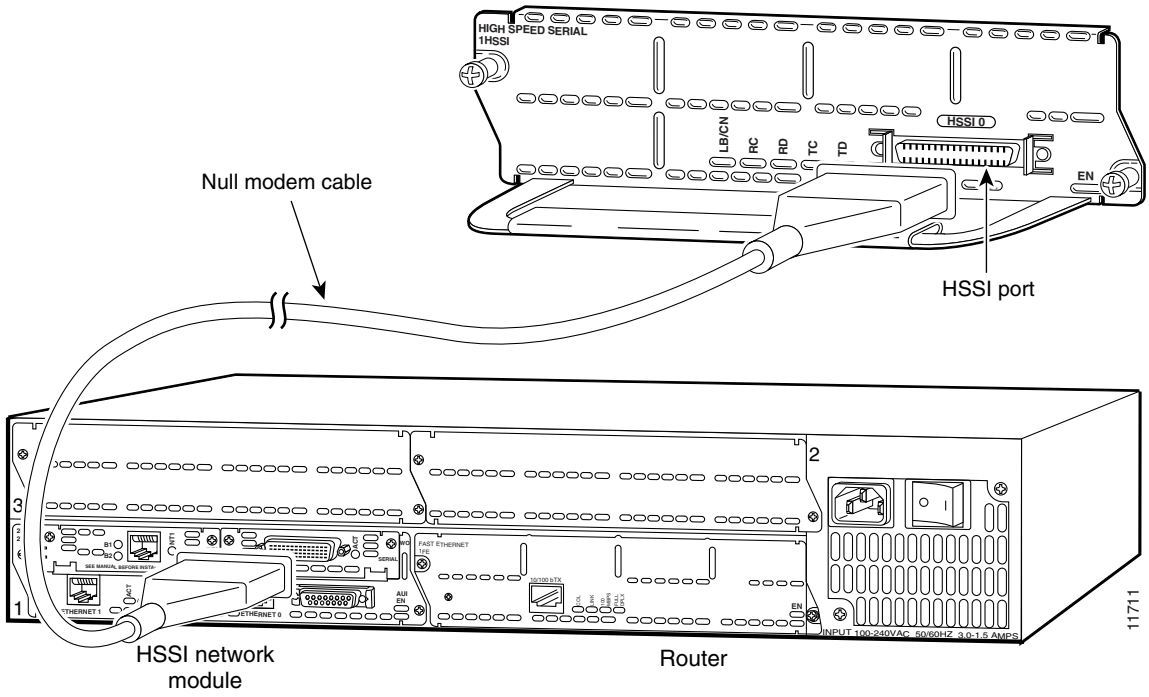


Figure 13-3 Connecting Two Routers Back to Back



HSSI Network Module LEDs

All network modules have an enable (EN) LED. The enable LED indicates that the module has passed its self-tests and is available to the router. The HSSI network module has the additional LEDs shown in Figure 13-4 and described in Table 13-1.

Figure 13-4 HSSI Network Module LEDs

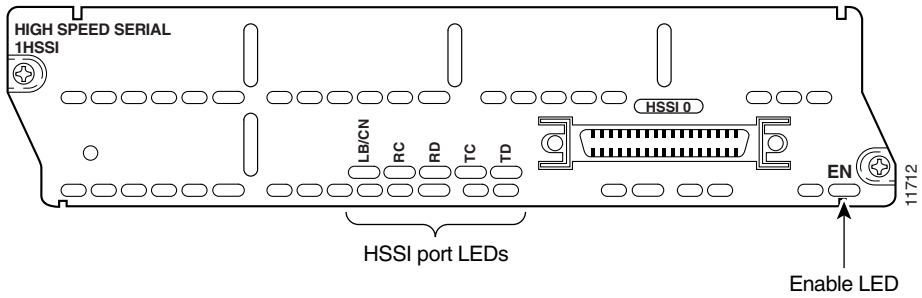


Table 13-1 HSSI Network Module LEDs

LED	Meaning
LB/C (Loopback/Connect)	Green indicates normal operation. The module is connected to the external DSU, and the signals TA (DTE available) and CA (DCE available) are active. Yellow indicates that the module is in loopback mode. If this LED is off, the port is neither connected to the DSU nor in loopback mode.
RC (Receive Clock)	Module has detected a receive clock signal. During normal operation, this signal is received from the external DSU. During loopback, it is generated internally.
RD (Receive Data)	Module has detected a receive clock signal. During normal operation, this signal is received from the external DSU. During loopback, it is generated internally.
TC (Transmit Clock)	Module is transmitting a clock signal to the external DSU. During normal operation, this signal is derived from the DSU's RT signal. During loopback, it is generated internally.
TD (Transmit Data)	Module has been detected by and can send packets to the external DSU.

Connecting Compression Network Modules

This chapter describes the compression network module for Cisco 3600 series routers and contains the following sections:

This module provides hardware assistance to protocols that use compression and decompression, reduces the load on the CPU caused by software compression, and improves router performance.

Tip To determine whether your router supports a specific network module, see Table 1-6 on page 1-16.

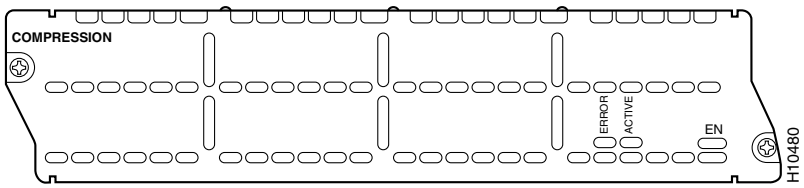
Compression Network Modules

The compression network module (NM-COMPR) does not provide network interfaces of its own, but instead compresses and decompresses data passing through interfaces on other network modules or WAN interface cards in the router. (See Figure 14-1.)

Hardware compression is supported only over Point-to-Point Protocol (PPP) links. The compression network module supports only the Stacker compression algorithm.

Cisco IOS Release 11.3 and later releases allow Frame Relay compression support using the FRF.9 compression algorithm.

Figure 14-1 Compression Network Module



Interfaces Supported

The compression network module supports the following interfaces:

- Channelized T1 Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI)
- Channelized E1 ISDN PRI
- ISDN Basic Rate Interface (BRI)
- Synchronous serial
- Switched 56-kbps data service unit/channel service unit (DSU/CSU)

Compression Network Module LEDs

Figure 14-2 shows compression network module LEDs. Table 14-1 describes their meaning.

Figure 14-2 Compression Network Module LEDs

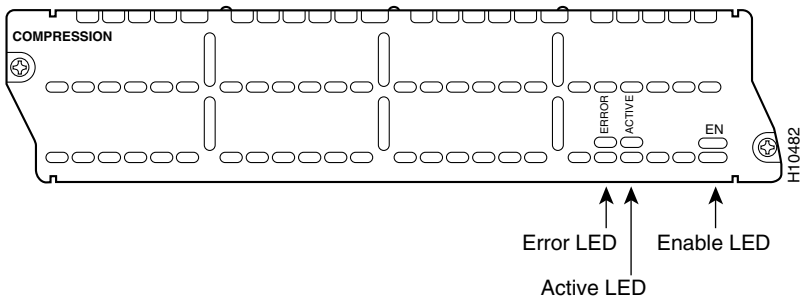


Table 14-1 Compression Network Module LEDs

LED	Meaning
EN	Green indicates that the module has passed its self-tests and is available to the router.
ERROR	Amber indicates that an error was found, and if the LED remains on, that the error might prevent accurate compression. Off during normal operation.
ACTIVE	Green indicates that the module is ready to process data. It comes on when the boot process is complete and stays on during normal operation.

CHAPTER 15

Connecting Wireless Multipoint Network Modules

This chapter explains how to connect the wireless multipoint network module and contains the following sections:

Tip To determine whether your router supports a specific network module, see Table 1-6 on page 1-16.

Wireless Multipoint Network Modules

The wireless multipoint network module, shown in Figure 15-1, also referred to as a s*ubscriber unit* (SU), provides a high-speed broadband fixed wireless radio-frequency (RF) link between each subscriber site and a single headend site. This link delivers full-duplex data in the licensed MMDS band (2.500 to 2.690 GHz) or unlicensed U-NII band (5.725 to 5.825 GHz).

The headend of the system consists of a Cisco uBR7200 series universal broadband router, one or more wireless modem cards, and the required subsystem for each modem card. The diversity option, which minimizes the effects of fading, uses two wireless transverters at each site, with each transverter connected to its own antenna. (See Figure 15-2.)

Figure 15-1 Wireless Multipoint Network Module with Diversity

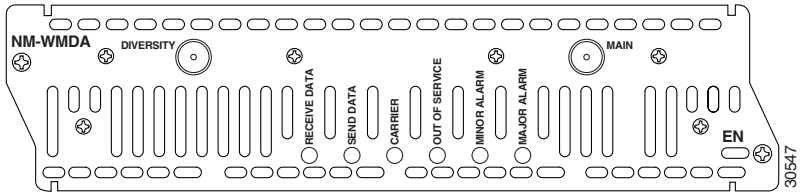
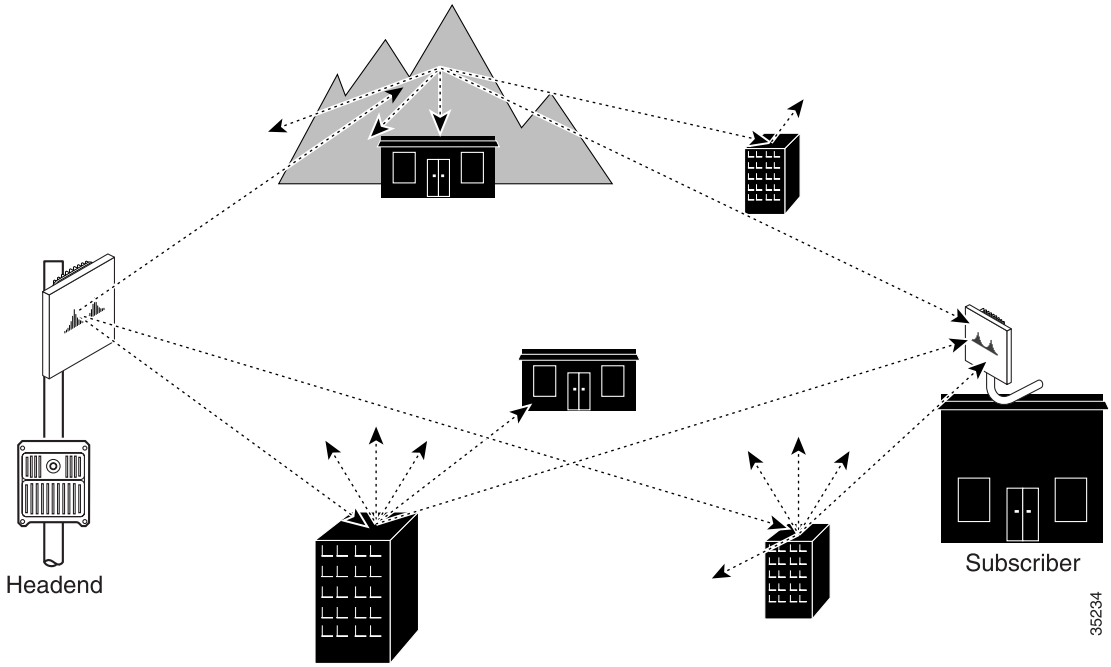


Figure 15-2 Multipoint Communications with Multipath and Diversity Reception



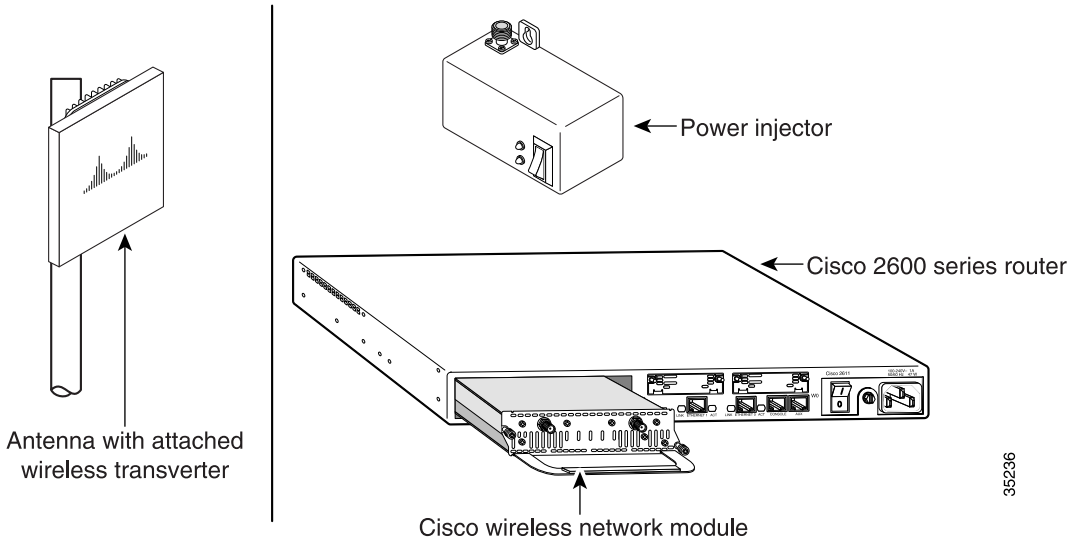
The network module provides the control and data interface to the radio frequency (RF) subsystem in the wireless transverter. It also provides the up-down conversion from baseband to intermediate frequency (IF). One network module supports one or two wireless transverters (main and diversity).

Subscriber-Unit System

Each subscriber unit system (see Figure 15-3) consists of the necessary cables and these items:

- A wireless multipoint network module in the router
- One or two antennas to transmit and receive RF signals to and from the headend. (Diversity reception of headend transmissions requires two antennas.)
- One wireless transverter for each antenna. The transverter can be attached to the back of the subscriber antenna, as shown in Figure 15-3, or mounted separately.
- One power injector for each transverter. The power injector connects the network module to the wireless transverter, and provides the transverter with DC power, control signals, and IF signals.

Figure 15-3 Components of the Multipoint Subscriber-Unit System



Note The antenna, wireless transverter, and power injector are third-party products. For further information about these components, see the manufacturer's documentation.

Hardware and Software Requirements

Wireless multipoint network modules require that the router have at least 16 MB of flash memory.

The wireless multipoint network modules require an external microcode bundle. You can download this microcode at http://www.cisco.com/cgi-bin/tablebuild.pl/rsu.

Connecting Wireless Ports to the Network

Use an indoor IF coaxial cable to connect the wireless network module Main connector to a power injector. If you are using the diversity feature, connect the network module Diversity connector to a second power injector.

Wireless Multipoint Network Module LEDs

Wireless multipoint network modules have the LEDs shown in Table 15-1.

Table 15-1 Wireless Multipoint Network Module LEDs

LED	Meaning
EN (Enable)	The module has passed its self-tests and is available to the router.
RECEIVE DATA	The module is receiving packets.
SEND DATA	The module is sending packets.

Table 15-1 Wireless Multipoint Network Module LEDs (continued)

LED	Meaning
CARRIER	Indicates the state of the radio link. Green means that the radio link is synchronized and the line protocol is up. Yellow indicates loss of link synchronization.
OUT OF SERVICE	Yellow means that the radio link is still up, but not available for use (typically in a test or loopback mode).
MINOR ALARM	Yellow means that the link is degraded and may need maintenance action, or one or more user-defined event thresholds have been exceeded.
MAJOR ALARM	The link is down.

Related Documents

For additional information, see the following documents.

Subscriber Unit

- *Multipoint Wireless Support for the Cisco 2600 and 3600 Series Routers* feature document

Headend

- *Multipoint Support for the Cisco uBR7200 Series Universal Broadband Router* feature document
- *Cisco uBR7200 Series Multipoint Wireless Modem Card and Subsystem Installation*
- *Cisco Multipoint Headend Wireless Transverter Duplexer Replacement Instructions*
- *Cisco Multipoint Headend Power Feed Panel Replacement Instructions*
- *Cisco Multipoint Headend Wireless Transverter Replacement Instructions*
- *Cisco Wireless Transverter Hail Shield Installation Instructions*

CHAPTER 16

Connecting High-Density Analog Telephony Network Modules

This chapter describes how to connect high-density analog telephony network modules for Cisco modular routers. It contains the following sections:

Tip To determine whether your router supports a specific network module, see Table 1-6 on page 1-16.

High-Density Analog Telephony Network Module

The high-density analog telephony network module is a modular, high-density voice network module that provides dual tone multifrequency (DTMF) detection, voice compression and decompression, call progress tone generation, voice activity detection (VAD), echo cancellation, and adaptive jitter buffering.

The high-density analog telephony network module supports two different expansion modules, providing up to 12 ports in addition to the 4 Foreign Exchange Service (FXS) ports on the base high-density analog telephony network module (NM-HDA). See Table 16-1 for expansion module support information.

Table 16-1 Expansion Modules Supported on the Cisco High-Density Analog Telephony Network Module (NM-HDA)

Expansion Modules	Port Type	Number of Ports
EM-HDA-8FXS	FXS	8
EM3-HDA-8FXS	FXS	8
EM-HDA-4FXO	FXO	4
EM2-HDA-4FXO	FXO[1]	4

1. FXO = Foreign Exchange Office

These expansion modules can be used in the following combinations:

- 12 Foreign Exchange Station (FXS) ports (NM-HDA with installed EM-HDA-8FXS and EM3-HDA-8FXS expansion modules)
- Ten Foreign Exchange Office (FXO) ports and four FXS ports (NM-HDA with two installed EM-HDA-4FXO or EM2-HDA-4FXO expansion modules)
- 12 FXS and 4 FXO ports (NM-HDA with installed EM-HDA-8FXS, EM3-HDA-8FXS, and EM-HDA-4FXO or EM2-HDA-4FXO expansion modules)

The FXO expansion module supports a power failure port that connects directly to the central office (CO) in case of failure. Physical ports are added as shown in Table 16-2.

Table 16-2 Physical Ports on the High-Density Analog Telephony Network Module

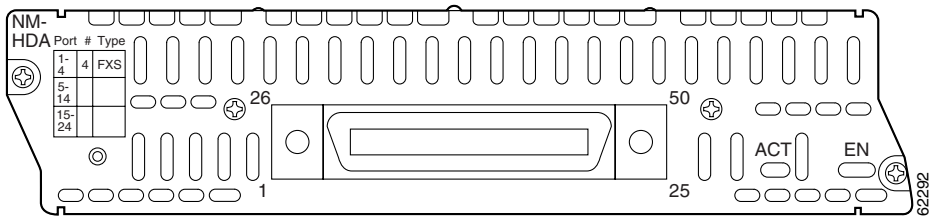
Physical Port	Location	FXS Ports	FXO Ports
1–4	Default on card	1–4	—
5–14	Expansion module 0	5–12 FXS 13–14 Not used	5–8 FXO 9–13 Not used 14 Power failure port **Note** Port 8 is hard-wired to port 14.
15–24	Expansion module 1	15–22 FXS 23–24 Not used	15–18 FXO 19–23 Not used 24 Power fail port **Note** Port 18 is hard-wired to port 24.
25	Not used	—	—

Tip To maintain an emergency connection during power outages, connect port 14 or port 24 to the public switched telephone network (PSTN). Phones connected to port 8 or port 18 fail over to the PSTN connections through port 14 or port 24 during power outages.

The digital signal processors (DSPs) on the card support up to 8 ports of high-complexity codecs or up to 16 ports of medium- and low-complexity codecs. The number of DSPs must be increased if more than eight ports of high-complexity codecs are needed. In this case, a DSP expansion module must be installed.

The high-density analog telephony network module is connected to the network using an RJ-21 Amphenol connector on the front panel. The front of the card is shown in Figure 16-1.

Figure 16-1 High-Density Analog Telephony Network Module



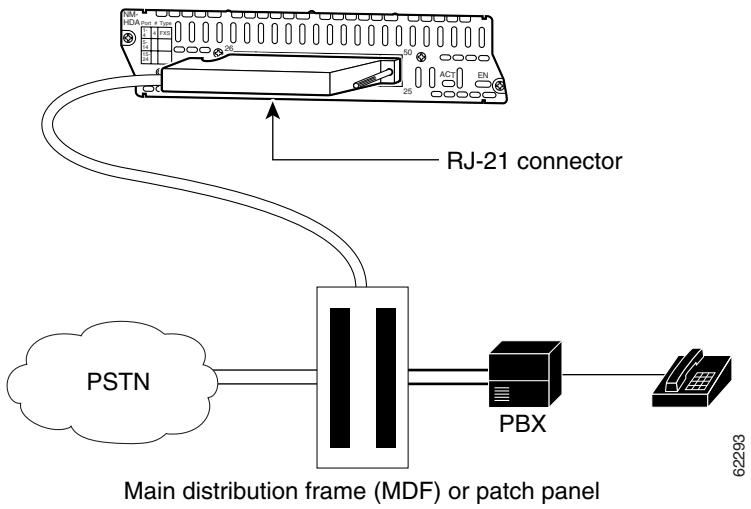
Connecting the High-Density Analog Telephony Network Module to the Network

The high-density analog telephony network module is connected to a distribution frame with an RJ-21 cable. (See Figure 16-2.) RJ-21 cables are not provided with the network module. Some recommended cables are as follows:

- 253PP10GYADI male-to-male cable and 253PC10GYADI male-to-female cable from Gray Bar
- AT125-SM patch panel (supports both male and female connection) from Gray Bar

For ordering information, see the "Obtaining Technical Assistance" section on page xi.

Figure 16-2 High-Density Analog Telephony Card Connected to a Main Distribution Frame



Adding DSP Expansion Modules

DSP expansion modules can be used if more than eight ports using high-complexity codecs are needed on the high-density analog telephony network module.

To install DSP expansion modules, follow these steps:

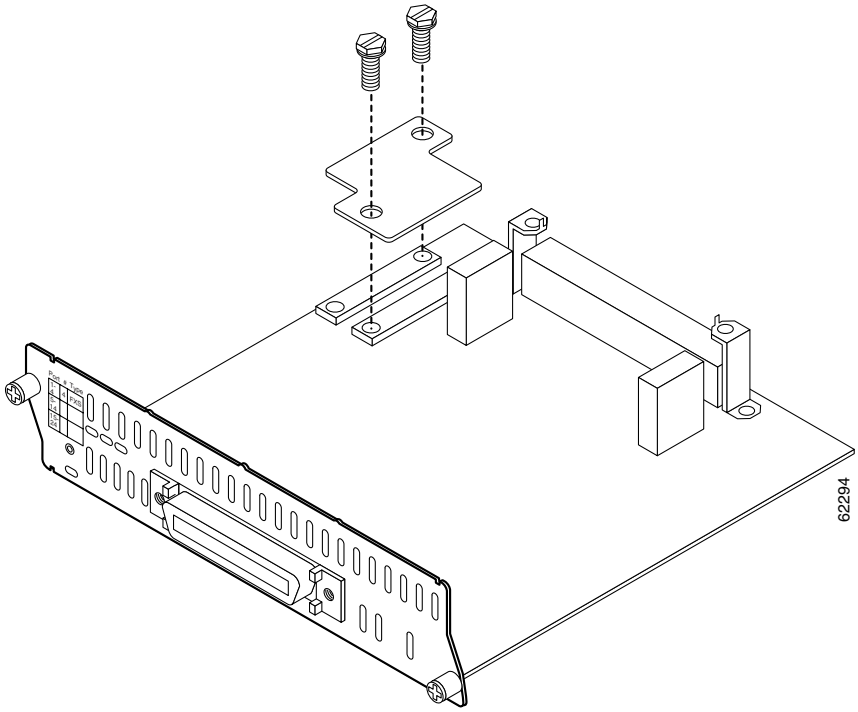
Step 1 Insert the connector on the DSP expansion module into the module connector on the network module. (See Figure 16-3.)

Note Be sure to press firmly on the DSP expansion module until the board seats onto the connector.

Step 2 Insert the screws from the hardware kit through the DSP expansion module into the brackets on the network module.

Step 3 Install the network module into the router, as described in the "Installing Cisco Network Modules in Cisco Access Routers" section on page 2-5.

Figure 16-3 Installing a DSP Expansion Module



Adding Port Expansion Modules

Port expansion modules can be used to increase the number of ports supported on the high-density analog telephony network module.

To install port expansion modules, follow these steps:

Step 1 Decide if the expansion board is going in the EM0 slot or EM1 slot, as shown in Figure 16-4.

Step 2 Insert the connector on the port expansion module into the module connector on the network module, as shown in Figure 16-4. Use the alignment pins on the bracket to correctly align the expansion module. If the pin does not properly align with the expansion module, the rear bracket can be adjusted by loosening the screw underneath the bracket and tightening it when the module is correctly in place.

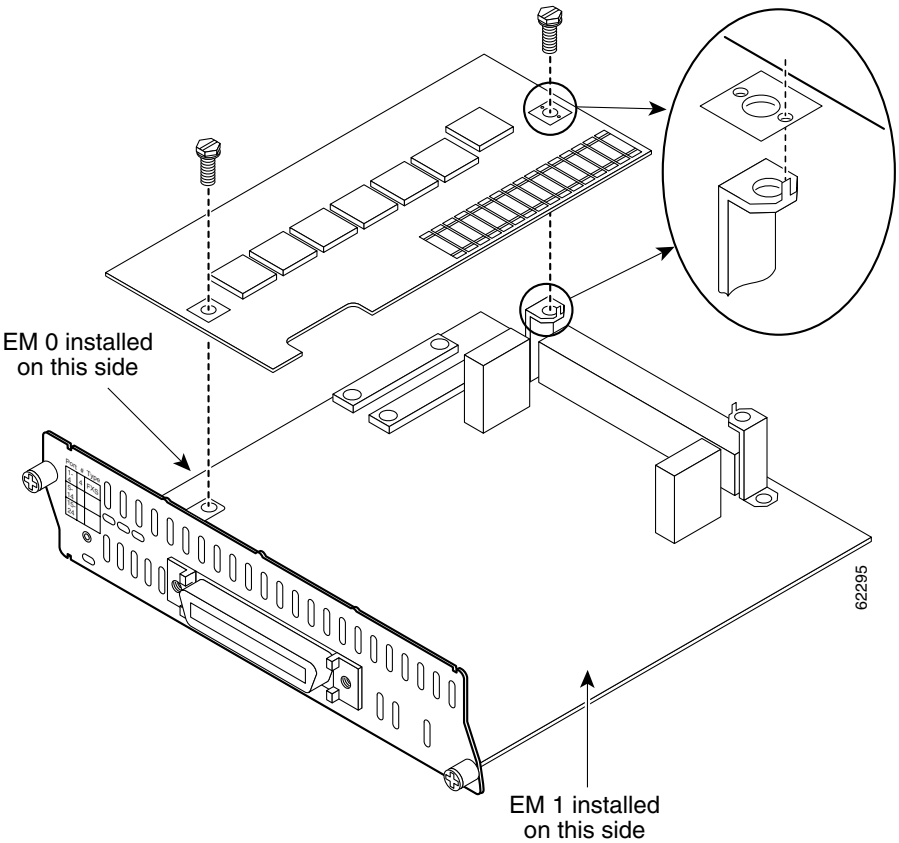
Note Be sure to press firmly on the port expansion module until the board seats securely on the connector.

Caution For each expansion module, two mounting screws must be installed with 6-8 lbs-in (67.8 N-cm) of torque. Failure to properly secure the expansion module to the base module with two screws compromises product reliability. **In the case of FXO ports, failure to properly tighten both mounting screws causes FXO ground-start outgoing call operation to fail**.

Step 3 Insert the screws from the hardware kit through the port expansion module into the brackets on the network module.

Warning **Failure to secure the expansion module to the base module with two screws defeats the earth ground, causing a potential safety hazard.** Statement 347

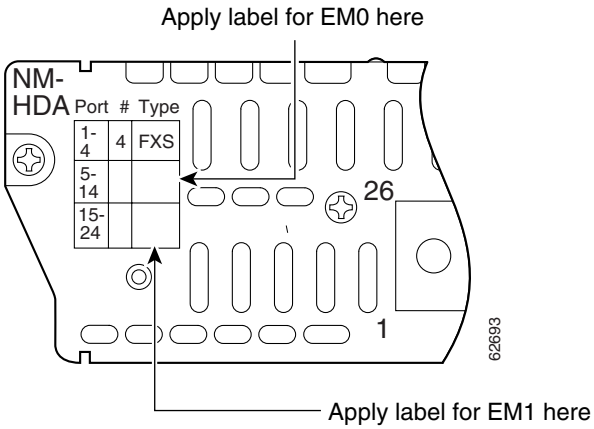
Figure 16-4 Installing a Port Expansion Module



Step 4 Apply the appropriate label on the front of the card, as shown in Figure 16-5.

Step 5 Install the network module into the router, as described in the "Installing Cisco Network Modules in Cisco Access Routers" section on page 2-5.

Figure 16-5 Label Locations for Expansion Ports



High-Density Analog Telephony Network Module LEDs

Figure 16-6 shows high-density analog telephony network module LEDs. Table 16-3 describes their meaning.

Figure 16-6 High-Density Analog Telephony Network Module LEDs

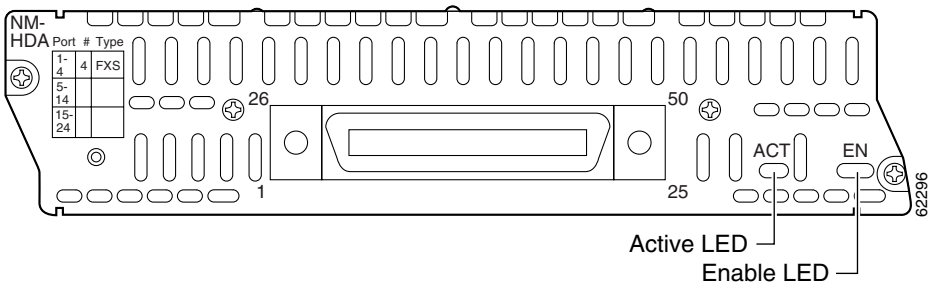


Table 16-3 High-Density Analog Telephony Network Module LEDs

LED	Meaning
EN	Green indicates that the module has passed its self-tests and is available to the router.
ACT	Green indicates that the module is ready to process data. It goes on when the boot process is complete and stays on during normal operation.

High-Density Analog Voice Card Pinouts

Figure 16-7 shows the RJ-21 connector wiring for the cable used for the high-density analog voice card; Table 16-4 lists the pinouts. The port usage depends on the type of expansion cards installed.

Figure 16-7 RJ-21 Connector Wiring

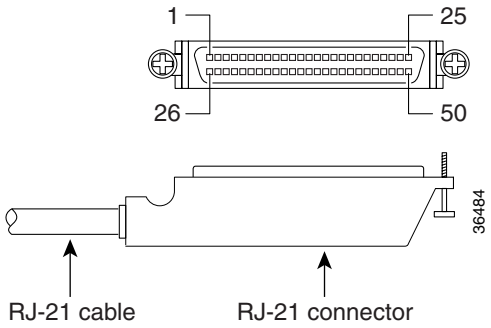


Table 16-4 RJ-21 Connections for the High-Density Analog Voice Network Module

RJ-21 Connector			NM-HDA Port	Network Module Reference		
Pair	Tip Conductor	Ring Conductor				
1	26	1	0	FXS		Base card
2	27	2	1	FXS		
3	28	3	2	FXS		
4	29	4	3	FXS		
5	30	5	4	FXS	FXO	Expansion board in slot 0
6	31	6	5	FXS	FXO	
7	32	7	6	FXS	FXO	
8	33	8	7	FXS	FXO	
9	34	9	8	FXS	Unused	
10	35	10	9	FXS	Unused	
11	36	11	10	FXS	Unused	
12	37	12	11	FXS	Unused	
13	38	13	12	Unused	Unused	
14	39	14	13	Unused	FXO failover	
15	40	15	14	FXS	FXO	Expansion board in slot 1
16	41	16	15	FXS	FXO	
17	42	17	16	FXS	FXO	
18	43	18	17	FXS	FXO	
19	44	19	18	FXS	Unused	
20	45	20	19	FXS	Unused	
21	46	21	20	FXS	Unused	
22	47	22	21	FXS	Unused	
23	48	23	22	Unused	Unused	
24	49	24	23	Unused	FXO failover	
25	50	25	—	Unused		

CHAPTER 17

Connecting Ethernet Switch Network Modules

This chapter describes how to connect Ethernet switch network modules and contains the following sections:

Tip To determine whether your router supports a specific network module, see Table 1-6 on page 1-16.

Ethernet Switch Network Modules

This chapter explains how to install the 16- and 36-port Ethernet switch network modules. The Ethernet switch network module is a modular, high-density voice network module that provides Layer 2 switching across Ethernet ports. The 16-port Ethernet switch network module has 16 10/100BASE-TX ports and an optional 10/100/1000BASE-T Gigabit Ethernet port. The 36-port Ethernet switch network module has 36 10/100BASE-TX ports and 2 optional 10/100/1000BASE-T Gigabit Ethernet ports. The 36-port Ethernet switch network module requires a double-wide slot. An optional power module can also be added to provide inline power for IP telephones.

The10/100BASE-TX ports and Gigabit Ethernet ports on the Ethernet switch network module are connected to the network using RJ-45 connectors on the front panel. The power module is connected to an external power supply using a power connection cable. The front of the 16-port card is shown in Figure 17-1. The front panel of the 36-port card is shown in Figure 17-2.

Figure 17-1 16-Port Ethernet Switch Network Module

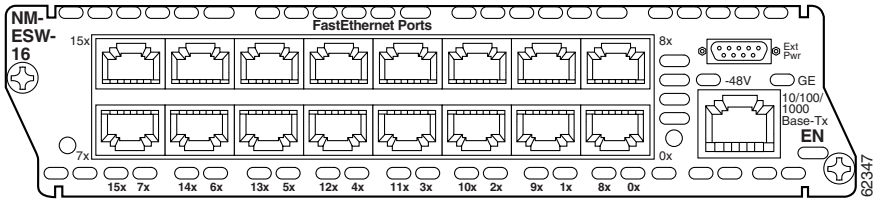
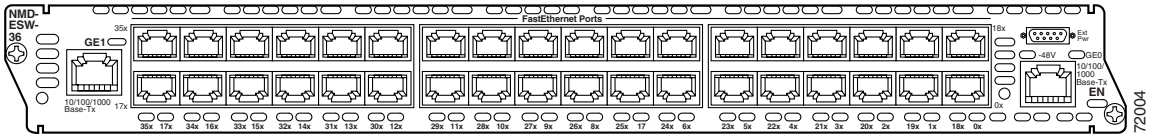


Figure 17-2 36-Port Ethernet Switch Network Module



Requirements for Installing Two Ethernet Switch Network Modules in a Single Chassis

A maximum of two Ethernet switch network modules can be installed in a single chassis. If two Ethernet switch network modules of any type are installed in the same chassis, the following configuration requirements must be met:

- Both Ethernet switch network modules must have an optional Gigabit Ethernet expansion board installed.
- An Ethernet crossover cable is connected to the two Ethernet switch network modules using the optional Gigabit Ethernet expansion board ports.
- Intrachassis stacking for the the optional Gigabit Ethernet expansion board ports is configured. For information about intrachassis stacking configuration, see the *16- and 36-Port Ethernet Switch Module for Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 series* feature document.

Without this configuration and connection, duplications will occur in the VLAN databases, and unexpected packet handling may occur.

Power Considerations

The Ethernet switch network module supports inline powering of IP telephones with –48-V power. This allows IP phones to be plugged into the standard RJ-45 jack and be powered from this source rather than having a separate plug into an AC wall outlet. The Ethernet switch network module requires delivery of –48-V power to the network module in order to provide inline powering of IP telephones.

Cisco 2800 series, Cisco 3700 series, and Cisco 3800 series routers supply –48 V power internally (with AC-IP power supplies) to the Ethernet switch service modules. To support Cisco 2600 series and Cisco 3600 series routers, which do not supply –48-V internal power, the network module has an external connector for connection to an external –48-V power supply.

The Ethernet switch network module distributes the –48-V power to each of the Ethernet ports that are configured for line power. Each port can be independently configured for line power.

Note When using the NM-16ESW network module with the MWR 1941-DC router, shielded cables are required, and IP phone inline power is not supported.

Restrictions for Cisco 3700 Series Routers

Cisco 3700 series routers contain internal –48-V power supplies to supply power to the Ethernet switch network module.

For the Cisco 3745 router, the following specifications apply:

- The Cisco 3745 router can have one or two internal –48-V power supplies. The internal supplies of the Cisco 3745 router are configured to be redundant by default.
- With a single power supply, the Cisco 3745 router can provide up to 360 W. This is enough power for up to 36 10-W IP phones. With two nonredundant power supplies, 640 W can be provided, supporting up to 64 10-W IP phones.
- The Cisco 3745 router main board has four independent signals to indicate status on both internal power supplies. Changes on the state of any of these four signals interrupts the main processor on the Cisco 3745 router so software can take the appropriate action.

Cisco 3725 routers have a single –48-V supply. Cisco 3725 routers do not report any power supply status. The only software indication of –48-V status is the –48-V status bit provided on the 16-port Ethernet switch network module board.

Restrictions for Cisco 2600 Series and Cisco 3600 Series Routers

Cisco 2600 series and Cisco 3600 series routers do not supply –48-V power, so an external –48-V supply is required to support inline power for IP phones. This external power supply connects to the Ethernet switch network module faceplate with a cable.

An external power supply plugged into an Ethernet switch network module provides power only for that specific network module. To supply redundant power, a Y cable can be used so that two external power supplies are connected to the same card.

For more information about external power supplies, see the *Cisco External Power Supply for Cisco Ethernet Switch Network Modules Installation Guide*.

Connecting the Ethernet Switch Network Module to the Network

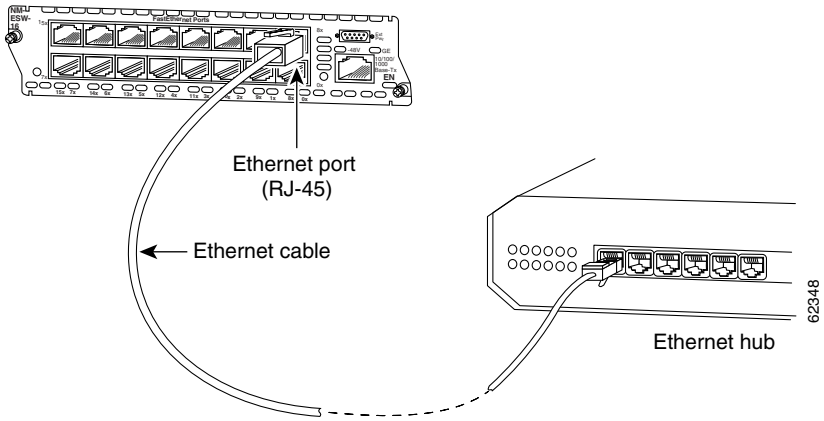
Warning **Voltages that present a shock hazard can exist on inline power circuits if interconnections are made by using uninsulated exposed metal contacts, conductors, or terminals. Avoid using such interconnection methods unless the exposed metal parts are in a restricted access location and users and service people who are authorized to access the location are made aware of the hazard. A restricted access area can be accessed only through the use of a special tool, lock and key, or other security means.** Statement 1072

The Ethernet switch network module is connected to an Ethernet switch or hub with RJ-45 cables. (See Figure 17-3.) RJ-45 cables are not provided with the network module. For ordering information, see the "Obtaining Technical Assistance" section on page xi.

Note When using the NM-16ESW with the MWR 1941-DC router, shielded cables are required.

Tip For information about RJ-45 crossover cables, go to the following URL: http://www-tac.cisco.com/Support_Library/Hardware/LAN_Switches_and_Modules/Cat6000/Troubleshooting/QuickTip.998950447.html

Figure 17-3 16-Port Ethernet Switch Card Connected to Ethernet Switch or Hub



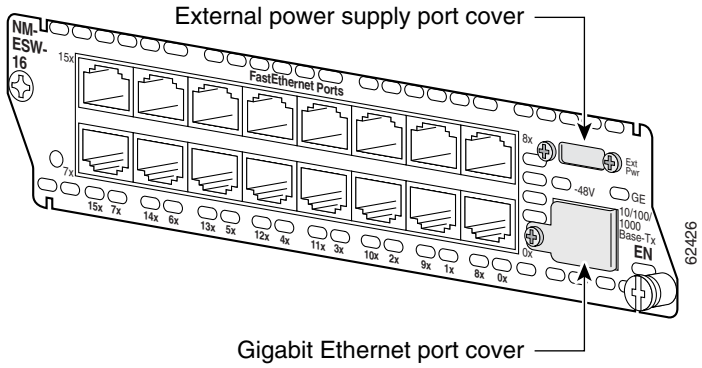
Adding an Optional Gigabit Ethernet Expansion Board

An optional Gigabit Ethernet expansion board can be installed to support a 10/100/1000BASE-T Gigabit Ethernet port.

To install a Gigabit Ethernet expansion board, follow these steps:

Step 1 Use a Phillips screwdriver to remove the cover on the Gigabit Ethernet board port, as shown in Figure 17-4.

Figure 17-4 Gigabit Ethernet Board Port Cover on the Ethernet Switch Network Module



Step 2 Guide the external connector through the Gigabit Ethernet expansion port opening on the card faceplate.

Step 3 Insert the connector on the Gigabit Ethernet expansion board into the board connector on the network module. Inspect the board to ensure that the board is fully connected. (See Figure 17-5 for 16-port Ethernet switch network modules or Figure 17-6 for 36-port Ethernet switch network modules.)

Caution Be sure to press firmly on the Gigabit Ethernet expansion board until the board seats correctly onto the connector. When the Gigabit Ethernet expansion board is seated properly, the standoff is flush with the board. If this board is not firmly seated, failures can occur.

Step 4 Insert the screw from the board installation kit through the Gigabit Ethernet expansion board into the standoff on the network module.

Figure 17-5 Installing a Gigabit Ethernet Expansion Board on a 16-Port Cisco Ethernet Switch Network Module

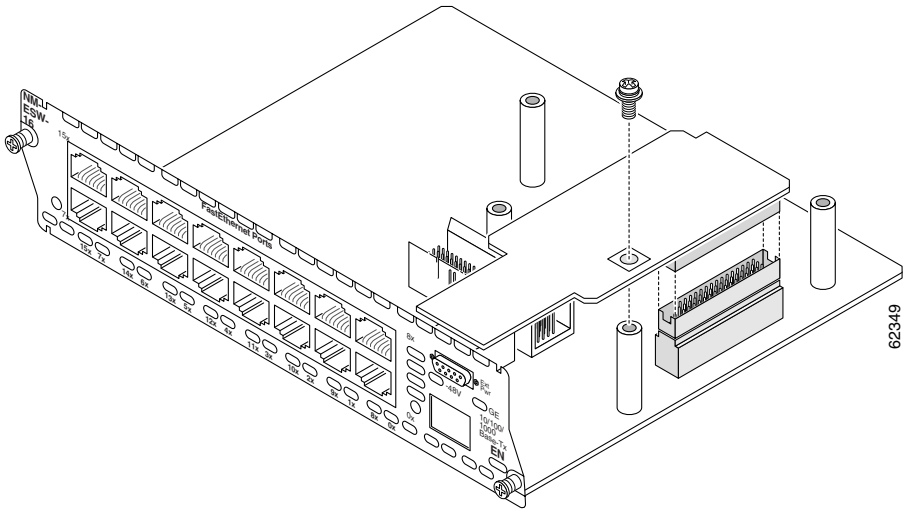
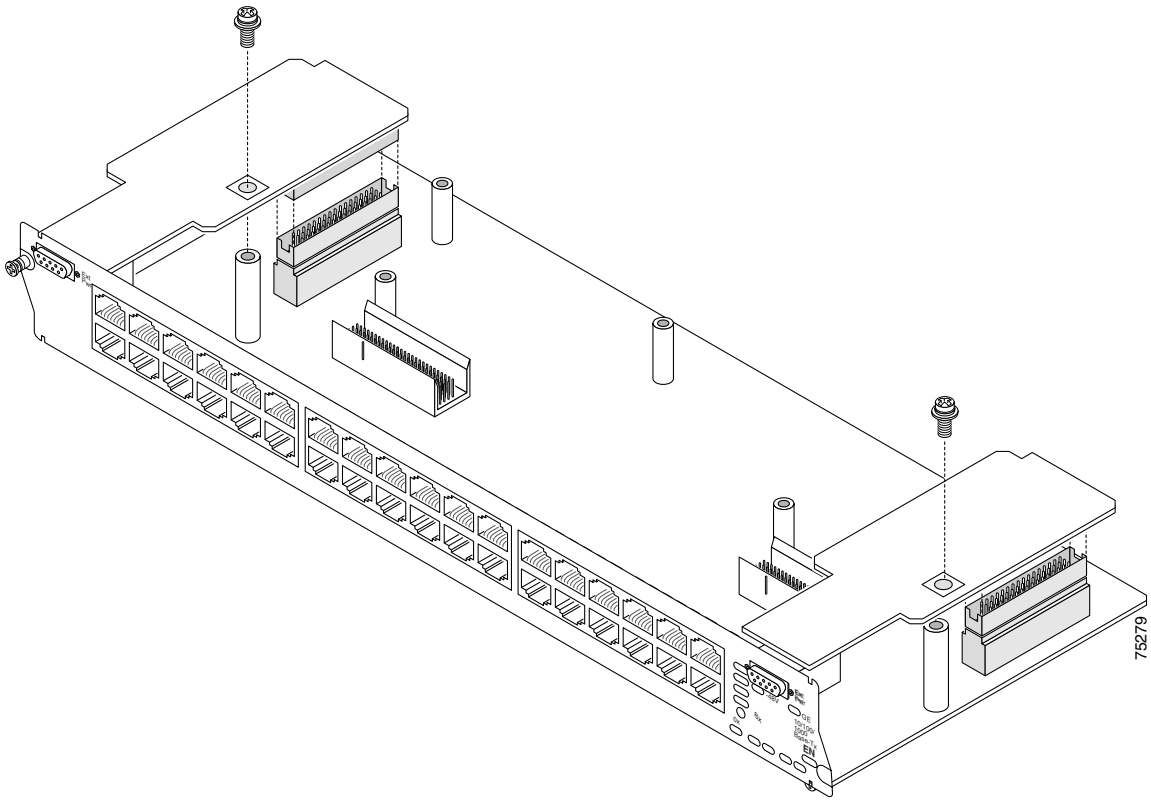


Figure 17-6 Installing a Gigabit Ethernet Expansion Board on a 36-Port Cisco Ethernet Switch Network Module



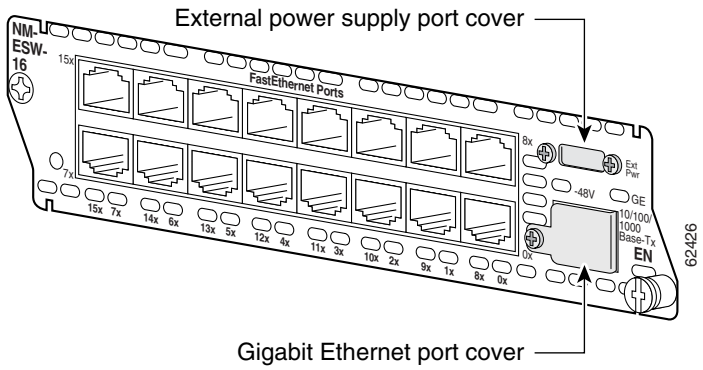
Adding an Optional Power Board

An optional power board can be used if the Ethernet switch network module requires external –48-V power for IP telephones. Installation and configuration of the external power supply system is described in the *Cisco External Power Supply for Cisco Ethernet Switch Network Modules Installation Guide*.

To install power boards, follow these steps:

Step 1 Use a Phillips screwdriver to remove the cover on the external power board port, as shown in Figure 17-7.

Figure 17-7 Power Board Port Cover on the Ethernet Switch Network Module



Step 2 On the power board, remove the thumb screws on either side of the power board port. Put these in a safe place, because they will be replaced when the power board is installed.

Step 3 Guide the external connector through the power board port opening on the card faceplate.

Step 4 Insert the connector on the power board into the connector on the network module. (See Figure 17-8 for 16-port Ethernet switch network modules and Figure 17-9 for 36-port Ethernet switch network modules.)

Note Be sure to press firmly on the power board until the board seats correctly onto the connector.

Step 5 Insert the screws from the board installation kit through the power board into the standoffs on the network module.

Step 6 Replace the thumbscrews on either side of the power board port. Make sure that the thumbscrews are tightened firmly.

Warning **Do not connect the external power supply cable to the power connector on the front of the network module until the network module has been inserted into the router chassis.**

Step 7 After installing the network module into the chassis, connect the power cable to the power module connector on the front of the network module. See the *Cisco External Power Supply for Cisco Ethernet Switch Network Modules Installation Guide* for more information.

Figure 17-8 Installing a Power Board in a 16-Port Ethernet Switch Network Module

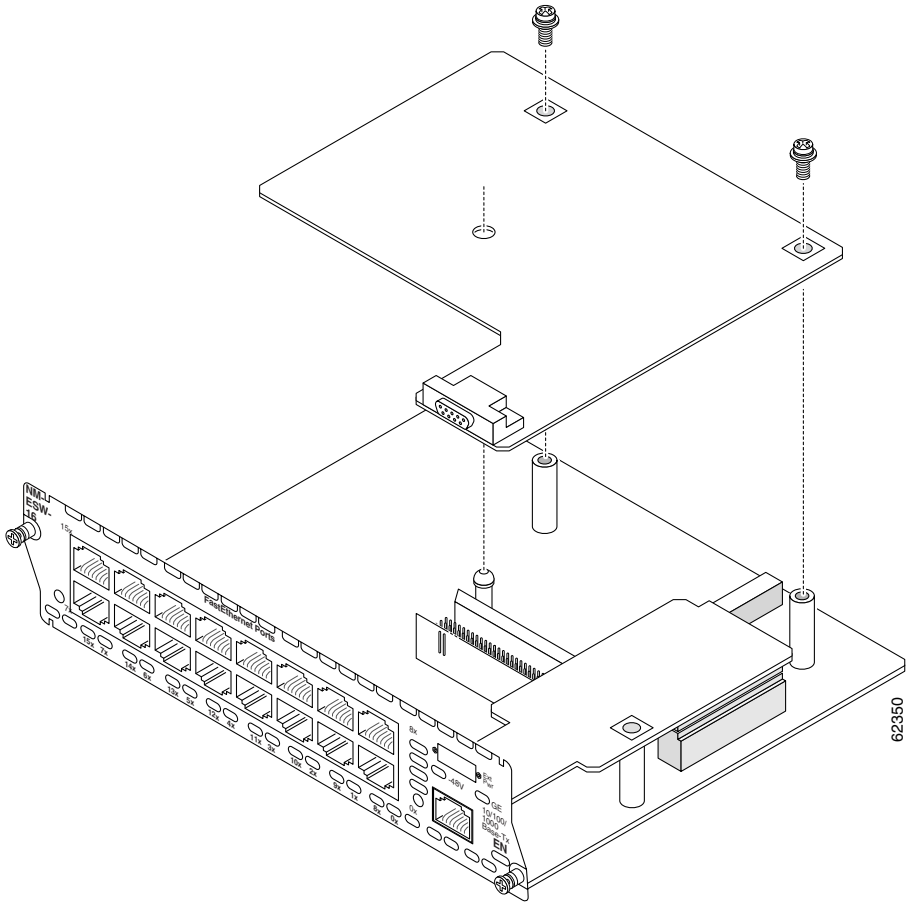
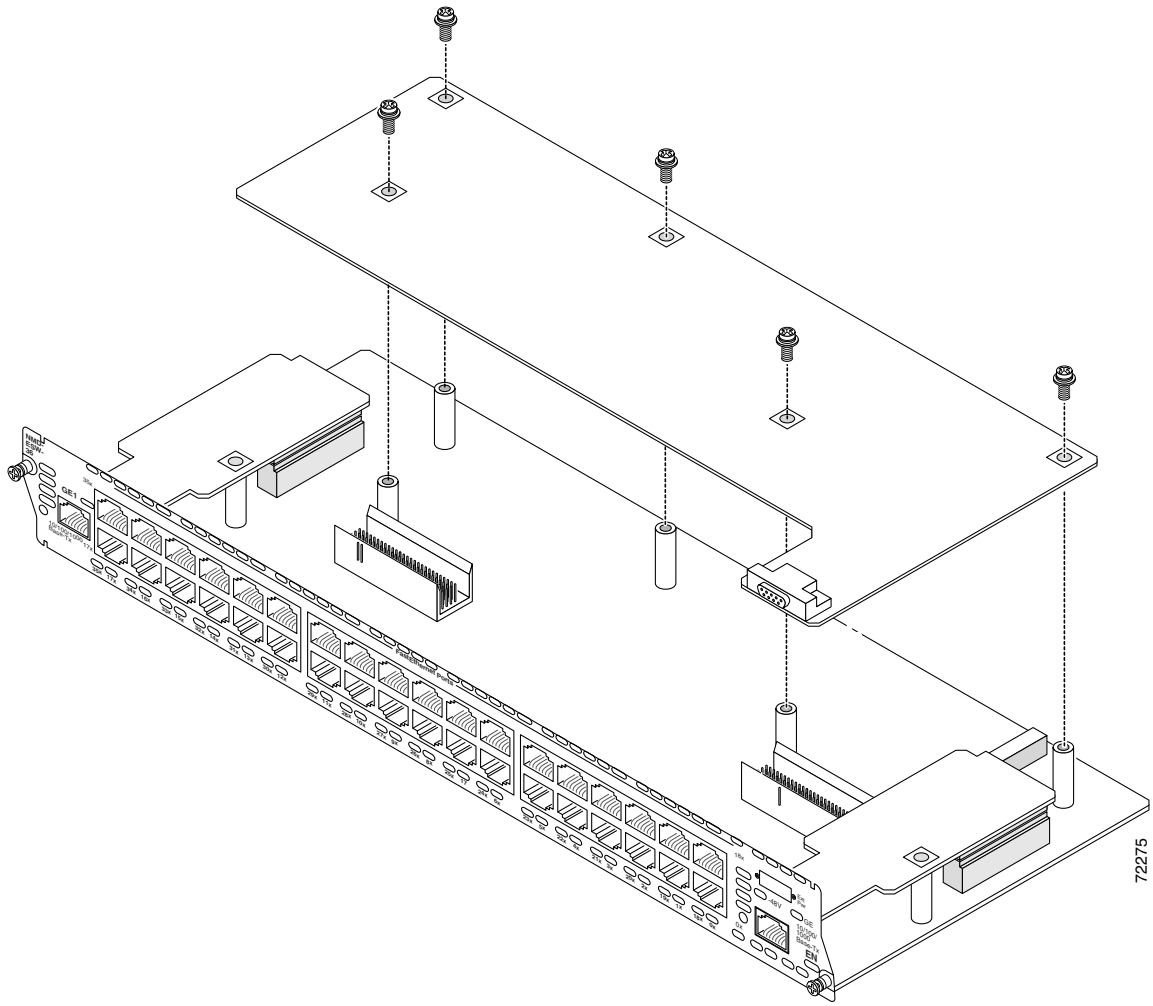


Figure 17-9 Installing a Power Board in a 36-Port Ethernet Switch Network Module



Ethernet Switch Network Module LEDs

Figure 17-10 shows 16-port Ethernet switch network module LEDs. Figure 17-11 shows 36-port Ethernet switch network module LEDs. Table 17-1 describes their meaning.

Figure 17-10 16-Port Ethernet Switch Network Module LEDs

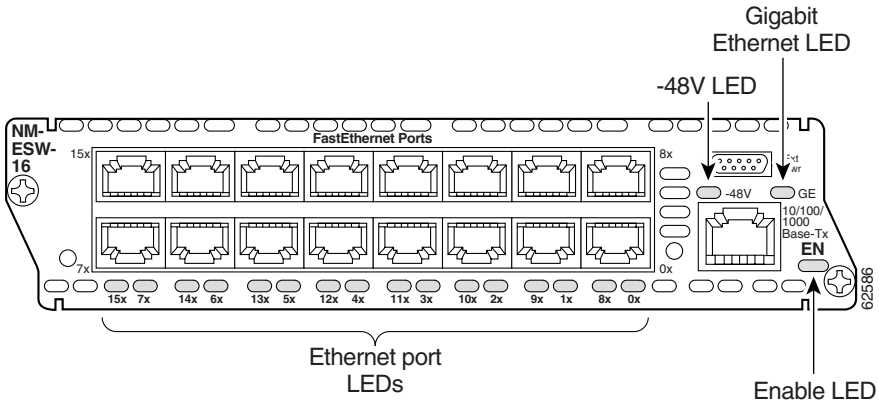


Figure 17-11 36-Port Ethernet Switch Network Module LEDs

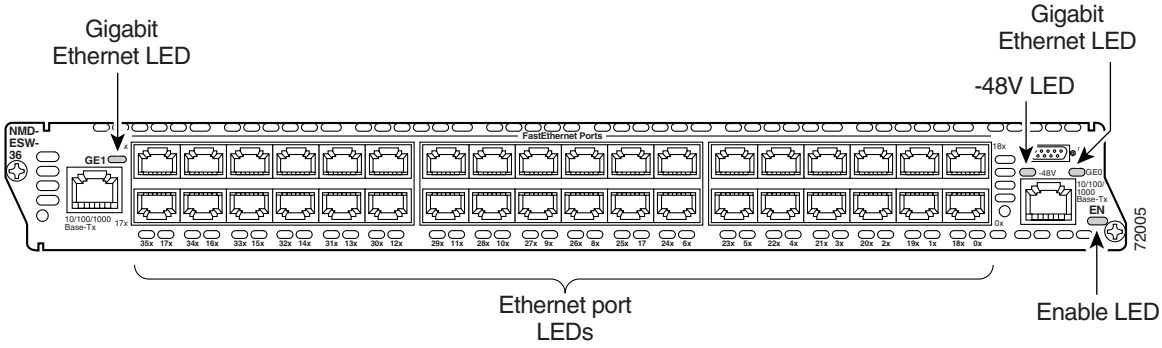


Table 17-1 Ethernet Switch Network Module LEDs

LED	Meaning
0–16 (for 16-port) 0–36 (for 36-port)	Green indicates that individual Ethernet port is functioning.
–48-V	Off indicates that no –48-V power is going to the network module. Green indicates –48-V power is present on the network module. Amber indicates that there is a problem with one or more of the internal or external –48-V power supplies.
GE	Green indicates that the Gigabit Ethernet port is functioning.
EN	Green indicates that the module has passed its self-tests and is available to the router.

CHAPTER 18

Connecting Cisco EtherSwitch Service Modules

This chapter describes how to connect Cisco EtherSwitch service modules. It contains the following sections:

Note This document describes the Cisco EtherSwitch service modules only. For information about other Cisco Ethernet switch network modules, see the "Connecting Ethernet Switch Network Modules to a Network" section at the following URL:

http://www.cisco.com/en/US/products/hw/modules/ps2797/products_module_installation_guide_chapter09186a00800b168c.html

Tip To determine whether your router supports a specific network module, see Table 1-6 on page 1-16.

Cisco EtherSwitch Services Modules

Cisco EtherSwitch service modules are complete switching platforms and can be stacked with other Cisco switches to form a switching stack integrated with the router and capable of supporting the following features:

- Dynamic addition and removal of individual Cisco EtherSwitch service modules from the switching stack
- Integrated management through all management interfaces (command-line interface [CLI], Simple Network Management Protocol [SNMP], and HTTP)
- Features such as UplinkFast, EtherChannel, and equal-cost routing across the switching stack that provide redundancy and reduce network disruption from individual component failure

For information about these and other Cisco EtherSwitch service module features, see the *Cisco EtherSwitch Service Modules* Feature Guide at the following URL:

http://www.cisco.com/en/US/products/hw/modules/ps2797/products_feature_guide09186a0080415bae.html

Note For release note information about Cisco Ethernet switch network modules, see the *Release Notes for the EtherSwitch Service Modules, Cisco IOS Release 12.2(25)SEC* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/12225sec/index.htm

This section describes the Cisco EtherSwitch service modules. It contains the following sections:

- Cisco EtherSwitch Service Module Overview
- Cisco EtherSwitch Service Module Ports
- Cisco EtherSwitch Service Module LEDs

Cisco EtherSwitch Service Module Overview

The Cisco EtherSwitch service modules are stackable modules to which you can connect Cisco IP telephones, Cisco wireless access point workstations, and other network devices such as servers, routers, switches, and other network switch modules.

The following modules are available with this release of the hardware:

- NME-16ES-1G—16 10/100 Ethernet ports, 1 10/100/1000 Ethernet port, no StackWise connector ports, single-wide, no Power over Ethernet (PoE) support (see Figure 18-1)

Caution To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the 16-port EtherSwitch service module (NME-16ES-1G) only to intra-building or non-exposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

- NME-16ES-1G-P—16 10/100 Ethernet ports, 1 10/100/1000 Ethernet port, no StackWise connector ports, single-wide, with PoE support (see Figure 18-1)

Caution To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the 16-port EtherSwitch service module with PoE (NME-16ES-1G-P) only to intra-building or non-exposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

- NME-X-23ES-1G—23 10/100 Ethernet ports, 1 10/100/1000 Ethernet port, no StackWise connector ports, extended single-wide, no PoE support (see Figure 18-2)

Caution To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the 23-port EtherSwitch service module (NME-X-23ES-1G) only to intra-building or non-exposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

- NME-X-23ES-1G-P—23 10/100 Ethernet ports, 1 10/100/1000 Ethernet port, no StackWise connector ports, extended single-wide, with PoE support (see Figure 18-2)

Caution To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the 23-port EtherSwitch service module with PoE (NME-X-23ES-1G-P) only to intra-building or non-exposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

- NME-XD-24ES-1S-P—24 10/100 Ethernet ports, 1 small form-factor pluggable (SFP) port, 2 StackWise connector ports, extended double-wide, with PoE support (see Figure 18-3)

Warning **To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the 24-port EtherSwitch service module with PoE (NME-XD-24ES-1S-P) only to intra-building or non-exposed wiring or cabling. The intra-building port(s) of the equipment or subassembly must not be metallically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE, Issue 4) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring.**

Note This module is hereafter referred to as the Cisco StackWise EtherSwitch service module.

- NME-XD-48ES-2S-P—48 10/100 Ethernet ports, 2 SFP ports, no StackWise connector ports, extended double-wide, with PoE support (see Figure 18-4)

Warning **To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the NME-XD-48ES-2S-P network module only to intra-building or unexposed wiring or cable. The intrabuilding cable must be shielded and the shield must be grounded at both ends. The intra-building port(s) of the equipment or subassembly must not be metallically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE, Issue 4) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring.**

Note

- You can install only one Cisco StackWise EtherSwitch NME-XD-24ES-1S-P service module in a single router chassis.
- You can install one Cisco EtherSwitch service module into a single Cisco 2821 or Cisco 2851 router, up to two Cisco EtherSwitch service modules into a single Cisco 3825, Cisco 3845 router, or up to four Cisco EtherSwitch NME-16ES-1G or NME-16ES-1G-P service modules in the Cisco 3745 or Cisco 3845 routers.
- Installing more than two Cisco EtherSwitch service modules in a router chassis requires specific cabling. For information about cabling multiple Cisco EtherSwitch service modules, see the *Cisco Network Modules Hardware Installation Guide* at the following URL:

  http://www.cisco.com/en/US/products/hw/modules/ps2797/products_module_installation_guide_book09186a00802d2910.html

Table 18-1 shows the Cisco router platforms that support the Cisco EtherSwitch service modules.

Table 18-1 Router Platforms Supporting Cisco EtherSwitch Service Modules

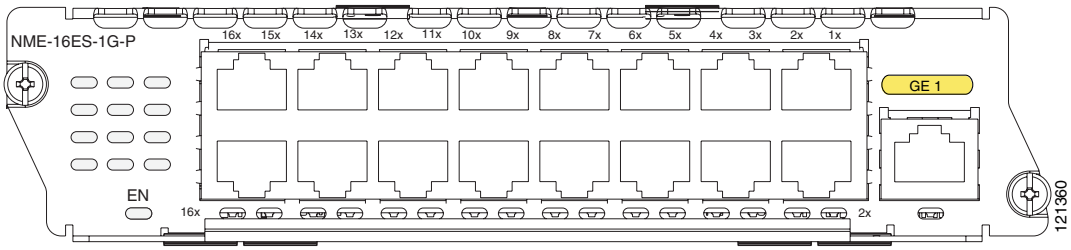
Router	NME-16ES-1G, NME-16ES-1G-P	NME-X-23ES-1G, NME-X-23ES-1G-P	NME-XD-24ES-1S-P	NME-XD-48ES-2S-P
Cisco 3845	Yes	Yes	Yes	Yes
Cisco 3825	Yes	Yes	Yes	Yes
Cisco 2851	Yes	Yes	Yes	Yes
Cisco 2821	Yes	Yes	No	No
Cisco 2811	Yes	No	No	No
Cisco 3745	Yes	No	No	No
Cisco 3725	Yes	No	No	No
Cisco 2691 (without –48 V)	Yes	No	No	No

16-Port Cisco EtherSwitch Service Module

Figure 18-1 shows the 16-port Cisco EtherSwitch service module.

Note The 10/100/1000 Gigabit Ethernet port on the 16-port Cisco EtherSwitch service module does not support PoE.

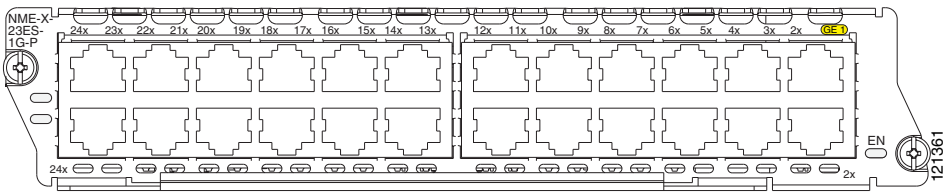
Figure 18-1 NME-16ES-1G and NME-16ES-1G-P Faceplate



23+1-Port Cisco EtherSwitch Service Module

Figure 18-2 shows the 23+1-port Cisco EtherSwitch service module.

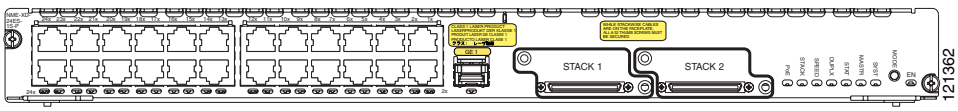
Figure 18-2 NME-X-23ES-1G and NME-X-23ES-1G-P Faceplate



24-Port Cisco StackWise EtherSwitch Service Module

Figure 18-3 shows the 24-port Cisco StackWise EtherSwitch service module.

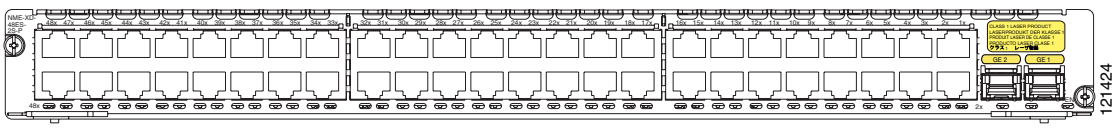
Figure 18-3 NME-XD-24ES-1S-P Faceplate Showing Two Cisco StackWise Connector Ports



48-Port Cisco EtherSwitch Service Module

Figure 18-4 shows the 48-port Cisco EtherSwitch service module.

Figure 18-4 NME-XD-48ES-2S-P Faceplate



Cisco EtherSwitch Service Module Ports

The following sections describes the port types and port numbering on the service modules:

- Port Types
- Port Numbering

Port Types

All Cisco EtherSwitch service modules, including the Cisco StackWise EtherSwitch service module, use RJ-45 connectors to provide Fast Ethernet (FE) connections.

The single-wide 16- and 24-port Cisco EtherSwitch service modules have one additional RJ-45 connector to support a Gigabit Ethernet connection. The double-wide, 48-port Cisco EtherSwitch service module has two SFP Gigabit Ethernet module slots.

The double-wide Cisco StackWise EtherSwitch service module has one SFP Gigabit Ethernet module slot.

Note Both SFP and Gigabit Ethernet interfaces can support trunks.

Note Cisco EtherSwitch service modules do not have a physical console interface, but are accessible for software configuration and other operational procedures through console sessions between the Cisco EtherSwitch service module and the host router.

10/100 and 10/100/1000 Ports

You can set the 10/100 ports on the Cisco EtherSwitch service module to operate in any combination of half duplex, full duplex, 10 Mbps, or 100 Mbps. You can set the 10/100/1000 ports to operate at 10 Mbps, 100 Mbps, or 1000 Mbps in full duplex. You can also set these ports for speed and duplex autonegotiation in compliance with IEEE 802.3ab. (The default setting is autonegotiate.)

When set for autonegotiation, the port senses the speed and duplex settings of the attached device and advertises its own capabilities. If the connected device also supports autonegotiation, the Cisco EtherSwitch service module port negotiates the best connection (that is, the fastest line speed that both devices support and full-duplex transmission if the attached device supports it) and configures itself accordingly. In all cases, the attached device must be within 100 meters (328 feet).

All 10/100 ports on the NME-16ES-1G-P, NME-X-23ES-1G-P, NME-XD-24ES-1S-P, and NME-XD-48ES-2S-P Cisco EtherSwitch service modules can provide power to IEEE 802.3af-compliant and noncompliant Power over Ethernet (PoE) devices. PoE devices are Cisco IP phones, Cisco access points, and some Cisco switches. PoE, formerly referred to as inline power, is available in all network module form factors supported by Cisco modular access routers.

Table 18-2 provides information on Cisco EtherSwitch service module port speed and duplex information.

Table 18-2 Port Speed and Duplex

Port Function	Explanation
Speed	The operating speed of the switch port. You can choose Auto (autonegotiation) if the connected device can negotiate the link speed with the switch port. The default settings are: • Auto for the external 10/100-Mbps Fast Ethernet ports • Auto for the external Gigabit Ethernet RJ-45 (10/100/1000-Mbps) ports • 1000 Mbps for the SFP module ports
Duplex	The duplex mode of the switch port. Choose from one of the following: • Auto (autonegotiation) if the connected device can negotiate with the switch • Full (full duplex) if both devices can send data at the same time • Half (half duplex) if one or both devices cannot send data at the same time The default settings are: • Auto for the external 10/100-Mbps Fast Ethernet ports • Auto for the external Gigabit Ethernet RJ-45 (10/100/1000-Mbps) ports • Full for the 1000-Mbps ports (SFP) **Note** You cannot set the port to half duplex if the port speed is set to Auto.

SFP Modules

The Cisco EtherSwitch service module supports Gigabit Ethernet SFP modules for fiber-optic connections. These laser optical transceiver modules are field-replaceable, and you can insert them into an SFP module slot. You use fiber-optic cables with LC connectors to connect to an SFP module. You can use the SFP modules for gigabit uplink connections to other devices.

The SFP modules support 850- to 1550-nm nominal wavelengths.

The Cisco StackWise EtherSwitch service module and the 48-port Cisco EtherSwitch service module have one or two SFP module slots into which you can install these SFP module types:

- 1000BASE-CWDM
- 1000BASE-LH
- 1000BASE-LX
- 1000BASE-SX
- 1000BASE-T
- 1000BASE-ZX

For more information about SFP modules, see the *Cisco Network Modules Hardware Installation Guide* at the following URL:

http://www.cisco.com/en/US/products/hw/modules/ps2797/products_module_installation_guide_book09186a00802d2910.html

Port Numbering

The Ethernet ports are numbered right to left, top to bottom. The port numbering scheme to configure the ports on the Cisco EtherSwitch service module includes the port type (such as **fa** or **fastethernet** for Fast Ethernet, or **gi** or **gigabitethernet** for Gigabit Ethernet), the stack member number (range is 1 to 9), the module slot number (always 0), and the switch port number.

For example, to configure the Fast Ethernet port 3 on stack member 1, the interface configuration command would be:

```
switch (config)# interface fa1/0/3
```

Cisco EtherSwitch Service Module LEDs

Cisco EtherSwitch service module LEDs provide green, amber, and off states for system and port status. The following sections describe LEDs on the service modules:

- EN LED
- System LED
- Master LED
- Port Mode LEDs
- Port LEDs
- Port LEDs in Stack Mode

Note LEDs for System, Master, Port Mode, and PoE are available on the 24-port Cisco StackWise EtherSwitch service module only. Port LEDs on nonstacking Cisco EtherSwitch service modules only show link status.

EN LED

All Cisco EtherSwitch service modules have an enable (EN) LED. This LED indicates that the module has passed its self-test and is available to the router. (See Figure 18-5.) Table 18-3 lists the EN LED colors and their meanings.

Figure 18-5 EN LED

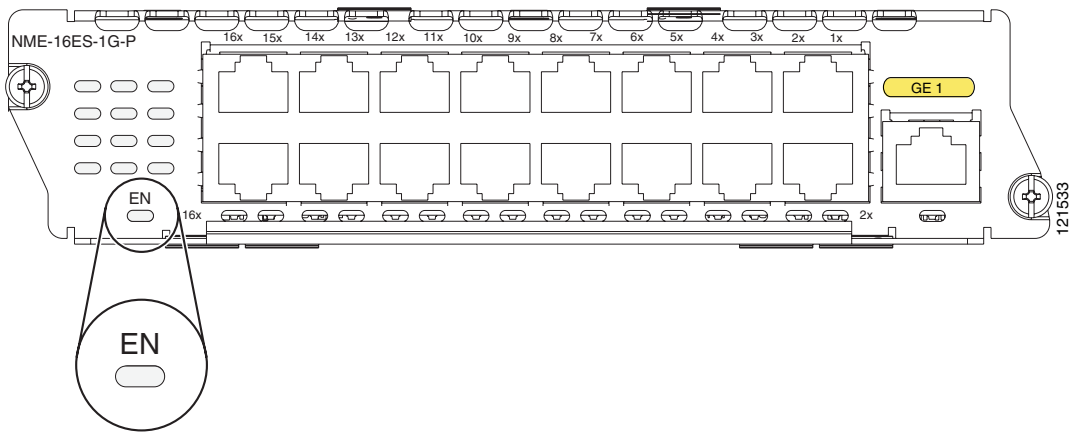


Table 18-3 EN LED

Color	System Status
Off	The Cisco EtherSwitch service module is not yet operational.
Green	The Cisco EtherSwitch service module is operational.
Amber	A stack error has occurred.

System LED

The Cisco StackWise EtherSwitch service module has a system (SYST) LED (see Figure 18-6), which indicates that the module POST is in progress. Table 18-4 lists the system LED colors and their meanings.

Figure 18-6 Mode Button and the EN, SYST, MASTR, and Mode LEDs

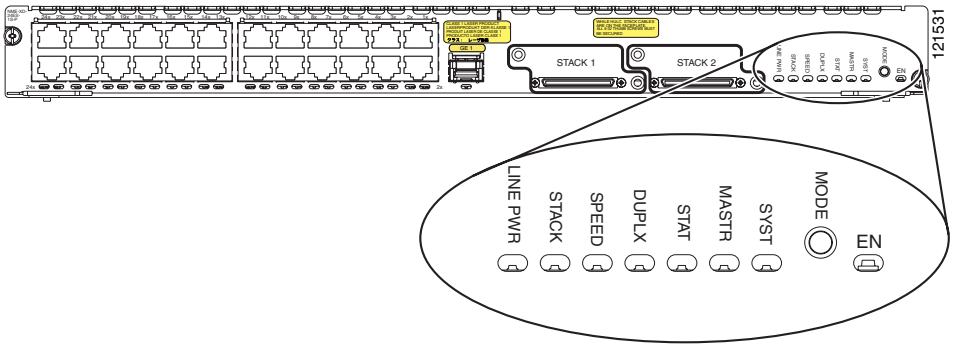


Table 18-4 System (SYST) LED

LED Color	Description
Off	Module POST is not in progress.
Green	Module POST is in progress.
Amber	System is receiving power but is not functioning properly.

Master LED

The Cisco StackWise EtherSwitch service module has a master LED (see Figure 18-6) that shows the stack master status. Table 18-5 lists the master LED colors and their meanings.

Table 18-5 Master (MASTR) LED

LED Color	Description
Off	The Cisco StackWise EtherSwitch service module is not the stack master.
Green	The Cisco StackWise EtherSwitch service module is the stack master or a standalone module.
Amber	An error occurred when the Cisco StackWise EtherSwitch service module was electing the stack master, or a stack error occurred.

Port Mode LEDs

The Cisco StackWise EtherSwitch service module has a Mode button that allows you to toggle through the port LED modes. (See Figure 18-6.) The port modes determine the type of information displayed through the port LEDs. For more information about port LEDs, see the "Port LEDs" section on page 18-11.

To choose or change a mode, press the Mode button until the desired mode is highlighted. When you change port modes, the meanings of the port LED colors also change.

Table 18-6 lists the modes and their meanings.

Table 18-6 Mode LEDs

LED	Mode	Description
STAT	Port status	The port status. In this mode, the LED shows link status and link activity. This is the default mode.
DUPLX	Port duplex mode	The port duplex mode: full duplex or half duplex.
SPEED	Port speed	The port operating speed: 10, 100, or 1000-Mbps.
STACK	Stack member status	The stack member status. If your Cisco StackWise EtherSwitch service modules are stacked and you press the Mode button on any one of the Cisco StackWise EtherSwitch service modules in the stack, all the Cisco StackWise EtherSwitch service modules in the stack change to display the same selected mode. For example, if you press the Mode button on the stack master to display SPEED, all the other Cisco StackWise EtherSwitch service modules in the stack also display SPEED.
	Cisco StackWise port status	The Cisco StackWise port status. In STACK mode, the last two port LEDs show the StackWise port status. See the "Port LEDs in Stack Mode" section on page 18-12 for more information.
LINE PWR	Inline power	The inline power status.

Port LEDs

Each port has a port LED. These port LEDs, as a group or individually, display information about the module and about the individual ports.

Table 18-7 explains how to interpret the port LED colors in different port modes on the Cisco StackWise EtherSwitch service module.

Table 18-8 explains how to interpret the port LED colors for link status on the Cisco EtherSwitch service modules.

Table 18-7 Port LEDs on the Cisco StackWise EtherSwitch Service Module

Port Mode	Port LED Color	Meaning
STAT (default mode)	Off	No link, or the port was administratively shut down.
	Green	A link is present.
	Flashing green	Activity is occurring. The port is transmitting or receiving data.
	Alternating green-amber	Link fault. Error frames can affect connectivity, and errors such as excessive collisions, Cyclic Redundancy Check (CRC) errors, and alignment and jabber errors are monitored for a link fault.
	Amber	The port is blocked by the Spanning-Tree Protocol (STP) and is not forwarding data. **Note** After a port is reconfigured, the port LED can remain amber for up to 30 seconds while STP checks the Cisco StackWise EtherSwitch service module for possible loops.
	Flashing amber	The port is blocked by STP and is transmitting or receiving packets.
DUPLX	Off	The port is operating in half-duplex mode.
	Green	The port is operating in full-duplex mode.
SPEED	**10/100 and 10/100/1000 ports**	
	Off	The port is operating at 10 Mbps.
	Green	The port is operating at 100 Mbps.
	Flashing green	The port is operating at 1000 Mbps.
	SFP ports	
	Off	The port is not operating.
	Green	The port is operating at 1000 Mbps.
STACK	Off	No stack member corresponds to that member number.
	Flashing green	Member number of the selected Cisco EtherSwitch service module.
	Green	Member number of other stack member Cisco EtherSwitch service modules.

Table 18-7 Port LEDs on the Cisco StackWise EtherSwitch Service Module (continued)

Port Mode	Port LED Color	Meaning
LINE PWR	Off	PoE mode is not selected. None of the 10/100 or 10/100/1000 ports have been denied power or are in a fault condition.
	Green	PoE mode is selected, and the PoE status is shown on the port LEDs.
	Blinking amber	PoE mode is not selected. At least one of the 10/100 or 10/100/1000 ports has been denied power, or at least one of the 10/100 or 10/100/1000 ports has a PoE fault.

Table 18-8 Port LED on the Cisco EtherSwitch Service Modules (Excluding the Cisco StackWise EtherSwitch Service Module)

Port LED Color	Description
Off	No link, or the port was administratively shut down. On PoE ports, no inline powered device (PD) detected, or the port is not connected.
Green	A link is present. The port or system is functioning normally. On PoE ports, the Cisco EtherSwitch service module is providing power to a PD.
Flashing green	Activity is occurring. The port is transmitting or receiving data. Module POST is in progress.
Alternating green-amber	Link fault. On PoE ports, the Cisco EtherSwitch service module is denying power to a PD, or is experiencing a power delivery fault.
Amber	The port is blocked by the Spanning-Tree Protocol (STP) and is not forwarding data. **Note** After a port is reconfigured, the port LED can remain amber for up to 30 seconds. On a PoE port, indicates that the port is denied power and that the port is administratively disabled. The system is receiving power but is not functioning properly.
Flashing amber	The port is blocked by STP and is transmitting or receiving packets. On a PoE port, indicates an inline power delivery fault.

Port LEDs in Stack Mode

The port LEDs in Stack mode show the stack member number of the Cisco StackWise EtherSwitch service modules in the stack. Up to nine service modules or switches can be members of a stack. Therefore, only the first nine port LEDs are used in Stack mode to reflect stack membership.

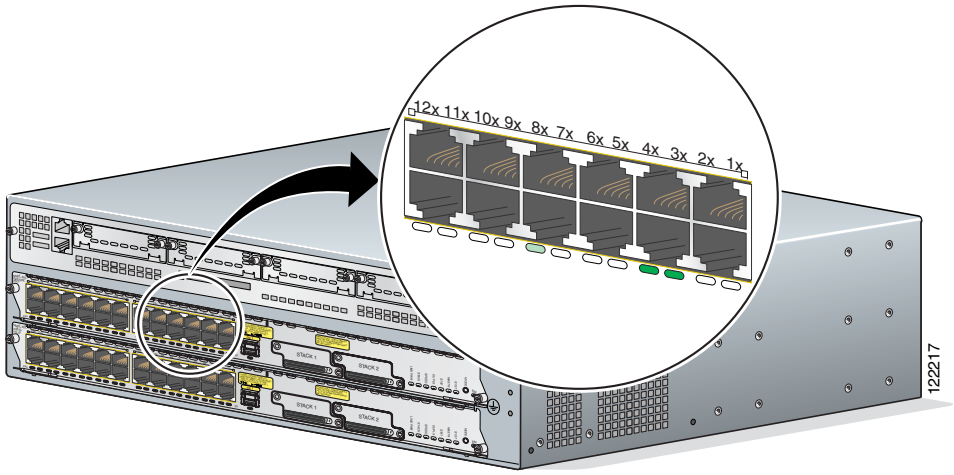
For example, you have a stack of three EtherSwitch service modules. Their stack member numbers are 3, 4, and 8. If you select the Stack mode on member number 8, then port 8x flashes green. Ports 3x and 4x display continuous green, showing you have two other stack members whose member numbers 3 and 4. All other LEDs are off since there are no other members in the stack. (See Figure 18-7.)

In addition, the last two port LEDs on the Cisco StackWise EtherSwitch service module show the status of the StackWise ports.

For more information on stack member numbers, see the *Catalyst 3750 Switch Software Configuration Guide*, Cisco IOS Release 12.2 at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/index.htm

Figure 18-7 Stack LEDs



Power Considerations

This section describes the power considerations for the router, the service module, and stacking the service modules:

- Power Considerations for the Router
- Power Considerations for the Service Module
- Powering Considerations for a Switch Stack

Warning **Voltages that present a shock hazard may exist on Power over Ethernet (PoE) circuits if interconnections are made using uninsulated exposed metal contacts, conductors, or terminals. Avoid using such interconnection methods, unless the exposed metal parts are located within a restricted access location and users and service people who are authorized within the restricted access location are made aware of the hazard. A restricted access area can be accessed only through the use of a special tool, lock and key or other means of security.** Statement 1072

Power Considerations for the Router

Cisco 2800 series, Cisco 3700 series, and Cisco 3800 series routers supply –48 V power internally (with AC-IP power supplies) to the Cisco EtherSwitch service modules.

Note that the Cisco 3700 routers are not 802.3af-compliant, and the Cisco 2691 routers do not provide PoE.

For the Cisco 3745 router, the following specifications apply:

- These routers can have one or two internal –48 V power supplies. The internal supplies of these routers are configured to be redundant by default.
- With a single power supply, these routers can provide up to 360 W. This is enough power for up to forty-eight 7-W IP phones.

Power Considerations for the Service Module

The Cisco EtherSwitch service module supports inline powering of IP telephones with –48 V power. This allows IP phones to be plugged into a standard RJ-45 jack and be powered from the switch rather than from an AC wall outlet.

Caution To comply with Telcordia GR-1089 NEBS, this product is suitable for connection to intrabuilding or nonexposed wiring or cabling only. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

The Cisco EtherSwitch service module distributes the –48 V power to each of the Ethernet ports that are configured for PoE. Each port can be independently configured for PoE.

Powering Considerations for a Switch Stack

Consider the following guidelines before you power the Cisco EtherSwitch service modules in a stack:

- The sequence in which the Cisco EtherSwitch service modules are initially powered up might affect the Cisco EtherSwitch service module that becomes the stack master.
- If you want a particular Cisco EtherSwitch service module to become the stack master, power up that Cisco EtherSwitch service module first. This Cisco EtherSwitch service module becomes the stack master and remains the stack master until a stack master re-election is required. After approximately 10 seconds, power up the other Cisco EtherSwitch service modules in the stack.
- If you have no preference about which Cisco EtherSwitch service module becomes the stack master, power up both Cisco EtherSwitch service modules in the stack within 10 seconds. These Cisco EtherSwitch service modules participate in the stack master election.

Connecting to the EtherSwitch Service Module Ports

Fast Ethernet (FE) ports are used to connect PCs or workstations to the network.

A 10/100/1000 Gigabit Ethernet (GE) port or a SFP module port can be used as an uplink port to connect to another router or a server, or can trunk to another Cisco EtherSwitch service module or switch located in the same chassis or in a separate installation.

Connecting a FE or GE port to the network requires a Category 5 cable with RJ-45 male connectors, not provided with the network module. Category 5 cables are widely available.

Stacking the Cisco EtherSwitch Service Modules

This section provides this information:

- Planning the Stack
- Stack Cabling Considerations
- Connecting to the Cisco StackWise Ports

Planning the Stack

You can stack two Cisco EtherSwitch service modules in a stack by connecting them through their Cisco StackWise ports.

Before connecting the Cisco EtherSwitch service modules in a stack, observe these planning considerations:

- Length of cable. Depending on the configurations you have, you might need different sized cables. If you require a 0.5-meter (0.6-ft) cable, 1-meter (3.3-ft) cable, or 3-meter (9.8-ft) cable, you can order it from your Cisco supplier.
- Make sure that there is access to the front of the rack if you are planning to stack the Cisco EtherSwitch service modules.
- For concepts and procedures to manage Cisco EtherSwitch service module stacks, see the *Catalyst 3750 Switch Software Configuration Guide*, Cisco IOS Release 12.2 at the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/index.htm
- See these sections for additional considerations: the "Powering Considerations for a Switch Stack" section on page 18-14 and the "Stack Cabling Considerations" section on page 18-15.

Note Creating a stack of multiple Catalyst 3750 switch modules or service modules (using the stacking ports on the Cisco StackWise EtherSwitch service modules) requires specific cabling.

Stack Cabling Considerations

The illustrations in this section display cabling configuration examples that show the stack bandwidth and possible stack partitioning.

Figure 18-8 shows a stack of Cisco EtherSwitch service modules and Catalyst 3750 switches that provides full bandwidth and redundant connections.

Figure 18-8 Switch Stack with Full Bandwidth Connections

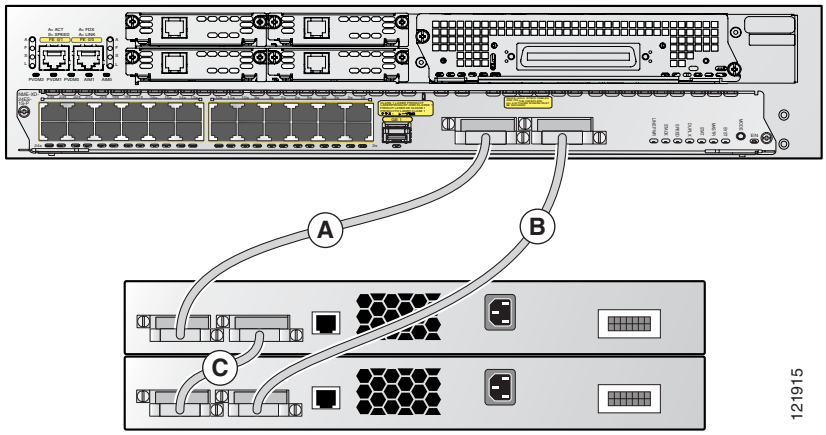


Figure 18-9 shows a stack of Cisco EtherSwitch service modules and Catalyst 3750 switches with incomplete cabling connections. This stack provides only half bandwidth and does not have redundant connections.

Figure 18-9 Switch Stack with Half Bandwidth Connections

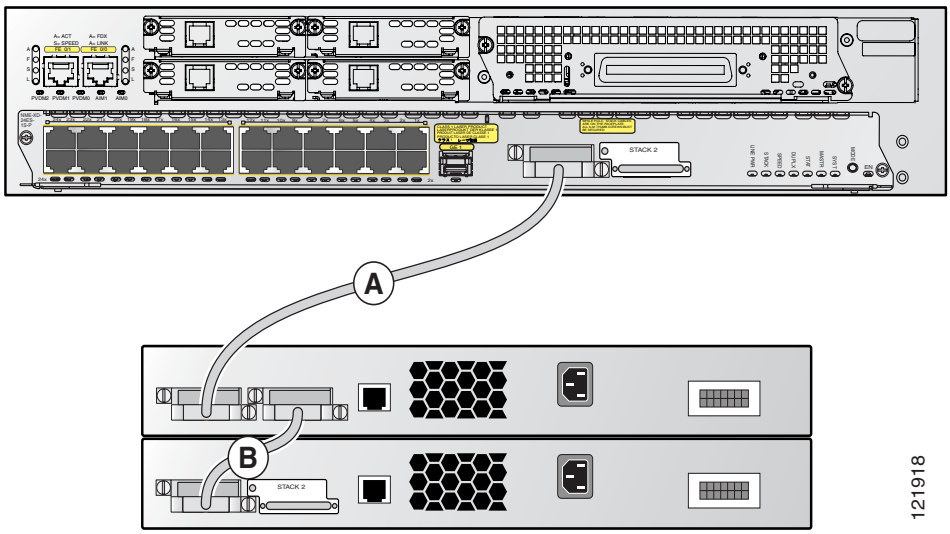


Figure 18-10 and Figure 18-11 show examples of stacks of Cisco EtherSwitch service modules and Catalyst 3750 switches with failover conditions.

In Figure 18-10, the cable in link B is bad; therefore, this stack provides only half bandwidth and does not have redundant connections.

In Figure 18-11, link B is bad, and the stack is partitioned into two separate stacks. The Cisco EtherSwitch service module 1 becomes the stack master of one stack and one of the Catalyst 3750 switches becomes the stack master of the second stack.

Figure 18-10 Example of a Stack with a Failover Condition

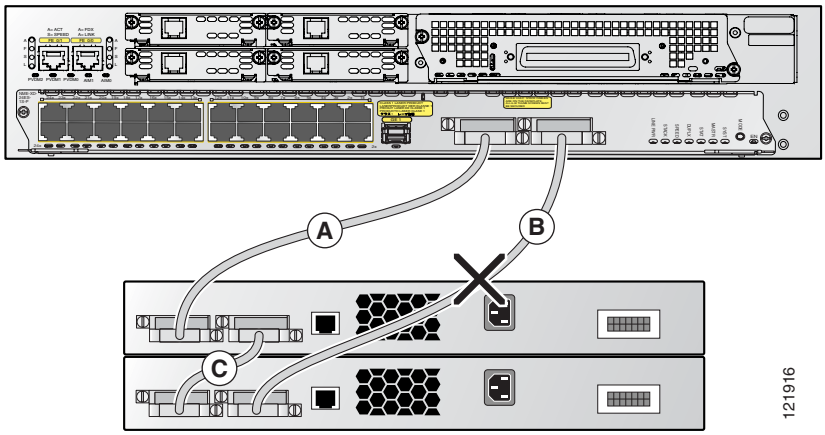
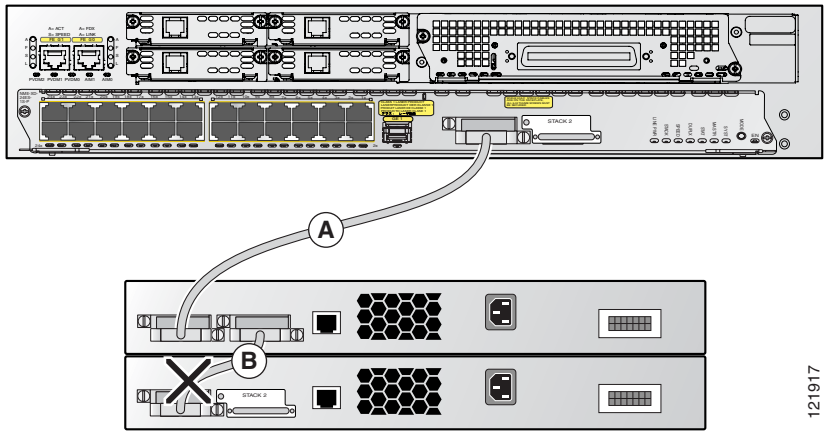


Figure 18-11 Example of a Partitioned Stack with a Failover Condition



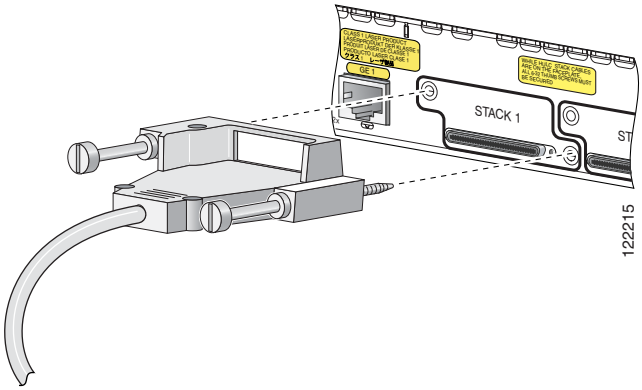
Connecting to the Cisco StackWise Ports

Follow these steps to connect the cable to the Cisco StackWise ports:

Step 1 Insert one end of the Cisco StackWise cable into the Cisco StackWise port. See Figure 18-12.

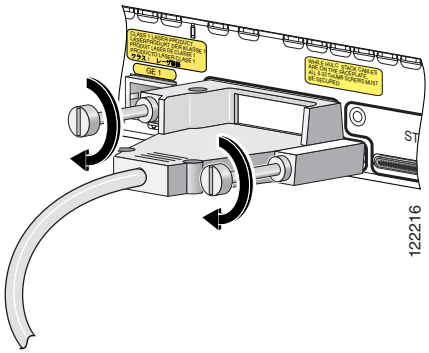
Note Always use a Cisco-approved Cisco StackWise cable to connect the Cisco StackWise EtherSwitch service modules.

Figure 18-12 Connecting the Cisco StackWise Cable



Step 2 Insert the other end of the cable into the connector of the other Cisco StackWise EtherSwitch service module and secure the screws tightly. See Figure 18-13.

Figure 18-13 Securing the Cisco StackWise Cable



CHAPTER 19

Connecting Content Engine Network Modules for Caching and Content Delivery

This chapter describes how to connect content engine (CE) network modules for caching and content delivery and contains the following sections:

Tip To determine whether your router supports a specific network module, see Table 1-6 on page 1-16.

CE Network Modules

This section provides overview information on CE network modules. The following CE network modules are available on Cisco modular routers:

- CE network module with a 40-GB Disk Expansion Module (NM-CE-BP-40G-K9) (see Figure 19-1)
- CE network module with a 80-GB Disk Expansion Module (NM-CE-BP-80G-K9) (see Figure 19-1)
- CE network module with a SCSI Controller Expansion Module and a 68-pin SCSI connector for connection to an external storage array (NM-CE-BP-SCSI-K9) (see Figure 19-2)

The 80-GB CE network module can run Application and Content Networking System (ACNS) software or Cisco Wide Area File Services (WAFS) software. The 40-GB CE network module and the CE network module with a SCSI controller can run ACNS software only. For information on configuring ACNS or WAFS, see the documentation listed in the "Related Documents" section on page 19-7.

Caution To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the CE network modules (NM-CE-BP-40G-K9 and NM-CE-BP-80G-K9) only to intrabuilding or nonexposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

Note The NM-CE-BP network module clock may be reset to 1980 if it is powered off for a long period. Several applications that depend on correct time being configured on the network module may not work in such a scenario. Therefore we strongly recommended that the NM-CE-BP network module be configured for NTP using the **ntp server** *server* Cisco IOS command, either after a software upgrade from Application and Content Networking System software Release 4.2.x to Release 5.x, or on obtaining a new network module, to maintain correct time on the network module.

Note There is no backup power for a network module's real time clock. Once power has been turned off or the network module has been removed from the router, the real time clock stops.

Figure 19-1 Faceplate for the CE Network Module with 40- or 80-GB Disk Expansion Module

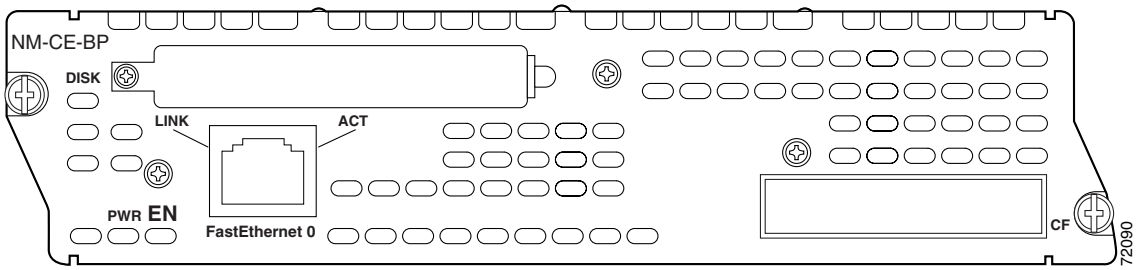
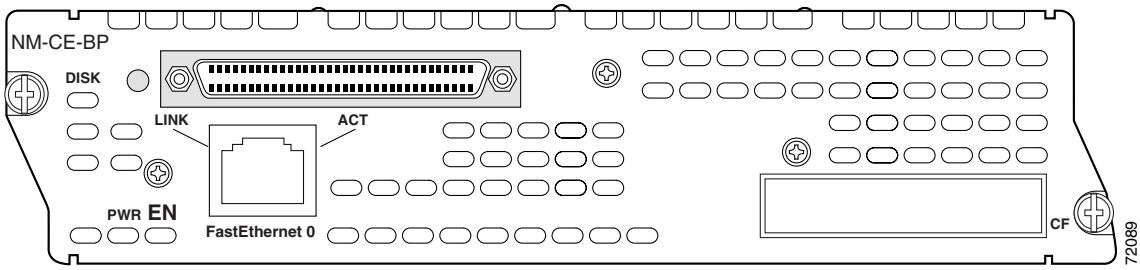


Figure 19-2 Faceplate for the CE Network Module with SCSI Connector Expansion Module



Note Some early CE network modules have an inactive USB port on the faceplate. This USB port has been removed in later Cisco CE network modules.

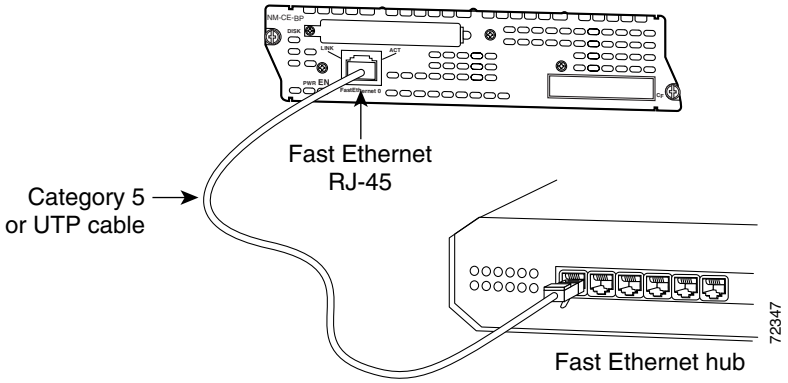
Tip For information on removing, replacing, and installing the expansion modules, see the *Installing Expansion Modules on Cisco CE Network Modules for Caching and Content Delivery* document.

Connecting CE Network Modules to the Network

To connect a CE network module to the network, from the RJ-45 port on the CE network module use a straight-through two-pair Category 5 unshielded twisted-pair (UTP) cable to connect to a switch, hub, repeater, server, or other network device. (See Figure 19-3.)

Note RJ-45 cables are not available from Cisco Systems. These cables are widely available and must be Category 5 cables.

Figure 19-3 Connecting a CE Network Module to a Fast Ethernet Hub



Connecting CE Network Modules with SCSI Controller Expansion Modules to an External Cisco Storage Array

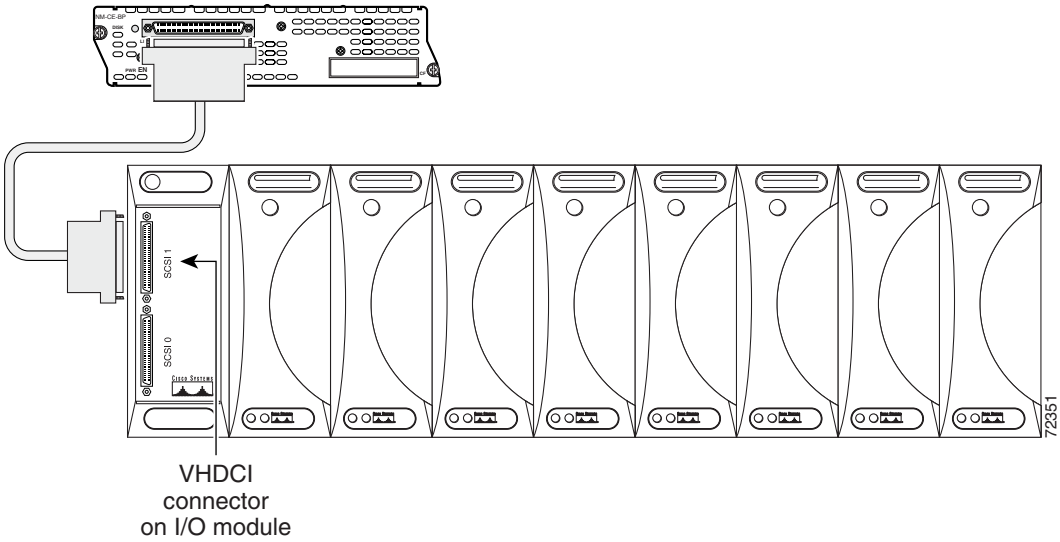
Timesaver Connecting the external Cisco storage array requires you to reboot the network module or router. To save time, connect the external Cisco storage array to the CE network module before powering on the router or network module.

To connect a CE network module with a SCSI controller expansion module to an external storage array, use a 68-pin, low-voltage differential (LVD) SCSI cable. Connect the cable to the SCSI port on the network module to the SCSI port on the external Cisco storage array. (See Figure 19-4.)

Cisco Storage Array 6 is supported on the CE network module with SCSI controller expansion module. (See the *Cisco Storage Array 6 Installation and Configuration Guide*.)

Tip Use either a 36- or 108-inch LVD SCSI cable, depending on the length required between the router and the external storage array.

Figure 19-4 Connecting a CE Network Module with SCSI Controller Expansion Module to an External Cisco Storage Array



CE Network Module LEDs

All CE network modules have an enable (EN) LED. This LED indicates that the module has passed its self-tests and is available to the router.

CE network modules also display an additional power (PWR) LED and a CompactFlash (CF) LED on the faceplate, and two additional LEDs for the Fast Ethernet port. (See Figure 19-5 and Table 19-1.)

Figure 19-5 CE Network Module LEDs

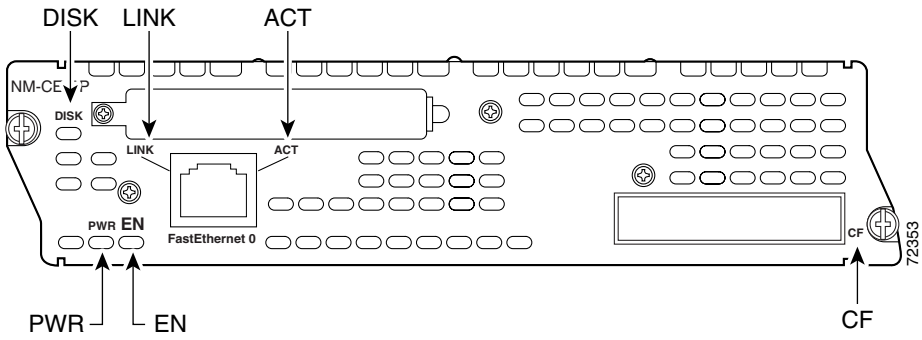


Table 19-1 Content Engine Network Modules for Caching and Content Delivery LEDs

LED	Meaning
ACT	There is activity on the Fast Ethernet connection.
CF	The compact flash module is active.

Table 19-1 Content Engine Network Modules for Caching and Content Delivery LEDs (continued)

LED	Meaning
DISK	There is activity on the 40- or 80-GB disk expansion module hard drive. **Note** The faceplate for the CE network module with SCSI controller expansion module also displays the disk LED, but the LED is not active.
EN	The module has passed self-test and is available to the router.
LINK	The Fast Ethernet connection is available to the network module.
PWR	Power is available to the network module.

Online Insertion and Removal with a CE Network Module

Some Cisco modular access routers allow you to replace network modules without switching off the router or affecting the operation of other interfaces. This feature is called online insertion and removal (OIR). OIR of network modules provides uninterrupted operation to network users, maintains routing information, and ensures session preservation. To find out if the router you are working on allows OIR, see the router model's hardware installation guide.

Caution Unlike other network modules, CE network modules use hard disks. Online removal of disks without proper shutdown can result in file system corruption and might render the disk unusable. The operating system on the CE network module must be shut down in an orderly fashion before the network module is removed.

Caution Cisco routers support OIR with similar modules only. If you remove a network module, install another module exactly like it in its place. If you remove a 2-slot network module (along with any installed WAN or voice interface cards), install another module and card combination exactly like it.

For a description of informational and error messages that may appear on the console during this procedure, see the hardware installation guide for your type of router.

To perform online removal of a CE network module and insertion of a replacement, follow these steps with the router in privileged EXEC mode:

Step 1 Initiate a CE network module console access session using the following command:

```
Router# service-module content-engine slot/unit session

Trying 10.10.10.1, 2129 ... Open

CE-netmodule con now available

Press RETURN to get started!

CE-netmodule> enable
CE-netmodule#
```

Step 2 Save the running configuration of the content engine using the following command from the CE-netmodule prompt:

```
CE-netmodule# copy running-config tftp tftp-server-address filename
```

Step 3 Exit the CE network module console access session by pressing **Control-Shift-6**, followed by **x**.

Step 4 On the router, clear the CE console access session using the following command:

```
Router# service-module content-engine slot/unit session clear
```

Step 5 Perform a graceful halt of the CE network module disk drive by using the following command:

```
Router# copy tftp running-config tftp-server-addresss filename
```

Step 6 Shut down the content engine interface:

```
Router (config)# interface content-engine slot/unit
Router (config-if)# shutdown
Router (config-if)# exit
```

Step 7 Unplug all network interface cables from the CE network module.

Step 8 Loosen the two captive screws holding the CE network module in the chassis slot.

Step 9 Slide the CE network module out of the slot.

Step 10 Align the replacement CE network module with the guides in the chassis slot, and slide it gently into the slot.

Note If the router is not fully configured with network modules, make sure that blank panels fill the unoccupied chassis slots to provide proper airflow.

Step 11 Push the module into place until you feel its edge connector mate securely with the connector on the backplane.

Step 12 Reconnect the network interface cables previously removed in Step 7.

Step 13 Check that the network module LEDs are on and that the power and enable LEDs on the front panel also are on. This inspection ensures that connections are secure and that the new unit is operational.

Step 14 Initiate a CE network module console access session with the following command:

```
Router# service-module content-engine slot/unit session

Trying 10.10.10.1, 2129 ... Open

CE-netmodule con now available

Press RETURN to get started!

CE-netmodule> enable
CE-netmodule#
```

Step 15 Restore the content engine's running configuration by using the following command from the CE-netmodule prompt:

```
CE-netmodule# copy tftp running-config tftp-server-address filename
```

Step 16 Exit the CE network module console access session by pressing **Control-Shift-6**, followed by **x**.

Step 17 On the router, clear the CE console access session using the following command:

```
Router# service-module content-engine slot/unit session clear
```

Related Documents

For information on configuring ACNS, see the documentation at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/webscale/uce/

For information on configuring WAFS, see the documentation at the following URL:

http://www.cisco.com/en/US/products/ps6469/tsd_products_support_series_home.html

Tip For information on obtaining documentation, see the "Obtaining Documentation" section on page viii. For information on obtaining technical assistance, see the "Obtaining Technical Assistance" section on page xi.

Hardware Documentation

For information on installing and removing CE network module expansion modules, see the *Installing Expansion Modules on Cisco CE Network Modules for Caching and Content Delivery* document.

Cisco IOS Software Documentation

For a description of the Cisco IOS features supported on CE network modules, see the *Content Engine Network Module for Caching and Content Delivery* document.

Content Engine Documentation

For information on the Cisco Content Engine, refer to the documents listed under *Cisco Content Engine*.

Cisco Storage Array Documentation

For information on installing and configuring the Cisco Storage Array 6, refer to the *Cisco Storage Array 6 Installation and Configuration Guide*.

CHAPTER 20

Connecting T3/E3 Network Modules

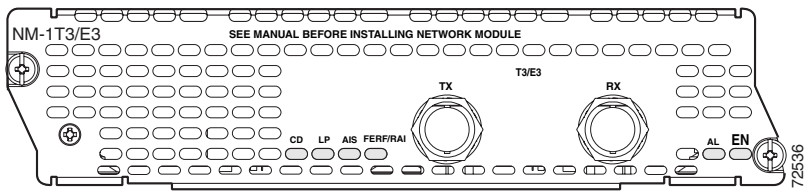
This chapter describes how to connect T3/E3 network modules for modular access routers and contains the following sections:

Tip To determine whether your router supports a specific network module, see Table 1-6 on page 1-16.

1-Port T3/E3 Network Modules

The NM-1T3/E3 network module is a single-port universal T3/E3 network module with integrated CSU/DSU, clear channel, and subrate support. (See Figure 20-1.) Channels on the network module can be configured as either T3 or E3 through Cisco IOS software.

Figure 20-1 1-Port T3/E3 Network Module Faceplate



Note The NM-1T3/E3 network module provides subrate T3 support for Digital Link, Kentrox, Larscom, Verilink, and Adtran. The NM-1T3/E3 network module also provides subrate E3 support for Digital Link and Kentrox.

Connecting T3/E3 Network Modules to the Network

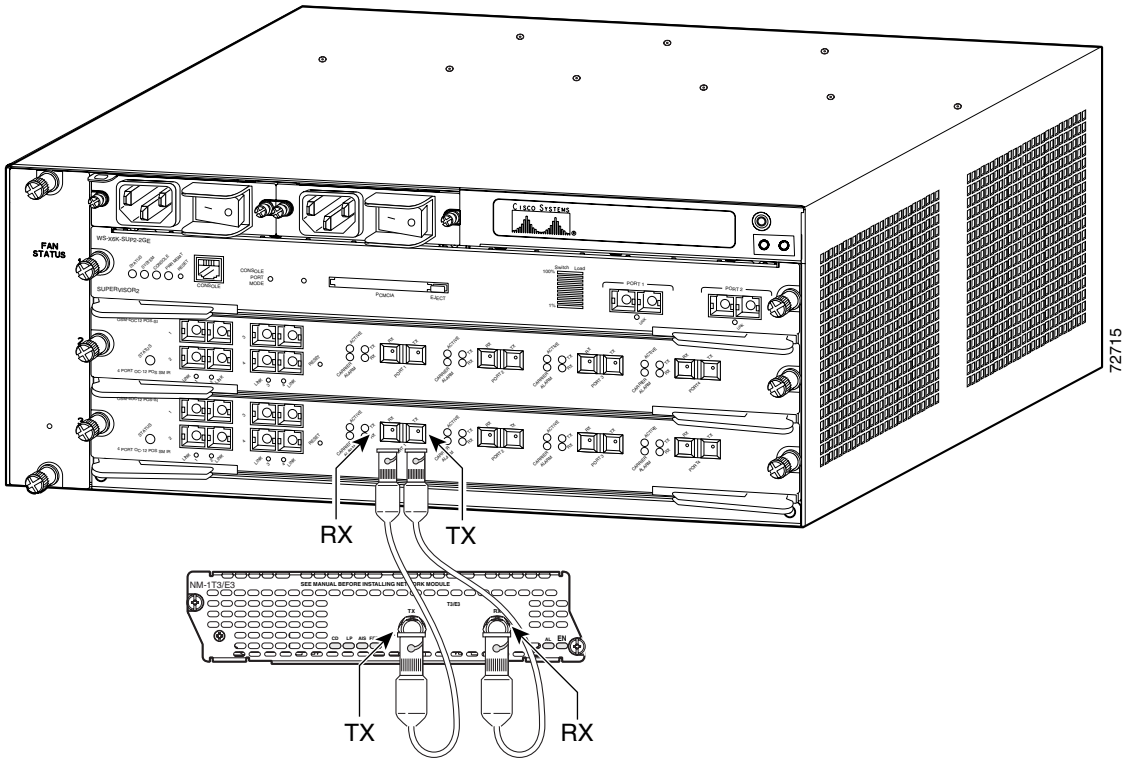
To connect a T3/E3 network module to the network, use a 75-ohm 728-A coaxial cable to connect the BNC connector on the network module to a networking device. (See Figure 20-2.)

Warning **This equipment contains a ring signal generator (ringer), which is a source of hazardous voltage. Do not touch the RJ-11 (phone) port wires (conductors), the conductors of a cable connected to the RJ-11 port, or the associated circuit-board when the ringer is active. The ringer is activated by an incoming call.** Statement 1042

Warning **If the symbol of suitability with an overlaid cross appears above a port, you must not connect the port to a public network that follows the European Union standards. Connecting the port to this type of public network can cause severe injury or damage your router.** Statement 1031

Caution To minimize transient surges, the internal wiring should not be routed in the same conduit with power lines or external telephone lines.

Figure 20-2 Connecting a T3/E3 Network Module to a Networking Device (Cisco 7603 Router Shown)



Tip When connecting the T3/E3 network module to a port adapter used in another router series, verify that you are connecting the TX port on the network module with the RX port on the port adapter, and the TX port on the port adapter to the RX port on the network module.

T3/E3 Network Module LEDs

All network modules have an enable (EN) LED. This LED indicates that the module has passed its self-tests and is available to the router. See Figure 20-3 and Table 20-1 for LEDs on the T3/E3 network module.

Figure 20-3 T3/E3 LEDs

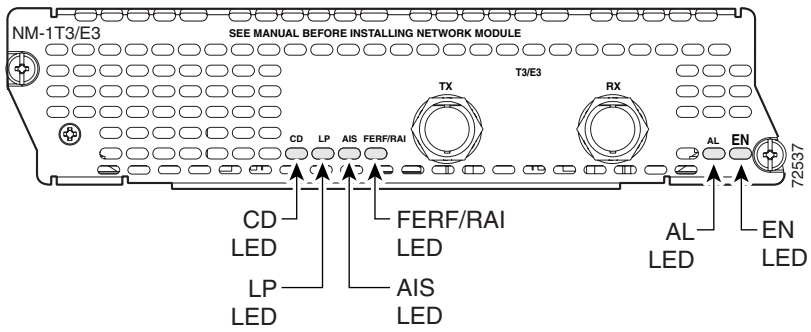


Table 20-1 T3/E3 Network Module LEDs

LED	Meaning
CD	Green indicates that a signal is present on the port.
LP	Yellow indicates that a loopback condition is present on the port.
AIS	Yellow indicates an alarm on the DS3 transmission.
FERF/RAI	Yellow indicates a remote failure at the far end of the connection.
AL	Yellow indicates that the port is out of frame.
EN	Green indicates that the network module has passed self-test and is available to the router.

Related Documents

For additional information, see the following documents.

Tip For information on obtaining documentation, see the "Obtaining Documentation" section on page viii. For information on obtaining technical assistance, see the "Obtaining Technical Assistance" section on page xi.

Cisco IOS Software Documentation

For information on Cisco IOS software features specific to the T3/E3 network module, see the *Clear Channel T3/E3 Network Module with Integrated CSU/DSU* document.

Connecting Gigabit Ethernet Network Modules

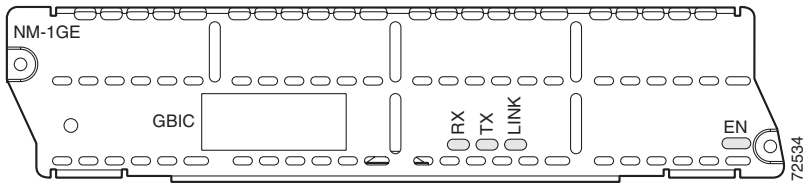
This chapter describes how to connect Gigabit Ethernet network modules for modular access routers and contains the following sections:

Tip To determine whether your router supports a specific network module, see Table 1-6 on page 1-16.

Gigabit Ethernet Network Modules

The Gigabit Ethernet network module provides single-port Gigabit Ethernet connectivity through an installed Gigabit interface converter (GBIC). The GBIC determines the type of connectivity available to the network module. (See Figure 21-1.)

Figure 21-1 Gigabit Ethernet Network Module Faceplate



See Table 21-1 for information on connection types supported by each GBIC.

Note 1000BASE-T ports cannot be looped back through use of an external loopback cable.

Table 21-1 Gigabit Ethernet Connection and Cable Types Supported on Gigabit Ethernet Network Modules

GBIC Part Number	GBIC Description	Required Cable Specifications
GBIC-ZX=	Extended distance 1000BASE-ZX	10-micron SMF cable (yellow) with SC connectors[1]
GBIC-LX/LH=	Long-wavelength or long-haul 1000BASE-LX/LH	10-micron SMF cable (yellow) with SC connectors[1] **Tip** If using an MMF cable, install a mode-conditioning patch cord (CAB-GELX-625).
GBIC-SX=	Short-wavelength 1000BASE-SX	62.5-micron MMF cable (orange) with SC connectors
GBIC-T=	UTP Category 5 or 6 1000BASE-T	Category 5 or 6 UTP cable with RJ-45 connectors
CWDM-GBIC-1470=	1000BASE-CWDM GBIC 1470 nm	10-micron SMF cable (yellow) with SC connectors[1]
CWDM-GBIC-1490=	1000BASE-CWDM GBIC 1490 nm	10-micron SMF cable (yellow) with SC connectors[1]
CWDM-GBIC-1510=	1000BASE-CWDM GBIC 1510 nm	10-micron SMF cable (yellow) with SC connectors[1]
CWDM-GBIC-1530=	1000BASE-CWDM GBIC 1530 nm	10-micron SMF cable (yellow) with SC connectors[1]
CWDM-GBIC-1550=	1000BASE-CWDM GBIC 1550 nm	10-micron SMF cable (yellow) with SC connectors[1]
CWDM-GBIC-1570=	1000BASE-CWDM GBIC 1570 nm	10-micron SMF cable (yellow) with SC connectors[1]
CWDM-GBIC-1590=	1000BASE-CWDM GBIC 1590 nm	10-micron SMF cable (yellow) with SC connector[1]s
CWDM-GBIC-1610=	1000BASE-CWDM GBIC 1610 nm	10-micron SMF cable (yellow) with SC connectors[1]

1. 10-dB SMF optical attenuators with SC connectors (two per duplex cable) are required for distances less than 25 km (15.5 miles). Install the attenuators between the male SC connector on the cable and the female SC connector on the network module.

Installing and Removing GBICs

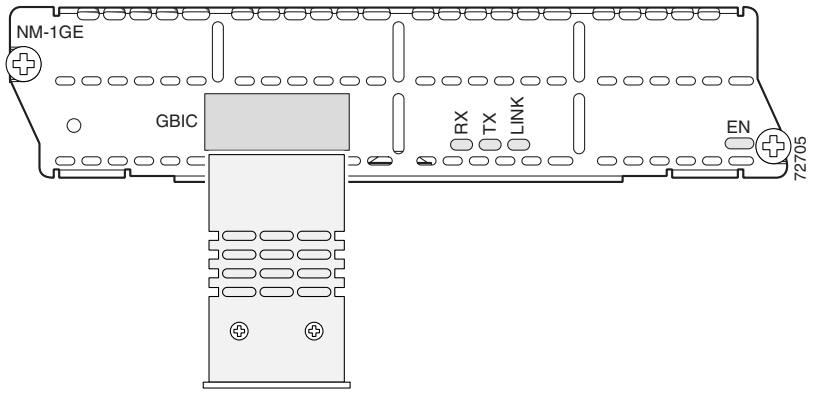
Gigabit Ethernet network modules support GBIC hot-swapping. To save time, do not power down the router and network module before installing or removing the GBIC.

Warning **Because invisible laser radiation may be emitted from the aperture of the port when no fiber cable is connected, avoid exposure to laser radiation and do not stare into open apertures.** Statement 240

Note GBICs from other vendors are not supported by the Cisco Gigabit Ethernet network module.

Step 1 Hold down the clips on the side of the GBIC while inserting the GBIC into the GBIC slot in the network module faceplate. (See Figure 21-2.)

Figure 21-2 Installing a GBIC into a Network Module



Step 2 Release the side clips on the GBIC.

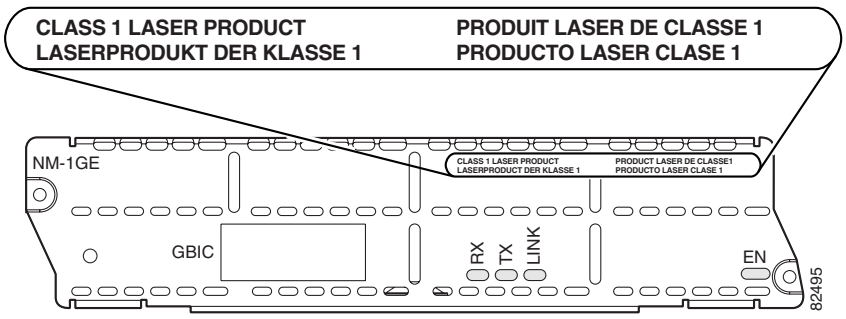
Step 3 Connect the Gigabit Ethernet network module to the network. (See Figure 21-4.) If installing the GBIC in an uninstalled network module, install the network module (see Chapter 2, "Installing Cisco Network Modules in Cisco Access Routers") before connecting the network module to the network.

Laser Safety Guidelines

Optical GBICs use a small laser to generate the fiber-optic signal. Keep the transmit port covered whenever a cable is not connected to the port.

The module faceplate carries a Class 1 laser warning label. (See Figure 21-3.)

Figure 21-3 Class 1 Laser Warning Label



Warning **Because invisible laser radiation may be emitted from the aperture of the port when no fiber cable is connected, avoid exposure to laser radiation and do not stare into open apertures.** Statement 240

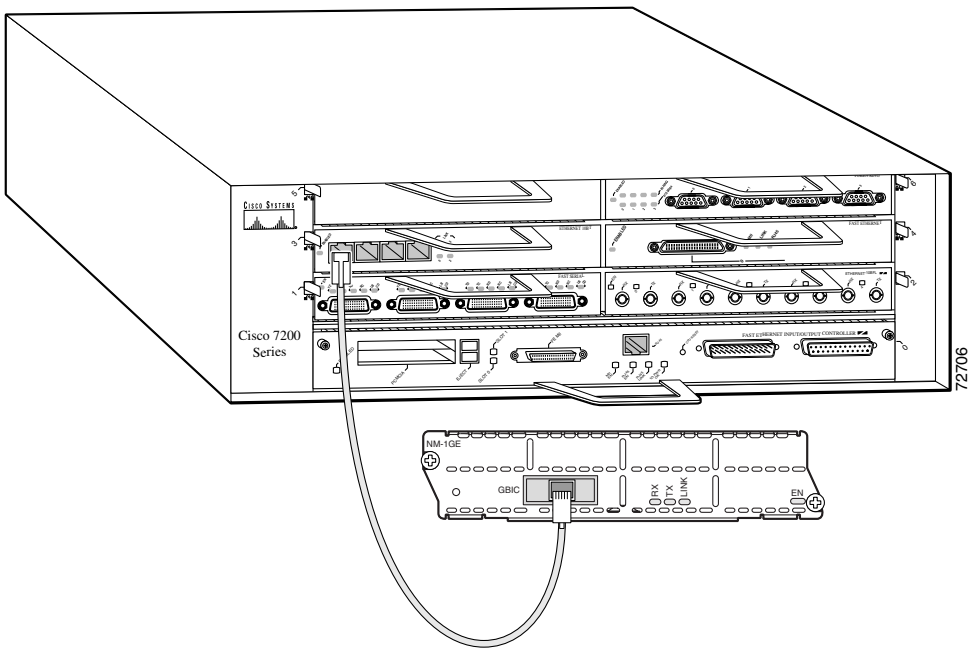
Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.** Statement 1040

Connecting Gigabit Ethernet Network Modules to the Network

Warning **Because invisible laser radiation may be emitted from the aperture of the port when no fiber cable is connected, avoid exposure to laser radiation and do not stare into open apertures.** Statement 240

Use the cables listed in Table 21-1 to connect the GBIC connectors on the network module to a networking device. (See Figure 21-4.)

Figure 21-4 Connecting a Gigabit Ethernet Network Module to a Cisco 7200 Series Router



Gigabit Ethernet Network Module LEDs

All network modules have an enable (EN) LED. This LED indicates that the module has passed its self-tests and is available to the router. See Figure 21-5 and Table 21-2 for LEDs specific to the Gigabit Ethernet network module.

Figure 21-5 Gigabit Ethernet Network Module LEDs

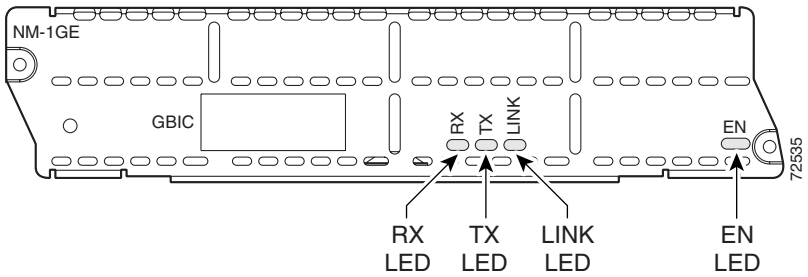


Table 21-2 Gigabit Ethernet Network Module LEDs

LED	Meaning
LINK	Green indicates that a link has been established between the network module and another networking device.
TX	Flashing green indicates transmit activity.
RX	Flashing green indicates receive activity.
EN	Green indicates that the network module has passed its self-test and is available to the router.

Related Documents

For additional information, see the following documents.

Tip For information on obtaining documentation, see the "Obtaining Documentation" section on page viii. For information on obtaining technical assistance, see the "Obtaining Technical Assistance" section on page xi.

CWDM Passive Optical System Documentation

For more information on the CWDM Passive Optical System, which is often used with CWDM GBICs, see the *Cisco 1000BASE-CWDM Series Passive Optical System Installation Note* document.

CHAPTER 22

Connecting Cisco Intrusion Detection System Network Modules

This chapter describes how to connect Cisco intrusion detection system (CIDS) network modules for modular access routers and contains the following sections:

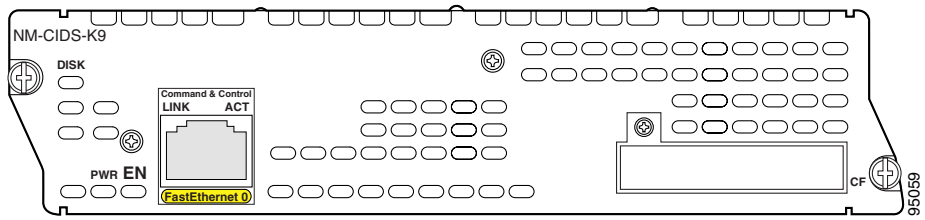
Tip To determine whether your router supports a specific network module, see Table 1-6 on page 1-16.

CIDS Network Modules

This section provides information on the CIDS network module (NM-CIDS-K9) (see Figure 22-1)

Caution To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the CIDS network module (NM-CIDS-K9) only to intrabuilding or nonexposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

Figure 22-1 Faceplate for the NM-CIDS-K9 Network Module



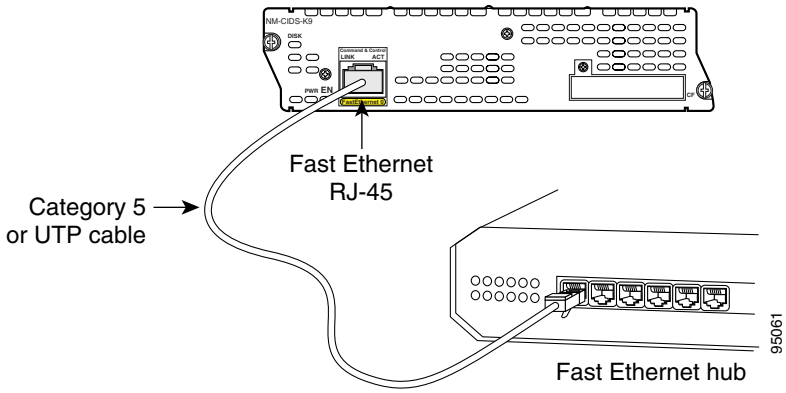
Connecting CIDS Network Modules to the Network

To connect a CIDS network module to the network, use a straight-through two-pair Category 5 unshielded twisted-pair (UTP) cable to connect the RJ-45 port on the CIDS network module to a switch, hub, repeater, server, or other network device. (See Figure 22-2.)

Note RJ-45 cables are not available from Cisco Systems. These cables are widely available and must be Category 5 cables.

Caution To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the CIDS network module (NM-CIDS-K9) only to intrabuilding or nonexposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

Figure 22-2 Connecting a CIDS Network Module to a Fast Ethernet Hub



CIDS Network Module LEDs

All network modules have an enable (EN) LED. This LED indicates that the module has passed its self-tests and is available to the router.

All CIDS network modules display an additional power (PWR) LED and a CompactFlash (CF) LED on the faceplate, and two additional LEDs for the Fast Ethernet port (see Figure 22-3 and Table 22-1).

Figure 22-3 CIDS Network Module LEDs

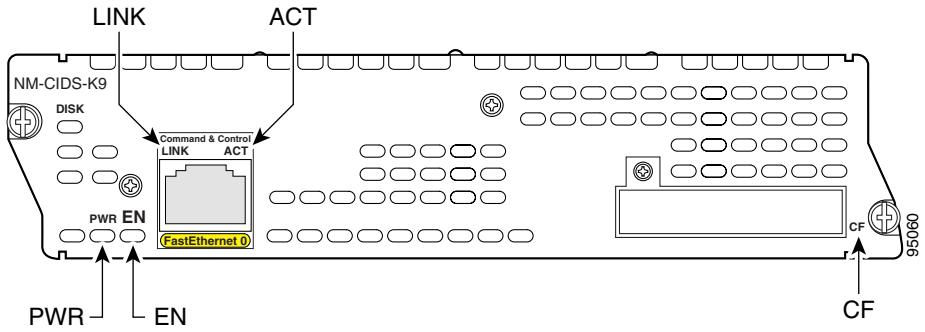


Table 22-1 CIDS Network Module LEDs

LED	Meaning
ACT	There is activity on the Fast Ethernet connection.
CF	The CompactFlash module is active. **Note** Since CompactFlash is not supported on the NM-CIDS-K9, this LED is not active except during self-test.
DISK	There is activity on the 20-GB disk expansion module hard drive.
EN	The module has passed self-test and is available to the router.
LINK	The Fast Ethernet connection is available to the network module.
PWR	Power is available to the network module.

Online Insertion and Removal with a CIDS Network Module

Some Cisco modular access routers allow you to replace network modules without switching off the router or affecting the operation of other interfaces. This feature is called online insertion and removal (OIR). OIR of network modules provides uninterrupted operation to network users, maintains routing information, and ensures session preservation.

Caution Unlike other network modules, CIDS network modules use hard disks. Online removal of disks without proper shutdown can result in file system corruption and might render the disk unusable. The operating system on the CIDS network module must be shut down in an orderly fashion before the network module is removed.

Caution Cisco routers support OIR with similar modules only. If you remove a network module, install another module exactly like it in its place. If you remove a two-slot network module (along with any installed WAN or voice interface cards), install another module and card combination exactly like it.

For a description of informational and error messages that may appear on the console during this procedure, see the hardware installation guide for your type of router.

To perform online removal of a CIDS network module and insertion of a replacement, follow these steps with the router in privileged EXEC mode:

Step 1 Perform a graceful halt of the CIDS network module by using the following command:

```
Router# service-module IDS-Sensor slot/0 shutdown
Trying 10.10.10.1, 2129 ... Open
```

Wait for the following status message (it may take a minute or two):

```
%SERVICEMODULE-5-SHUTDOWN2:Service module IDS-Sensor1/0 shutdown complete
```

Step 2 Unplug the network interface cable from the CIDS network module.

Step 3 Loosen the two captive screws holding the CIDS network module in the chassis slot.

Step 4 Slide the CIDS network module out of the slot.

Step 5 Align the replacement CIDS network module with the guides in the chassis slot, and slide it gently into the slot.

Note If the router is not fully configured with network modules, make sure that blank panels fill the unoccupied chassis slots to provide proper airflow.

Step 6 Push the module into place until you feel its edge connector mate securely with the connector on the backplane.

Step 7 Reconnect the network interface cable previously removed in Step 2.

Step 8 Tighten the two captive screws on the faceplate.

Step 9 Reset the CIDS network module using the **reset** command.

```
Router# service-module IDS-Sensor slot/0 reset

Use reset only to recover from shutdown or failed state
Warning: May lose date on the hard disc!
Do you want to reset?[confirm]
```

Step 10 Press **Enter** to confirm the request. The CIDS network module resets itself.

Step 11 Check that the network module LEDs are on and that the power and enable LEDs on the front panel also are on. This inspection ensures that connections are secure and that the new unit is operational.

Related Documents

For additional information, refer to the following documents.

Tip For information on obtaining documentation, see the "Obtaining Documentation" section on page viii. For information on obtaining technical assistance, see the "Obtaining Technical Assistance" section on page xi.

Cisco IDS Software Documentation

Tip For more information on Cisco IDS software documentation, see the *Cisco Intrusion Detection System (IDS) Hardware and Software Documentation Guide*.

For a list of caveats, documentation changes, and important last-minute information for Cisco Intrusion Detection System Version 4.1, see the *Release Notes for the Cisco Intrusion Detection System Version 4.1*.

For a quick overview of the tasks required to install and initially configure Cisco IDS components, see the *Quick Start Guide for the Cisco Intrusion Detection System Version 4.1*.

For installation instructions for all Cisco IDS version 4.1 hardware components, including appliances, modules, accessories, and upgrades (such as the IDS XL card), and basic configuration tasks using command line interface (CLI), see the *Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.1*.

For information on installing and using Cisco IDS Device Manager and Cisco IDS Event Viewer, see the *Installing and Using the Cisco Intrusion Detection System Device Manager and Event Viewer Version 4.1*.

For IDS CLI reference, including syntax and usage guidelines, see the *Cisco Intrusion Detection System Command Reference Version 4.1*.

CHAPTER 23

Connecting Cisco Unity Express Network Modules

This chapter describes Cisco Unity Express network modules for modular access routers and contains the following sections:

Tip To determine whether your router supports a specific network module, see Table 1-6 on page 1-16.

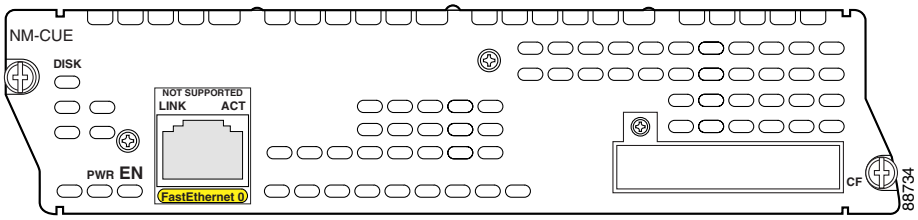
Cisco Unity Express Network Module Overview

This section provides information on the Cisco Unity Express network module (NM-CUE). (See Figure 23-1.)

Caution To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the Cisco Unity Express network module (NM-CUE) only to intrabuilding or nonexposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

Note The Fast Ethernet port and CompactFlash slot, though available on the hardware, are not supported by the Cisco Unity Express network module. The compact Flash slot has a metal cover.

Figure 23-1 NM-CUE Faceplate



Cisco Unity Express Network Module LEDs

All network modules have an enable (EN) LED. This LED indicates that the module has passed its self-tests and is available to the router.

All Cisco Unity Express network modules display an additional power (PWR) LED and a CompactFlash (CF) LED on the faceplate, and two additional LEDs for the Fast Ethernet port. (See Figure 23-2 and Table 23-1.)

Note The CF and Fast Ethernet port LEDs are not used by the Cisco Unity Express network module.

Figure 23-2 NM-CUE LEDs

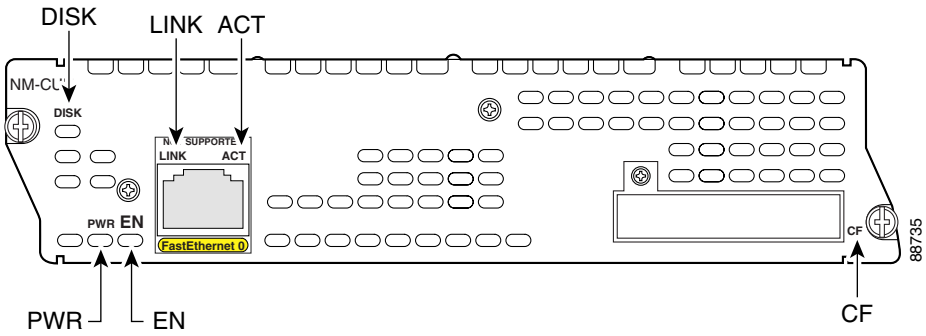


Table 23-1 Cisco Unity Express Network Module LEDs

LED	Meaning
ACT	There is activity on the Fast Ethernet connection. **Note** This LED is not used on the NM-CUE.
CF	The compact Flash module is active. **Note** This LED is not used on the NM-CUE.
DISK	There is activity on the 20-GB disk-expansion module hard drive.
EN	The module has passed self-test and is available to the router.
LINK	The Fast Ethernet connection is available to the network module. **Note** This LED is not used on the NM-CUE.
PWR	Power is available to the network module.

Online Insertion and Removal with a Cisco Unity Express Network Module

Some Cisco modular access routers allow you to replace network modules without switching off the router or affecting the operation of other interfaces. This feature is often called hot-swapping or online insertion and removal (OIR). Hot-swapping of network modules provides uninterrupted operation to network users, maintains routing information, and ensures session preservation.

Caution Cisco Unity Express network modules use hard disks. Online removal of disks without proper shutdown can result in file system corruption and might render the disk unusable. The operating system on the Cisco Unity Express network module must be shut down in an orderly fashion before the network module is removed.

Caution Cisco routers support hot-swapping with similar modules only. If you remove a network module, install another module exactly like it in its place.

For a description of informational and error messages that may appear on the console during this procedure, see the hardware installation guide for your type of router.

To perform online removal of a Cisco Unity Express network module and insertion of a replacement, follow these steps with the router in privileged EXEC mode:

Step 1 Initiate a Cisco Unity Express network module console access session using the following command:

```
Router# service-module service-engine slot/port session

Trying 10.10.10.1, 2129 ... Open

SE-netmodule> enable
Password:
SE-netmodule#

SE-netmodule con now available

Press RETURN to get started!

SE-netmodule> enable
Password:
SE-netmodule#
```

Timesaver The Cisco Unity Express network module uses a blank password. Press **Enter** at the password prompt.

Step 2 Save the running configuration of the Cisco Unity Express network module using the following command from the SE-netmodule prompt:

```
SE-netmodule# copy running-config ftp:

Address or name or remote host? username/password/remote host
Destination filename? filename
```

Step 3 Exit the Cisco Unity Express network module console access session by pressing **Ctrl-Shift-6**, followed by **x**.

Step 4 On the router, clear the Cisco Unity Express network module console access session by using the following command:

```
Router# service-module service-engine slot/port session clear
```

Step 5 Perform a graceful halt of the Cisco Unity Express network module disk drive by using the following command:

```
Router# service-module service-engine slot/port shutdown
```

Step 6 Loosen the two captive screws holding the Cisco Unity Express network module in the chassis slot.

Step 7 Slide the Cisco Unity Express network module out of the slot.

Step 8 Align the replacement Cisco Unity Express network module with the guides in the chassis slot, and slide it gently into the slot.

Note If the router is not fully configured with network modules, make sure that blank panels fill the unoccupied chassis slots to provide proper airflow.

Step 9 Push the module into place until you feel its edge connector mate securely with the connector on the backplane.

Step 10 Tighten the two captive screws on the module faceplate.

Step 11 Check that the network module LEDs come on and that the power and enable LEDs on the front panel have also come on. This inspection ensures that connections are secure and that the new unit is operational.

Step 12 Initiate a Cisco Unity Express network module console access session with the following command:

```
Router# service-module service-engine slot/port session

Trying 10.10.10.1, 2129 ... Open

SE-netmodule con now available

Press RETURN to get started!

SE-netmodule> enable
SE-netmodule#
```

Step 13 Restore the Cisco Unity Express running configuration by using the following command from the SE-netmodule prompt:

```
SE-netmodule# copy ftp: running-config

Address or name or remote host? username/password/remote host
Source filename? filename
```

Step 14 Exit the Cisco Unity Express network module console access session by pressing **Ctrl-Shift-6**, followed by **x**.

Step 15 On the router, clear the console access session using the following command:

```
Router# service-module service-engine slot/port session clear
```

Related Documents

For additional information, see the following documents.

Tip For information on obtaining documentation, see the "Obtaining Documentation" section on page viii. For a list of orderable documentation, search the Cisco Price List under "Documentation."

Cisco Unity Express Software Documentation

For end-user information on Cisco Unity Express software, see the *Cisco Unity Express End-User Card*.

For system admininstrator information on the Cisco Unity Express software, see the *Cisco Unity Express System Administrator's Guide*.

CHAPTER 24

Connecting Cisco Unity Express Enhanced Network Modules

This chapter describes Cisco Unity Express enhanced network modules for Cisco integrated services routers, and contains the following sections:

Tip To determine whether your Cisco router supports a specific network module, see Table 1-6 on page 1-16.

Cisco Unity Express Enhanced Network Modules

The Cisco Unity Express enhanced network module (NME-CUE) provides 24 ports that store a maximum of 250 voice mailboxes and 300 hours of voice messages. (See Figure 24-1.)

Caution To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the Cisco Unity Express enhanced network module (NME-CUE) only to intrabuilding or nonexposed wiring or cabling. The intrabuilding cable must be shielded, and the shield must be grounded at both ends

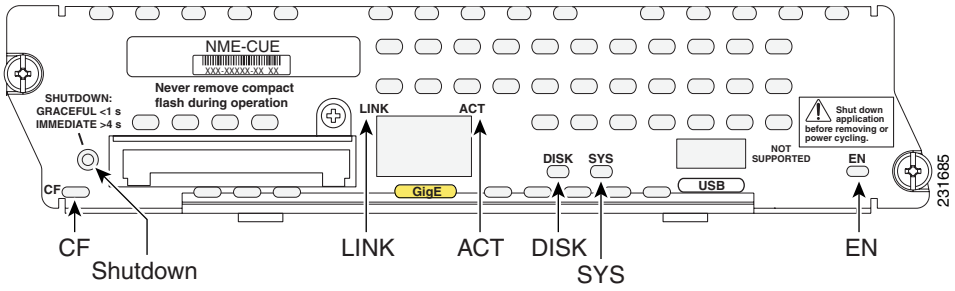
The NME-CUE ships from the factory with the following hardware preinstalled. (See Table 24-1.)

Table 24-1 Preinstalled Hardware in Cisco Unity Express Enhanced Network Modules

Model	Hard Disk	Memory
NME-CUE	80 GB (SATA)	512 MB

Note The Gigabit Ethernet port and compact flash (CF) slot, though available on the hardware, are not supported by the Cisco Unity Express enhanced network module. The CF slot has a metal cover.

Figure 24-1 NME-CUE Faceplate



SHUTDOWN	Press the SHUTDOWN button for less than 2 seconds to gracefully shut down the module. Press the SHUTDOWN button for more than 4 seconds to cause an immediate module shutdown, which may impact file operations that are in progress.
DISK	Status of hard drive activity: On—Active. Off—Inactive.
SYS	Status of system shutdown: **Note** Do not remove power without first shutting down the application. On—Application is stable. Off—System is shut down and ready for host power down. Flashing—System shutdown is in progress.
EN	Status of the network module: On—Detected by the host Cisco IOS software and enabled. Off—Disabled.

Shutting Down Cisco Unity Express Enhanced Network Modules

Press the Shutdown button on the network module faceplate for less than 2 seconds to perform a graceful shutdown of the network module before removing power from the router or before starting an online insertion and removal (OIR) sequence on the router. The application may take up to 2 minutes to fully shut down.

Caution If you press the Shutdown button for *more than 4 seconds*, a nongraceful shutdown of the hard disk will occur and may corrupt files on the network module's hard disk. After a nongraceful shutdown, the HD and SYS LEDs remain lit. Press the Shutdown button for *less than 2 seconds* to gracefully reboot the network module.

Online Insertion and Removal of Cisco Unity Express Enhanced Network Modules

Some Cisco routers allow you to replace network modules without switching off the router or affecting the operation of other interfaces. This feature is called *online insertion and removal* (OIR). OIR of a module provides uninterrupted operation to network users, maintains routing information, and ensures session preservation.

Caution Unlike other network modules, Cisco Unity Express enhanced network modules use hard disks. Online removal of disks without proper shutdown can cause file system corruption and might render the disk unusable. You must shut down the operating system on the network module in an orderly way before removing or powering down the module.

Caution Cisco routers support OIR with similar modules only. If you remove a module, install another module exactly like it in its place. If you remove a 2-slot module (along with any installed WAN or voice interface cards), install another module and card combination exactly like it.

For a description of informational and error messages that may appear on the console during this procedure, see the hardware installation guide for your router.

Caution If you need to preserve the data on the Cisco Unity Express enhanced network module, or need to transfer the data to a new Cisco Unity Express enhanced network module, perform a backup of the data before removing the module, and restore the data after installing the new module. For more information about backing up and restoring data, see the "Backup and Restore" chapter in the *Cisco Unity Express 3.0 Voice-Mail and Auto-Attendant CLI Administrator Guide:*
http://www.cisco.com/en/US/products/sw/voicesw/ps5520/products_administration_guide_chapter09186a0080874eb2.html

To perform online removal of a network module and insertion of a replacement, follow these steps, with the router in privileged EXEC mode:

Step 1 Initiate a network module session by using the following command:

```
Router# service-module integrated-service-engine slot/unit session

Trying 10.10.10.1, 2065 ... Open


SE-Module> enable
SE-Module#
```

Step 2 Save the running configuration of the network module by using the following command from the SE-Module# prompt:

```
SE-Module# copy running-config tftp tftp-server-address filename
```

Step 3 Exit the network module session by pressing **Control-Shift-6**, followed by pressing **x**.

Step 4 On the router, clear the integrated-service-engine console session by using the following command:

```
Router# service-module integrated-service-engine slot/unit session clear
```

Step 5 Perform a graceful shutdown of the network module disk drive by using the following command:

```
Router# service-module integrated-service-engine slot/unit shutdown
```

Step 6 Shut down the network module interface:

```
Router (config)# interface integrated-service-engine slot/unit
Router (config-if)# shutdown
Router (config-if)# exit
```

Step 7 Unplug all network interface cables from the network module.

Step 8 Loosen the two captive screws that are holding the network module in the chassis slot.

Step 9 Slide the network module out of the slot.

Step 10 Align the replacement network module with the guides in the chassis slot, and slide it gently into the slot.

Note If the router is not fully configured with network modules, make sure that blank panels fill the unoccupied chassis slots to provide proper airflow.

Step 11 Push the module into place until you feel its edge connector mate securely with the connector on the backplane.

Step 12 Reconnect the network interface cables previously removed in Step 7.

Step 13 Check that the network module LEDs are on and that the power (PWR) and enable (EN) LEDs on the front panel are also on. This inspection ensures that connections are secure and that the new unit is operational.

Step 14 Initiate a network module session by using the following command:

```
Router# service-module integrated-service-engine slot/unit session

Trying 10.10.10.1, 2129 ... Open

ISE-network module now available

SE-Module> enable
```

```
SE-Module#
```

Step 15 Restore the network module running configuration by using the following command from the service module prompt:

```
Se# copy tftp running-config tftp-server-address filename
```

Step 16 Exit the network module session by pressing **Control-Shift-6**, followed by pressing **x**.

Step 17 On the router, clear the network module session by using the following command:

```
Router# service-module integrated-service-engine slot/unit session clear
```

Additional References

For additional information, see the following documents and resources.

Related Topic	Document Title
Cisco Unity Express software installation and administration, configuration, and operation	*Cisco Unity Express* at http://www.cisco.com/en/US/products/sw/voicesw/ps5520/tsd_products_support_series_home.html
Cisco IOS software website and reference documentation	*Cisco IOS Software* at http://www.cisco.com/en/US/products/sw/iosswrel/tsd_products_support_category_home.html
Technical documentation, including feedback and assistance	*What's New in Cisco Product Documentation* (including monthly listings of new and revised documents) at http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

CHAPTER 25

Connecting Cisco Network Analysis Modules

This chapter describes how to connect Cisco network analysis modules for modular access routers and contains the following sections:

Note The Network Analysis Module (NAM) is available in multiple hardware forms for some Cisco routers and Catalyst switches. This document applies only to the NAM for branch routers, also known as modular access, multiservice, or integrated services routers.

Tip To determine whether your router supports a specific network module, see Table 1-6 on page 1-16.

Network Analysis Module Overview

This section provides information on the network analysis module (NM-NAM). (See Figure 25-1.)

All network modules have an enable (EN) LED. This LED indicates that the module has passed its self-tests and is available to the router.

All network analysis modules display an additional power (PWR) LED, a disk (DISK) LED, and two additional LEDs for the Fast Ethernet port (see Figure 25-1 and Table 25-1).

Caution To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the network analysis module (NM-NAM) only to intrabuilding or nonexposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

Figure 25-1 Cisco Network Analysis Module (NM-NAM) Faceplate and LEDs

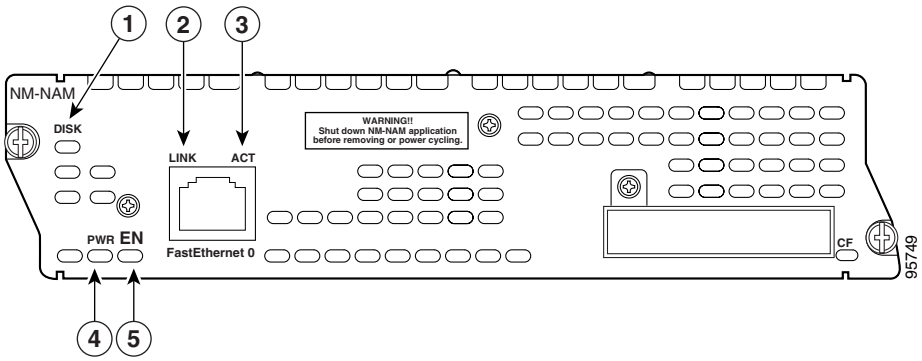


Table 25-1 Cisco Network Analysis Module (NM-NAM) LEDs

Callout	LED	Meaning
1	DISK	There is activity on the hard drive.
2	LINK	The Fast Ethernet connection is available to the network module.
3	ACT	There is activity on the Fast Ethernet connection.
4	PWR	Power is available to the network module.
5	EN	The module has passed self-test and is available to the router.

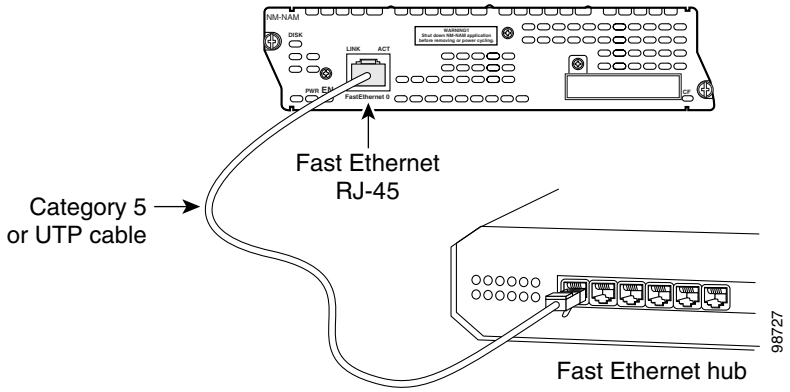
Connecting Cisco Network Analysis Modules to the Network

To connect a network analysis module to the network, use a straight-through 2-pair Category 5 unshielded twisted-pair (UTP) cable to connect the RJ-45 port on the network analysis module to a switch, hub, repeater, server, or other network device. (See Figure 25-2.)

Caution To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the network analysis module (NM-NAM) only to intrabuilding or nonexposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

Note RJ-45 cables are not available from Cisco Systems. These cables are widely available and must be Category 5 cables.

Figure 25-2 Connecting a Cisco Network Analysis Module to a Fast Ethernet Hub



Online Insertion and Removal with a Cisco Network Analysis Module

Some Cisco modular access routers allow you to replace network modules without switching off the router or affecting the operation of other interfaces. This feature is called *online insertion and removal* (OIR). OIR of network modules provides uninterrupted operation to network users, maintains routing information, and ensures session preservation.

Caution Unlike other network modules, network analysis modules use hard disks. Online removal of disks without proper shutdown can result in file system corruption and might render the disk unusable. The operating system on the network analysis module must be shut down in an orderly fashion before the network module is removed.

Caution Cisco routers support OIR with similar modules only. If you remove a network module, install another module exactly like it in its place. If you remove a two-slot network module (along with any installed WAN or voice interface cards), install another module and card combination exactly like it.

For a description of informational and error messages that may appear on the console during this procedure, see the hardware installation guide for your type of router.

To perform online removal of a network analysis module and insertion of a replacement, follow these steps with the router in privileged EXEC mode:

Step 1 Perform a graceful halt of the network analysis module by using the following command:

```
Router# service-module analysis-module slot/0 shutdown

Shutdown is used for Online removal of Service Module.
Do you want to proceed with shutdown? [confirm]
Use service module resent command to recover from shutdown
```

Step 2 Press **Enter** to confirm the request. Wait for the following status message (it may take a minute or two):

```
%SERVICEMODULE-5-SHUTDOWN2:Service module NAM-Sensor1/0 shutdown complete
```

Step 3 Unplug the network interface cable from the network analysis module.

Step 4 Loosen the two captive screws holding the network analysis module in the chassis slot.

Step 5 Remove the network analysis module from the slot.

Step 6 Align the replacement network analysis module with the guides in the chassis slot, and slide it gently into the slot.

Note If the router is not fully configured with network modules, make sure that blank panels fill the unoccupied chassis slots to provide proper airflow.

Step 7 Push the module into place until you feel the edge connector mate securely with the connector on the backplane.

Step 8 Reconnect the network interface cable previously removed in Step 3.

Step 9 Tighten the two captive screws on the faceplate.

Step 10 Reset the network analysis module using the **reset** command.

```
Router# service-module analysis-module slot/0 reset

Use reset only to recover from shutdown or failed state
Warning: May lose date on the hard disc!
Do you want to reset?[confirm]
```

Step 11 Press **Enter** to confirm the request. The network analysis module resets itself.

Step 12 Check that the network module LEDs are on and that the power and enable LEDs on the front panel also are on. This inspection ensures that connections are secure and that the new unit is operational.

Related Documents

For additional information, see the following documents.

Tip For information on obtaining documentation, see the "Obtaining Documentation" section on page viii. For information on obtaining technical assistance, see the "Obtaining Technical Assistance" section on page xi.

Cisco IOS Software Documentation

For information on Cisco IOS software configuration, see the *Network Analysis Module (NM-NAM)* document.

CHAPTER 26

Connecting NAM Enhanced Network Modules

This chapter describes Network Analysis Module (NAM) enhanced network modules for Cisco integrated services routers, and contains the following sections:

Tip To determine whether your Cisco router supports a specific network module, see Table 1-6 on page 1-16.

NAM Enhanced Network Modules

The NAM enhanced network module (NME-NAM-80S) monitors and analyzes network traffic using remote monitoring (RMON), RMON extensions for switched networks (SMON), and other management information bases (MIBs). (See Figure 26-1 on page 26-2.)

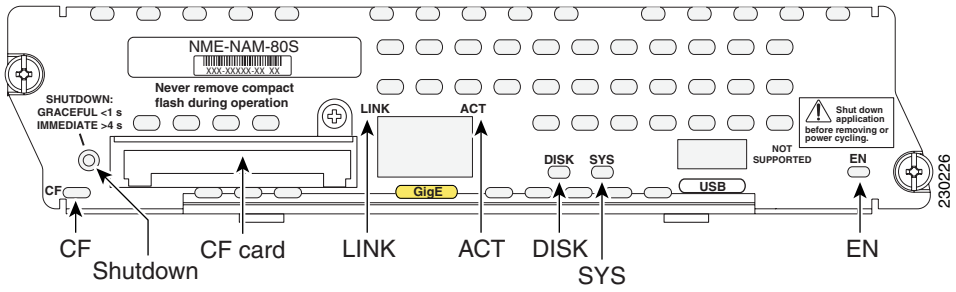
The NAM enhanced network module ships from the factory with the following hardware preinstalled. (See Table 26-1.)

Table 26-1 Preinstalled Hardware in NAM Enhanced Network Modules

Model	Hard Disk	Memory	Daughter Card	CompactFlash
NME-NAM-80S	80 GB (SATA)	512 MB	Included	64 MB

f

Figure 26-1 NME-NAM-80S Faceplate



CF	Status of the CompactFlash Off—CompactFlash is not used Flashing—Application detected CompactFlash at boot up
SHUTDOWN	Press the SHUTDOWN button for less than 2 seconds to gracefully shut down the module. Press the SHUTDOWN button for more than 4 seconds to cause an immediate module shutdown, which may impact file operations that are in progress.
LINK	Status of Gigabit Ethernet link On—Link is enabled Off—Link is disabled
ACT	Status of Gigabit Ethernet activity On—Active Off—Inactive
DISK	Status of hard drive activity On—Active Off—Inactive
SYS	Status of system shutdown **Note** Do not remove power without first shutting down the application. On—Application is stable. Off—System is shut down and ready for host power down Flashing—System shutdown is in progress
EN	Status of the enhanced network module On—Detected by the host Cisco IOS software and enabled Off—Disabled

Shutting Down NAM Enhanced Network Modules

Press the reset button on the network module faceplate for less than 2 seconds to perform a graceful shutdown of the network module before removing power from the router or before starting an online insertion and removal (OIR) sequence on the router. The application may take up to 2 minutes to fully shut down.

Caution If you press the shutdown button for *more than 4 seconds*, a nongraceful shutdown of the hard disk will occur and may cause file corruption on the network module's hard disk. After a nongraceful shutdown, the HD and SYS LEDs remain lit. Press the shutdown button for *less than 2 seconds* to gracefully reboot the network module.

Connecting NAM Enhanced Network Modules

Warning **To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the NAM enhanced network module (NME-NAM-80S) only to intra-building or non-exposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends. The intra-building port(s) of the equipment or subassembly must not be metallically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE, Issue 4) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring.**

To connect NAM enhanced network modules to an external device, use a straight-through two-pair Category 5e unshielded twisted-pair (UTP) cable, and connect the RJ-45 Gigabit Ethernet port on the network module to a switch, hub, repeater, server, or other Gigabit Ethernet network device.

Note RJ-45 cables are not available from Cisco Systems, Inc. These cables are widely available and must be Category 5e cables.

Online Insertion and Removal of Cisco NAM Enhanced Network Modules Procedure

Some Cisco routers allow you to replace network modules without switching off the router or affecting the operation of other interfaces. This feature is called online insertion and removal (OIR). OIR of a module provides uninterrupted operation to network users, maintains routing information, and ensures session preservation.

Caution Unlike other network modules, NAM enhanced network modules use hard disks. Online removal of disks without proper shutdown can result in file system corruption and might render the disk unusable. The operating system on the network module must be shut down in an orderly way before removing or powering down the module.

Caution Cisco routers support OIR with similar modules only. If you remove a module, install another module exactly like it in its place. If you remove a 2-slot module (along with any installed WAN or voice interface cards), install another module and card combination exactly like it.

For a description of informational and error messages that may appear on the console during this procedure, see the hardware installation guide for your router.

To perform online removal of a network module and insertion of a replacement, follow these steps, with the router in privileged EXEC mode:

Step 1 Initiate a network module session using the following command:

```
Router# service-module integrated-service-engine slot/unit session

Trying 10.10.10.1, 2065 ... Open
```

Step 2 Save the running configuration of the network module using the following command from the **Router #** prompt:

```
root@nam.localdomain# config upload ftp://username@host/path
```

Step 3 Exit the network module session by pressing **Control-Shift-6**, followed by **x**.

Step 4 On the router, clear the integrated-service-engine console session using the following command:

```
Router# service-module integrated-service-engine slot/unit session clear
```

Step 5 Perform a graceful shutdown of the network module disk drive by using the following command:

```
Router# service-module integrated-service-engine slot/unit shutdown
```

Step 6 Shut down the network module interface:

```
Router (config)# interface integrated-service-engine slot/unit
Router (config-if)# shutdown
Router (config-if)# exit
```

Step 7 Unplug all network interface cables from the network module.

Step 8 Loosen the two captive screws holding the network module in the chassis slot.

Step 9 Slide the network module out of the slot.

Step 10 Align the replacement network module with the guides in the chassis slot, and slide it gently into the slot.

Note If the router is not fully configured with network modules, make sure that blank panels fill the unoccupied chassis slots to provide proper airflow.

Step 11 Push the module into place until you feel its edge connector mate securely with the connector on the backplane.

Step 12 Reconnect the network interface cables previously removed in Step 7.

Step 13 Check that the network module LEDs are on and that the power (PWR) and enable (EN) LEDs on the front panel are also on. This inspection ensures that connections are secure and that the new unit is operational.

Step 14 Initiate a network module session with the following command:

```
Router# service-module integrated-service-engine slot/unit session
```

```
Trying 10.10.10.1, 2129 ... Open
```

Step 15 Restore the network module running configuration by using the following command from the service module prompt:

```
root@nam.localdomain# config network ftp://username@host/path/filename
```

Step 16 Exit the network module session by pressing **Control-Shift-6**, followed by **x**.

Step 17 On the router, clear the network module session by using the following command:

```
Router# service-module integrated-service-engine slot/unit session clear
```

Additional References

For additional information, see the following documents and resources.

Related Topic	Document Title
NAM software installation and administration, configuration, and operation	*Cisco Branch Router Series (NME-NAM) Installation and Configuration Note* at http://www.cisco.com/en/US/products/sw/cscowork/ps5401/products_installation_and_configuration_guide09186a00807ee90a.html
Cisco IOS software website and reference documentation	Cisco IOS Software at http://www.cisco.com/en/US/products/sw/iosswrel/tsd_products_support_category_home.html
Technical documentation, including feedback and assistance	*What's New in Cisco Product Documentation* (including monthly listings of new and revised documents) at http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

CHAPTER 27

Connecting Circuit Emulation Over IP Network Modules

This chapter describes how to connect circuit emulation over Internet Protocol (CEoIP) network modules and contains the following sections:

Tip To determine whether your router supports a specific network module, see Table 1-6 on page 1-16.

Cisco CEoIP Network Modules

Cisco CEoIP network modules provide a virtual circuit through an IP network (similar to a leased line). Transport of data, regardless of the content or structure of the data stream, is entirely transparent to the destination; bits arriving at one end are delivered unchanged to the destination address.

This chapter provides information on the following two Cisco CEoIP network modules:

- 4-port serial interface network module (NM-CEM-4SER), shown in Figure 27-1
- 4-port T1/E1 RJ-48 interface network module (NM-CEM-4TE1), shown in Figure 27-2

Figure 27-1 4-Port Serial Interface Network Module (NM-CEM-4SER) Faceplate

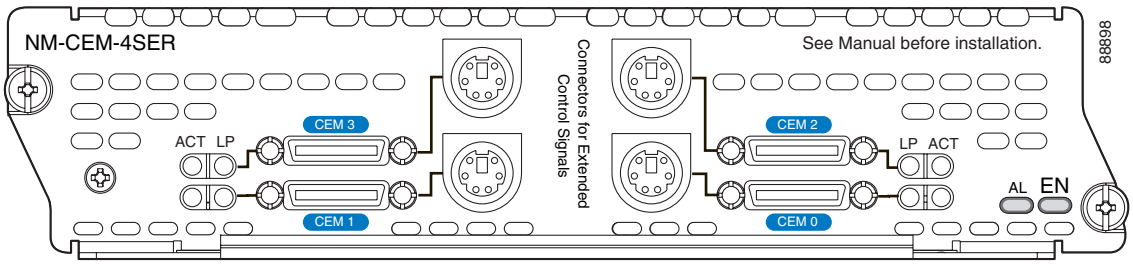
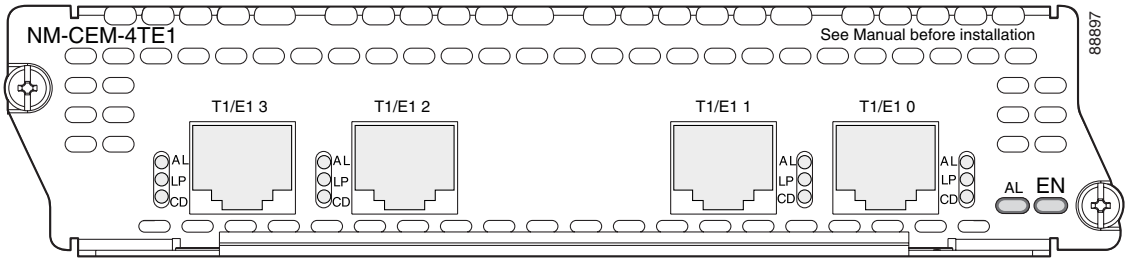


Figure 27-2 4-Port T1/E1 RJ-48 Interface Network Module (NM-CEM-4TE 1) Faceplate



4-Port Serial Interface Network Modules (NM-CEM-4SER)

The 4-port serial interface network module (NM-CEM-4SER) is a single-wide CEoIP network module with four serial ports that support the following interfaces:

- EIA/TIA-232
- EIA/TIA-449
- EIA-530
- EIA-530A
- V.35
- X.21

Caution To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the 4-port serial interface network module (NM-CEM-4SER) only to intrabuilding or nonexposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

The interface type provided by the port is determined by the cable connected to the port. For information on interface-specific cabling requirements, see the "Connecting 4-Port Serial Interface Network Modules to the Network" section on page 27-3.

For information on network module LEDs, see the "4-Port Serial Interface Network Module (NM-CEM-4SER) LEDs" section on page 27-3.

4-Port Serial Interface Network Module (NM-CEM-4SER) LEDs

See Figure 27-3 for the location of network module LEDs and Table 27-1 for LED descriptions.

Figure 27-3 4-Port Serial Interface Network Module (NM-CEM-4SER) LEDs

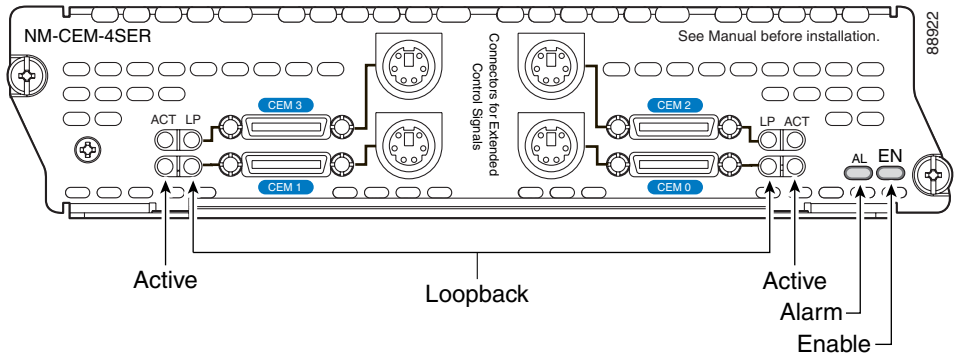


Table 27-1 4-Port Serial Interface Network Module (NM-CEM-4SER) LEDs

LED	Color	Meaning
ACT	Green	The channel on this port is operational.
LP	Yellow	A local or network loopback is present on the port.
AL	Red	Not used.
EN	Green	The network module has passed self-test and is available to the router.

Connecting 4-Port Serial Interface Network Modules to the Network

The 4-port serial interface network module uses Smart Serial connectors, permitting each port to support a basic or extended set of serial control signals, depending on the cable connected to the port.

Caution To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the 4-port serial interface network module (NM-CEM-4SER) only to intrabuilding or nonexposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

The following basic set of control signals is used on Cisco 12-in-1 cables:

- Data Terminal Ready (DTR)
- Data Set Ready (DSR)
- Request to Send (RTS)
- Clear to Send (CTS)
- Data Carrier Detect (DCD)
- Local Loop (LL)

The following control signals are part of the extended set, in addition to the basic set listed above, and are used on Cisco Extended 12-in-1 cables:

- Remote Loop (RL)
- Test Mode (TM)
- Ring Indicator (RI)

Note Control signal support depends on the interface type. Not all of the control signals listed above are supported by every interface type.

Note The control signal names used in this document are the names commonly used in the industry for RS-232. Other interface types may use other names for the equivalent control signals.

The 4-port serial interface network module (NM-CEM-4SER) supports both Cisco 12-in-1 interface cables and Cisco Extended 12-in-1 interface cables with user-defined end-connectors permitting connection to either DTE or DCE interfaces.

Interfaces and DTE or DCE modes are defined by the type of cable connected to the network module.

Tip Use the Cisco 12-in-1 cable for X.21 interfaces. The X.21 interface connector does not require an additional DIN connector.

For information on using Cisco 12-in-1 cables with the 4-port serial interface network module, see Table 27-3. Figure 27-4 illustrates how to connect the Cisco 12-in-1 cable to the network module.

For information on using Cisco Extended 12-in-1 cables with the 4-port serial interface network module, see Table 27-4. Figure 27-5 illustrates how to connect the Cisco Extended 12-in-1 cable to the network module.

All serial interface types are available in DTE or DCE format: DTE requires a plug connector at the customer premises equipment (CPE) end, and DCE requires a receptacle connector at the CPE end.

Serial Interface Data Rates and Distance Limitations

All serial signals are subject to distance limits, beyond which the signal degrades significantly or is completely lost. Generally, the slower the data rate, the greater the distance the signal can travel.

Table 27-2 lists maximum recommended speeds and distances for each serial interface type. If you understand and compensate for potential electrical problems, you may get good results at speeds and distances greater than those listed. For instance, the recommended maximum rate for V.35 is 2 Mbps, but 4 Mbps is commonly used.

Table 27-2 Maximum Recommended Speeds and Distances for Each Serial Interface Type

	EIA/TIA-232 Distance		EIA/TIA-449, -530, -530A, V.35, X.21 Distance	
Data Rate, bps	**Feet**	**Meters**	**Feet**	**Meters**
2400	200	60	4100	1250
4800	100	30	2050	625

Table 27-2 Maximum Recommended Speeds and Distances for Each Serial Interface Type (continued)

	EIA/TIA-232 Distance		EIA/TIA-449, -530, -530A, V.35, X.21 Distance	
Data Rate, bps	**Feet**	**Meters**	**Feet**	**Meters**
9600	50	15	1025	312
19200	25	8	500	150
38400	12	4	250	75
56000	9	3	100	30

Balanced drivers allow EIA/TIA-449, EIA/TIA-530, EIA/TIA-530A, V.35, and X.21 signals to travel greater distances than EIA/TIA-232 signals. All balanced interfaces easily support 4 to 8 Mbps.

Using Cisco 12-in-1 Interface Cables with the 4-Port Serial Interface Network Module (NM-CEM-4SER)

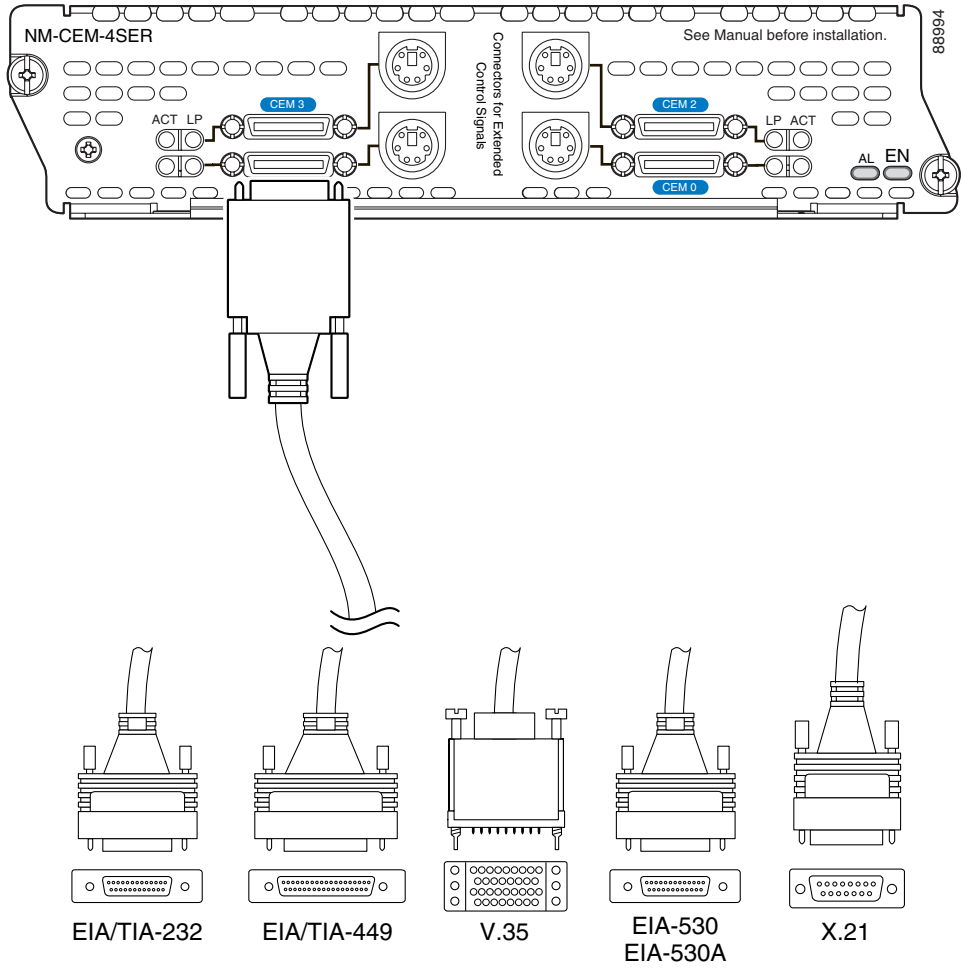
Table 27-3 lists the Cisco 12-in-1 interface cables supported by the 4-port serial interface network module. Use the cable part number to order replacement or spare cables for the interface and DTE or DCE mode appropriate for your network.

Figure 27-4 illustrates how to connect the Cisco 12-in-1 cable to the network module.

Table 27-3 Cisco 12-in-1 Interface Cable Part Numbers Used with the 4-Port Serial Interface Network Module (NM-CEM-4SER)

Interface	DCE/DTE	Cisco Cable Part Number
EIA/TIA-232	Female DCE Male DTE	CAB-SS-232FC CAB-SS-232MT
EIA/TIA-449	Female DCE Male DTE	CAB-SS-449FC CAB-SS-449MT
EIA-530	Male DTE	CAB-SS-530MT
EIA-530A	Male DTE	CAB-SS-530AMT
V.35	Female DCE Female DTE Male DCE Male DTE	CAB-SS-V35FC CAB-SS-V35FT CAB-SS-V35MC CAB-SS-V35MT
X.21	Female DCE Male DTE	CAB-SS-X21FC CAB-SS-X21MT

Figure 27-4 Connecting the Cisco 12-in-1 Interface Cable to the 4-Port Serial Interface Network Module (NM-CEM-4SER)



Connections at the CPE

Using Cisco Extended 12-in-1 Interface Cables with the 4-Port Serial Interface Network Module (NM-CEM-4SER)

Table 27-4 lists the Cisco Extended 12-in-1 interface cables supported by the 4-port serial interface network module. Use the cable part number to order replacement or spare cables for the interface and DTE or DCE mode appropriate for your network.

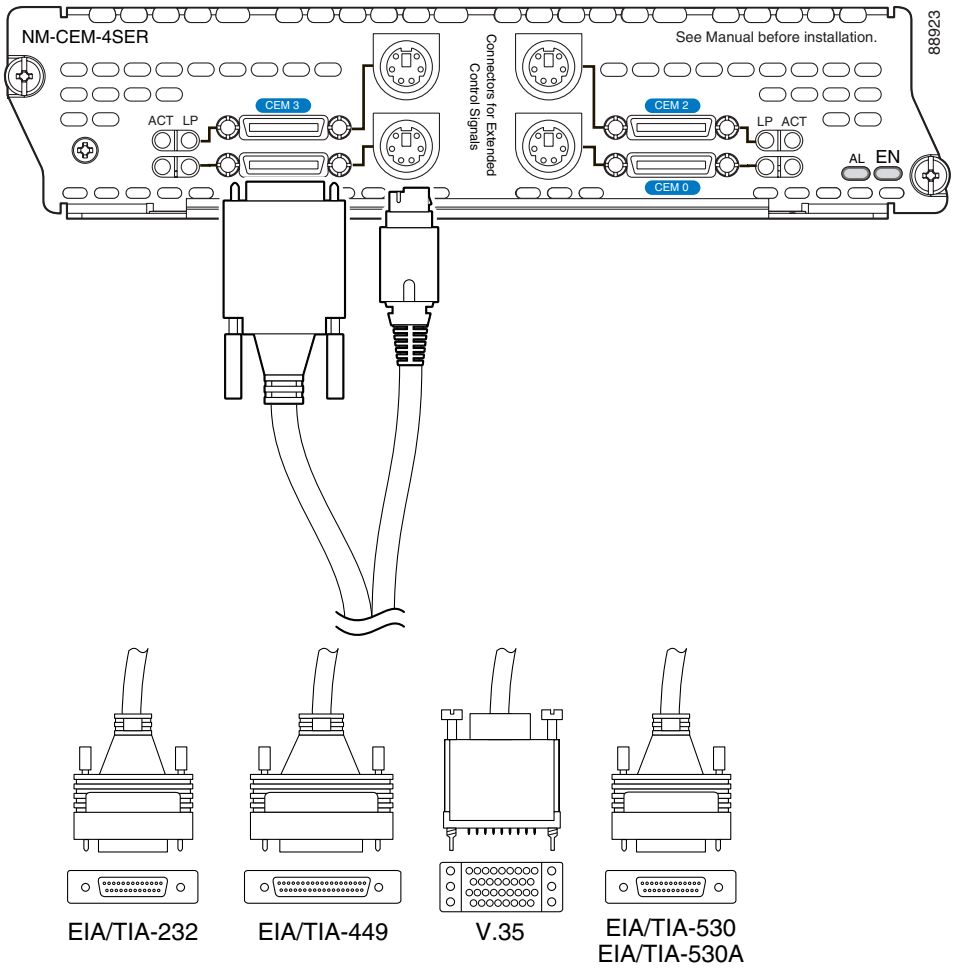
Figure 27-5 illustrates how to connect the Cisco 12-in-1 cable to the network module.

Table 27-4 Cisco Extended 12-in-1 Interface Cable Part Numbers Used with the 4-Port Serial Interface Network Module (NM-CEM-4SER)

Interface	DCE/DTE	Cisco Cable Part Number
EIA/TIA-232	Female DCE Male DTE	CAB-SS-232FC-EXT CAB-SS-232MT-EXT
EIA/TIA-449	Female DCE Male DTE	CAB-SS-449FC-EXT CAB-SS-449MT-EXT
EIA-530	Female DCE Male DTE	CAB-SS-530FC-EXT CAB-SS-530MT-EXT
EIA-530A	Female DCE Male DTE	CAB-SS-530AFC-EXT CAB-SS-530AMT-EXT
V.35	Female DCE Female DTE Male DCE Male DTE	CAB-SS-V35FC-EXT CAB-SS-V35FT-EXT CAB-SS-V35MC-EXT CAB-SS-V35MT-EXT

Note Cisco Extended 12-in-1 cables provide additional control signals through the DIN cable connection.

Figure 27-5 Connecting the Cisco Extended 12-in-1 Interface Cable to the 4-Port Serial Interface Network Module (NM-CEM-4SER)



Connections at the CPE

4-Port T1/E1 RJ-48 Interface Network Modules (NM-CEM-4TE1)

The 4-port T1/E1 RJ-48 interface network module (NM-CEM-4TE1) is a single-wide CEoIP network module with four T1/E1 ports. (See Figure 27-2.) The NM-CEM-4TE1 connects to any T1/E1 interface for voice or data.

4-Port T1/E1 RJ-48 Interface Network Module (NM-CEM-4TE1) LEDs

See Figure 27-6 for the location of network module LEDs and Table 27-5 for LED descriptions.

Figure 27-6 4-Port T1/E1 RJ-48 Interface Network Module (NM-CEM-4TE1) LEDs

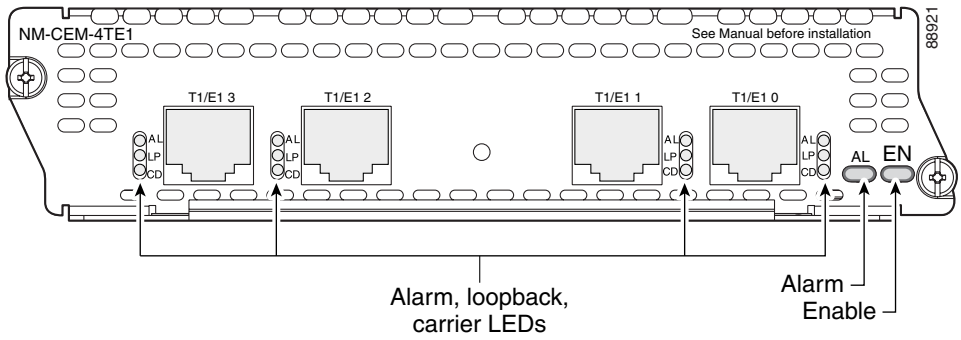


Table 27-5 4-Port T1/E1 RJ-48 Interface Network Module (NM-CEM-4TE1) LEDs

LED	Color	Meaning
AL	Yellow	Loss of signal or loss of frame has occurred, or the network module is unavailable because of excessive errors on the interface.
LP	Yellow	A local or network loopback on the port.
CD	Green	Activity is occurring on the interface (carrier detect).
EN	Green	The network module has passed self-test and is available to the router.
AL	Yellow	Not used.

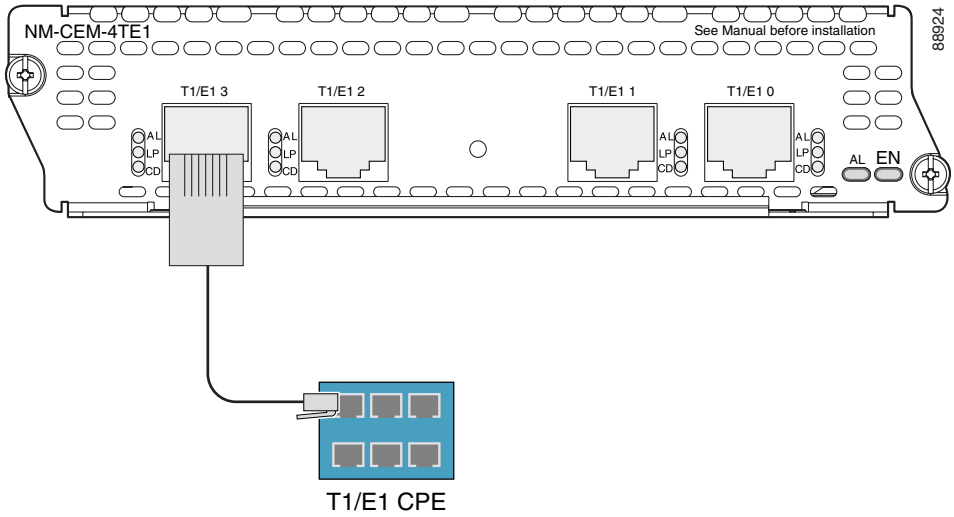
Connecting 4-Port T1/E1 RJ-48 Interface Network Modules (NM-CEM-4TE1) to the Network

The 4-port T1/E1 RJ-48 interface network module (NM-CEM-4TE1) uses a RJ-48 straight-through cable to connect to the customer premises equipment (CPE) for use in T1 or E1 circuit emulation. (See Figure 27-7.)

Note All four ports on the network module must operate in the same software-configured mode, either as T1 ports or as E1 ports. The NM-CEM-4TE1 network module does not support combinations of T1 and E1 ports on the same network module.

When configured for E1 operation, the NM-CEM-4TE1 network module provides four 120-ohm balanced ports. To connect any of these ports to a 75-ohm unbalanced network, use Cisco cable CAB-ADP-75-120. For more information, see the *Installing the 75-120-Ohm Adapter Cable on E1 Multichannel Port Adapters* document.

Figure 27-7 Connecting the 4-Port T1/E1 RJ-48 Interface Network Module (NM-CEM-4TE1) to the Network



CHAPTER 28

Connecting Cisco High-Density Extension Modules

This chapter describes how to connect Cisco high-density extension modules to the network and contains the following sections:

Tip To determine whether your router supports a specific network module, see Table 1-5 on page 1-15.

Cisco High-Density Analog and Digital Extension Module for Voice and Fax

The Cisco high-density analog and digital extension module for voice and fax is available as an 8-port analog voice module (EVM-HD-8FXS/DID). Each port can be configured in Foreign Exchange Station (FXS) or Direct Inward Dialing (DID) mode through Cisco IOS software commands.

Note FXS supports on-premises applications only.

Cisco high-density extension modules provide an integrated high-density analog and digital voice interface for small or medium branch offices. Together with certain expansion modules (see the "Expansion Modules for Cisco High-Density Extension Modules" section on page 28-3), the Cisco high-density extension module provides a maximum of 24 analog voice ports with 8 ports of DID capability.

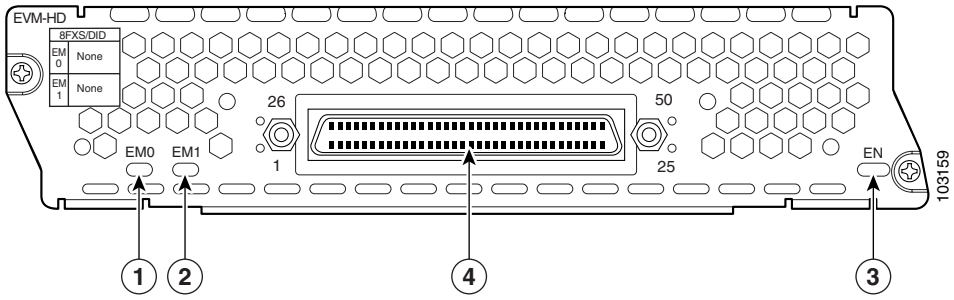
Note Cisco high-density extension modules can only be used in certain slots of modular access routers. To determine which slots on your router support high-density extension modules, see the "Platform and Slot Limitations for Cisco Network Modules" section in Chapter 1, "Overview of Cisco Network Modules for Cisco Access Routers."

Caution To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the 8-port analog voice/fax expansion module (EM-HDA-8FXS) and 4-port digital voice/fax expansion module (EM-4BRI-NT/TE) only to intrabuilding or nonexposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

Cisco High-Density Extension Module LEDs and Interfaces

Figure 28-1 shows high-density extension module LEDs and interfaces.

Figure 28-1 Cisco High-Density Extension Module (EVM-HD-8FXS/DID) LEDs



1	EM0: Green indicates presence of an installed expansion module in slot EM0.	**3**	EN: Green indicates that the network module has passed self-test and is available to the router.
2	EM1: Green indicates presence of an installed expansion module in slot EM1.	**4**	RJ-21 connector for use with RJ-21 cable.

Expansion Modules for Cisco High-Density Extension Modules

The Cisco high-density extension module supports up to two expansion modules (EMs) in the configurations shown in Table 28-1.

Table 28-1 Example Hardware Configurations Supported on Cisco High-Density Extension Modules (EVM-HD-8FXS/DID)

Base Board (FXS or DID)	EM0	EM1	Total Ports					Total Voice Sessions
			FXS or DID	FXS	FXO	BRI		
						Ports	B-channel	
EVM-HD-8FXS/DID	—	—	8	—	—	—	—	8
	EM-HDA-8FXS	—	8	8	—	—	—	16
	EM-HDA-8FXS	EM-HDA-8FXS	8	16	—	—	—	24
	EM-HDA-8FXS	EM-HDA-3FXS/4FXO	8	11	4	—	—	23
	EM-HDA-8FXS	EM-HDA-6FXO	8	8	6	—	—	22
	EM-HDA-8FXS	EM-4BRI-NT/TE	8	8	—	4	8	24
	EM-HDA-3FXS/4FXO	—	8	3	4	—	—	15
	EM-HDA-3FXS/4FXO	EM-HDA-3FXS/4FXO	8	6	8	—	—	22
	EM-HDA-3FXS/4FXO	EM-HDA-6FXO	8	3	10	—	—	21
	EM-HDA-3FXS/4FXO	EM-4BRI-NT/TE	8	3	4	4	8	23
	EM-HDA-6FXO	—	8	—	6	—	—	14
	EM-HDA-6FXO	EM-HDA-6FXO	8	—	12	—	—	20
	EM-HDA-6FXO	EM-4BRI-NT/TE	8	—	6	4	8	22
	EM-4BRI-NT/TE	—	8	—	—	4	8	16
	EM-4BRI-NT/TE	EM-4BRI-NT/TE	8	—	—	8	16	24

The 4-port digital voice/fax expansion module (EM-4BRI-NT/TE) operates as an S/T interface and is capable of NT or TE functionality. In NT mode, the expansion module can supply in-line power for the far end of the connection.

The 7-port analog voice/fax expansion module (EM-HDA-3FXS/4FXO) provides three additional FXS ports and four FXO ports for off-premises analog voice applications.

The 6-port analog voice/fax expansion module (EM-HDA-6FXO) provides six FXO ports for off-premises analog voice applications. The sixth port (port 5) provides a trunk bypass (TBP) or power failover capability.

The 8-port analog voice/fax expansion module (EM-HDA-8FXS) adds an additional eight FXS ports to the Cisco high-density extension module.

Tip When router power is off, connect an analog phone to the FXO line to make a call. (See the "Connecting Cisco High-Density Extension Modules to the Network" section on page 28-6 for more information).

Installing Expansion Modules on Cisco High-Density Extension Modules

Expansion modules can be used to increase the number of ports supported on the high-density extension module.

Note ESD straps should be worn when handling all modules, including during installation of expansion modules. An ESD wrist strap is shipped with the product.

To install expansion modules, follow these steps:

Step 1 Decide if the expansion board is going in the EM0 slot or EM1 slot.

Note The EM0 slot is on the left, and the EM1 slot is on the right as you look at the face plate.

Step 2 Align the connectors on the underside of the expansion module with the connectors for the slot you plan to use on the network module. (See Figure 28-2.)

Step 3 Using gentle pressure, insert the connectors on the underside of the expansion module into the connectors on the network module.

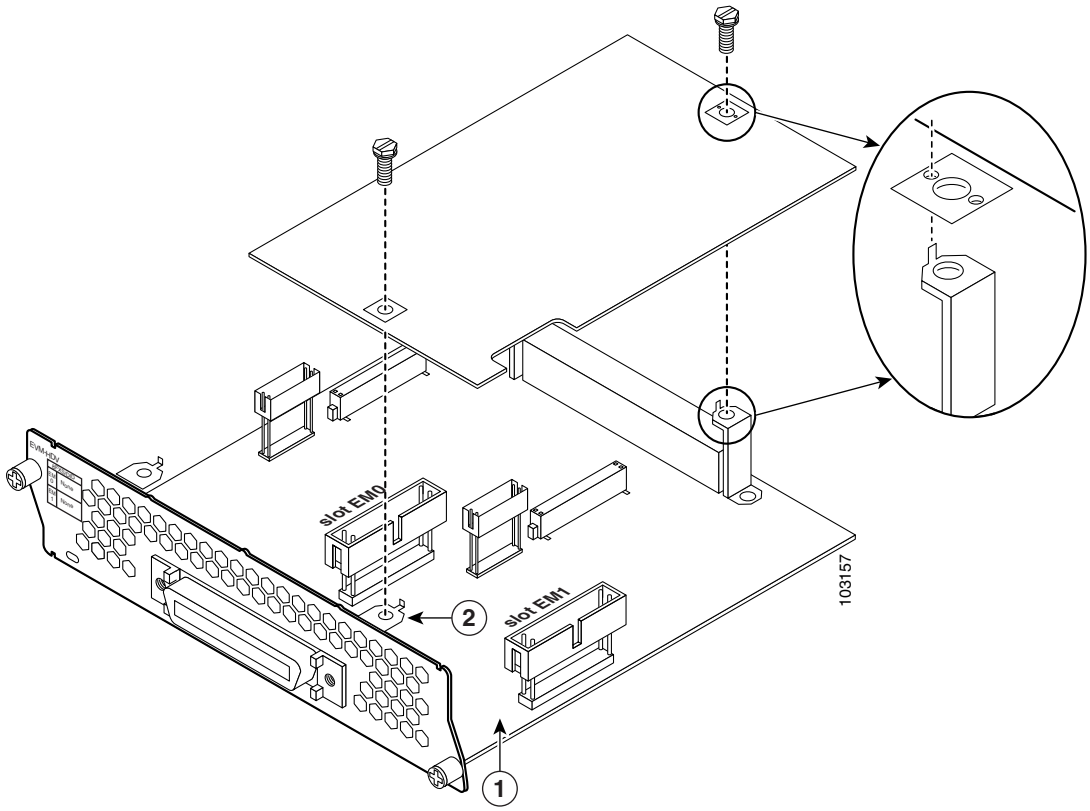
Tip Use the alignment pins on the network module brackets to guide the expansion module during installation.

Note Press firmly on the expansion module until the board seats to ensure proper network connections.

Caution For each expansion module, two mounting screws must be installed with 6-8 lbs-in (67.8 N-cm) of torque. Failure to properly secure the expansion module to the base module with two screws compromises product reliability. **In the case of FXO ports, failure to properly tighten both mounting screws causes FXO ground-start outgoing call operation to fail**.

Step 4 Insert two screws from the hardware kit through the screw guides on the expansion module into the threaded holes on the network module brackets.

Figure 28-2 Installing an Expansion Module on Extension Module Slot EM1



1	Expansion module connector on the network module (for slot EM1).	**2**	Screw bracket on the network module faceplate (for slot EM1).

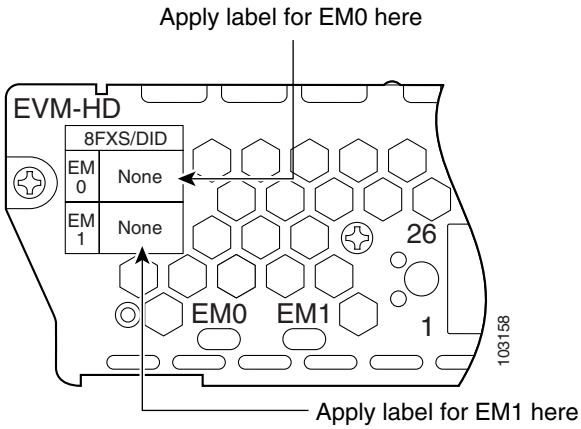
Step 5 Using a small flat-blade screwdriver, tighten the screws to secure the expansion module to the network module.

Warning **Failure to secure the expansion module to the base module with two screws defeats the earth ground, causing a potential safety hazard.** Statement 347

Tip To maintain proper seating of the network module, tighten the rear screw first.

Step 6 Apply the appropriate label on the front of the network module faceplate. (See Figure 28-3.)

Figure 28-3 Label Locations for Expansion Modules on Cisco High-Density Expansion Modules



Step 7 Install the network module into the router. (See the "Installing Cisco Network Modules in Cisco Access Routers" section on page 2-5.)

Connecting Cisco High-Density Extension Modules to the Network

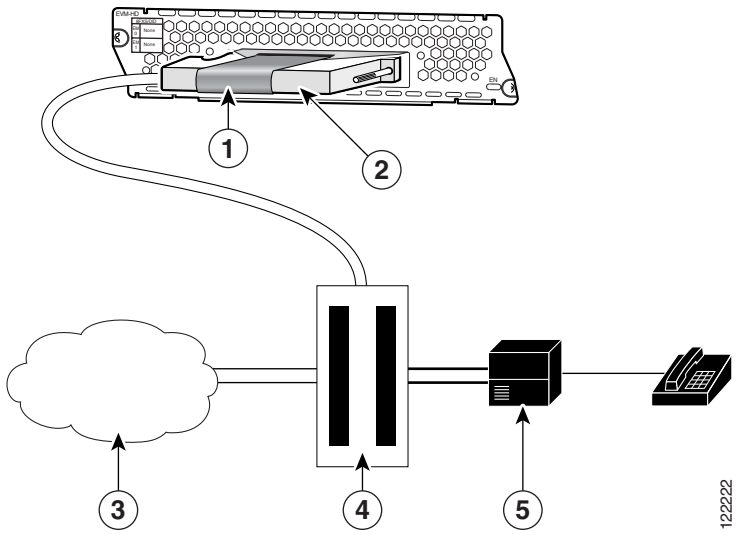
The Cisco high-density extension module is connected to a distribution frame or patch panel with an RJ-21 cable. (See Figure 28-4.) RJ-21 cables are not provided with the network module.

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

Caution To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the 8-port analog voice/fax expansion module (EM-HDA-8FXS) and 4-port digital voice/fax expansion module (EM-4BRI-NT/TE) only to intrabuilding or nonexposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

For ordering information, see the "Obtaining Technical Assistance" section on page xi.

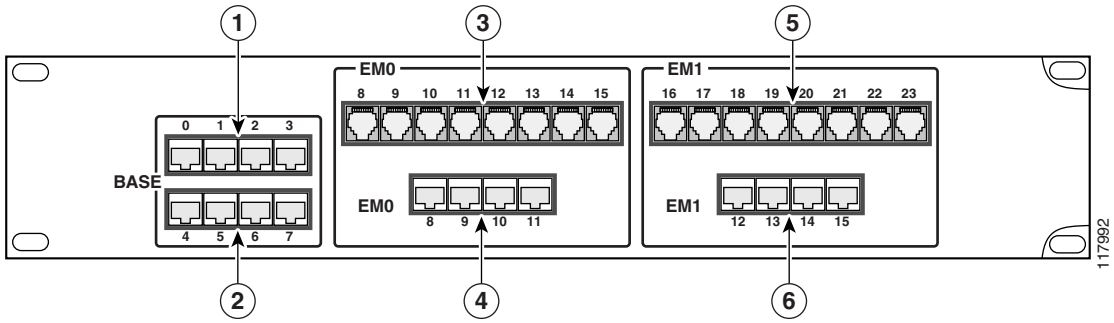
Figure 28-4 Connecting Cisco High-Density Extension Modules (EVM-HD-8FXS/DID) to a Main Distribution Frame or Patch Panel



1	Strap to secure connector	**4**	Main distribution frame
2	RJ-21 connector	**5**	PBX
3	Public switched telephone network		

Distribution panels are generally available from multiple cable and network adapter vendors. Customers may, at their sole discretion, consider using a patch panel from Black Box Corporation (JPM2194A—see Figure 28-5). ***(Mention of products or services other than Cisco products or services is for information purposes only and constitutes neither an endorsement nor a recommendation.)*** The Black Box patch panel accommodates RJ-11 and RJ-45 combinations possible on Cisco high-density expansion modules, and offers flexibility for expansion module upgrades (either analog or digital). For ordering information, see the Cisco High-Density Extension Module data sheet.

Figure 28-5 Black Box Patch Panel (JPM2194A) for Use with Cisco High-Density Expansion Modules



1	RJ-11 receptacles for FXS/DID ports on the EVM-HD-8FXS/DID baseboard.	**4**	RJ-45 receptacles for BRI ports on the EM-4BRI-NT/TE when installed in slot EM0.
2	RJ-11 receptacles for FXS/DID ports on the EVM-HD-8FXS/DID baseboard.	**5**	RJ-11 receptacles for FXS or FXO ports on an FXS or FXO expansion module when installed in slot EM1. **Note** Applies to EM-HDA-8FXS, EM-HDA-6FXO, or EM-HDA-3FXS/4FXO expansion modules only.
3	RJ-11 receptacles for FXS or FXO ports on an FXS or FXO expansion module when installed in slot EM0. **Note** Applies to EM-HDA-8FXS, EM-HDA-6FXO, or EM-HDA-3FXS/4FXO expansion modules only.	**6**	RJ-45 receptacles for BRI ports on the EM-4BRI-NT/TE when installed in slot EM1.

Table 28-2 provides pin definitions for the RJ-11 and RJ-45 receptacle types:

Table 28-2 Pinouts for RJ-11 and RJ-45 Receptacle Types

Receptacle Type	Pin Definitions
RJ-11	Pin 3 = Ring Pin 4 = Tip
RJ-45	Pin 3 = ISDN BRI-S/T Bus Transmit+ Pin 4 = ISDN BRI-S/T Bus Receive+ Pin 5 = ISDN BRI-S/T Bus Receive– Pin 6 = ISDN BRI-S/T Bus Transmit–

Establishing Emergency or Power-Fail Connections

During power failures or when router power is off, emergency voice connections can be made through power-fail ports on the EM-HDA-6FXO expansion module. The expansion module must be properly installed on the Cisco high-density extension module. (See the "Installing Expansion Modules on Cisco High-Density Extension Modules" section on page 28-4.)

To provide an emergency connection, connect an analog phone using the port information listed in Table 28-3.

Note There will not be a dial tone on port 15 or port 23 until the router is powered down.

Table 28-3 Establishing Emergency Connections through Cisco High-Density Extension Modules

Expansion Module Slot	Analog Phone Port	PSTN Port
EM0	Port 15 Tip/Ring	Port 13 Tip/Ring
EM1	Port 23 Tip/Ring	Port 21 Tip/Ring

Caution Analog phones connected to the power-fail ports should not be connected in parallel to a normal FXS port on Cisco high-density extension modules. The protection circuit on the FXS port can interfere with phone operation when router power is off.

Cisco High-Density Extension Module Cable Pinouts

Figure 28-6 shows the RJ-21 connector wiring for the cable used for the high-density extension module, and Table 28-4 lists cable pinouts. Port usage depends on the type of installed expansion module.

Figure 28-6 Close-Up of the RJ-21 Connector Pinout for Cisco High-Density Extension Modules (EVM-HD-8FXS/DID)

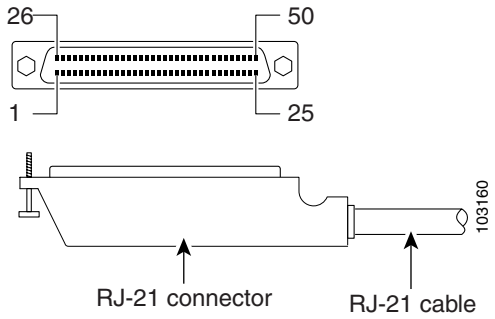


Table 28-4 RJ-21 Connections for the Cisco High-Density Extension Module

RJ-21 Pin	Hardware Component	Base Card Ports	Expansion Module Ports			
		8FXS/DID	EM-HDA-8FXS	EM-HDA-3FXS/4FXO	EM-HDA-6FXO	EM-4BRI-NT/TE
26	Base card (EVM-HD-8FXS	Port 0 Tip	—	—	—	—
1		Port 0 Ring				
27		Port 1 Tip				
2		Port 1 Ring				
28		Port 2 Tip				
3		Port 2 Ring				
29		Port 3 Tip				
4		Port 3 Ring				
30		Port 4 Tip				
5		Port 4 Ring				
31		Port 5 Tip				
6		Port 5 Ring				
32		Port 6 Tip				
7		Port 6 Ring				
33		Port 7 Tip				
8		Port 7 Ring				
34	EM0	—	Port 8 Tip	FXS Port 8 Tip	Port 8 Tip	Port *x*/0 SX–
9			Port 8 Ring	FXS Port 8 Ring	Port 8 Ring	Port *x*/0 SX+
35			Port 9 Tip	FXS Port 9 Tip	Port 9 Tip	Port *x*/0 SR-
10			Port 9 Ring	FXS Port 9 Ring	Port 9 Ring	Port *x*/0 SR+
36			Port 10 Tip	FXS Port 10 Tip	Port 10 Tip	Port *x*/1 SX–
11			Port 10 Ring	FXS Port 10 Ring	Port 10 Ring	Port *x*/1 SX+
37			Port 11 Tip	Unused	Port 11 Tip	Port *x*/1 SR-
12			Port 11 Ring	Unused	Port 11 Ring	Port *x*/1 SR+
38			Port 12 Tip	FXO Port 12 Tip	Port 12 Tip	Port *x*/2 SX–
13			Port 12 Ring	FXO Port 12 Ring	Port 12 Ring	Port *x*/2 SX+
39			Port 13 Tip	FXO Port 13 Tip	Port 13 Tip	Port *x*/2 SR-
14			Port 13 Ring	FXO Port 13 Ring	Port 13 Ring	Port *x*/2 SR+
40			Port 14 Tip	FXO Port 14 Tip	Unused	Port *x*/3 SX–
15			Port 14 Ring	FXO Port 14 Ring	Unused	Port *x*/3 SX+
41			Port 15 Tip	FXO Port 15 Tip	PFP[1] Tip	Port *x*/3 SR-
16			Port 15 Ring	FXO Port 15 Ring	PFP Ring	Port *x*/3 SR+

Table 28-4 RJ-21 Connections for the Cisco High-Density Extension Module (continued)

RJ-21 Pin	Hardware Component	Base Card Ports	Expansion Module Ports			
		8FXS/DID	EM-HDA-8FXS	EM-HDA-3FXS/4FXO	EM-HDA-6FXO	EM-4BRI-NT/TE
42	EM1	—	Port 16 Tip	FXS Port 16 Tip	Port 16 Tip	Port *x*/4 SX–
17			Port 16 Ring	FXS Port 16 Ring	Port 16 Ring	Port *x*/4 SX+
43			Port 17 Tip	FXS Port 17 Tip	Port 17 Tip	Port *x*/4 SR-
18			Port 17 Ring	FXS Port 17 Ring	Port 17 Ring	Port *x*/4 SR+
44			Port 18 Tip	FXS Port 18 Tip	Port 18 Tip	Port *x*/5 SX–
19			Port 18 Ring	FXS Port 18 Ring	Port 18 Ring	Port *x*/5 SX+
45			Port 19 Tip	Unused	Port 19 Tip	Port *x*/5 SR-
20			Port 19 Ring	Unused	Port 19 Ring	Port *x*/5 SR+
46			Port 20 Tip	FXO Port 20 Tip	Port 20 Tip	Port *x*/6 SX–
21			Port 20 Ring	FXO Port 20 Ring	Port 20 Ring	Port *x*/6 SX+
47			Port 21 Tip	FXO Port 21 Tip	Port 21 Tip	Port *x*/6 SR-
22			Port 21 Ring	FXO Port 21 Ring	Port 21 Ring	Port *x*/6 SR+
48			Port 22 Tip	FXO Port 22 Tip	Unused	Port *x*/7 SX–
23			Port 22 Ring	FXO Port 22 Ring	Unused	Port *x*/7 SX+
49			Port 23 Tip	FXO Port 23 Tip	PFP Tip	Port *x*/7 SR-
24			Port 23 Ring	FXO Port 23 Ring	PFP Ring	Port *x*/7 SR+
50			Unused	Unused	Unused	Unused
25			Unused	Unused	Unused	Unused

1. During power failures or when router power is off, emergency voice connections can be made through power-fail ports (PFP) on the EM-HDA-6FXO expansion module.

Note If there is only one EM-4BRI-NT/TE and it is installed in EM1, number the ports *x*/0 through *x*/3.

CHAPTER 29

Connecting Alarm Interface Controller Network Modules

This chapter describes how to install the alarm interface controller (AIC) network module and contains the following sections:

Tip To determine whether your router supports a specific network module, see Table 1-6 on page 1-16.

Alarm Interface Controller Network Module

The AIC network module, shown in Figure 29-1, supports 64 alarm inputs. Fifty-six alarm inputs are discrete and can operate on dry contact closure when a patch panel is used. The last eight alarm inputs can be provisioned to accept analog inputs. The AIC network module has 16 control relay outputs.

The AIC network module can be connected to a patch panel. The patch panel provides the bias to the circuit.

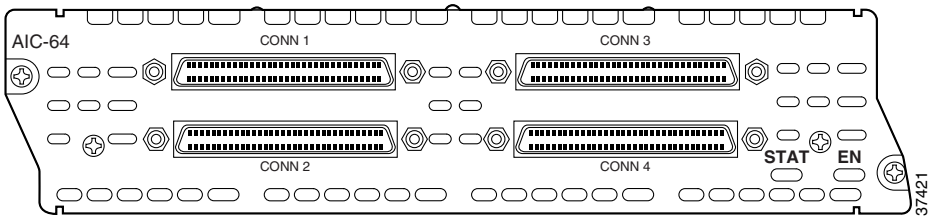
The analog alarm inputs can be configured to monitor either DC voltage or current. The AIC can measure voltage from –60 to 60 V or current from 0 to 20 mA. The control relay can be operated to turn an external device on or off. When an event is detected, notification messages are sent to the Operations Support System (OSS) in the network operation center (NOC). These alarm inputs are configured in Cisco IOS software. Some reportable events include:

- Equipment alarm
- Building intrusion (door/window)
- Temperature threshold violation
- Voltage fluctuation

The AIC network module converts relay contact alarm signals to TL1 and SNMP message formats, providing TL1 over TCP/IP and SNMP protocols. All the contact closure-related alarms are routed and reported through the existing OSS and the associated OSS networks. With this network module, the Cisco router sends the TL1 or SNMP messages to the OSS autonomously or in response to TL1 or SNMP commands from the OSS.

The AIC network module is connected to the network using four high-density SCSI-type connectors on the front panel.

Figure 29-1 Alarm Interface Controller Network Module



Connecting the AIC Network Module to the Network

An AIC network module provides four 50-pin receptacles. Use cables that have male Micro DB-50 connectors at both ends with all conductors straight-wired. Central office equipment is cabled to the patch panel, and then cross-connected to the AIC cable.

Two different patch panels can be used. The AIC-1 patch panel terminates one AIC and has voltage terminations with lugs and fuses for voltage monitoring. The AIC-2 patch panel terminates up to two AICs or 128 contact closure points

See Figure 29-2 through Figure 29-6 for examples of the AIC connections to the patch panels.

See the AIC data sheet on www.cisco.com for recommended patch panel and cable vendors.

Caution Damage to the AIC network module can occur if an alarm set for monitoring current is connected to a sensor for monitoring voltage. Make sure that your alarms are connected to the proper sensors.

Caution Connect the cable to the AIC before connecting it to the patch panel or other connection. Otherwise, voltage could be present on the male pins that connect to the AIC.

Caution The signal I/O connections on this unit are intended only for connection to NEC/CEC Class 2 or equivalent circuit. This means that the voltages applied to I/O connections should not exceed 42.4 Vpk or 60 Vdc and it should be a limited/fused power source. For more details on Class 2 circuits, refer to the National Electrical Code/Canadian Electrical Code. This does not apply to the analog input/output terminal strip numbers 1–8 on the AIC-1 patch panel.

Caution This unit is not intended for connection to exposed plant leads. Therefore, it should not be connected to circuit conductors that extend beyond one building and are run so as to be subject to accidental contact with AC main conductors, or are exposed to lightning on interbuilding circuits on the same premises.

Ports are numbered from right to left and from bottom to top, as labeled on the module rear panel. Pinouts for the AIC-1 patch panel are shown in Table 29-1. The connector 3 voltage monitor pinouts for AIC-1 are shown in Table 29-2. Pinouts for the AIC-2 patch panel are shown in Table 29-3.

Cables are not provided with the network module. For ordering information, see the "Obtaining Technical Assistance" section on page xi.

Figure 29-2 AIC Network Module Connection Diagram

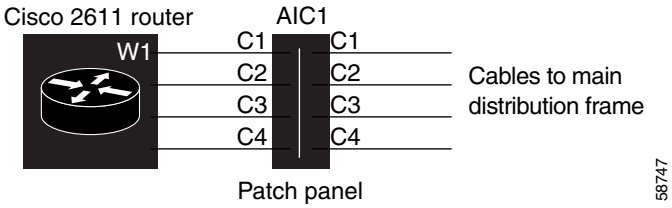


Figure 29-3 AIC Network Module Faceplate Connections

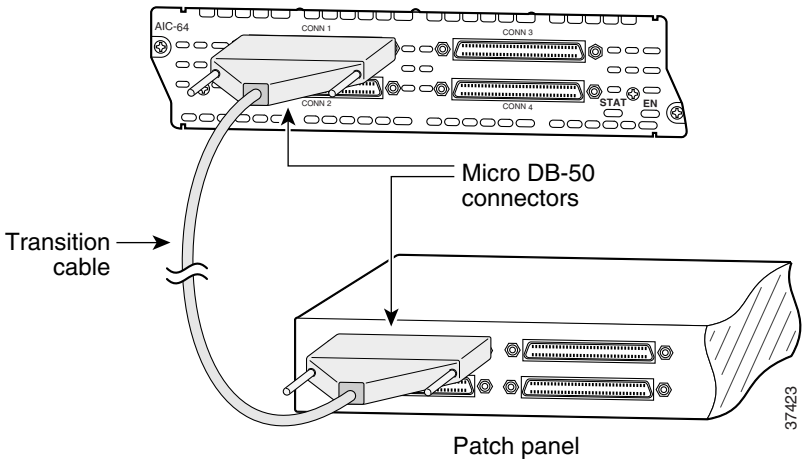


Figure 29-4 AIC Network Module Connected to AIC-1 Patch Panel

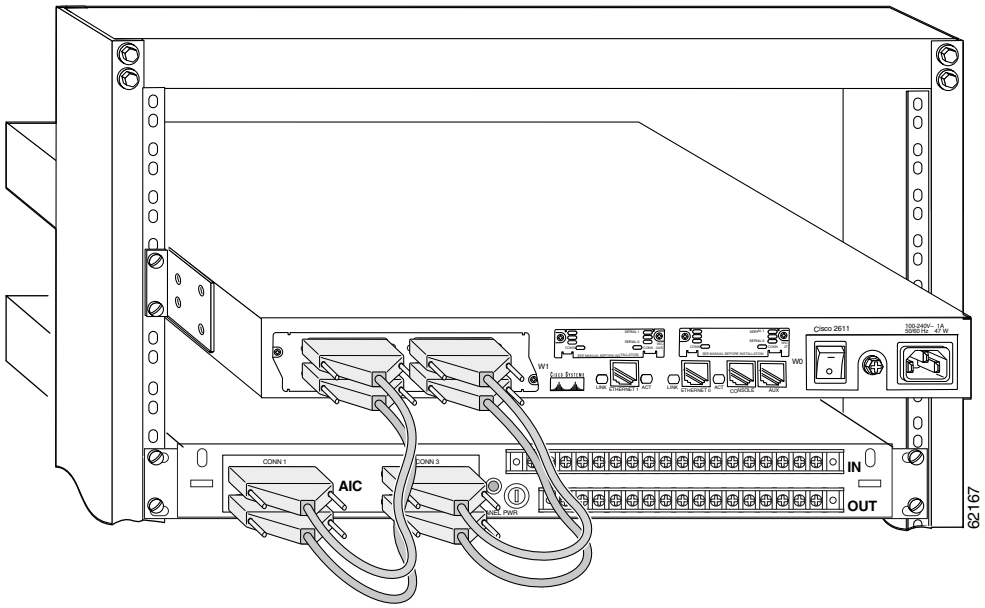


Figure 29-5 AIC Network Module Connected to AIC-2 Patch Panel

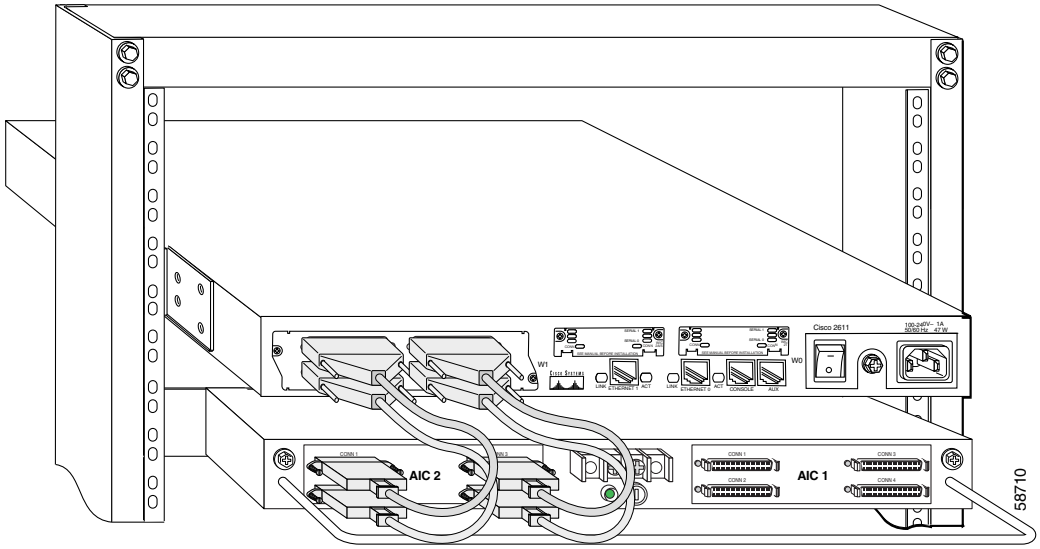


Figure 29-6 AIC-2 Patch Panel Connected to MDF

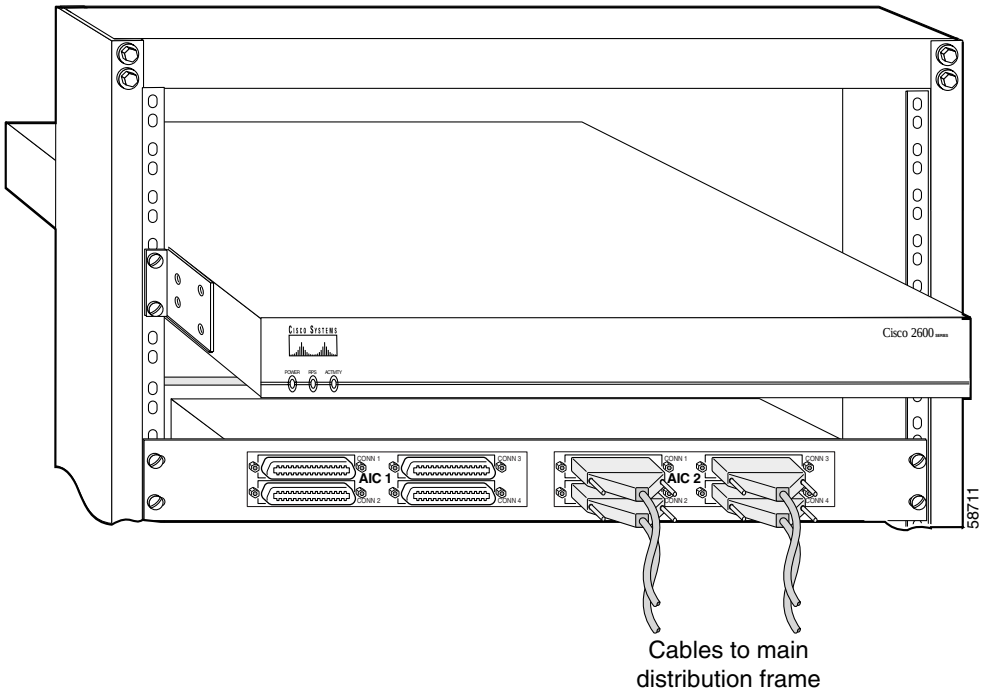


Table 29-1 AIC-1 Connector Pinouts

Telco Connector	Connector 1	Connector 2	Connector 3	Connector 4
1	Alarm Neg1	Alarm Neg 26	Alarm Neg 51	Control Common 1
26	Alarm Pos 1	Alarm Pos 26	Alarm Pos 51	Control N.O. 1
2	Alarm Neg 2	Alarm Neg 27	Alarm Neg 52	Control Common 2
27	Alarm Pos 2	Alarm Pos 27	Alarm Pos 52	Control N.O. 2
3	Alarm Neg 3	Alarm Neg 28	Alarm Neg 53	Control Common 3
28	Alarm Pos 3	Alarm Pos 28	Alarm Pos 53	Control N.O. 3
4	Alarm Neg 4	Alarm Neg 29	Alarm Neg 54	Control Common 4
29	Alarm Pos 4	Alarm Pos 29	Alarm Pos 54	Control N.O. 4
5	Alarm Neg 5	Alarm Neg 30	Alarm Neg 55	Control Common 5
30	Alarm Pos 5	Alarm Pos 30	Alarm Pos 55	Control N.O. 5
6	Alarm Neg 6	Alarm Neg 31	Alarm Neg 56	Control Common 6
31	Alarm Pos 6	Alarm Pos 31	Alarm Pos 56	Control N.O. 6
7	Alarm Neg 7	Alarm Neg 32	See Table 29-2	Control Common 7
32	Alarm Pos 7	Alarm Pos 32	See Table 29-2	Control N.O. 7
8	Alarm Neg 8	Alarm Neg 33	See Table 29-2	Control Common 8
33	Alarm Pos 8	Alarm Pos 33	See Table 29-2	Control N.O. 8
9	Alarm Neg 9	Alarm Neg 34	See Table 29-2	Control Common 9
34	Alarm Pos 9	Alarm Pos 34	See Table 29-2	Control N.O. 9
10	Alarm Neg 10	Alarm Neg 35	See Table 29-2	Control Common 10
35	Alarm Pos 10	Alarm Pos 35	See Table 29-2	Control N.O. 10
11	Alarm Neg 11	Alarm Neg 36	See Table 29-2	Control Common 11
36	Alarm Pos 11	Alarm Pos 36	See Table 29-2	Control N.O. 11
12	Alarm Neg 12	Alarm Neg 37	See Table 29-2	Control Common 12
37	Alarm Pos 12	Alarm Pos 37	See Table 29-2	Control N.O. 12
13	Alarm Neg 13	Alarm Neg 38	See Table 29-2	Control Common 13
38	Alarm Pos 13	Alarm Pos 38	See Table 29-2	Control N.O. 13
14	Alarm Neg 14	Alarm Neg 39	See Table 29-2	Control Common 14
39	Alarm Pos 14	Alarm Pos 39	See Table 29-2	Control N.O. 14
15	Alarm Neg 15	Alarm Neg 40	Not used	Control Common 15
40	Alarm Pos 15	Alarm Pos 40	Not used	Control N.O. 15
16	Alarm Neg 16	Alarm Neg 41	Not used	Control Common 16
41	Alarm Pos 16	Alarm Pos 41	Not used	Control N.O. 16
17	Alarm Neg 17	Alarm Neg 42	Not used	Not used
42	Alarm Pos 17	Alarm Pos 42	Not used	Not used
18	Alarm Neg 18	Alarm Neg 43	Not used	Not used
43	Alarm Pos 18	Alarm Pos 43	Not used	Not used

Table 29-1 AIC-1 Connector Pinouts (continued)

Telco Connector	Connector 1	Connector 2	Connector 3	Connector 4
19	Alarm Neg 19	Alarm Neg 44	Not used	Not used
44	Alarm Pos 19	Alarm Pos 44	Not used	Not used
20	Alarm Neg 20	Alarm Neg 45	Not used	Not used
45	Alarm Pos 20	Alarm Pos 45	Not used	Not used
21	Alarm Neg 21	Alarm Neg 46	Not used	Not used
46	Alarm Pos 21	Alarm Pos 46	Not used	Not used
22	Alarm Neg 22	Alarm Neg 47	Not used	Not used
47	Alarm Pos 22	Alarm Pos 47	Not used	Not used
23	Alarm Neg 23	Alarm Neg 48	Not used	Not used
48	Alarm Pos 23	Alarm Pos 48	Not used	Not used
24	Alarm Neg 24	Alarm Neg 49	Not used	Not used
49	Alarm Pos 24	Alarm Pos 49	Not used	Not used
25	Alarm Neg 25	Alarm Neg 50	Not used	Not used
50	Alarm Pos 25	Alarm Pos 50	Not used	Not used

Table 29-2 Voltage Monitor Connections on Connector 3 for the AIC-1 Patch Panel

Terminal Strip		Signal
1	RET	Alarm Pos 57
	BAT	Alarm Neg 57
2	RET	Alarm Pos 58
	BAT	Alarm Neg 58
3	RET	Alarm Pos 59
	BAT	Alarm Neg 59
4	RET	Alarm Pos 60
	BAT	Alarm Neg 60
5	RET	Alarm Pos 61
	BAT	Alarm Neg 61
6	RET	Alarm Pos 62
	BAT	Alarm Neg 62
7	RET	Alarm Pos 63
	BAT	Alarm Neg 63
8	RET	Alarm Pos 64
	BAT	Alarm Neg 64

Table 29-3 AIC-2 Connector Pinouts

Telco Connector	Connector 1	Connector 2	Connector 3	Connector 4
1	Alarm Neg1	Alarm Neg 26	Alarm Neg 51	Control Common 1
26	Alarm Pos 1	Alarm Pos 26	Alarm Pos 51	Control N.O. 1
2	Alarm Neg 2	Alarm Neg 27	Alarm Neg 52	Control Common 2
27	Alarm Pos 2	Alarm Pos 27	Alarm Pos 52	Control N.O. 2
3	Alarm Neg 3	Alarm Neg 28	Alarm Neg 53	Control Common 3
28	Alarm Pos 3	Alarm Pos 28	Alarm Pos 53	Control N.O. 3
4	Alarm Neg 4	Alarm Neg 29	Alarm Neg 54	Control Common 4
29	Alarm Pos 4	Alarm Pos 29	Alarm Pos 54	Control N.O. 4
5	Alarm Neg 5	Alarm Neg 30	Alarm Neg 55	Control Common 5
30	Alarm Pos 5	Alarm Pos 30	Alarm Pos 55	Control N.O. 5
6	Alarm Neg 6	Alarm Neg 31	Alarm Neg 56	Control Common 6
31	Alarm Pos 6	Alarm Pos 31	Alarm Pos 56	Control N.O. 6
7	Alarm Neg 7	Alarm Neg 32	Alarm Neg 57	Control Common 7
32	Alarm Pos 7	Alarm Pos 32	Alarm Pos 57	Control N.O. 7
8	Alarm Neg 8	Alarm Neg 33	Alarm Neg 58	Control Common 8
33	Alarm Pos 8	Alarm Pos 33	Alarm Pos 58	Control N.O. 8
9	Alarm Neg 9	Alarm Neg 34	Alarm Neg 59	Control Common 9
34	Alarm Pos 9	Alarm Pos 34	Alarm Pos 59	Control N.O. 9
10	Alarm Neg 10	Alarm Neg 35	Alarm Neg 60	Control Common 10
35	Alarm Pos 10	Alarm Pos 35	Alarm Pos 60	Control N.O. 10
11	Alarm Neg 11	Alarm Neg 36	Alarm Neg 61	Control Common 11
36	Alarm Pos 11	Alarm Pos 36	Alarm Pos 61	Control N.O. 11
12	Alarm Neg 12	Alarm Neg 37	Alarm Neg 62	Control Common 12
37	Alarm Pos 12	Alarm Pos 37	Alarm Pos 62	Control N.O. 12
13	Alarm Neg 13	Alarm Neg 38	Alarm Neg 63	Control Common 13
38	Alarm Pos 13	Alarm Pos 38	Alarm Pos 63	Control N.O. 13
14	Alarm Neg 14	Alarm Neg 39	Alarm Neg 64	Control Common 14
39	Alarm Pos 14	Alarm Pos 39	Alarm Pos 64	Control N.O. 14
15	Alarm Neg 15	Alarm Neg 40	Not used	Control Common 15
40	Alarm Pos 15	Alarm Pos 40	Not used	Control N.O. 15
16	Alarm Neg 16	Alarm Neg 41	Not used	Control Common 16
41	Alarm Pos 16	Alarm Pos 41	Not used	Control N.O. 16
17	Alarm Neg 17	Alarm Neg 42	Not used	Not used
42	Alarm Pos 17	Alarm Pos 42	Not used	Not used
18	Alarm Neg 18	Alarm Neg 43	Not used	Not used
43	Alarm Pos 18	Alarm Pos 43	Not used	Not used

Table 29-3 AIC-2 Connector Pinouts (continued)

Telco Connector	Connector 1	Connector 2	Connector 3	Connector 4
19	Alarm Neg 19	Alarm Neg 44	Not used	Not used
44	Alarm Pos 19	Alarm Pos 44	Not used	Not used
20	Alarm Neg 20	Alarm Neg 45	Not used	Not used
45	Alarm Pos 20	Alarm Pos 45	Not used	Not used
21	Alarm Neg 21	Alarm Neg 46	Not used	Not used
46	Alarm Pos 21	Alarm Pos 46	Not used	Not used
22	Alarm Neg 22	Alarm Neg 47	Not used	Not used
47	Alarm Pos 22	Alarm Pos 47	Not used	Not used
23	Alarm Neg 23	Alarm Neg 48	Not used	Not used
48	Alarm Pos 23	Alarm Pos 48	Not used	Not used
24	Alarm Neg 24	Alarm Neg 49	Not used	Not used
49	Alarm Pos 24	Alarm Pos 49	Not used	Not used
25	Alarm Neg 25	Alarm Neg 50	Not used	Not used
50	Alarm Pos 25	Alarm Pos 50	Not used	Not used

AIC Network Module LEDs

This section describes AIC network module LEDs. (See Figure 29-7.)

All network modules have an enable (EN) LED. This LED indicates that the module is receiving power from the router chassis.

The AIC network module also has a status (STAT) LED, which is a software-controlled bicolor (green and orange) LED. Both the EN and STAT LEDs turn on when the router is powered up, recycled, or power-cycled, or the AIC is hot-swapped. When the AIC starts to boot up, the STAT LED is initially turned off. It turns green when the software has initialized, has passed POST, and has established communication with IOS.

The STAT LED turns from green to orange when POST has failed or when the software encounters any other fatal fault in its firmware during normal operation.

Table 29-4 defines the state of the card with respect to the states of the LEDs.

Figure 29-7 AIC Network Module LEDs

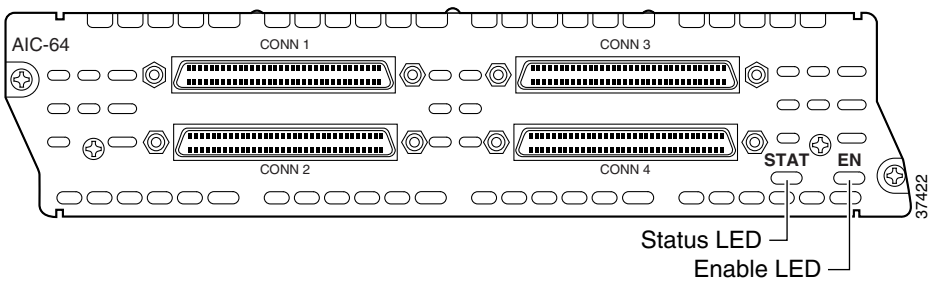


Table 29-4 AIC LED Description

	STAT LED		
EN LED	**Green**	**Orange**	**Description**
Off	Off	Off	No power to the AIC
On	Off	Off	Software initializing
On	On	Off	Normal operation
On	Off	On	Fault encountered

CHAPTER 30

Connecting AON Network Modules

This chapter describes the Cisco Application-Oriented Networking (AON) network modules for Cisco access routers, and contains the following sections:

Tip To determine whether your Cisco router supports a specific network module, see Table 1-6 on page 1-16.

Cisco AON Network Modules

The Cisco AON network modules provide application-level intelligence, improved message visibility and security, and reduced total cost of ownership by consolidating elements of network and application infrastructures.

Two models of Cisco AON network modules are available:

- NM-AON-K9= — See Figure 30-1 on page 30-2
- NME-AON-K9= — See Figure 30-2 on page 30-2

Both Cisco AON network modules (NM) and enhanced network modules (NME) ship from the factory with the following hardware preinstalled.

Model	Hard Disk	Memory
NM-AON-K9=	40 GB (PATA)	512 MB
NME-AON-K9=	40 GB (SATA)	1 GB

Figure 30-1 NM-AON-K9= Faceplate

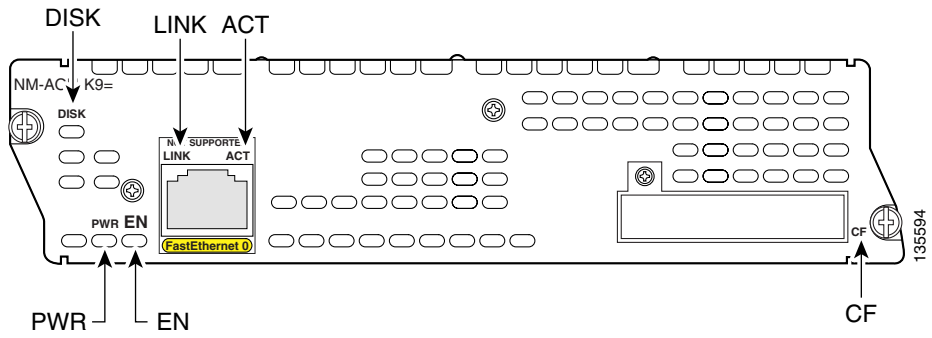
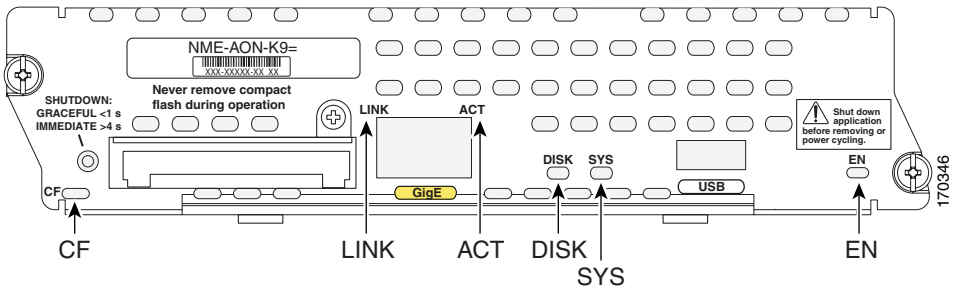


Figure 30-2 NME-AON-K9= Faceplate



DISK	Status of hard drive activity On—Active Off—Inactive
LINK	Status of Gigabit Ethernet link On—Link is enabled Off—Link is disabled
ACT	Status of Gigabit Ethernet activity On—Active Off—Inactive
PWR/SYS	Status of system shutdown **Note** Do not remove power without first shutting down the application. On—Application is stable. Off—System is shut down and ready for host power down Flashing—System shutdown is in progress

EN	Status of the network module On—Detected by the host Cisco IOS software and enabled Off—Disabled
CF	Status of the CompactFlash **Note** CompactFlash is not supported. Off—CompactFlash is not used Flashing—Application detected CompactFlash at boot up

Note The Cisco NM-AON-K9= network module does not support a Fast Ethernet port.

Shutting Down the NME-AON-K9=

Press the reset button on the network module faceplate for less than 2 seconds to perform a graceful shutdown of the network module before removing power from the router or before starting an online insertion and removal (OIR) sequence on the router. The application may take up to 2 minutes to fully shut down.

Caution If you press the shutdown button for *more than 4 seconds*, a nongraceful shutdown of the hard disk will occur and may cause file corruption on the network module's hard disk. After a nongraceful shutdown, the HD and SYS LEDs remain lit. Press the shutdown button for *less than 2 seconds* to gracefully reboot the network module.

Connecting AON Network Modules

To connect Cisco AON network modules and enhanced network modules to an external device, use a straight-through two-pair Category 5 unshielded twisted-pair (UTP) cable, and connect the RJ-45 Gigabit Ethernet port on the network module to a switch, hub, repeater, server, or other Gigabit Ethernet network device.

Warning **To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the NME-AON-K9 network module only to intra-building or unexposed wiring or cable. The intrabuilding cable must be shielded and the shield must be grounded at both ends. The intra-building port(s) of the equipment or subassembly must not be metallically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE, Issue 4) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring.**

Note RJ-45 cables are not available from Cisco Systems. These cables are widely available and must be Category 5 cables.

Establishing a Gigabit Ethernet Internal Connection

Use the Cisco High-Speed Intrachassis Module Interconnect (HIMI) feature to establish a Gigabit Ethernet internal logical connection between two enhanced network modules, or between an onboard small-form-factor pluggable (SFP) Gigabit Ethernet module and an enhanced network module on Cisco 3825 and Cisco 3845 routers.

Connections can be only established as follows:

- Between the Gigabit Ethernet port in an installed onboard SFP module on the Cisco 3825 and Cisco 3845 routers
- Between Gigabit Ethernet interfaces in network module slots 1 and 2 on the Cisco 3825 router
- Between Gigabit Ethernet interfaces in network module slots 2 and 4 on the Cisco 3845 router

Note The Cisco NM-AON-K9= network module does not support Gigabit Ethernet connections.

Note A module interconnection between the Gigabit Ethernet port on an SFP module and a network module slot or a network module-to-network module cross-connection is permitted at any given time, but both types of connections cannot exist at the same time.

Note Connections between the onboard Ethernet ports and network module slots are not supported.

For details about configuring HIMI connections, see the *Cisco High-Speed Intrachassis Module Interconnect (HIMI) Configuration Guide* on Cisco.com:

http://www.cisco.com/en/US/products/ps5855/prod_configuration_guide09186a008068ea83.html

Online Insertion and Removal of Cisco Network Modules

Some Cisco access routers allow you to replace network modules without switching off the router or affecting the operation of other interfaces. This feature is called online insertion and removal (OIR). OIR of a module provides uninterrupted operation to network users, maintains routing information, and ensures session preservation.

Caution Unlike other network modules, enhanced network modules use hard disks. Online removal of disks without proper shutdown can result in file system corruption and might render the disk unusable. The operating system on the network module must be shut down in an orderly fashion before the module is removed or powered down.

Caution Cisco routers support OIR with similar modules only. If you remove a module, install another module exactly like it in its place. If you remove a 2-slot module (along with any installed WAN or voice interface cards), install another module and card combination exactly like it.

For a description of informational and error messages that may appear on the console during this procedure, see the hardware installation guide for your router.

To perform online removal of a network module and insertion of a replacement, follow these steps, with the router in privileged EXEC mode:

Step 1 Initiate a network module session using the following command:

```
Router# service-module integrated-service-engine slot/unit session

Trying 10.10.10.1, 2065 ... Open

Press RETURN to get started!

Router> enable
Router#
```

Step 2 Save the running configuration of the network module using the following command from the **router #** prompt:

```
Router# copy running-config tftp tftp-server-address filename
```

Step 3 Exit the network module session by pressing **Control-Shift-6**, followed by **x**.

Step 4 On the router, clear the integrated-service-engine console session using the following command:

```
Router# service-module integrated-service-engine slot/unit session clear
```

Step 5 Perform a graceful shutdown of the network module disk drive by using the following command:

```
Router# service-module integrated-service-engine slot/unit shutdown
```

Step 6 Shut down the network module interface:

```
Router (config)# interface integrated-service-engine slot/unit
Router (config-if)# shutdown
Router (config-if)# exit
```

Step 7 Unplug all network interface cables from the network module.

Step 8 Loosen the two captive screws holding the network module in the chassis slot.

Step 9 Slide the network module out of the slot.

Step 10 Align the replacement network module with the guides in the chassis slot, and slide it gently into the slot.

Note If the router is not fully configured with network modules, make sure that blank panels fill the unoccupied chassis slots to provide proper airflow.

Step 11 Push the module into place until you feel its edge connector mate securely with the connector on the backplane.

Step 12 Reconnect the network interface cables previously removed in Step 7.

Step 13 Check that the network module LEDs are on and that the power (PWR) and enable (EN) LEDs on the front panel are also on. This inspection ensures that connections are secure and that the new unit is operational.

Step 14 Initiate a network module session with the following command:

```
Router# service-module integrated-service-engine slot/unit session

Trying 10.10.10.1, 2129 ... Open

ISE-network module now available
```

```
Press RETURN to get started!

Router> enable
Router#
```

Step 15 Restore the network module running configuration by using the following command from the service module prompt:

```
Router# copy tftp running-config tftp-server-address filename
```

Step 16 Exit the network module session by pressing **Control-Shift-6**, followed by **x**.

Step 17 On the router, clear the network module session by using the following command:

```
Router# service-module integrated-service-engine slot/unit session clear
```

Related Documents

For additional information, refer to the following documents and resources.

Related Topic	Document Title
Cisco Application-Oriented Networking software installation and administration, and user guides	*Cisco Application-Oriented Networking Installation and Administration Guide* http://www.cisco.com/univercd/cc/td/doc/product/aon/aonadmin.pdf *Cisco Application-Oriented Networking Development Studio User Guide* http://www.cisco.com/univercd/cc/td/doc/product/aon/ads/index.htm
Cisco IOS software website and reference documentation	*Cisco IOS Software* http://www.cisco.com/en/US/products/sw/iosswrel/tsd_products_support_category_home.html
Technical documentation, including feedback and assistance	*What's New in Cisco Product Documentation* (including monthly listings of new and revised documents) at http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

CHAPTER 31

Connecting Cisco Wireless LAN Controller Modules

This chapter describes how to connect Cisco wireless LAN (WLAN) controller modules (WLCM) and contains the following sections:

The Cisco wireless LAN (WLAN) controller module is designed to provide small and medium-sized businesses (SMBs) and enterprise branch office customers 802.11 wireless networking solutions for Cisco 2800 and Cisco 3800 series integrated services routers (ISRs) and Cisco 3700 series routers.

Note The Cisco 2801 integrated services router does not support the Cisco WLAN controller module.

Tip For information about which Cisco routers support the Cisco WLAN controller module, see the "Platform Support for Cisco Network Modules" section on page 1-15.

Cisco WLAN controller modules ship with and boot from an installed 256-MB CompactFlash (CF) memory card. The CompactFlash memory card contains the boot loader, Linux kernel, Cisco WLAN controller module and access points executable file, and Cisco WLAN controller module configuration.

Note The wireless LAN controller module is supported only in network module slots. It is *not* supported in EVM slots available in the Cisco 2821 and Cisco 2851 integrated services routers.

Note Before installing, configuring, or upgrading the Cisco WLAN controller module, see the *Cisco Wireless LAN Solution Product Guide* at the following URL:

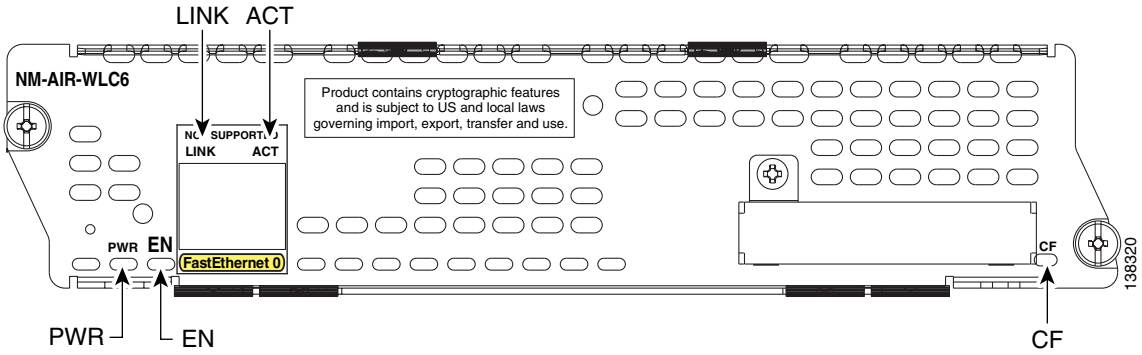
http://www.cisco.com/en/US/products/ps6305/products_configuration_guide_book09186a00804f988b.html

Cisco Wireless LAN Controller Modules

Figure 31-1 shows the faceplate of the Cisco WLAN controller module.

Note The 256-MB CompactFlash memory card in the Cisco WLAN controller module is not field-replaceable.

Figure 31-1 Cisco Wireless LAN Controller Module Faceplate



Note The external Fast Ethernet port on the faceplate of the Cisco WLAN controller module is not supported.

Cisco Wireless LAN Controller Module LEDs

Table 31-1 lists the Cisco wireless LAN controller module LEDs and their meanings.

Table 31-1 Cisco Wireless LAN Controller Module LED Meanings

LED	Meaning
CF	The CompactFlash memory card is active.
EN	The module has passed self-test and is available to the router.
PWR	Power is available to the controller module.

Connecting Cisco Wireless LAN Controller Modules to the Network

The Cisco wireless LAN controller module connects to the network through internal connections within the router and requires no additional cables for network connectivity.

Online Insertion and Removal with a Cisco Wireless LAN Controller Module

The Cisco integrated services routers (ISRs) allow you to replace network modules without switching off the router or affecting the operation of other interfaces. This feature is called online insertion and removal (OIR). OIR of network modules provides uninterrupted operation to network users, maintains routing information, and ensures session preservation.

Note OIR of the controller module is supported only on the Cisco 3745 router and the Cisco 3845 ISR.

Tip For information about module slot locations and numbering on Cisco routers, see "Network Module Slot Locations and Numbering on Cisco Access Routers" section on page 1-3.

For a description of informational and error messages that may appear on the console during this procedure, see the hardware installation guide for your type of router.

Saving the Configuration File

This configuration assumes a configuration file already exists on the Cisco WLAN controller module CompactFlash memory card. To save the configuration file, follow these steps with the router in privileged EXEC mode.

Step 1 Initiate a WLAN controller module console access session using the following command:

```
Router# service-module wlan-controller 1/0 session
Trying 192.0.2.254, 2066 ... Open
```

Step 2 Set the TFTP server IP address from the WLAN controller module console access session:

```
(WLAN-Controller) > transfer upload serverip 192.0.2.24
```

Step 3 Set the datatype configuration using the following command:

```
(WLAN-Controller) > transfer upload datatype configuration
```

Step 4 Set the running configuration file using the following command:

```
(WLAN-Controller) > transfer upload filename <config-running.bin>
```

Step 5 Start the TFTP transfer using the following command from the WLAN-Controller prompt:

```
(WLAN-Controller) > transfer upload start

Mode..................................................... TFTP
TFTP Server IP........................................... 192.0.2.24
TFTP Path................................................ /
TFTP Filename............................................ config.bin
Data Type................................................ Config File
Encryption............................................... Disabled

*********************************************
***  WARNING: Config File Encryption Disabled  ***
*********************************************
```

```
Are you sure you want to start? (y/n) y

Tftp Config transfer starting.

File transfer operation completed successfully.

(WLAN-Controller) >
```

Step 6 Exit the WLAN controller module console access session by pressing **Control-Shift-6**, followed by **x**.

Step 7 Disconnect the WLAN controller interface connection on the router by using the **disconnect** command and confirming the action by pressing **Enter**:

```
Router# disconnect
Closing connection to 192.0.2.254 [confirm]
Router#
```

Step 8 On the router, clear the WLAN controller access session using the following command:

```
Router# service-module wlan-controller 1/0 session clear

[confirm]
 [OK]
Router#
[Resuming connection 1 to 192.0.2.254 ... ]

[Connection to 192.0.2.254 closed by foreign host]
Router#
```

Step 9 Shut down the content engine interface:

```
Router (config)# interface wlan-controller 1/0
Router (config-if)# shutdown
Router (config-if)# exit
```

Replacing the Cisco WLAN Controller Module

Follow these steps to remove and replace the Cisco WLAN controller module.

Step 1 Loosen the two captive screws holding the WLAN controller module in the chassis slot.

Step 2 Slide the WLAN controller module out of the slot.

Step 3 Align the replacement WLAN controller module with the guides in the chassis slot, and slide it gently into the slot.

Step 4 Push the module into place until you feel its edge connector mate securely with the connector on the backplane.

Step 5 Check that the WLAN controller module LEDs are on and that the power and enable LEDs on the front panel also are on. This inspection ensures that connections are secure and that the new unit is operational.

Note Because the WLAN controller module needs to initialize itself, the EN (Enable) LED takes at least 10 seconds to come on after the PWR LED.

Configuring the Replacement WLAN Controller Module

Follow these steps to configure the replacement Cisco WLAN controller module.

Step 1 Reset the WLAN controller module:

```
Router# service-module wlan-controller 1/0 reset

Use reset only to recover from shutdown or failed state
Warning: May lose data on the hard disc!
Do you want to reset?[confirm]
Trying to reset Service Module wlan-controller1/0.
```

Step 2 Turn on the WLAN controller interface, if it is necessary for further configuration:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface wlan-controller 1/0
Router(config-if)# ip address 192.0.2.254 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# end
Router#
Router#
```

Step 3 Initiate a WLAN controller module console access session and access the bootloader prompt using the following command:

Note The following typical example assumes there is already a configuration image available on the WLAN controller module CompactFlash memory card. To configure a WLAN controller module without an available configuration image, see the *Cisco Wireless LAN Solution Product Guide* at the following URL:

http://www.cisco.com/en/US/products/ps6305/products_configuration_guide_book09186a00804f988b.html

```
Router# service-module wlan-controller slot/unit session
Trying 192.0.2.254, 2066 ... Open

    Cisco Bootloader (Version 3.2.10.0)

Booting Primary Image...
Press <ESC> now for additional boot options...
Detecting hardware . . . .

Cisco is a trademark of Cisco Systems, Inc.
Software Copyright Cisco Systems, Inc. All rights reserved.

Cisco AireOS Version 3.2.10.0
Initializing OS Services: ok
Initializing Serial Services: ok
Initializing Network Services: ok
...
   Web Server: ok
   CLI: ok
   Secure Web: ok

(WLAN-Controller)

Enter User Name (or 'Recover-Config' to reset configuration to factory defaults)
```

Step 4 Enter the User ID and password at the WLAN controller prompt:

```
User: admin
Password: *****
(WLAN-Controller) >
```

Step 5 Set the TFTP server IP address from the WLAN controller module console access session:

```
(WLAN-Controller) > transfer download serverip 192.0.2.24
```

Step 6 Set the datatype configuration using the following command:

```
(WLAN-Controller) > transfer download datatype configuration
```

Step 7 Set the running configuration file using the following command:

```
(WLAN-Controller) > transfer download filename <config-running.bin>
```

Step 8 Start the TFTP transfer using the following command:

```
(WLAN-Controller) > transfer download start

Mode............................................ TFTP
TFTP Server IP.................................. 192.0.2.24
TFTP Path....................................... /
TFTP Filename................................... config-running.bin
Data Type....................................... Config File
Encryption...................................... Disabled

************************************************
***  WARNING: Config File Encryption Disabled  ***
************************************************

Are you sure you want to start? (y/n) y

Tftp Config transfer starting.

File transfer operation completed successfully.

(WLAN-Controller) >
```

Note After the successful file transfer, the WLAN controller module automatically reboots.

Related Documents

For additional information, see the following documents.

Tip For information on obtaining documentation, see the "Obtaining Documentation" section on page viii. For information on obtaining technical assistance, see the "Obtaining Technical Assistance" section on page xi.

Hardware Documentation

For general information on installing and removing Cisco modules, see the *Cisco Network Modules Hardware Installation Guide* (this document).

Cisco IOS Software Documentation

For a description of the Cisco IOS features supported on Cisco wireless LAN controller modules, see the "Cisco IOS Software Documentation" section on page 1-31.

Cisco Wireless LAN Controller Module Documentation

For additional information about WLAN support on the Cisco wireless LAN controller module, see the wireless support resources documentation at the following URL:

http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

CHAPTER 32

Connecting Cisco Wireless LAN Controller Enhanced Network Modules

This chapter describes how to connect Cisco wireless LAN (WLAN) controller enhanced network modules (WLCM) and contains the following sections:

Cisco Wireless LAN Controller Network Modules

The Cisco wireless LAN (WLAN) controller network module is designed to provide 802.11 wireless networking solutions to small- and medium-sized businesses (SMBs) and enterprise branch office customers.

Two models of Cisco WLAN controller network module are available:

- NME-AIR-WLC8-K9— See Figure 32-1 on page 32-2
- NME-AIR-WLC12-K9— See Figure 32-1 on page 32-2

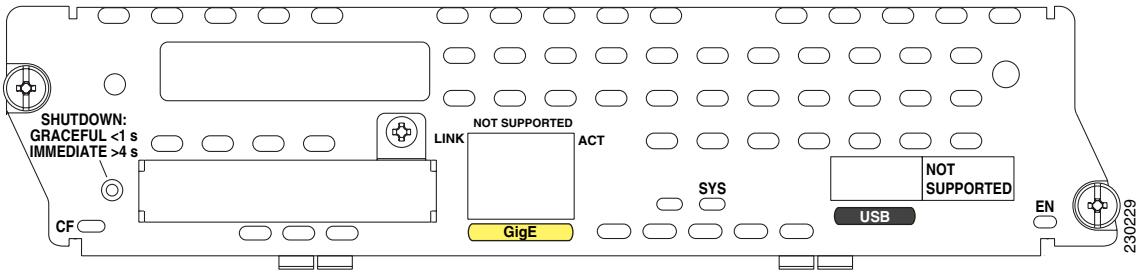
For information about the Cisco Wireless LAN controller module NM-AIR-WLC6 solution, see the *Cisco Network Modules Hardware Installation Guide* at the following URL:

http://www.cisco.com/en/US/products/hw/modules/ps2797/products_installation_guide_chapter09186a008078984f.html

Both models of Cisco WLAN controller enhanced network modules (NMEs) ship from the factory with the following hardware preinstalled.

Model	Hard Disk	Memory
NME-AIR-WLC8-K9=	N/A	256 MB
NME-AIR-WLC12-K9=	N/A	256 MB

Figure 32-1 Cisco WLAN Controller Network Module Faceplate



LINK	Status of Gigabit Ethernet link On—Link is enabled. Off—Link is disabled. **Note** This interface is not supported in this Cisco IOS software release.
ACT	Status of Gigabit Ethernet activity On—Active. Off—Inactive.
PWR/SYS	Status of system shutdown ⚠ **Caution** Do not remove power without first shutting down the application. On—Application is stable. Off—System is shut down and ready for host power down. Flashing—System shutdown is in progress.
EN	Status of the network module On—Detected by the host Cisco IOS software and enabled. Off—Disabled.
CF	Status of the CompactFlash Off—CompactFlash is not used. Flashing—Application detected CompactFlash at bootup.

Shutting Down the WLAN Controller

Insert a narrow pin into the shutdown opening on the faceplate, and press the button for *less than 2 seconds* to perform a graceful shutdown of the hard disk before removing power from the router or before starting an online insertion and removal (OIR) sequence on the router. The application may take up to 2 minutes to fully shut down.

Caution If you press the shutdown button for *more than 2 seconds*, an immediate shutdown of the hard disk will occur and may cause file corruption on the network module's hard disk. After an immediate shutdown, the HD and SYS LEDs remain lighted. Press the shutdown button for *less than 2 seconds* to gracefully reboot the network module.

Establishing a Gigabit Ethernet Internal Connection

The Cisco WLAN controller-enhanced network module lets you establish an internal Gigabit Ethernet connection between an onboard small-form-factor pluggable (SFP) Gigabit Ethernet module and a WLAN controller-enhanced network module installed in Cisco 3700 series routers, Cisco 2800 Integrated Services Routers (ISR), or Cisco 3800 ISRs.

Note The Cisco 2801 Integrated Services Router does not support the Cisco WLAN controller network module.

Internal connections must be established as follows:

- Cisco 2811 router—Install the WLAN controller network module in slot 1
- Cisco 2821 router—Install the WLAN controller network module in slot 1
- Cisco 2851 router—Install the WLAN controller network module in slot 1
- Cisco 3725 router—Install the WLAN controller network module in slot 1
- Cisco 3745 router—Install the WLAN controller network module in any of slots 1 through 4
- Cisco 3825 router—Install the WLAN controller network module in slots 1 and 2
- Cisco 3845 router—Install the WLAN controller network module in any of slots 1 through 4

Online Insertion and Removal of Cisco Network Modules

Some Cisco access routers allow you to replace network modules without switching off the router or affecting the operation of other interfaces. This feature is called *online insertion and removal* (OIR). OIR of a module provides uninterrupted operation to network users, maintains routing information, and ensures session preservation.

Caution Cisco routers support OIR with similar modules only. If you remove a module, install another module exactly like it in its place. If you remove a 2-slot module (along with any installed WAN or voice interface cards), install another module and card combination exactly like it.

For a description of informational and error messages that may appear on the console during this procedure, see the hardware installation guide for your router.

To perform online removal of a network module and insertion of a replacement, follow these steps, with the router in privileged EXEC mode:

Step 1 Initiate a network module session by using the following command:

```
Press RETURN to get started!

Router> enable
Router# service-module integrated-service-engine 1/0 session
Trying 10.10.10.1, 2065 ... Open
User:
```

Step 2 Exit the network module session by pressing **Control-Shift-6**, and then pressing **x**.

Step 3 Save the running configuration of the network module by using the following command from the router # prompt:

```
Router# copy running-config tftp tftp-server-address filename
```

Step 4 On the router, clear the integrated-service-engine console session by using the following command:

```
Router# service-module integrated-service-engine slot/unit session clear
```

Step 5 Perform a graceful shutdown of the network module disk drive by using the following command:

```
Router# service-module integrated-service-engine slot/unit shutdown
```

Step 6 Shut down the network module interface:

```
Router (config)# interface integrated-service-engine slot/unit
Router (config-if)# shutdown
Router (config-if)# exit
```

Step 7 Loosen the two captive screws holding the network module in the chassis slot.

Step 8 Slide the network module out of the slot.

Step 9 Align the replacement network module with the guides in the chassis slot, and slide it gently into the slot.

Note If the router is not fully configured with network modules, make sure that blank panels fill the unoccupied chassis slots to provide proper airflow.

Step 10 Push the module into place until you feel its edge connector mate securely with the connector on the backplane.

Step 11 Check that the network module LEDs are on and that the power (PWR) and enable (EN) LEDs on the front panel are also on. This inspection ensures that connections are secure and that the new unit is operational.

Step 12 Initiate a network module session by using the following command:

```
Router# service-module Integrated-Service-Engine 2/0 session

Trying 21.21.21.1, 2130 ... Open

(Cisco Controller) >
```

Step 13 Restore the network module running configuration by using the following command from the service module prompt:

```
Router# copy tftp running-config tftp-server-address filename
```

Step 14 On the router, clear the network module session by using the following command:

```
Router# service-module integrated-service-engine slot/unit session clear
```

Related Documents

For additional information, refer to the following documents and resources.

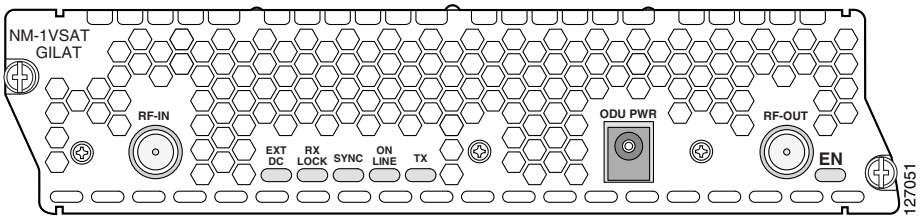
Related Topic	Document Title
Hardware installation instructions for the Cisco Wireless LAN controller module NM-AIR-WLC6 solution	*Connecting Cisco Wireless LAN Controller Modules* http://www.cisco.com/en/US/products/sw/iosswrel/tsd_products_support_category_home.html
Cisco IOS software website and reference documentation	*Cisco IOS Software* http://www.cisco.com/en/US/products/sw/iosswrel/tsd_products_support_category_home.html
Technical documentation, including feedback and assistance	*What's New in Cisco Product Documentation* (including monthly listings of new and revised documents) at http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

CHAPTER 33

Connecting Cisco IP VSAT Satellite WAN Network Modules

This document provides hardware information about the NM-1VSAT-GILAT network module, which provides Cisco modular access routers with two-way satellite WAN connectivity in Gilat SkyEdge–compatible satellite communications networks. The NM-1VSAT-GILAT network module functions as the indoor unit (IDU) of a very small aperture terminal (VSAT), or earthbound station of a satellite communications network. A "very small" dish antenna is called the outdoor unit (ODU) of a VSAT. As the IDU, the NM-1VSAT-GILAT network module serves as the interface between the ODU and the VSAT LAN. The ODU receives and sends signals to a satellite, and the satellite sends and receives signals from an earthbound central hub, which controls the entire operation of the satellite network. Figure 33-1 shows the NM-1VSAT-GILAT network module faceplate.

Figure 33-1 Cisco IP VSAT Satellite WAN Network Module (NM-1VSAT-GILAT) Faceplate



Contents

Prerequisites for the NM-1VSAT-GILAT Network Module

- You need a router that supports the NM-1VSAT-GILAT network module. For a list of supported platforms, see the *Cisco IP VSAT Satellite WAN Network Module (NM-1VSAT-GILAT) Data Sheet*.
- The NM-1VSAT-GILAT network module requires an associated central hub, which monitors and controls the satellite network. Therefore, you must take one of the following actions:
  - Subscribe to service from a Gilat SkyEdge satellite service provider.
  - Purchase your own Gilat SkyEdge hub equipment.
- The NM-1VSAT-GILAT network module requires a "Sat Kit" provided by a Gilat SkyEdge satellite service provider. The Sat Kit includes the dish antenna equipment and an external power supply.

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

Note For software-related prerequisites, see the *Cisco IP VSAT Satellite WAN Network Module (NM-1VSAT-GILAT)* Cisco IOS feature module.

Restrictions for the NM-1VSAT-GILAT Network Module

- The NM-1VSAT-GILAT network module is supported only in Gilat SkyEdge–compatible satellite communications networks. For more information, go to http://www.gilat.com/.
- One-way satellite connectivity is currently not supported.
- The NM-1VSAT-GILAT network module is designed for Ku-band and C-band satellite networks using the Gilat SkyEdge Frequency and Time Division Multiple Access (FTDMA) technology. The NM-1VSAT-GILAT network module is *not* compatible with these items:
  - Other frequency bands, such as Ka-band
  - Other satellite TDMA systems, including Digital Video Broadcasting–Return Channel by Satellite (DVB-RCS), and Data Over Cable Service Interface Specification (DOCSIS)
  - Other media access methods, such as Single Channel Per Carrier (SCPC)
- The following hardware tasks are not described in this document and must be performed by a Gilat SkyEdge–certified installer:
  - Installing and aligning the dish antenna
  - Running cables from the ODU to the IDU area
  - Connecting two NM-1VSAT-GILAT network modules to one ODU for Hot Standby Router Protocol (HSRP) redundancy

- To avoid damaging the NM-1VSAT-GILAT network module, disconnect the power supply from the ODU PWR connector on the NM-1VSAT-GILAT network module *before* you attempt any of the following actions:
  - Connecting a cable to the RF-IN or RF-OUT connector
  - Disconnecting a cable from the RF-IN or RF-OUT connector
  - Inserting the NM-1VSAT-GILAT network module into the router chassis
  - Removing the NM-1VSAT-GILAT network module from the router chassis
- After completing the hardware installation, moving the router with the installed NM-1VSAT-GILAT network module may require longer radio frequency (RF) cables. Depending on the ODU type and the additional length required for the cables, you may need a technician to install line amplifiers. Contact your satellite service provider if you plan to extend your cables by more than 35 feet (11 m).

Note For software-related restrictions, see the *Cisco IP VSAT Satellite WAN Network Module (NM-1VSAT-GILAT)* Cisco IOS feature module.

Information About the NM-1VSAT-GILAT Network Module

Before performing the tasks in this document, you should understand the following concepts:

- General Satellite Network Components, page 33-3
- NM-1VSAT-GILAT Network Module Connectors, page 33-7
- Outbound and Inbound Directions in a Satellite Communications Network, page 33-7
- NM-1VSAT-GILAT Network Module LEDs, page 33-7

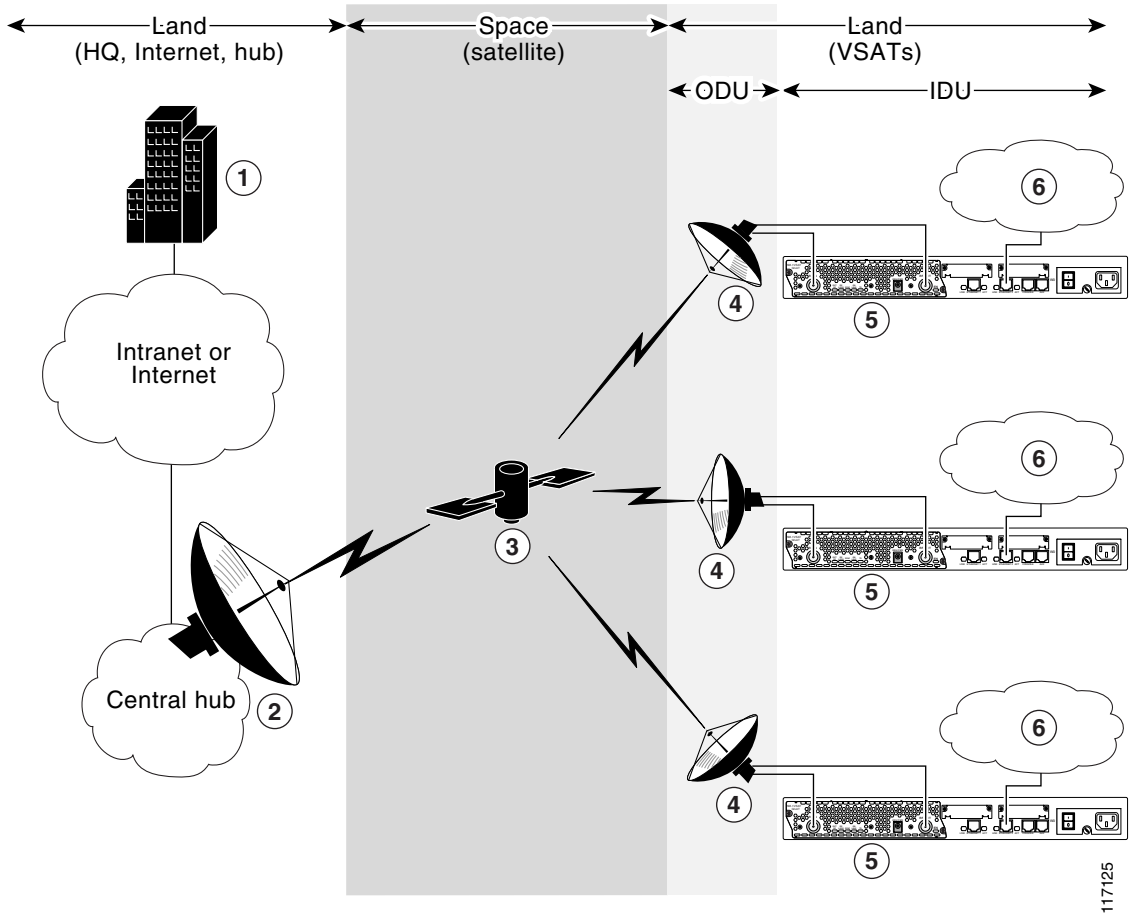
Note For NM-1VSAT-GILAT network module features and benefits, supported hardware and software, and other product information, see the *Cisco IP VSAT Satellite WAN Network Module (NM-1VSAT-GILAT) Data Sheet*.

General Satellite Network Components

Figure 33-2 shows a satellite communications network that includes NM-1VSAT-GILAT network modules.

Note Not shown in Figure 33-2 are the terrestrial WAN connections that are also commonly used to connect VSAT routers to the Internet or an intranet. A terrestrial WAN connection can be used to back up a satellite link or can serve as a primary link that is backed up by a satellite link.

Figure 33-2 Satellite Communications Network Using the NM-1VSAT-GILAT Network Module



1	Corporate headquarters/campus	**4**	Dish antenna (ODU[1]) at VSAT[2]
2	Dish antenna at hub	**5**	NM-1VSAT-GILAT network module at VSAT
3	Satellite in space	**6**	Local network at VSAT; for example, a branch office network connected to an Ethernet port on the router

1. ODU = outdoor unit
2. VSAT = very small aperture terminal

At a high level, the many components of an enterprise satellite communications network can be divided into three categories:

- Satellite
- Hub
- VSATs

Satellite

Placed in orbit around the earth, a satellite is a specialized repeater that receives radio-frequency signals from earth stations and retransmits them to other earth stations. The satellite also amplifies the signals and switches the frequencies between the uplink and the downlink carriers. Gilat SkyEdge systems use geostationary satellites with a fixed satellite-to-earth delay of about 250 ms.

Hub

The central hub—sometimes referred to as the "master earth station" but most often simply called the "hub"—contains many components, including:

- Large dish antenna (15 to 36 feet [4.5 to 11 m] in diameter)
- Satellite network management system (NMS) and provisioning stations, from which a network operator can monitor and control all components of the enterprise satellite communications network.
- Baseband equipment that handles satellite access, routing between the hub and remote earth stations, dial backup, quality of service (QoS), TCP acceleration, and HTTP acceleration.
- Optional components: web caches, MPEG transport coder/decoder, application server farms, and audio/video broadcast programming devices.

Note Throughout this document, the "hub" refers specifically to a Gilat SkyEdge hub.

VSATs

A very small aperture terminal (VSAT) is an earth station that can be divided into two areas:

- Indoor unit (IDU), which generally serves to connect the local network to the hub through the satellite link. The IDU components vary, depending on the functions required, but the components typically include these items:
  - Integrated receiver decoder (IRD) for the tuning
  - Demodulation and decoding of L-band or other type of intermediate frequency (IF) passed from the dish
  - End-user input/output
- Outdoor unit (ODU), which includes a "very small" dish antenna (2 to 6 feet [0.5 to 2 m] in diameter) and its components, shown in Figure 33-3. The ODU is typically mounted on a building roof or outer wall, or placed on the ground.

The NM-1VSAT-GILAT network module functions as the IDU of a VSAT and is connected to the ODU through coaxial cables. A power supply is connected to the NM-1VSAT-GILAT network module to provide power over the coaxial cables to the ODU.

Note The NM-1VSAT-GILAT network module supports only the ODU equipment and power supply that comes in the "Sat Kit" provided by a Gilat SkyEdge satellite service provider.

Figure 33-3 ODU Components

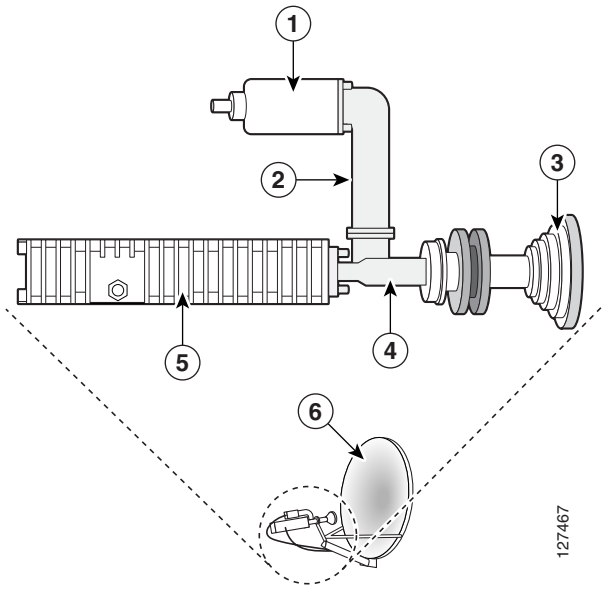


Figure Callout	ODU Component	Function
1	Low noise block converter (LNB)	Amplifies and converts high-frequency satellite signals into lower-frequency signals.
2	Transmit reject filter	Filters out transmitted signals so that only signals received from the satellite enter the LNB.
3	Feed horn	Captures signals from and transmits energy to the reflector.
4	Orthomode transducer (OMT)	Separates transmitted signals from received signals, which have different polarization and frequency.
5	Solid state block converter and power amplifier (SSPA)	Amplifies and converts the low-frequency signals from the IDU to high-frequency signals for transmission across the satellite link.
6	Reflector	Concave dish surface which focuses the energy received from the satellite to the feed horn and which transfers the energy transmitted by the feed horn to the satellite.

NM-1VSAT-GILAT Network Module Connectors

Table 33-1 lists the physical connectors that appear on the NM-1VSAT-GILAT network module faceplate.

Table 33-1 NM-1VSAT-GILAT Network Module Connectors

Connector	Type	Connects To
RF-IN	75-ohm female F connector	LNB on the dish antenna
RF-OUT	75-ohm female F connector	SSPA on the dish antenna
ODU PWR	2-mm DC jack	External 24 V-DC power supply

Outbound and Inbound Directions in a Satellite Communications Network

The *outbound* direction applies to signals transmitted from the hub to the VSAT. Within a VSAT network, the outbound direction applies to RF communication from the dish antenna (ODU) to the NM-1VSAT-GILAT network module (IDU). From the VSAT perspective, the outbound direction is the *receive* path. Gilat SkyEdge outbound signals include user data and timing data that are compatible with the Digital Video Broadcasting–Satellite (DVB-S) standard.

The *inbound* direction applies to signals transmitted from the VSAT to the hub. Within a VSAT network, the inbound direction applies to RF communication from the NM-1VSAT-GILAT network module (IDU) to the dish antenna (ODU). From the VSAT perspective, the inbound direction is the *transmit* path. Inbound signals include user data and retransmission requests.

NM-1VSAT-GILAT Network Module LEDs

The Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT) has six LEDs, shown in Figure 33-4 and described in Table 33-2.

Figure 33-4 NM-1VSAT-GILAT Network Module LEDs

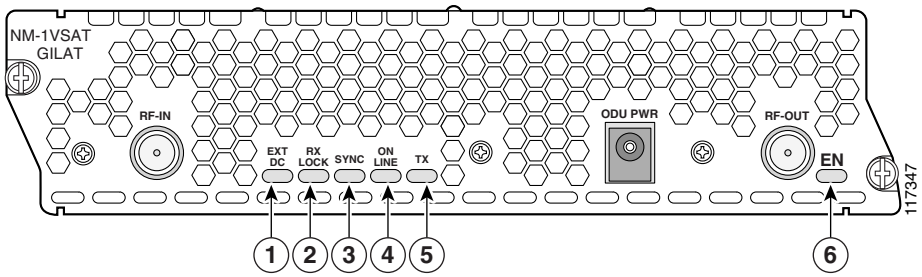


Table 33-2 NM-1VSAT-GILAT Network Module LED Descriptions

Figure Ref.	LED	State	Meaning	Possible Causes and Corrective Actions
1	EXT DC	Blinking	ODU[1] power DC level is correct, and the network module VSAT[2] software is running.	Normal indication. No action required.
		Steady on	ODU power supply is connected properly, but the network module VSAT software is not running.	Wait until the VSAT software completes the boot process.
		Off	ODU power supply is not connected or is outside the specified DC range.	Check ODU power supply connections. See the "Connecting the NM-1VSAT-GILAT Network Module to the External Power Supply" section on page 33-12.
2	RX LOCK	On	DVB[3] (outbound[4]) receiver is locked.	Normal indication. No action required.
		Off	NM-1VSAT-GILAT network module does not see or recognize the DVB carrier signal from the hub.	The VSAT parameters are configured incorrectly. See the *Cisco IP VSAT Satellite WAN Network Module (NM-1VSAT-GILAT)* Cisco IOS feature module. The network module is not properly connected to the LNB.[5] Check the RF[6] cables or contact your satellite service provider. The dish antenna is misaligned. Contact your satellite service provider. There is a hub failure, or the hub is configured incorrectly. Contact your satellite service provider.
3	SYNC	On	NM-1VSAT-GILAT network module is synchronized with the hub timing.	Normal indication. No action required.
		Off	NM-1VSAT-GILAT network module is not synchronized with the hub timing.	If the RX LOCK LED is also off, then see the corrective actions for RX LOCK. If the RX LOCK LED is on while the SYNC LED is off, then the following apply: • The VSAT parameters are configured incorrectly. See the *Cisco IP VSAT Satellite WAN Network Module (NM-1VSAT-GILAT)* Cisco IOS feature module. • There is a hub failure, or the hub is configured incorrectly. Contact your satellite service provider.

Table 33-2 NM-1VSAT-GILAT Network Module LED Descriptions (continued)

Figure Ref.	LED	State	Meaning	Possible Causes and Corrective Actions
4	ON LINE	On	IP connectivity to the hub is fully established.	Normal indication. No action required.
		Off	IP connectivity to the hub was unsuccessful.	If the SYNC LED is also off, then see the corrective actions for SYNC. If the SYNC LED is on while the ON LINE LED is off, then the following apply: • There is a problem somewhere in the return path from the network module to the hub. Check the cabling between the RF-OUT connector and the SSPA.[7] • The SSPA may not be working. Contact your satellite service provider. • The dish antenna is misaligned. Contact your satellite service provider. • There is a hub failure, or the hub is configured incorrectly. Contact your satellite service provider.
5	TX	Flickering	Inbound[8] transmission is in progress.	Normal indication. No action required.
		Off	No inbound transmission is in progress.	If you are concerned about the TX LED being off, then try to ping the hub or another destination on the other side of the satellite link. If the TX LED does not flicker during the ping, then the network module is not attempting to send data to the hub. • Wait until the VSAT software completes the boot process. • Verify that your Cisco IOS software configuration is correct. See the *Cisco IP VSAT Satellite WAN Network Module (NM-1VSAT-GILAT)* Cisco IOS feature module. • The VSAT software has failed. Contact your satellite service provider.

Table 33-2 NM-1VSAT-GILAT Network Module LED Descriptions (continued)

Figure Ref.	LED	State	Meaning	Possible Causes and Corrective Actions
6	EN	On	The router's Cisco IOS software recognizes the network module.	Normal indication. No action required.
		Off	The router's Cisco IOS software does not recognize the network module.	Verify that the network module is properly installed in the router chassis. See the "Installing Cisco Network Modules in Cisco Access Routers" chapter.

1. ODU = outdoor unit.
2. VSAT = very small aperture terminal.
3. DVB = Digital Video Broadcasting.
4. The *receive* direction at the remote VSAT is called the *outbound* direction from the hub. See the "Outbound and Inbound Directions in a Satellite Communications Network" section on page 33-7.
5. LNB = low noise block converter.
6. RF = radio frequency.
7. SSPA = solid state block converter and power amplifier.
8. The *transmit* direction at the remote VSAT is called the *inbound* direction to the hub. See the "Outbound and Inbound Directions in a Satellite Communications Network" section on page 33-7.

How to Install, Connect, or Replace the NM-1VSAT-GILAT Network Module

This section contains the following procedures, each of which may or may not be required, depending on which tasks your satellite service provider performs for you:

- Installing the NM-1VSAT-GILAT Network Module in the Router Chassis, page 33-10
- Connecting the NM-1VSAT-GILAT Network Module to the ODU, page 33-10
- Connecting the NM-1VSAT-GILAT Network Module to the External Power Supply, page 33-12
- Replacing the NM-1VSAT-GILAT Network Module in the Router Chassis, page 33-14

Installing the NM-1VSAT-GILAT Network Module in the Router Chassis

To install the NM-1VSAT-GILAT network module in the router chassis, see the "Installing Cisco Network Modules in Cisco Access Routers" chapter of the *Cisco Network Modules Hardware Installation Guide*.

Connecting the NM-1VSAT-GILAT Network Module to the ODU

This section describes how to connect the NM-1VSAT-GILAT network module to the ODU.

Shielded RG-6, RG-11, or both types of RF cables are used to connect the NM-1VSAT-GILAT network module to the ODU. Typically, a satellite service provider installation technician installs the ODU, connects RG-11 cables to the dish antenna, and runs the RG-11 cables to the area near the router. The technician also typically terminates the RG-11 cables and adds short RG-6 cables, which are then connected to the NM-1VSAT-GILAT network module in the router.

Note If an installation technician has already connected the NM-1VSAT-GILAT to the ODU, then do not perform this task. Instead, proceed directly to the "Connecting the NM-1VSAT-GILAT Network Module to the External Power Supply" section on page 33-12.

Prerequisites

- Install the NM-1VSAT-GILAT network module in the router chassis. See the "Installing Cisco Network Modules in Cisco Access Routers" chapter of the *Cisco Network Modules Hardware Installation Guide*.
- Make sure that your ODU is installed and connected to RF cables that lead to the area near the NM-1VSAT-GILAT network module. Contact your satellite service provider for ODU and cable installation information.

Steps

To connect the NM-1VSAT-GILAT network module to the ODU, follow these steps:

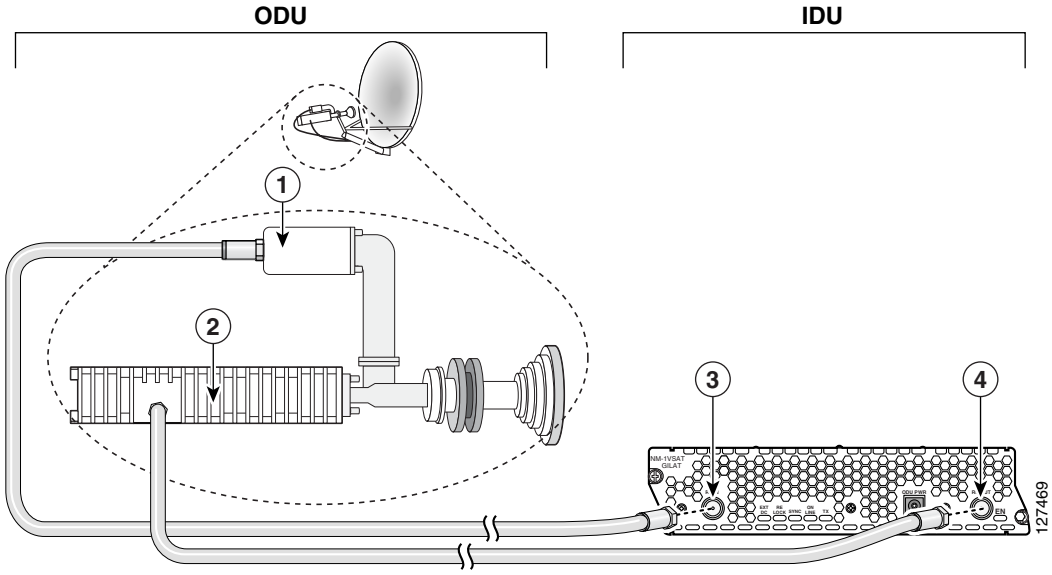
Step 1 Disconnect the power supply from the ODU PWR connector on the NM-1VSAT-GILAT network module.

Caution Make sure that the external power supply is disconnected from the NM-1VSAT-GILAT network module before connecting cables to the RF-IN or RF-OUT connectors. If the external power supply is connected to the ODU PWR connector while you connect or disconnect cables to the RF-IN or RF-OUT connectors, you might short-circuit the NM-1VSAT-GILAT network module F connectors. This may cause the network module to reset itself or lose data.

Step 2 Take the indoor end of the cable that leads to the LNB, and connect it to the RF-IN connector on the NM-1VSAT-GILAT network module. (See Figure 33-5.)

Step 3 Take the indoor end of the cable that leads to the SSPA, and connect it to the RF-OUT connector on the NM-1VSAT-GILAT network module. (See Figure 33-5.)

Figure 33-5 Connecting the NM-1VSAT-GILAT Network Module to the ODU



1	LNB	**3**	RF-IN connector
2	SSPA	**4**	RF-OUT connector

What to Do Next

Proceed to the "Connecting the NM-1VSAT-GILAT Network Module to the External Power Supply" section on page 33-12.

Connecting the NM-1VSAT-GILAT Network Module to the External Power Supply

This section describes how to connect the NM-1VSAT-GILAT network module to the external power supply that comes in the "Sat Kit" provided by a Gilat SkyEdge satellite service provider. The NM-1VSAT-GILAT network module requires additional power to operate the ODU, which includes the dish antenna and its parts, such as the LNB, SSPA, OMT, and feed horn.

Note If an installation technician has already connected a power supply to the ODU, then do not perform this task. Instead, proceed directly to the software configuration tasks for your NM-1VSAT-GILAT network module. See the *Cisco IP VSAT Satellite WAN Network Module (NM-1VSAT-GILAT)* Cisco IOS feature module.

Prerequisites

- Install the NM-1VSAT-GILAT network module in the router chassis. See the "Installing Cisco Network Modules in Cisco Access Routers" chapter of the *Cisco Network Modules Hardware Installation Guide*.
- Connect the NM-1VSAT-GILAT network module to the ODU. See the "Connecting the NM-1VSAT-GILAT Network Module to the ODU" section on page 33-10.

Restrictions

Only use the power supply provided in the Gilat ODU kit. Use of any other power supply will void the warranties for your NM-1VSAT-GILAT network module and outdoor equipment.

Steps

To connect the NM-1VSAT-GILAT network module to the external power supply, follow these steps:

Step 1 Connect the power supply cable to the ODU PWR connector on the NM-1VSAT-GILAT network module. (See Figure 33-6.)

Step 2 Connect the power supply to a general-purpose electrical outlet. (For the United States, see Figure 33-6. For Europe, see Figure 33-7.)

Figure 33-6 Connecting the NM-1VSAT-GILAT Network Module to the Power Supply (USA)

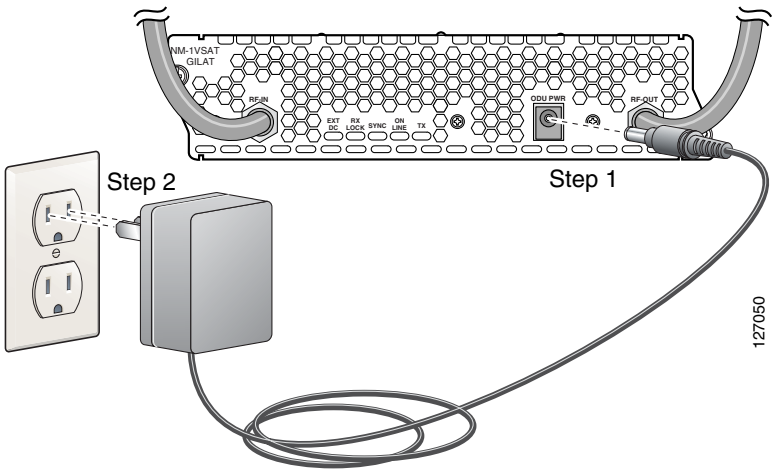
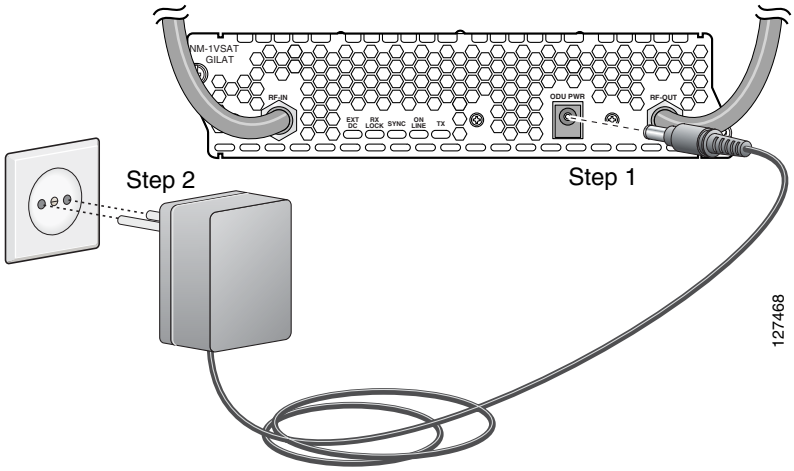


Figure 33-7 Connecting the NM-1VSAT-GILAT Network Module to the Power Supply (Europe)



What to Do Next

Proceed to the software configuration for your NM-1VSAT-GILAT network module. See the *Cisco IP VSAT Satellite WAN Network Module (NM-1VSAT-GILAT)* Cisco IOS feature module.

Replacing the NM-1VSAT-GILAT Network Module in the Router Chassis

This section describes how to replace the NM-1VSAT-GILAT network module in your router. Complete one of the following tasks, depending on whether or not your router supports online insertion and removal (OIR):

- Performing Online Insertion and Removal of the NM-1VSAT-GILAT Network Module, page 33-14
- Replacing the NM-1VSAT-GILAT Network Module in a Router, page 33-17

Performing Online Insertion and Removal of the NM-1VSAT-GILAT Network Module

The online insertion and removal (OIR) feature enables some Cisco modular access routers to support the replacement of network modules without switching off the router or affecting the operation of other interfaces. Also, routing information is maintained during OIR of network modules.

If your router does not support OIR, do not perform this task to replace your NM-1VSAT-GILAT network module. Instead, go to the "Replacing the NM-1VSAT-GILAT Network Module in a Router" section on page 33-17.

Restrictions

- Only the Cisco 3745 and Cisco 3845 routers support OIR of the NM-1VSAT-GILAT network module.
- All connections made through the NM-1VSAT-GILAT network module are reset during OIR.
- You must perform OIR with similar modules. If you remove a network module, install another network module exactly like it in its place.

Steps

To perform OIR of the NM-1VSAT-GILAT network module in your router, follow these steps:

Step 1 Initiate a console session with your router.

Step 2 Enter satellite interface configuration mode and shut down the interface:

```
Router> enable
Router# configure terminal
Router(config)# interface satellite slot/0
Router(config-if)# shutdown
Router(config-if)# end
Router#
```

Step 3 Disconnect the power supply cable from the ODU PWR connector on the NM-1VSAT-GILAT network module.

Caution Make sure that the external power supply is disconnected from the NM-1VSAT-GILAT network module before connecting or disconnecting cables from the RF-IN or RF-OUT connectors. If the external power supply is connected to the ODU PWR connector while you connect or disconnect cables from the RF-IN or RF-OUT connectors, you might short-circuit the NM-1VSAT-GILAT network module F connectors. This may cause the network module to reset itself or lose data.

Step 4 (Optional but recommended) Label the RF cables "RF-IN" and "RF-OUT."

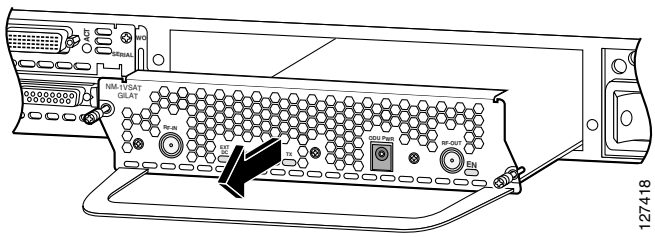
Step 5 Disconnect the cables from the RF-IN and RF-OUT connectors on the NM-1VSAT-GILAT network module.

Step 6 Using a number 1 Phillips or flat-blade screwdriver, loosen the captive mounting screws on the network module faceplate.

Caution To avoid damaging the network module, always handle the network module by the handle or faceplate. Do not touch the circuit board.

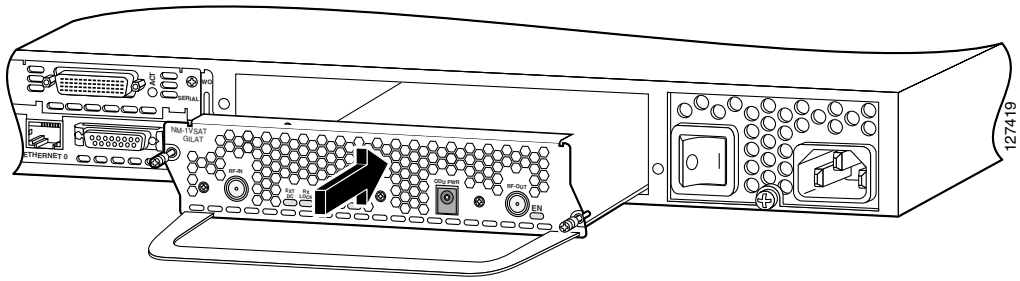
Step 7 Using the module handle, pull the network module from the router slot. (See Figure 33-8.)

Figure 33-8 Removing a Single-Wide Network Module



Step 8 Align the replacement network module with the guides in the chassis walls or slot divider and slide it gently into the slot. (See Figure 33-9.)

Figure 33-9 Installing a Single-Wide Network Module



Step 9 Using the network module handle, push the NM-1VSAT-GILAT network module into place until you feel the edge connector seat securely into the connector on the router backplane. The network module faceplate should contact the chassis rear panel.

Step 10 Using a number 1 Phillips or flat-blade screwdriver, tighten the captive mounting screws on the network module faceplate.

Caution Make sure that the external power supply is disconnected from the NM-1VSAT-GILAT network module before connecting or disconnecting cables from the RF-IN or RF-OUT connectors. If the external power supply is connected to the ODU PWR connector while you connect or disconnect cables from the RF-IN or RF-OUT connectors, you might short-circuit the NM-1VSAT-GILAT network module F connectors. This may cause the network module to reset itself or lose data.

Step 11 Connect the RF cables to the RF-IN and RF-OUT connectors on the NM-1VSAT-GILAT network module.

Step 12 Connect the power supply cable to the ODU PWR connector on the NM-1VSAT-GILAT network module.

Step 13 Confirm that the network module LEDs come on. For more information about the LEDs, see the "NM-1VSAT-GILAT Network Module LEDs" section on page 33-7.

Step 14 Initiate a console session with your router.

Step 15 Enter satellite interface configuration mode, and enable the satellite interface:

```
Router> enable
Router# configure terminal
Router(config)# interface satellite slot/0
Router(config-if)# no shutdown
Router(config-if)# end
Router#
```

What to Do Next

Configure the initial VSAT parameters for the new NM-1VSAT-GILAT network module. See the *Cisco IP VSAT Satellite WAN Network Module (NM-1VSAT-GILAT)* Cisco IOS feature module.

Note Satellite initial configuration mode can only be accessed by a password that is unique to each NM-1VSAT-GILAT network module. If an installation technician does not configure the initial VSAT parameters, then your satellite service provider will provide the password for your new NM-1VSAT-GILAT network module.

Replacing the NM-1VSAT-GILAT Network Module in a Router

This section describes how to replace the NM-1VSAT-GILAT network module when your router does not support online insertion and removal (OIR). If your router supports OIR, do not perform this task. Instead, go to the "Performing Online Insertion and Removal of the NM-1VSAT-GILAT Network Module" section on page 33-14.

To replace the NM-1VSAT-GILAT network module in your router, follow these steps:

Step 1 Disconnect the power supply cable from the ODU PWR connector on the NM-1VSAT-GILAT network module.

Caution Make sure that the external power supply is disconnected from the NM-1VSAT-GILAT network module before connecting or disconnecting cables from the RF-IN or RF-OUT connectors. If the external power supply is connected to the ODU PWR connector while you connect or disconnect cables from the RF-IN or RF-OUT connectors, you might short-circuit the NM-1VSAT-GILAT network module F connectors. This may cause the network module to reset itself or lose data.

Step 2 (Optional but recommended) Label the RF cables "RF-IN" and "RF-OUT."

Step 3 Disconnect the cables from the RF-IN and RF-OUT connectors on the NM-1VSAT-GILAT network module.

Step 4 Turn off electrical power to the router. Leave the power cable plugged in to channel ESD voltages to ground.

The following warning applies only to routers that use DC power.

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 7

Timesaver Label the cables or prepare a network cabling diagram before removing cables.

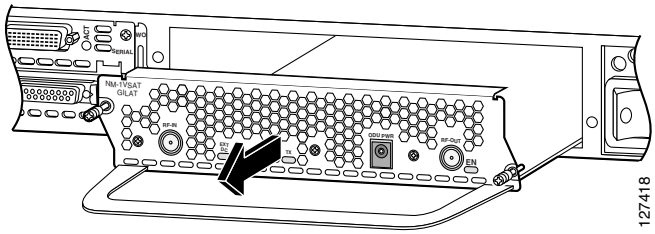
Step 5 Remove all network cables, including telephone cables, from the rear panel of the router.

Step 6 Using a number 1 Phillips or flat-blade screwdriver, loosen the captive mounting screws on the NM-1VSAT-GILAT network module faceplate.

Caution To avoid damaging the network module, always handle the network module by the handle or faceplate. Do not touch the circuit board.

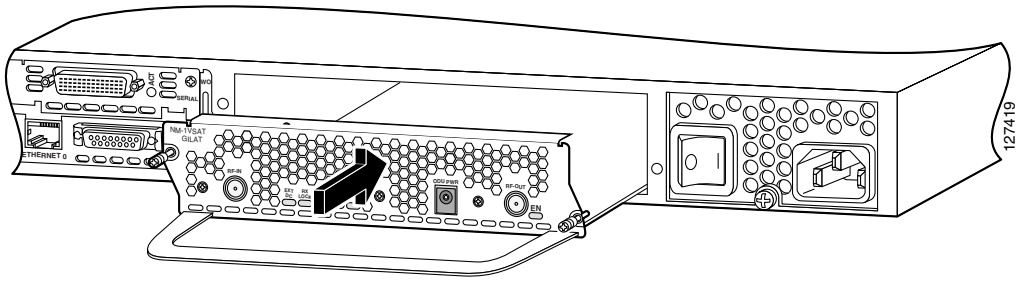
Step 7 Using the module handle, pull the network module from the router slot. (See Figure 33-10.)

Figure 33-10 Removing a Single-Wide Network Module



Step 8 Align the replacement network module with the guides in the chassis walls or slot divider and slide it gently into the slot. (See Figure 33-11.)

Figure 33-11 Installing a Single-Wide Network Module



Step 9 Using the network module handle, push the module into place until you feel the edge connector seat securely into the connector on the router backplane. The network module faceplate should contact the chassis rear panel.

Step 10 Using a number 1 Phillips or flat-blade screwdriver, tighten the captive mounting screws on the network module faceplate.

Step 11 Turn on electrical power to the router.

The following warning applies only to routers that use DC power.

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

Caution Make sure that the external power supply is disconnected from the NM-1VSAT-GILAT network module before connecting or disconnecting cables from the RF-IN or RF-OUT connectors. If the external power supply is connected to the ODU PWR connector while you connect or disconnect cables from the RF-IN or RF-OUT connectors, you might short-circuit the NM-1VSAT-GILAT network module F connectors. This may cause the network module to reset itself or lose data.

Step 12 Connect the RF cables to the RF-IN and RF-OUT connectors on the NM-1VSAT-GILAT network module.

Step 13 Connect the power supply cable to the ODU PWR connector on the NM-1VSAT-GILAT network module.

Step 14 Reconnect all other network cables, including telephone cables, to the rear panel of the router.

Step 15 Confirm that the NM-1VSAT-GILAT network module LEDs come on. For more information about the LEDs, see the "NM-1VSAT-GILAT Network Module LEDs" section on page 33-7.

What to Do Next

Configure the initial VSAT parameters for the new NM-1VSAT-GILAT network module. See the *Cisco IP VSAT Satellite WAN Network Module (NM-1VSAT-GILAT)* Cisco IOS feature module.

Note Satellite initial configuration mode can only be accessed by a password that is unique to each NM-1VSAT-GILAT network module. If an installation technician does not configure the initial VSAT parameters, then your satellite service provider will provide the password for your new NM-1VSAT-GILAT network module.

Related Documents

Related Topic	Document Title or URL
Regulatory compliance and safety information	*Cisco Network Modules and Interface Cards Regulatory Compliance and Safety Information*
Cisco IOS software configuration for the NM-1VSAT-GILAT network module	*Cisco IP VSAT Satellite WAN Network Module (NM-1VSAT-GILAT)*
Platform documentation for the Cisco 2600 series, Cisco 2800 series, Cisco 3700 series, and Cisco 3800 series routers	http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/index.htm
Cisco IOS release notes	http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123relnt/

CHAPTER 34

Connecting Cisco Network Admission Control Network Modules

This chapter describes Cisco Network Admission Control (NAC)- network modules for Cisco access routers, and contains the following sections:

Tip To determine whether your Cisco router supports a specific network module, see Table 1-6 on page 1-16.

Cisco NAC Network Modules

Cisco NAC network modules allow network administrators to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines before allowing users onto a network. The NAC module identifies whether networked devices, such as laptops, desktops, and corporate assets are compliant with a network's security policies, and it addresses vulnerabilities before permitting access to the network.

The Cisco NAC network module ships from the factory with the following hardware preinstalled.

Note See the Cisco NAC network module data sheet for supported Cisco Internet Operating System (IOS) version information, http://www.cisco.com/en/US/products/ps6128/products_data_sheets_list.html.

Model	Hard Disk	Memory	CompactFlash
NME-NAC-K9	80 GB	512 MB	64 MB

The Cisco NAC network module LEDs are shown in Figure 34-1 and described in Table 34-1.

Figure 34-1 NME-NAC-K9 Faceplate

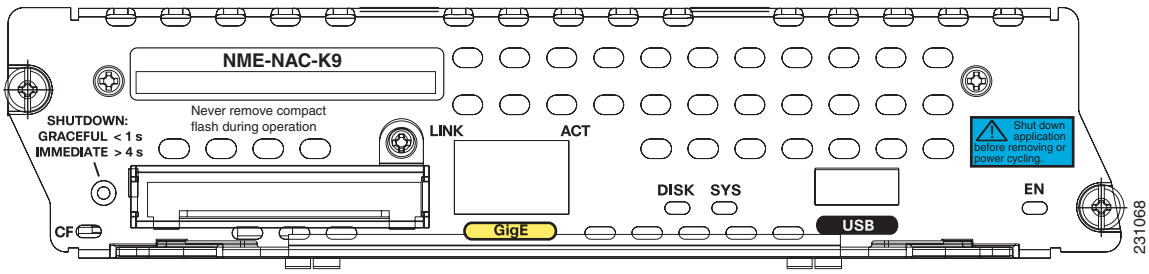


Table 34-1 NME-NAC-K9 LED Descriptions

CF	Status of the CompactFlash Off—CompactFlash is not detected Flashing—Application detected CompactFlash at bootup
LINK	Status of Gigabit Ethernet link On—Link is enabled Off—Link is disabled
ACT	Status of Gigabit Ethernet activity On—Active Off—Inactive
DISK	Status of hard drive activity On—Active Off—Inactive
PWR/SYS	Status of system shutdown **Note** Do not remove power without first shutting down the application. See the "Shutting Down the NAC Network Module" section on page 34-23. On—Application is stable Off—System is shut down and ready for host power down Flashing—System shutdown is in progress
EN	Status of the network module On—Detected by the host Cisco IOS software and enabled Off—Disabled

Shutting Down the NAC Network Module

Press the shutdown button on the network module faceplate for less than 2 seconds to perform a graceful shutdown of the hard disk before removing power from the router or before starting an online insertion and removal (OIR) sequence on the router. The application may take up to 2 minutes to fully shut down.

Note See the *Getting Started with NAC Network Modules in Cisco Access Routers* document on Cisco.com for instructions that describe how to shut down the network module from the command line interface on the router, http://www.cisco.com/en/US/products/ps6128/prod_installation_guides_list.html

Caution If you press the shutdown button for *more than 4 seconds*, a non-graceful shutdown of the hard disk will occur and may cause file corruption on the network module's hard disk. After a non-graceful shutdown, the DISK and SYS LEDs remain lighted. Press the shutdown button for *less than 1 second* to gracefully reboot the network module.

Connecting NAC Network Modules

To connect Cisco NAC network modules to an external device use a straight-through two-pair Category 5 unshielded twisted-pair (UTP) cable and connect the RJ-45 Gigabit Ethernet port on the network module to a switch, hub, repeater, or other Gigabit Ethernet network device.

Warning **To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the Network Admission Control Network Modules (NME-NAC-K9) only to intra-building or unexposed wiring or cable. The intrabuilding cable must be shielded and the shield must be grounded at both ends. The intra-building port(s) of the equipment or subassembly must not be metallically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE, Issue 4) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring.**

Note RJ-45 cables are not available from Cisco Systems. These cables are widely available and must be Category 5 cables.

Establishing a Gigabit Ethernet Internal Logical Connection

Use the Cisco High-Speed Intrachassis Module Interconnect (HIMI) feature to establish a Gigabit Ethernet (GE) internal logical connection between two NMEs, or between an onboard small-form-factor pluggable (SFP) GE module and an NME on Cisco 3825 and Cisco 3845 routers.

Connections can be established only as follows:

- Between the GE port in an installed onboard SFP module on the Cisco 3825 and Cisco 3845 routers
- Between GE interfaces in NME slots 1 and 2 on the Cisco 3825 router
- Between GE interfaces in NME slots 2 and 4 on the Cisco 3845 router

Note A module interconnection between the GE port on an SFP module and an NME slot or an NME-to-NME cross-connection is permitted at any given time, but both types of connections cannot exist at the same time.

Note Connections between the onboard RJ-45 GE ports and NME slots are not supported.

For details about configuring HIMI connections, see the *Cisco High-Speed Intrachassis Module Interconnect (HIMI) Configuration Guide* on Cisco.com, http://www.cisco.com/en/US/products/ps5855/prod_configuration_guide09186a008068ea83.html

Online Insertion and Removal of Cisco NAC Network Modules

Some Cisco access routers allow you to replace network modules without switching off the router or affecting the operation of other interfaces. This feature is called online insertion and removal (OIR). *Module OIR* provides uninterrupted operation to network users, maintains routing information, and ensures session preservation.

Caution Unlike other network modules, the Cisco NAC network module uses a hard disk. Online removal of disks without proper shutdown can result in file system corruption and might render the disk unusable. The operating system on the network module must be shut down in an orderly fashion before the module is removed or powered down.

Caution Cisco routers support OIR with similar modules only. If you remove a module, install another module exactly like it in its place. If you remove a 2-slot module (along with any installed WAN or voice interface cards), install another module and card combination exactly like it.

For a description of informational and error messages that may appear on the console during this procedure, see the hardware installation guide for your router.

To perform online removal of a network module and insertion of a replacement, follow these steps, beginning in privileged EXEC mode:

Step 1 Initiate a network module session using the following command:

```
Router# service-module integrated-service-engine 1/0 session

Trying 10.10.10.1, 2065 ... Open

Press RETURN to get started!

Router> enable
Router#
```

Step 2 Save the running configuration of the network module by using the following command from the **router #** prompt:

```
Router# copy running-config tftp tftp-server-address filename
```

Step 3 Exit the network module session by pressing **Control-Shift-6**, followed by **x**.

Step 4 On the router, clear the integrated-service-engine console session by using the following command:

```
Router# service-module integrated-service-engine slot/unit session clear
```

Step 5 Perform a graceful shutdown of the network module disk drive by using the following command:

```
Router# service-module integrated-service-engine slot/unit shutdown
```

Step 6 Shut down the network module interface:

```
Router (config)# interface integrated-service-engine slot/unit
Router (config-if)# shutdown
Router (config-if)# exit
```

Step 7 Unplug all network interface cables from the network module.

Step 8 Loosen the two captive screws holding the network module in the chassis slot.

Step 9 Slide the network module out of the slot.

Step 10 Align the replacement network module with the guides in the chassis slot, and slide it gently into the slot.

Note If the router is not fully configured with network modules, make sure that blank panels fill the unoccupied chassis slots to provide proper airflow.

Step 11 Push the module into place until you feel its edge connector mate securely with the connector on the backplane.

Step 12 Reconnect the network interface cables that you disconnected in Step 7.

Step 13 Check that the network module LEDs are on and that the power (PWR) and enable (EN) LEDs on the front panel are also on. This inspection ensures that connections are secure and that the new unit is operational.

Step 14 Initiate a network module session with the following command:

```
Router# service-module integrated-service-engine slot/unit session
Trying 11.1.1.8, 2130 ... Open

Fedora Core release 4 (stentz)
Kernel 2.6.11-perfigo on an 1686

login:
```

Step 15 Exit the network module session by pressing **Control-Shift-6**, followed by **x**.

Step 16 Restore the network module running configuration by using the following command from the service module prompt:

```
Router# copy tftp running-config tftp-server-address filename
```

Step 17 On the router, clear the network module session by using the following command:

```
Router# service-module integrated-service-engine slot/unit session clear
```

Related Documents

For additional information, refer to the following documents and resources.

Related Topic	Document Title
Cisco Network Admission Control (NAC) Software and Hardware Documentation	*Getting Started with Cisco NAC Network Modules in Cisco Access Routers* http://www.cisco.com/en/US/products/ps6128/prod_installation_guides_list.html *Cisco NAC Appliance Clean Access Manager Installation and Configuration Guide* *Cisco NAC Appliance Clean Access Server Installation and Configuration Guide* http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html *Cisco Network Admission Control Installation and Administration Guides* http://www.cisco.com/en/US/products/ps6128/products_user_guide_list.html *Cisco NAC Appliance Service Contract and Licensing Support* http://www.cisco.com/en/US/products/ps6128/prod_installation_guides_list.html
Cisco IOS software website and reference documentation	*Cisco IOS Software* http://www.cisco.com/en/US/products/sw/iosswrel/tsd_products_support_category_home.html
Technical documentation, including feedback and assistance	*What's New in Cisco Product Documentation* (including monthly listings of new and revised documents) at http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

CHAPTER 35

Connecting Application Performance Assurance Enhanced Network Modules

Last Updated: Aug 21, 2007

This chapter describes the Application Performance Assurance enhanced network module (NME-APA) for Cisco access routers, and contains the following sections:

Tip To determine whether your Cisco router supports a specific network module, see Table 1-6 on page 1-16.

Application Performance Assurance Enhanced Network Module

The Application Performance Assurance NME (NME-APA) actively manages traffic flow based on multiple criteria such as business priorities, application or protocol recognition, user awareness and other criteria as described in the *NME-APA User Guide*.

This section provides information about the following network modules:

- The NME-APA-E2—Supports the Cisco 2811, 2821, and 2851 Integrated Services Routers.
- The NME-APA-E3— Supports the Cisco 3825 and 3845 Integrated Services Routers

Both are shipped from the factory, preinstalled with the following hardware listed below.

Table 35-1 NME-APA Hardware

Model	Hard Disk	Memory	Compact Flash Memory	USB	RJ45
NME-APA-E2	80 GB (SATA)	1 GB	None	Not Used	Not Used
NME-APA-E3	80 GB (SATA)	1 GB	None	Not Used	Not Used

Figure 35-1 NME-APA1Faceplate

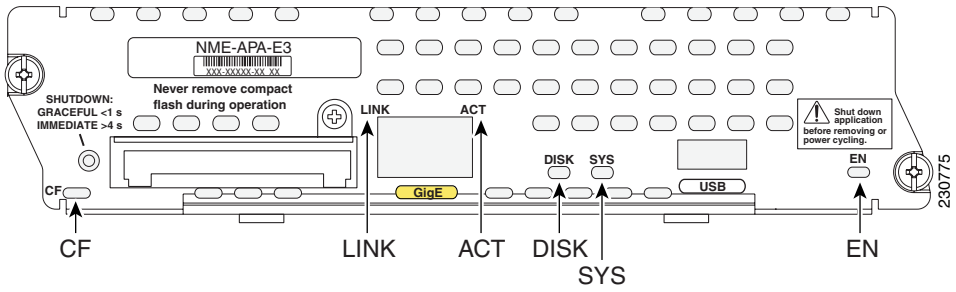


Table 35-2 LED Colors Functions

LED	Color	Function	Notes
CF	Green	Status of compact flash On—CF detected Off—No CF detected	There is no compact flash memory. Therefore this LED is unused.
LINK	Green	Status of Gigabit Ethernet (GE) link On—Link is up Off—Link is down	Gigabit Ethernet is not supported. Therefore this LED is unused.
ACT	Green	Status of GE activity On—Active Off—Inactive	Gigabit Ethernet is not supported. Therefore this LED is unused.
DISK	Green	Status of disk On—Active Off—Inactive	

LED	Color	Function	Notes
SYS	Green	Status of system ON – Shutdown complete and the system is ready for power off OFF – Shutdown not complete	This LED functions only when a shutdown is attempted. This LED is off until the system shutdown is complete and the module can be safely powered off, Then the LED turns green.
EN	Green	Status of the network module On—Detected by the host Cisco IOS software and enabled Off—Disabled	This LED is off when the NME-APA card is plugged into a chassis that does not support it. This LED turns on briefly when detecting a card type, then goes off after determining the card type is not supported. Note that a network module that is shut down is not disabled.

Shutting Down and Removing the NME-APA

Enhanced network modules contain hard disks. Removing a module without a graceful shutdown may result in disk file corruption. Before removing power from the router or starting an online insertion and removal (OIR) sequence, perform a graceful shutdown by pressing the Reset button on the network module for less than 1 second, or using an appropriate command-line interface command.

Note See the *NME-APA User Guide* for details about shutting down the application software on the network module.

Caution Do not remove or insert a module with power on unless it is an NME-APA-E3 in a Cisco 3845 Integrated Services Router.

The application may take 3 minutes to fully shut down. See the *NME-APA User Guide* for instructions on shutting down the software application on the module.

Caution Pressing the shutdown button for *more than 4 seconds* initiates a non-graceful shutdown of the hard disk which may cause file corruption. After a non-graceful shutdown, the HD and SYS LEDs remain lighted.

Connecting the Application Performance Assurance Enhanced Network Module

The external RJ-45 connector on the NME-APA is not supported at this time; we recommend that you do not make any connections to it.

Online Insertion and Removal of NME-APA-E3

Only Cisco 3845 Integrated Services Routers (ISRs) allow replacing NME-APA-E3 modules without first removing power from the router. This ability is called online insertion and removal (OIR). While traffic monitoring stops during a module's removal, OIR provides uninterrupted network connectivity.

Enhanced network modules contain hard disks that require graceful shutdown. Removing a module without graceful shutdown may result in disk file corruption.

Caution Before removing power from the router or starting an online insertion and removal (OIR) sequence, perform a graceful shutdown by pressing the Reset button on the network module for less than 1 second, or using an appropriate CLI command.

Caution OIR operates only with modules that are the same type. If you remove a module, install another module exactly like it in its place. If you remove a 2-slot module (along with any installed WAN or voice interface cards), install another module and card combination exactly like it.

For descriptions of informational and error messages that may appear on the console during this procedure, see the hardware installation guide for your router.

Saving the NME-APA Configuration File

The NME-APA has its own configuration file which is separate from that of the router. Save the existing configuration file before you replace the module to ensure that the new module will operate exactly as the old module did.

To perform online removal of a network module and insertion of a replacement, follow these steps in privileged EXEC mode:

Step 1 Telnet to the NME-APA:

```
Router# telnet 10.10.10.2

Trying 10.10.10.2...
Connected to 10.10.10.2.
Escape character is '^]'.

User Access Verification

Username:
Password:
NME-APA> enable
```

```
Password:

NME-APA#
```

Step 2 Save the running configuration of the network module by using the following command:

```
NME-APA# copy running-config startup-config
Writing general configuration file to temporary location...
Backing-up general configuration file...
Copy temporary file to final location...
NME-APA#>copy startup-config backup.config
```

Step 3 Confirm that your **backup.config** file is created by entering the following command and reviewing the file list:

```
NME-APA# dir
File list for /root/tffs0/
     200    Thu Apr  5 10:25:42 200       .                    DIR
      72    Thu Mar 22 03:45:31 200       ..                   DIR
      80    Thu Mar 22 03:45:31 200       app                  DIR
     136    Thu Mar 22 03:45:31 200       engage               DIR
      48    Thu Mar 22 03:46:14 200       images               DIR
    1663    Thu Apr  5 10:25:42 200       backup.config
     512    Thu Apr  5 10:24:56 200       system               DIR
```

Step 4 Back up the configuration file to a host:

```
NME-APA# copy backup.config ftp://[[[username[:password]@]location]/directory/source-file
```

Step 5 Exit the network module session by entering the following command:

```
NME-APA# logout

Are you sure? y

*** CLI session terminated due to timeout ***

Connection to 172.29.52.242 closed by foreign host.
```

Step 6 Telnet to the NME-APA's router as follows:

```
Router# telnet 10.10.10.1

Trying 10.10.10.1, 2065 ... Open

Press RETURN to get started!

router> enable

router#
```

Step 7 Perform a graceful shutdown of the network module by pressing the **Reset** button on the NME-APA and waiting for the SYS LED to turn green. Or you can use the following command:

```
Router# service-module integrated-service-engine slot/unit shutdown

Do you want to proceed with shutdown?[confirm]Y
Use service module reset command to recover from shutdown.

WARNING: Confirm that the service-module status shows 'is Shutdown' before remo!
```

Step 8 Confirm that the NME-APA has shut down by using the following command (Shutdown takes several minutes):

```
Router# service-module integrated-service-engine slot/unit status

Service Module is Cisco Integrated-Service-Engine1/0
Service Module supports session via TTY line 66
Service Module is Shutdown
Service Module status is not available
```

Note Before the module shuts down, the returned text reads "Service Module **is being** Shutdown." When the module has completely shut down, the returned text reads "Service Module **is** Shutdown"

Step 9 Do not Exit from the router telnet session. Replacing the NME-APA assumes that you have not exited the session.

Replacing the NME-APA

To physically remove the old module and replace it with a new one, follow these steps.

Step 1 If you have not previously performed the "Saving the NME-APA Configuration File" procedure on page 35-4, perform the procedure now.

- If you are replacing an NME-APA-E3 in a Cisco 3845 ISR continue to Step 2. If you are replacing an NME-APA-E2, remove power from the router before you continue directly to Step 2.

Step 2 Unplug all network interface cables from the network module.

Step 3 Loosen the two captive screws holding the network module in the chassis slot.

Step 4 Slide the network module out of the slot.

Step 5 Align the replacement network module with the guides in the chassis slot, and slide it gently into the slot.

Note If the router is not fully configured with network modules, make sure that blank panels are installed on the unoccupied chassis slots to provide proper airflow.

Step 6 Push the module into place until you feel its edge connector mate securely with the connector on the backplane. Tighten the captive screws that secure the module in the slot.

Step 7 Reconnect the network interface cables that you removed in Step 2.

- If you are replacing an NME-APA-E3 in a 3845 ISR continue to Step 8. If you are replacing an NME-APA-E2, power up the router before continuing to the next step.

Step 8 Check that the network module LEDs are on and that the power (PWR) and enable (EN) LEDs on the front panel are also on. This inspection ensures that connections are secure and that the new unit is operational.

Step 9 Confirm that the NME-APA is running by using the following command:

```
Router# service-module integrated-service-engine slot/unit status
Service Module is Cisco Integrated-Service-Engine1/0
Service Module supports session via TTY line 66
Service Module is in Steady state
Getting status from the Service Module, please wait.
Network Module Enhanced - Application Performance Assurance 0.1.2.1
NME-APA running on BRYCE
```

Step 10 Exit the router Telnet session:

```
Router # exit
```

Configuring the Replacement NME-APA

Follow these steps to configure the replacement module exactly like the original.

The module will not respond to Telnet commands until it has finished restarting. You must wait several minutes before performing Step 2. The exact time depends on the system configuration.

Step 1 If you have not performed the "Saving the NME-APA Configuration File" procedure on page 35-4, perform the procedure now.

Step 2 Telnet to the NME-APA:

```
Router# telnet 10.10.10.2

Trying 10.10.10.2...
Connected to 10.10.10.2.
Escape character is '^]'.

User Access Verification

Username:
Password:
NME-APA> enable

Password:

NME-APA#
```

Step 3 Restore the network module's running configuration from the file saved in the "Saving the NME-APA Configuration File" procedure on page 35-4 by using the following command from the service module prompt:

```
NME-APA# copy ftp://[[[username[:password]@]location]/directory]/backup.config
NME-APA# copy /directory/source-file /directory/destination-file
NME-APA# copy running-config startup-config
```

Step 4 Exit the network module session by using the following command:

```
NME-APA# logout
```

Confirming the Startup Configuration (Optional)

To confirm that the startup configuration file was restored properly, you can use a reload command on the module.

Step 1 Telnet to the NME-APA's router:

```
Router# telnet 10.10.10.1

Trying 10.10.10.1, 2065 ... Open

Press RETURN to get started!

router> enable

router#
```

Step 2 Reload the NME-APA:

```
Router# service-module integrated-service-engine slot/unit reload
Do you want to proceed with reload?[confirm]
Trying to reload Service Module Integrated-Service-Engine1/0.
```

Step 3 After several minutes check the module status and logout:

```
router# service-module integrated-Service-Engine slot/unit status
Service Module is Cisco Integrated-Service-Engine1/0
Service Module supports session via TTY line 66
Service Module is in Steady state
Getting status from the Service Module, please wait..
Network Module Enhanced - Application Performance Assurance 0.1.2.1
NME-APA running on BRYCE

router# logout
Connection to 172.29.52.241 closed by foreign host.
```

Step 4 After a few minutes, telnet to the NME-APA.

Note The module will not accept a telnet session until it has restarted the application which may take several minutes.

```
Router# telnet 10.10.10.1

Trying 10.10.10.1...
Connected to 10.10.10.1.
Escape character is '^]'.

User Access Verification

Username:
Password:
NME-APA> enable

Password:

NME-APA#
```

Step 5 Check the running configuration and confirm that it is correct:

```
NME-APA# show running-config
#This is a general configuration file (running-config).
```

```
#Created on 14:48:18  UTC  MON  April  9  2007
.
.
.
```

Step 6 Log out of the module:

```
NME-APA# logout
Are you sure? y


*** CLI session terminated due to timeout ***

Connection to 172.29.52.242 closed by foreign host.
```

Related Documents

For additional information, refer to the following documents and resources.

Related Topic	Document Title
Application Performance Assurance software installation and administration, configuration, operation, and user guides	NME-APA Device Console User Guide NME-APA Device Console Installation Guide NME-APA Device Console Release Notes NME-APA User Guide NME-APA Command Line Reference Guide NME-APA Release Notes NME-APA Trouble Shooting Guide http://www.cisco.com/en/US/products/ps7045/tsd_products_support_category_home.html
Cisco IOS software website and reference documentation	*Cisco IOS Software* http://www.cisco.com/en/US/products/sw/iosswrel/tsd_products_support_category_home.html
Technical documentation, including feedback and assistance	*What's New in Cisco Product Documentation* (including monthly listings of new and revised documents) at http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

CHAPTER 36

Connecting WAAS Enhanced Network Modules

This chapter describes WAAS enhanced network modules for Cisco integrated services routers, and contains the following sections:

Tip To determine whether your Cisco router supports a specific network module, see Table 1-6 on page 1-16.

WAAS Enhanced Network Modules

The WAAS enhanced network module (NME-WAE family of devices) works together with other wide-area application engines (WAEs) in your network to optimize TCP traffic over your network.

When client and server applications attempt to communicate with each other, the network intercepts and redirects this traffic to the WAEs so that they can act on behalf of the client application and the destination server. The WAEs examine the traffic and use built-in application policies to determine whether to optimize the traffic or allow it to pass through your network unoptimized. Three models of the WAAS enhanced network module are available. (See Figure 36-1 on page 36-2.)

- NME-WAE-302-K9
- NME-WAE-502-K9
- NME-WAE-522-K9

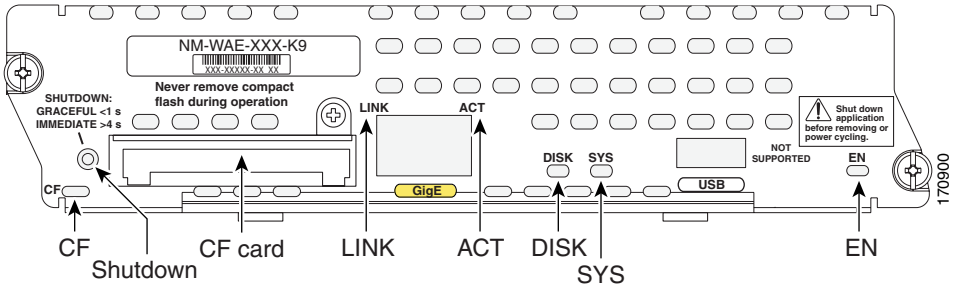
Warning **To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the WAAS enhanced network modules (NME-WAE-302-K9, NME-WAE-502-K9 and NME-WAE-522-K9) only to intra-building or unexposed wiring or cable. The intrabuilding cable must be shielded and the shield must be grounded at both ends. The intra-building port(s) of the equipment or subassembly must not be metallically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE, Issue 4) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring.**

All models ship from the factory with the following hardware preinstalled. (See Table 36-1.)

Table 36-1 Preinstalled Hardware in WAAS Enhanced Network Modules

Model	Hard Disk	Memory	Daughter Card	CompactFlash
NME-WAE-302-K9	80 GB (SATA)	512 MB	Included	64 MB
NME-WAE-502-K9	120 GB (SATA)	1 GB	Included	64 MB
NME-WAE-522-K9	160 GB (SATA)	2 GB	Included	64 MB

Figure 36-1 NME-WAE Faceplate



CF	Status of the CompactFlash Off—CompactFlash is not used Flashing—Application detected CompactFlash at boot up
SHUTDOWN	Press the SHUTDOWN button for less than 2 seconds to gracefully shut down the module. Press the SHUTDOWN button for more than 4 seconds to cause an immediate module shutdown, which may impact file operations that are in progress.
LINK	Status of Gigabit Ethernet link On—Link is enabled Off—Link is disabled
ACT	Status of Gigabit Ethernet activity On—Active Off—Inactive
DISK	Status of hard drive activity On—Active Off—Inactive

SYS	Status of system shutdown **Note** Do not remove power without first shutting down the application. On—Application is stable. Off—System is shut down and ready for host power down Flashing—System shutdown is in progress
EN	Status of the network module On—Detected by the host Cisco IOS software and enabled Off—Disabled

Shutting Down WAAS Enhanced Network Modules

Press the reset button on the network module faceplate for less than 2 seconds to perform a graceful shutdown of the network module before removing power from the router or before starting an online insertion and removal (OIR) sequence on the router. The application may take up to 2 minutes to fully shut down.

Caution If you press the shutdown button for *more than 4 seconds*, a nongraceful shutdown of the hard disk will occur and may cause file corruption on the network module's hard disk. After a nongraceful shutdown, the HD and SYS LEDs remain lit. Press the shutdown button for *less than 2 seconds* to gracefully reboot the network module.

Connecting WAAS Enhanced Network Modules

To connect WAAS enhanced network modules to an external device, use a straight-through two-pair Category 5e unshielded twisted-pair (UTP) cable, and connect the RJ-45 Gigabit Ethernet port on the network module to a switch, hub, repeater, server, or other Gigabit Ethernet network device.

Note RJ-45 cables are not available from Cisco Systems, Inc. These cables are widely available and must be Category 5e cables.

Establishing a Gigabit Ethernet Internal Connection

Use the Cisco High-Speed Intrachassis Module Interconnect (HIMI) feature to establish a Gigabit Ethernet internal logical connection between two network modules, or between an onboard small-form-factor pluggable (SFP) Gigabit Ethernet module and a network module on Cisco 3825 and Cisco 3845 routers.

Connections can be only established as follows:

- Between the Gigabit Ethernet port in an installed onboard SFP module on the Cisco 3825 and Cisco 3845 routers and a network module Gigabit Ethernet interface installed in network module slots 1 and 2 on a Cisco 3825 router or Cisco 3845 router
- Between Gigabit Ethernet interfaces in network module slots 1 and 2 on the Cisco 3825 router
- Between Gigabit Ethernet interfaces in network module slots 2 and 4 on the Cisco 3845 router

Note A module interconnection between the Gigabit Ethernet port on an SFP module and a network module slot or a network module-to-network module cross-connection is permitted at any given time, but both types of connections cannot exist at the same time.

Note Connections between the onboard Ethernet ports and network module slots are not supported.

For details about configuring HIMI connections, see the *Cisco High-Speed Intrachassis Module Interconnect (HIMI) Configuration Guide* on Cisco.com:

http://www.cisco.com/en/US/products/ps5855/prod_configuration_guide09186a008068ea83.html

Online Insertion and Removal of Cisco Network Modules Procedure

Some Cisco routers allow you to replace network modules without switching off the router or affecting the operation of other interfaces. This feature is called online insertion and removal (OIR). OIR of a module provides uninterrupted operation to network users, maintains routing information, and ensures session preservation.

Caution Unlike other network modules, WAAS enhanced network modules use hard disks. Online removal of disks without proper shutdown can result in file system corruption and might render the disk unusable. The operating system on the network module must be shut down in an orderly way before removing or powering down the module.

Caution Cisco routers support OIR with similar modules only. If you remove a module, install another module exactly like it in its place. If you remove a 2-slot module (along with any installed WAN or voice interface cards), install another module and card combination exactly like it.

For a description of informational and error messages that may appear on the console during this procedure, see the hardware installation guide for your router.

To perform online removal of a network module and insertion of a replacement, follow these steps, with the router in privileged EXEC mode:

Step 1 Initiate a network module session using the following command:

```
Router# service-module integrated-service-engine slot/unit session

Trying 10.10.10.1, 2065 ... Open

Press RETURN to get started!

Router> enable
Router#
```

Step 2 Save the running configuration of the network module using the following command from the **Router #** prompt:

```
Router# copy running-config tftp tftp-server-address filename
```

Step 3 Exit the network module session by pressing **Control-Shift-6**, followed by **x**.

Step 4 On the router, clear the integrated-service-engine console session using the following command:

```
Router# service-module integrated-service-engine slot/unit session clear
```

Step 5 Perform a graceful shutdown of the network module disk drive by using the following command:

```
Router# service-module integrated-service-engine slot/unit shutdown
```

Step 6 Shut down the network module interface:

```
Router (config)# interface integrated-service-engine slot/unit
Router (config-if)# shutdown
Router (config-if)# exit
```

Step 7 Unplug all network interface cables from the network module.

Step 8 Loosen the two captive screws holding the network module in the chassis slot.

Step 9 Slide the network module out of the slot.

Step 10 Align the replacement network module with the guides in the chassis slot, and slide it gently into the slot.

Note If the router is not fully configured with network modules, make sure that blank panels fill the unoccupied chassis slots to provide proper airflow.

Step 11 Push the module into place until you feel its edge connector mate securely with the connector on the backplane.

Step 12 Reconnect the network interface cables previously removed in Step 7.

Step 13 Check that the network module LEDs are on and that the power (PWR) and enable (EN) LEDs on the front panel are also on. This inspection ensures that connections are secure and that the new unit is operational.

Step 14 Initiate a network module session with the following command:

```
Router# service-module integrated-service-engine slot/unit session

Trying 10.10.10.1, 2129 ... Open

ISE-network module now available

Press RETURN to get started!

Router> enable
Router#
```

Step 15 Restore the network module running configuration by using the following command from the service module prompt:

```
Router# copy tftp running-config tftp-server-address filename
```

Step 16 Exit the network module session by pressing **Control-Shift-6**, followed by **x**.

Step 17 On the router, clear the network module session by using the following command:

```
Router# service-module integrated-service-engine slot/unit session clear
```

Additional References

For additional information, see the following documents and resources.

Related Topic	Document Title
WAAS software installation and administration, configuration, and operation	*Configuring Cisco WAAS Enhanced Network Modules for Cisco Access Routers*
Cisco WAAS software website and reference documentation	*Cisco WAAS Software* http://www.cisco.com/en/US/products/ps6870/tsd_products_support_series_home.html
Cisco IOS software website and reference documentation	*Cisco IOS Software* http://www.cisco.com/en/US/products/sw/iosswrel/tsd_products_support_category_home.html
Technical documentation, including feedback and assistance	*What's New in Cisco Product Documentation* (including monthly listings of new and revised documents) at http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

CHAPTER 37

Connecting Cisco Unified Messaging Gateway Enhanced Network Modules

This chapter describes Cisco Unified Messaging Gateway enhanced network modules for Cisco integrated services routers, and contains the following sections:

Tip To determine whether your Cisco router supports a specific network module, see Table 1-6 on page 1-16.

Cisco Unified Messaging Gateway Enhanced Network Modules

The Cisco Unified Messaging Gateway enhanced network module provides centralized management for larger Cisco Unity Express voicemail networks. The Cisco Unified Messaging Gateway enhanced network module:

- Intelligently routes voicemail messages
- Exchanges subscriber and directory information among the voicemail systems
- Provides interoperability with third party voicemail vendors within a voice messaging network

There are two versions of the Cisco Unified Messaging Gateway enhanced network module:

- NME-UMG supports up to 250 nodes.
- NME-UMG-EC supports up to 1000 nodes.

Note Cisco recommends attaching an uninterruptible power supply (UPS) to the router that houses the Cisco Unified Messaging Gateway enhanced network module. The UPS should include a signaling mechanism that directs the router to shut down the Cisco Unified Messaging Gateway application properly and then powers off the router.

Cisco IOS Release 12.3(4)T and later supports automatic switchover to the UPS device.

Note The Gigabit Ethernet port and compact flash (CF) slot, though available on the hardware, are not supported by the Cisco Unified Messaging Gateway enhanced network module. The CF slot has a metal cover.

The Cisco Unified Messaging Gateway enhanced network module LEDs are shown in Figure 37-1 and described in Table 37-1.

Figure 37-1 NME-UMG Faceplate

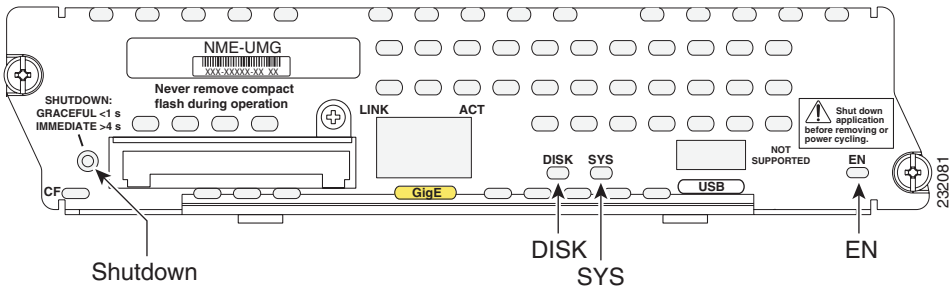


Table 37-1 NME-UMG LED Descriptions

SHUTDOWN	Press the SHUTDOWN button for less than 2 seconds to gracefully shut down the module. Press the SHUTDOWN button for more than 4 seconds to cause an immediate module shutdown, which may impact file operations that are in progress.
DISK	Status of hard drive activity: On—Active. Off—Inactive.
SYS	Status of system shutdown **Note** Do not remove power without first shutting down the application. On—Application is stable. Off—System is shut down and ready for host power-down. Flashing—System shutdown is in progress.
EN	Status of the network module: On—Detected by the host Cisco IOS software and enabled. Off—Disabled.

Shutting Down Cisco Unified Messaging Gateway Enhanced Network Modules

Press the SHUTDOWN button on the network module faceplate for less than 2 seconds to perform a graceful shutdown of the network module before removing power from the router or before starting an online insertion and removal (OIR) sequence on the router. The application may take up to 2 minutes to fully shut down.

Caution If you press the SHUTDOWN button for *more than 4 seconds*, a nongraceful shutdown of the hard disk will occur and may corrupt files on the network module's hard disk. After a nongraceful shutdown, the HD and SYS LEDs remain lit. Press the SHUTDOWN button for *less than 2 seconds* to gracefully reboot the network module.

Online Insertion and Removal of Cisco Network Modules Procedure

Some Cisco routers allow you to replace network modules without switching off the router or affecting the operation of other interfaces. This feature is called *online insertion and removal* (OIR). OIR of a module provides uninterrupted operation to network users, maintains routing information, and ensures session preservation.

Caution Unlike other network modules, Cisco Unified Messaging Gateway enhanced network modules use hard disks. Online removal of network modules without proper shutdown can cause file system corruption and might render the disk unusable. You must shut down the operating system on the network module in an orderly way before removing or powering down the module.

Caution Cisco routers support OIR with identical modules only. If you remove a module, install in its place another module exactly like the one you removed. If you remove a 2-slot module (along with any installed WAN or voice interface cards), install another module and card combination exactly like it.

For descriptions of informational and error messages that may appear on the console during this procedure, see the hardware installation guide for your router.

To perform online removal of a network module and insertion of a replacement, follow these steps, with the router in privileged EXEC mode:

Step 1 Initiate a network module session by using the following command:

```
Router# service-module integrated-Service-Engine slot/unit session

Trying 10.10.10.1, 2065 ... Open

SE-Module> enable
SE-Module#
```

Step 2 Save the running configuration of the network module by using the following command from the `SE-Module#` prompt:

```
SE-Module# copy running-config tftp:
Address or name or remote host? tftp-server-address
```

```
Destination filename? filename
```

Note Depending on the specific TFTP server you are using, you might need to create a file with the same name on the TFTP server and verify that the file has the correct permissions before transferring the running configuration to the TFTP server.

Step 3 Exit the network module session by pressing **Control-Shift-6**, followed by pressing **x**.

Step 4 On the router, clear the integrated-Service-Engine console session by using the following command:

```
Router# service-module integrated-Service-Engine slot/unit session clear
```

Step 5 Perform a graceful shutdown of the network module disk drive by using the following command:

```
Router# service-module integrated-Service-Engine slot/unit shutdown
```

Step 6 Shut down the network module interface:

```
Router (config)# interface integrated-Service-Engine slot/unit
Router (config-if)# shutdown
Router (config-if)# exit
```

Step 7 Loosen the two captive screws that are holding the network module in the chassis slot.

Step 8 Slide the network module out of the slot.

Step 9 Align the replacement network module with the guides in the chassis slot, and slide it gently into the slot.

Note If the router is not fully configured with network modules, make sure that blank panels fill the unoccupied chassis slots to provide proper airflow.

Step 10 Push the module into place until you feel its edge connector mate securely with the connector on the backplane.

Step 11 Check that the network module LEDs are on. This inspection ensures that connections are secure and that the new unit is operational.

Step 12 Initiate a network module session by using the following command:

```
Router# service-module integrated-Service-Engine slot/unit session

Trying 10.10.10.1, 2129 ... Open

SE-Module> enable
SE-Module#
```

Step 13 Restore the network module running configuration by using the following command from the service module prompt:

```
SE-Module# copy tftp: running-config
Address or name or remote host? tftp-server-address
Source filename? filename
```

Step 14 Exit the network module session by pressing **Control-Shift-6**, followed by pressing **x**.

Step 15 On the router, clear the network module session by using the following command:

```
Router# service-module integrated-Service-Engine slot/unit session clear
```

Additional References

For additional information, see the following documents and resources.

Related Topic	Document Title
Regulatory compliance and safety information	*Cisco Network Modules and Interface Cards Regulatory Compliance and Safety Information*
Cisco Unified Messaging Gateway application software website and reference documentation	http://www.cisco.com/en/US/products/ps8605/tsd_products_support_series_home.html
Cisco IOS software website and reference documentation	http://www.cisco.com/en/US/products/sw/iosswrel/tsd_products_support_category_home.html
Technical documentation, including feedback and assistance	*What's New in Cisco Product Documentation* (including monthly listings of new and revised documents) at http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

CHAPTER 38

Connecting 8-Port T1/E1 Network Modules

This chapter describes how to connect 8-port T1/E1 network modules for Cisco integrated service routers. It contains the following sections:

Cisco T1/E1 Network Module

The Cisco T1/E1 network module provides 8 ports of clear channel or channelized T1 and E1 support to Cisco 3800 series integrated services routers:

- Cisco 3825
- Cisco 3845

T1 support has integrated CSU/DSU capability.

Safety Warnings for the Cisco T1/E1 Network Module

The following safety warnings apply to installation procedures involving the Cisco T1/E1 network module. Translations of these warnings are available in the *Cisco Network Modules and Interface Cards Regulatory Compliance and Safety Information* document, which is available online.

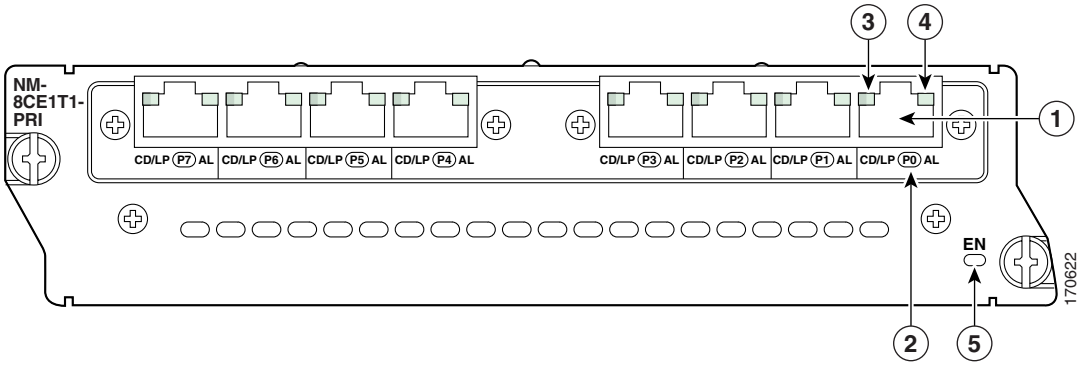
Warning **To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.** Statement 1021

Warning **Hazardous network voltages are present in WAN ports regardless of whether power to the unit is OFF or ON. To avoid electric shock, use caution when working near WAN ports. When detaching cables, detach the end away from the unit first.** Statement 1026

Cisco T1/E1 Network Module LEDs

The T1/E1 network module has 2 LEDs for each port that indicate the functionality of the T1 or E1 connection. Figure 38-1 shows the front panel and LEDs. The LEDs are described in Table 38-1.

Figure 38-1 8-Port T1/E1 Network Module Front Panel



1	RJ-48C connector	**2**	Port number
3	CD/LP LED (bicolor LED)	**4**	AL LED
5	EN LED		

CD/LP LEDs are bicolor LEDs with both green and yellow emitters.

Table 38-1 T1/E1 Network Module LEDs

LED	Color	Description
CD/LP	Green/Yellow	Off: No carrier detected Green on (CD): Carrier detected Yellow on (LP): Port in loopback mode
AL	Yellow	Off: No alarms On: Port in alarm mode
EN	Green	Off: Network module does not pass self-test and is not available to the router. There is a failure with either the module or the slot. On: Network module has passed self-test and is available to the router. The network module may be removed from router when the EN LED is off.

Connecting a T1/E1 Network Module to a Network

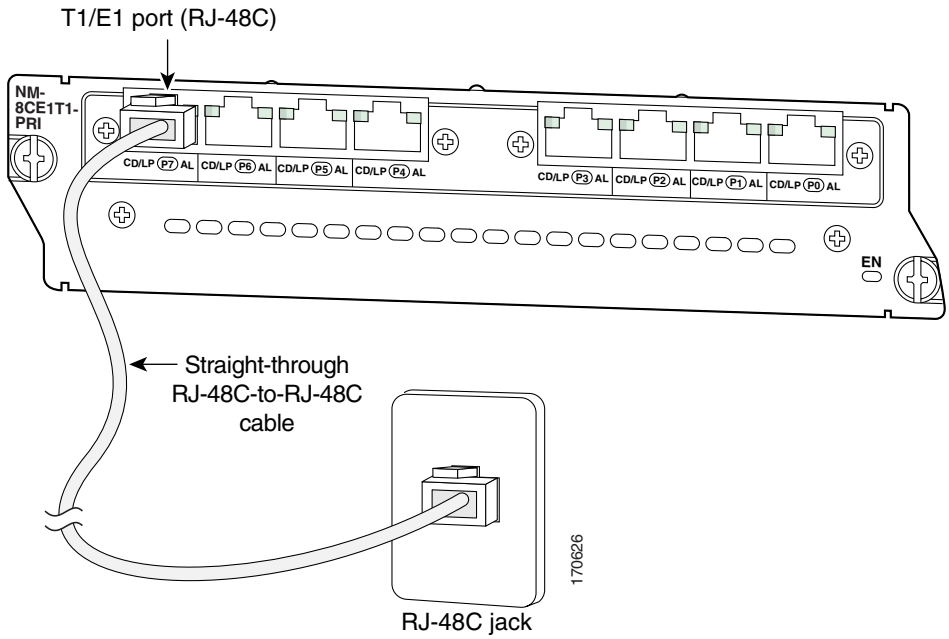
Use straight-through RJ-48C-to-RJ-48C cables to connect T1/E1 ports to RJ-48C jacks.

To connect a T1/E1 port to the network, complete the following steps:

Step 1 Connect one end of the cable to a T1/E1 port on the network module.

Step 2 Connect the other end to the RJ-48C jack at your site, as shown in Figure 38-2.

Figure 38-2 Connecting a T1/E1 Port to an RJ-48C Jack

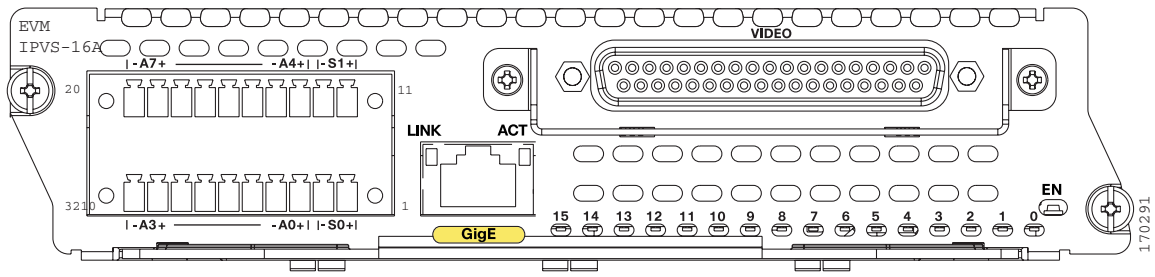


CHAPTER 39

Connecting Cisco Analog Video Gateway Network Modules

This document provides hardware information about the EVM-IPVS-16A network module, which enables Cisco integrated services routers to capture analog video signals. The EVM-IPVS-16A network module supports up to 16 simultaneous composite video inputs, such as video surveillance cameras. The EVM-IPVS-16A network module also provides alarm input detection, control relay outputs, and RS-485 serial communication interfaces. Figure 39-1 shows the EVM-IPVS-16A network module faceplate.

Figure 39-1 Cisco Analog Video Gateway Network Module (EVM-IPVS-16A) Faceplate



Tip To determine whether your Cisco router supports a specific network module, see Table 1-6 on page 1-16.

Contents

Information About the EVM-IPVS-16A Network Module

- You need a router that supports the EVM-IPVS-16A network module. For a list of supported platforms, see the *Cisco Analog Video Gateway Network Module (EVM-IPVS-16A) Data Sheet*.

Warning **Equipment connected to outdoor cameras must be permanently grounded in accordance with national and local codes.** Statement 374

Warning **Hazardous voltages may be present in the outdoor camera cables under fault conditions. Disconnect all cables from the outdoor cameras before servicing this equipment.** Statement 376

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

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

Note The compact flash module installed in the EVM-IPVS-16A network module is not field-replaceable.

Note For software-related prerequisites and restrictions, see the *Configuring the Analog Video Gateway for Integrated Service Routers* Cisco IOS feature module.

Note For EVM-IPVS-16A network module features and benefits, supported hardware and software, and other product information, see the *Cisco Analog Video Gateway Network Module (EVM-IPVS-16A) Data Sheet*.

Video Ports

16 video ports are provided, video ports 0 and 1 can be configured for input or output. The remaining 14 video ports can be configured for input only.

RS-485 Serial Communication Interfaces

The EVM-IPVS-16A network module supports a half-duplex, two-wire RS-485 communication network, which sometimes is called a ring. The EIA/TIA RS-485 communications standard supports up to 32 devices (driver/receiver pairs) on a cable of up to 4,000 feet. The EVM-IPVS-16A network module has two RS-485 ports, supporting up to 64 devices. The EVM-IPVS-16A network module typically acts as the master for each of the two RS-485 networks.

The RS-485 ports can be used to control camera pan, tilt, and zoom (PTZ) functions, as well as other RS-485 devices. Because PTZ camera types use different protocols, the EVM-IPVS-16A network module only supports pass-through mode. In pass-through mode PTZ commands and other data will not be interpreted.

Alarm Inputs and Control Relay Outputs

The EVM-IPVS-16A network module supports eight contact closure interfaces. Interfaces A0, A1, A2, and A3 can be configured as alarm input or relay output, the other interfaces are input only. They are used to detect contact trigger events and control external devices.

In most cases, the contact closure interfaces will be connected to a patch panel through the two terminal block ports on the network module. The patch panel can provide the bias to the circuit.

Caution The alarm signal input and output (I/O) connections on this unit are intended only for connection to NEC/CEC Class 2 or equivalent circuit. This means that the voltages applied to alarm signal I/O connections should not exceed 42.4 Vpk or 60 Vdc and it should be a limited/fused power source. For more details on Class 2 circuits, refer to the National Electrical Code/Canadian Electrical Code.

Table 39-1 Alarm Input and Output Interface Specifications

Specification	Range
Alarm Input Sense Voltage Range	12 V to 24 V
Alarm Output Current Load Range	0 mA to 170 mA

Gigabit Ethernet Port

The external Gigabit Ethernet port is disabled by default. If you enable the Gigabit Ethernet interface, it can act as a routable interface in your network.

EVM-IPVS-16A Network Module Connectors

The physical connectors that appear on the EVM-IPVS-16A network module are shown in Figure 39-2 and described in Table 39-2.

Figure 39-2 EVM-IPVS-16A Network Module Connectors

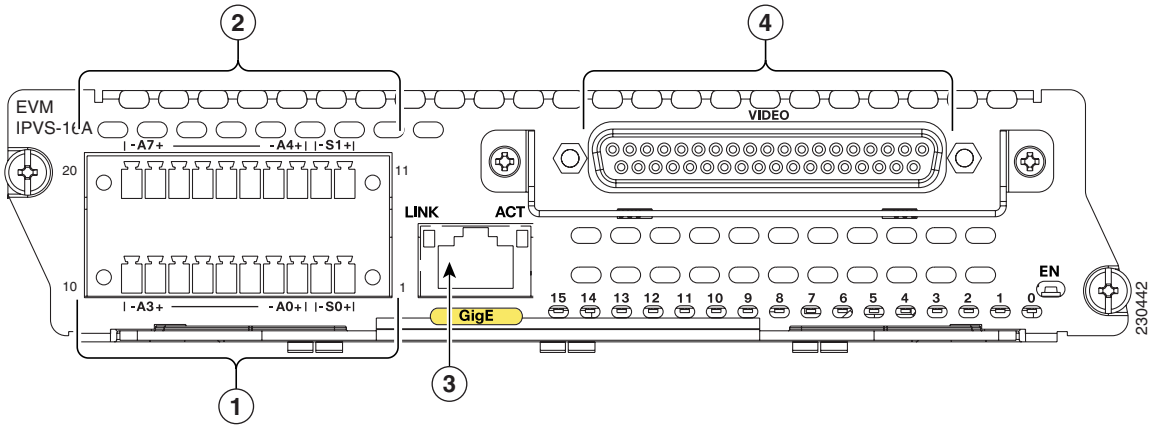


Table 39-2 EVM-IPVS-16A Network Module Connectors

Figure Ref.	Connector	Type	Connects To
1	Terminal block 0	10-input terminal block (ports A0-A3 and S0)	10-position terminal block connector (provided)
2	Terminal block 1	10-input terminal block (ports A4-A7 and S1)	10-position terminal block connector (provided)
3	Gigabit Ethernet (labeled GigE)	RJ-45 female connector	Straight-through two-pair Category 5 unshielded twisted-pair (UTP) cable
4	Video (labeled VIDEO)	DB-37 female connector	DB-37 to BNC video breakout cable (provided)

EVM-IPVS-16A Network Module LEDs

The Cisco analog video gateway network module (EVM-IPVS-16A) has LEDs which denote the status of the network module, shown in Figure 39-3 and described in Table 39-3.

Figure 39-3 EVM-IPVS-16A Network Module LEDs

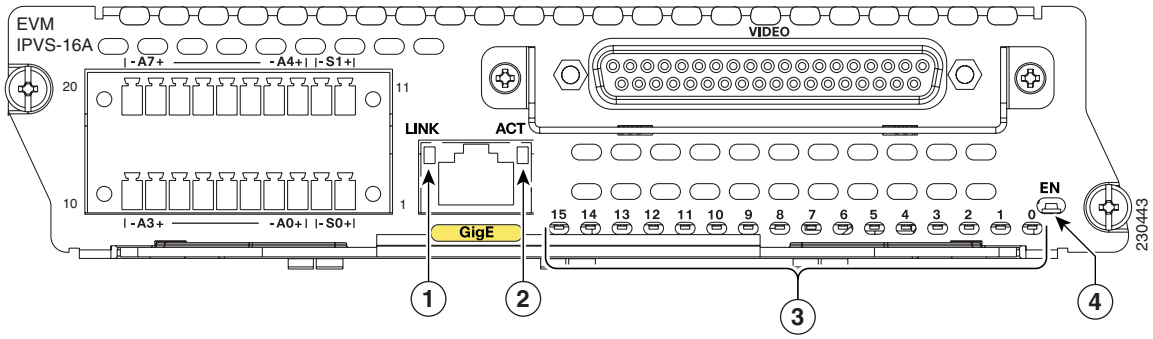


Table 39-3 EVM-IPVS-16A Network Module LED Descriptions

Figure Ref.	LED	State	Meaning	Possible Causes and Corrective Actions
1	LINK	Green	Gigabit Ethernet link is up.	Normal indication. No action required.
		Off	Gigabit Ethernet link is down.	Check Gigabit Ethernet cable connections.
2	ACT	Amber	Gigabit Ethernet link is actively transmitting or receiving.	Normal indication. No action required.
		Off	Gigabit Ethernet link is not actively transmitting or receiving.	Normal indication. No action required.
3	Video signal ports 0-15	Green	There is an active video session for this port, and input video is detected.	Normal indication. No action required.
		Amber	There is an active video session for this port, but no input video is detected.	Check the camera is on, then check the video port cable connections.
		Off	There is no active video session for this port.	Check the video port cable connections. See the "Connecting the EVM-IPVS-16A Network Module to the Network" section on page 39-7.
4	EN	On	The router's Cisco IOS software recognizes the network module.	Normal indication. No action required.
		Off	The router's Cisco IOS software does not recognize the network module.	Verify that the network module is properly installed in the router chassis. See the "Installing Cisco Network Modules in Cisco Access Routers" chapter.

How to Install, Connect, or Replace the EVM-IPVS-16A Network Module

This section contains the following procedures, each of which may or may not be required, depending on which tasks your service provider performs for you:

- Installing the EVM-IPVS-16A Network Module in the Router Chassis, page 39-6
- Connecting the EVM-IPVS-16A Network Module to the Network, page 39-7

- Performing Online Insertion and Removal of the EVM-IPVS-16A Network Module, page 39-9

Installing the EVM-IPVS-16A Network Module in the Router Chassis

To install the EVM-IPVS-16A network module in the router chassis, see the "Installing Cisco Network Modules in Cisco Access Routers" chapter of the *Cisco Network Modules Hardware Installation Guide*.

Note The EVM-IPVS-16A network module can only be installed in slots that support extension modules. For information about which slots support extension modules, see Table 1-1 on page 1-5

Wiring the Terminal Block Connectors

Wire the provided terminal block connectors using the pinout information provided in Table 39-4. (See Figure 39-4.)

Note The wires used to connect to the terminal block are required to be between 26 AWG and 18 AWG.

Figure 39-4 Wiring the Terminal Block Connectors

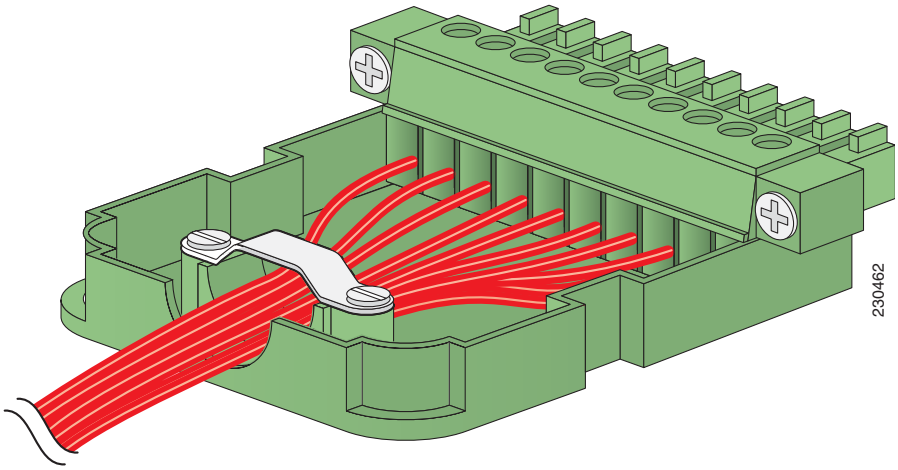


Table 39-4 lists each pin on the terminal block, and the corresponding port information.

Tip When you wire the terminal block connector, label each wire with the pin number, so you can easily connect the wires to the alarm or RS-485 devices in your network.

Note In Table 39-4 a plus (+) sign and minus (–) sign are used to note the polarity for the contact closure and RS-485 ports. For contact closure ports, pins noted with a plus sign must be connected to positive potential; pins noted with a minus sign must be connected to negative potential. For RS-485 ports, pins noted with a plus sign must be connected to an RS-485 device non-inverting terminal; pins noted with a minus sign must be connected to an RS-485 device inverting terminal.

Table 39-4 EVM-IPVS-16A Terminal Block Pinouts

Pin	Type
Terminal Block 0 (Lower)	
1	RS-485 S0 +
2	RS-485 S0 –
3	In-Out A0 +
4	In-Out A0 –
5	In-Out A1 +
6	In-Out A1 –
7	In-Out A2 +
8	In-Out A2 –
9	In-Out A3 +
10	In-Out A3 –
Terminal Block 1 (Upper)	
11	RS-485 S1 +
12	RS-485 S1 –
13	In A4 +
14	In A4 –
15	In A5 +
16	In A5 –
17	In A6 +
18	In A6 –
19	In A7 +
20	In A7 –

Connecting the EVM-IPVS-16A Network Module to the Network

This section describes how to connect the EVM-IPVS-16A network module to devices in the video surveillance network.

Note If an installation technician has already connected the EVM-IPVS-16A to the devices in your network, then do not perform this task. Instead, proceed directly to the software configuration for your EVM-IPVS-16A network module. See the *Configuring the Analog Video Gateway for Integrated Service Routers* Cisco IOS feature module.

Prerequisites

- Install the EVM-IPVS-16A network module in the router chassis. See the "Installing Cisco Network Modules in Cisco Access Routers" chapter of the *Cisco Network Modules Hardware Installation Guide*.

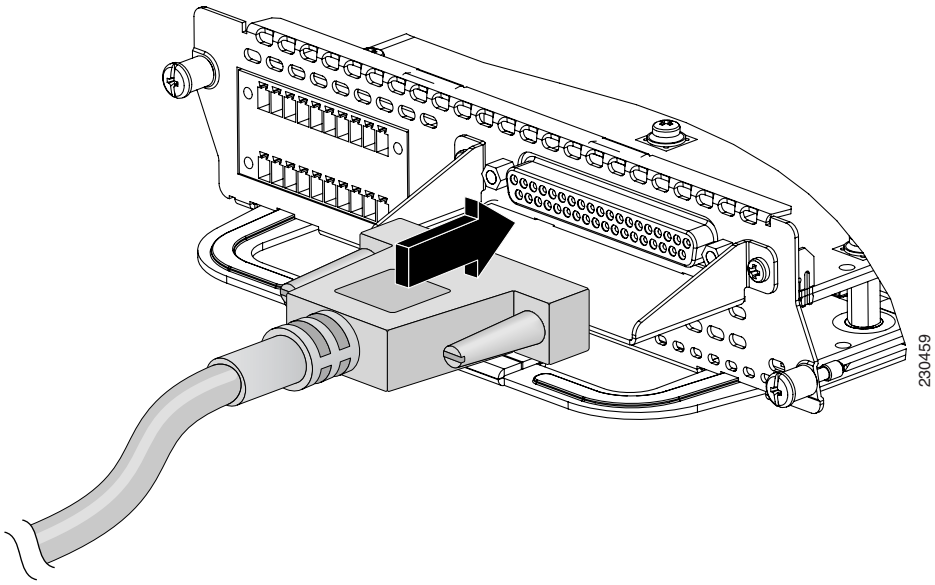
- Wire the provided terminal block connectors. See the "Wiring the Terminal Block Connectors" section on page 39-6.

Steps

To connect the EVM-IPVS-16A network module to the network, follow these steps:

Step 1 Take the DB-37 end of the provided DB-37 to BNC video breakout cable, and connect it to the VIDEO connector on the EVM-IPVS-16A network module.

Figure 39-5 Connecting the Video Breakout Cable to the EVM-IPVS-16A Network Module

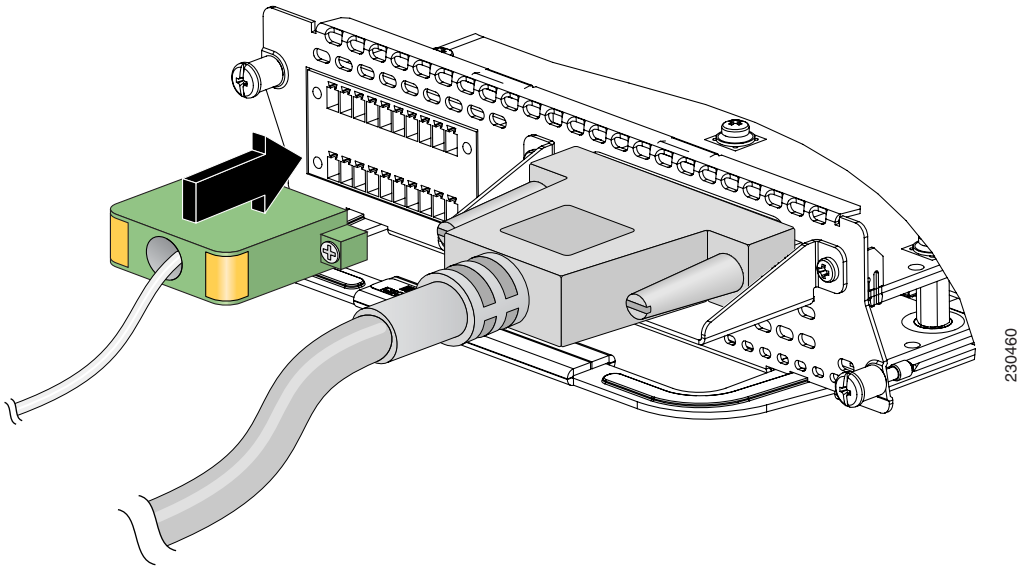


Warning **Equipment connected to outdoor cameras must be permanently grounded in accordance with national and local codes.** Statement 374

Step 2 Connect the BNC ends of the video breakout cable to the cameras in your network. The cable ends are labeled with the corresponding port number (0-15).

Step 3 After you have wired the provided terminal block connectors according to the pinout information provided in Table 39-4, connect the terminal block connectors to the terminal block on the EVM-IPVS-16A network module and tighten the screws using a small slotted screwdriver.

Figure 39-6 Connecting the Terminal Block Connectors to the EVM-IPVS-16A Network Module



Step 4 Connect the other end of the wired terminal block connectors to the RS-485 and contact closure devices in your network. In most cases, the wires will be connected to a patch panel.

Step 5 (Optional) To connect the EVM-IPVS-16A network module to an external device, use a straight-through two-pair Category 5e unshielded twisted-pair (UTP) cable, and connect the RJ-45 Gigabit Ethernet port on the network module to a switch, hub, repeater, server, or other Gigabit Ethernet network device.

What to Do Next

Proceed to the software configuration for your EVM-IPVS-16A network module. See the *Configuring the Analog Video Gateway for Integrated Service Routers* Cisco IOS feature module.

Performing Online Insertion and Removal of the EVM-IPVS-16A Network Module

The online insertion and removal (OIR) feature enables some Cisco modular access routers to support the replacement of network modules without switching off the router or affecting the operation of other interfaces. Also, routing information is maintained during OIR of network modules.

Note If your router does not support OIR, do not perform this task to replace your EVM-IPVS-16A network module. Instead, see the "Installing Cisco Network Modules in Cisco Access Routers" chapter.

Restrictions

- Only the Cisco 3845 router supports OIR of the EVM-IPVS-16A network module.
- All connections made through the EVM-IPVS-16A network module are reset during OIR.
- You must perform OIR with similar modules. If you remove a network module, install another network module exactly like it in its place.

Steps

To perform OIR of the EVM-IPVS-16A network module in your router, follow these steps:

Step 1 Initiate a console session with your router.

Step 2 Enter configuration mode and shut down the interface:

```
Router> enable
Router# configure terminal
Router(config)# interface video-Service-Engine slot/0
Router(config-if)# shut
Router(config-if)# shutdown
Router(config-if)# exit
```

Step 3 Disconnect the terminal block connector cables from the terminal blocks on the EVM-IPVS-16A network module.

Warning **Hazardous voltages may be present in the outdoor camera cables under fault conditions. Disconnect all cables from the outdoor cameras before servicing this equipment.** Statement 376

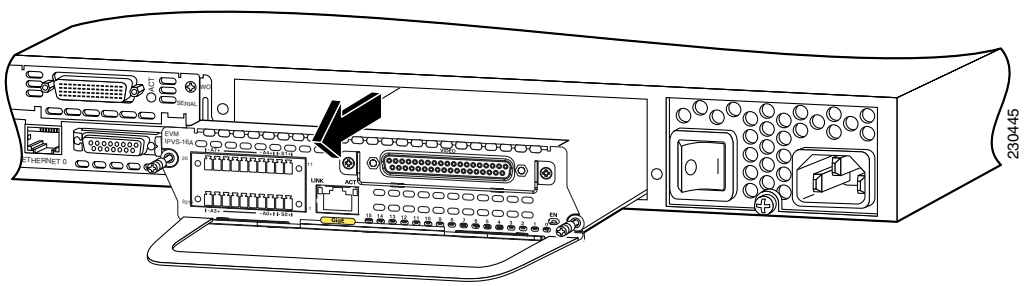
Step 4 Disconnect the DB-37 to BNC video breakout cable from the VIDEO connector on the EVM-IPVS-16A network module.

Step 5 Using a number 1 Phillips or flat-blade screwdriver, loosen the captive mounting screws on the network module faceplate.

Caution To avoid damaging the network module, always handle the network module by the handle or faceplate. Do not touch the circuit board.

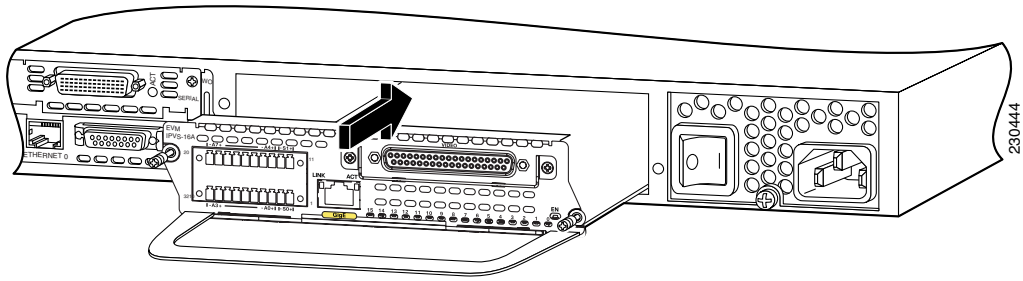
Step 6 Using the module handle, pull the network module from the router slot. (See Figure 39-7.)

Figure 39-7 Removing a Network Module



Step 7 Align the replacement network module with the guides in the chassis walls or slot divider and slide it gently into the slot. (See Figure 39-8.)

Figure 39-8 Installing a Network Module



Step 8 Using the network module handle, push the EVM-IPVS-16A network module into place until you feel the edge connector seat securely into the connector on the router backplane. The network module faceplate should contact the chassis rear panel.

Step 9 Using a number 1 Phillips or flat-blade screwdriver, tighten the captive mounting screws on the network module faceplate.

Step 10 Connect the DB-37 to BNC video breakout cable to the VIDEO connector on the EVM-IPVS-16A network module.

Step 11 Connect the terminal block connector cables to the terminal blocks on the EVM-IPVS-16A network module.

Step 12 Confirm that the network module LEDs come on. For more information about the LEDs, see the "EVM-IPVS-16A Network Module LEDs" section on page 39-4.

Step 13 Initiate a console session with your router.

Step 14 Enter configuration mode, and restart the network module:

```
Router> enable
Router# configure terminal
Router(config)# interface video-Service-Engine slot/0
Router(config-if)# no shutdown
Router(config-if)# exit
Router# service-module video-Service-Engine slot/0 reset
```

What to Do Next

Configure the new EVM-IPVS-16A network module, if changes are necessary. See the *Configuring the Analog Video Gateway for Integrated Service Routers* Cisco IOS feature module.

Related Documents

Related Topic	Document Title or URL
Regulatory compliance and safety information	*Cisco Network Modules and Interface Cards Regulatory Compliance and Safety Information*
Cisco Analog Video Gateway software website and reference documentation	*Cisco Network Modules Configuration Guides* http://www.cisco.com/en/US/products/hw/modules/ps2797/products_installation_and_configuration_guides_list.html
Cisco Video Management and Storage System software website and reference documentation	*Cisco Network Modules Configuration Guides* http://www.cisco.com/en/US/products/hw/modules/ps2797/products_installation_and_configuration_guides_list.html
Cisco Video Management and Storage System network module (NME-VMSS) hardware documentation	*Cisco Network Modules Install and Upgrade Guides* http://www.cisco.com/en/US/products/hw/modules/ps2797/prod_installation_guides_list.html
Cisco product support and technical documentation	*Product Support* http://www.cisco.com/web/psa/products/index.html
Technical documentation, including feedback and assistance	*What's New in Cisco Product Documentation* (including monthly listings of new and revised documents) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

CHAPTER 40

Cisco Video Management and Storage System Enhanced Network Modules

This chapter describes Cisco Video Management and Storage System enhanced network modules for Cisco integrated services routers, and contains the following sections:

Tip To determine whether your Cisco router supports a specific network module, see Table 1-6 on page 1-16.

Cisco Video Management and Storage System Enhanced Network Modules

The Cisco Video Management and Storage System enhanced network module is a network video recorder for Cisco integrated services routers, which archives video captured by the Cisco Analog Video Gateway network module (EVM-IPVS-16A) or other cameras connected to your network.

All models ship from the factory with the following hardware preinstalled. (See Table 40-1.)

Table 40-1 Preinstalled Hardware in Cisco Video Management and Storage System Enhanced Network Modules

Model	Processor	Hard Disk	Memory	Compact Flash
NME-VMSS-16	1.0 GHz	120 GB (SATA)	512 MB	256 MB
NME-VMSS-HP16	1.4 GHz	160 GB (SATA)	2 GB	256 MB
NME-VMSS-HP32	1.4 GHz	160 GB (SATA)	2 GB	256 MB

The Cisco Video Management and Storage System enhanced network module LEDs are shown in Figure 40-1 and described in Table 40-2.

Figure 40-1 NME-VMSS Faceplate

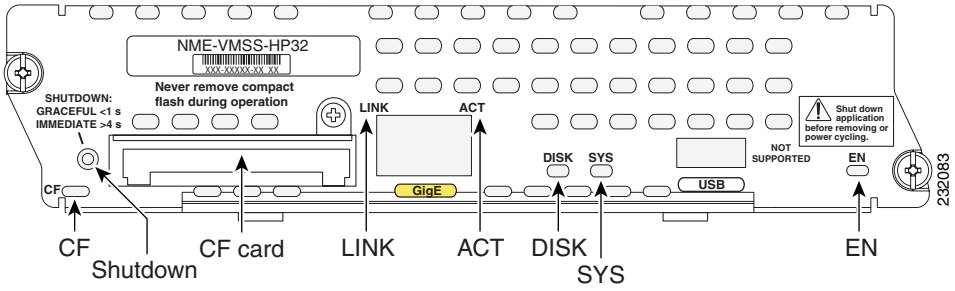


Table 40-2 NME-VMSS LED Description

CF	Status of the Compact Flash Off—Compact Flash is not used Flashing—Application detected Compact Flash at boot up
SHUTDOWN	Press the SHUTDOWN button for less than 2 seconds to gracefully shut down the module. Press the SHUTDOWN button for more than 4 seconds to cause an immediate module shutdown, which may affect file operations that are in progress.
LINK	Status of Gigabit Ethernet link On—Link is enabled Off—Link is disabled
ACT	Status of Gigabit Ethernet activity On—Active Off—Inactive
DISK	Status of hard drive activity On—Active Off—Inactive
SYS	Status of system shutdown **Note** Do not remove power without first shutting down the application. On—Application is stable. Off—System is shut down and ready for host power-down Flashing—System shutdown is in progress
EN	Status of the network module On—Detected by the host Cisco IOS software and enabled. Off—Disabled.

Shutting Down Cisco Video Management and Storage System Enhanced Network Modules

Press the SHUTDOWN button on the network module faceplate for less than 2 seconds to perform a graceful shutdown of the network module before removing power from the router or before starting an online insertion and removal (OIR) sequence on the router. The application may take up to 2 minutes to fully shut down.

Caution If you press the SHUTDOWN button for *more than 4 seconds*, a nongraceful shutdown of the hard disk will occur and may corrupt files on the network module's hard disk. After a nongraceful shutdown, the HD and SYS LEDs remain lit. Press the SHUTDOWN button for *less than 2 seconds* to gracefully reboot the network module.

Connecting Cisco Video Management and Storage System Network Modules

To connect Cisco Video Management and Storage System network modules to an external device, use a straight-through two-pair Category 5e unshielded twisted-pair (UTP) cable, and connect the RJ-45 Gigabit Ethernet port on the network module to a switch, hub, repeater, server, or other Gigabit Ethernet network device.

Note RJ-45 cables are not available from Cisco. These cables are widely available and must be Category 5e cables.

Connecting to an External Storage Device using iSCSI

The Cisco Video Management and Storage System enhanced network module supports an Internet SCSI (iSCSI) connection to an external storage device. The Gigabit Ethernet port on the faceplate of the network module and the Gigabit Ethernet port on the router can be configured as iSCSI connections.

To connect Cisco Video Management and Storage System enhanced network modules to an external storage device using iSCSI, use a straight-through two-pair Category 5e unshielded twisted-pair (UTP) cable.

Note RJ-45 cables are not available from Cisco. These cables are widely available and must be Category 5e cables.

For details about configuring iSCSI connections, see the TBD (software document) on Cisco.com:

TBD

Establishing a Gigabit Ethernet Internal Connection

Use the Cisco High-Speed Intrachassis Module Interconnect (HIMI) feature to establish a Gigabit Ethernet internal logical connection between two network modules, or between an onboard small-form-factor pluggable (SFP) Gigabit Ethernet module and a network module on a Cisco 3825 router or a Cisco 3845 router.

Connections can be established only as follows:

- Between the Gigabit Ethernet port in an installed onboard SFP module on the Cisco 3825 router or Cisco 3845 router
- Between Gigabit Ethernet interfaces in network module slots 1 and 2 on a Cisco 3825 router
- Between Gigabit Ethernet interfaces in network module slots 2 and 4 on a Cisco 3845 router

Note A module interconnection between the Gigabit Ethernet port on an SFP module on a Cisco 3825 router or a Cisco 3845 router and a network module slot *or* a network module-to-network module cross-connection is permitted at any given time. However, both types of connections cannot be implemented at the same time.

Note Connections between the onboard Ethernet ports and network module slots are not supported.

For details about configuring High-Speed Intrachassis Module Interconnect (HIMI) connections, see the *Cisco High-Speed Intrachassis Module Interconnect (HIMI) Configuration Guide* on Cisco.com:

http://www.cisco.com/en/US/products/ps5855/prod_configuration_guide09186a008068ea83.html

Online Insertion and Removal of Cisco Network Modules Procedure

Some Cisco routers allow you to replace network modules without switching off the router or affecting the operation of other interfaces. This feature is called *online insertion and removal* (OIR). OIR of a module provides uninterrupted operation to network users, maintains routing information, and ensures session preservation.

Caution Unlike other network modules, Cisco Video Management and Storage System enhanced network modules use hard disks. Online removal of network modules without proper shutdown can cause file system corruption and might render the disk unusable. You must shut down the operating system on the network module in an orderly way before removing or powering down the module.

Caution Cisco routers support OIR with identical modules only. If you remove a module, install in its place another module exactly like the one you removed. If you remove a 2-slot module (along with any installed WAN or voice interface cards), install another module and card combination exactly like the one you removed.

For a description of informational and error messages that may appear on the console during this procedure, see the hardware installation guide for your router.

To perform online removal of a network module and insertion of a replacement, follow these steps, with the router in privileged EXEC mode:

Step 1 Initiate a network module session by using the following command:

```
Router# service-module integrated-Service-Engine slot/unit session

Trying 10.10.10.1, 2065 ... Open


SE-Module> enable
SE-Module#
```

Step 2 Save the running configuration of the network module by using the following command from the `SE-Module#` prompt:

```
SE-Module# copy running-config tftp tftp-server-address filename
```

Step 3 Exit the network module session by pressing **Control-Shift-6**, followed by pressing **x**.

Step 4 On the router, clear the integrated-Service-Engine console session by using the following command:

```
Router# service-module integrated-Service-Engine slot/unit session clear
```

Step 5 Perform a graceful shutdown of the network module disk drive by using the following command:

```
Router# service-module integrated-Service-Engine slot/unit shutdown
```

Step 6 Shut down the network module interface:

```
Router (config)# interface integrated-Service-Engine slot/unit
Router (config-if)# shutdown
Router (config-if)# exit
```

Step 7 Unplug all network interface cables from the network module.

Step 8 Loosen the two captive screws that are holding the network module in the chassis slot.

Step 9 Slide the network module out of the slot.

Step 10 Align the replacement network module with the guides in the chassis slot, and slide it gently into the slot.

Note If the router is not fully configured with network modules, make sure that blank panels fill the unoccupied chassis slots to provide proper airflow.

Step 11 Push the module into place until you feel its edge connector mate securely with the connector on the backplane.

Step 12 Reconnect the network interface cables that you removed in Step 7.

Step 13 Check that the network module LEDs are on. This inspection ensures that connections are secure and that the new unit is operational.

Step 14 Initiate a network module session by using the following command:

```
Router# service-module integrated-Service-Engine slot/unit session

Trying 10.10.10.1, 2129 ... Open

SE-Module> enable
SE-Module#
```

Step 15 Restore the running configuration of the network module by using the following command from the service module prompt:

```
SE-Module# copy tftp running-config tftp-server-address filename
```

Step 16 Exit the network module session by pressing **Control-Shift-6**, followed by pressing **x**.

Step 17 On the router, clear the network module session by using the following command:

```
Router# service-module integrated-Service-Engine slot/unit session clear
```

Additional References

For additional information, see the following documents and resources.

Related Topic	Document Title
Regulatory compliance and safety information	*Cisco Network Modules and Interface Cards Regulatory Compliance and Safety Information*
Cisco Analog Video Gateway software website and reference documentation	*Cisco Network Modules Configuration Guides* http://www.cisco.com/en/US/products/hw/modules/ps2797/products_installation_and_configuration_guides_list.html
Cisco Video Management and Storage System software website and reference documentation	*Cisco Network Modules Configuration Guides* http://www.cisco.com/en/US/products/hw/modules/ps2797/products_installation_and_configuration_guides_list.html
Cisco Video Management and Storage System network module (NME-VMSS) hardware documentation	*Cisco Network Modules Install and Upgrade Guides* http://www.cisco.com/en/US/products/hw/modules/ps2797/prod_installation_guides_list.html
Cisco product support and technical documentation	*Product Support* http://www.cisco.com/web/psa/products/index.html
Technical documentation, including feedback and assistance	*What's New in Cisco Product Documentation* (including monthly listings of new and revised documents) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html