









Cisco DOCSIS®/EuroDOCSIS™
Transponder for GainMaker Nodes
Installation and Operation Guide

For Your Safety

Explanation of Warning and Caution Icons

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

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

-  You may find this symbol in the document that accompanies this product. This symbol indicates important operating or maintenance instructions.
-  You may find this symbol affixed to the product. This symbol indicates a live terminal where a dangerous voltage may be present; the tip of the flash points to the terminal device.
-  You may find this symbol affixed to the product. This symbol indicates a protective ground terminal.
-  You may find this symbol affixed to the product. This symbol indicates a chassis terminal (normally used for equipotential bonding).
-  You may find this symbol affixed to the product. This symbol warns of a potentially hot surface.
-  You may find this symbol affixed to the product and in this document. This symbol indicates an infrared laser that transmits intensity-modulated light and emits invisible laser radiation or an LED that transmits intensity-modulated light.

Important

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

Notices

Trademark Acknowledgments

- Cisco, the Cisco logo, Cisco Systems, the Cisco Systems logo, and GainMaker are trademarks or registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.
- *All other trademarks mentioned in this document are the property of their respective owners.*

Publication Disclaimer

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

Copyright

© 2012, 2014 Cisco Systems, Inc. All rights reserved. Printed in the United States of America.

Information in this publication is subject to change without notice. No part of this publication may be reproduced or transmitted in any form, by photocopy, microfilm, xerography, or any other means, or incorporated into any information retrieval system, electronic or mechanical, for any purpose, without the express permission of Cisco Systems, Inc.

Contents

Important Safety Instructions	v
Introduction	1
Description.....	3
Features	3
Part Number List	3
Transponder Diagram.....	4
Connector Summary.....	4
Installation and Configuration	7
Before You Begin.....	8
About the USB Driver	8
Important Concepts.....	8
To Install the USB Driver	8
Mounting.....	12
Transponder Mounting Location	12
To Mount the Transponder	12
To Connect the Transponder to Your Computer	13
To Reset the Transponder's IP address.....	14
Checking the LEDs	16
LED Overview	16
LED Status Summary	16
Operation	19
Preparation	20
Before You Begin.....	20
To Configure CMTS for the Transponder	20
Telnet Console Interface.....	21
About Telnet Console Interface	21
To Obtain Telnet Access.....	21
Web UI Overview	22
About Web UI.....	22
User Accounts	22
Login Management.....	23
To Log in to the Web UI.....	23
Status Information	25
Introduction.....	25
General Information	25

Connection Information.....	26
Constellation.....	27
Interpreting QAM Constellation Data by Visual Inspection.....	28
Trend Track.....	32
Event Log.....	35
Transponder Configurations.....	36
Introduction.....	36
Configuration Data.....	36
Device Files.....	37
Firmware Upgrade.....	38
DOCSIS Mode.....	39
Security.....	41
Restore Default.....	42
HSIA Diagnostics.....	45
Introduction.....	45
To Perform the Diagnostics.....	45
Device Configurations.....	46
Introduction.....	46
Status.....	46
Alarm.....	47
Reverse Switch Configuration.....	48
Device Log.....	49
Monitored and Controlled Parameters.....	50
About.....	50
Web UI Monitored Parameters.....	50
Web UI Controlled Parameters.....	51
ROSA Element Management System.....	52
About the ROSA Element Manager.....	52
To Build Connection with the ROSA Element Manager.....	52
Troubleshooting	55
Transponder Signaling.....	56
To Troubleshoot from the LEDs.....	56
Further Assistance.....	58
Contact Cisco for Support.....	58
Customer Support Information	60

Important Safety Instructions

Read and Retain Instructions

Carefully read all safety and operating instructions before operating this equipment, and retain them for future reference.

Follow Instructions and Heed Warnings

Follow all operating and use instructions. Pay attention to all warnings and cautions in the operating instructions, as well as those that are affixed to this equipment.

Terminology

The terms defined below are used in this document. The definitions given are based on those found in safety standards.

Service Personnel - The term *service personnel* applies to trained and qualified individuals who are allowed to install, replace, or service electrical equipment. The service personnel are expected to use their experience and technical skills to avoid possible injury to themselves and others due to hazards that exist in service and restricted access areas.

User and Operator - The terms *user* and *operator* apply to persons other than service personnel.

Ground(ing) and Earth(ing) - The terms *ground(ing)* and *earth(ing)* are synonymous. This document uses *ground(ing)* for clarity, but it can be interpreted as having the same meaning as *earth(ing)*.

Electric Shock Hazard

This equipment meets applicable safety standards.



WARNING:

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

Electric shock can cause personal injury or even death. Avoid direct contact with dangerous voltages at all times.

Know the following safety warnings and guidelines:

- Only qualified service personnel are allowed to perform equipment installation or replacement.

Important Safety Instructions

- Only qualified service personnel are allowed to remove chassis covers and access any of the components inside the chassis.

Equipment Placement



WARNING:

Avoid personal injury and damage to this equipment. An unstable mounting surface may cause this equipment to fall.

To protect against equipment damage or injury to personnel, comply with the following:

- Install this equipment in a restricted access location (access restricted to service personnel).
- Make sure the mounting surface or rack is stable and can support the size and weight of this equipment.

Strand (Aerial) Installation



CAUTION:

Be aware of the size and weight of strand-mounted equipment during the installation operation.

Ensure that the strand can safely support the equipment's weight.

Pedestal, Service Closet, Equipment Room or Underground Vault Installation



WARNING:

Avoid the possibility of personal injury. Ensure proper handling/lifting techniques are employed when working in confined spaces with heavy equipment.

- Ensure this equipment is securely fastened to the mounting surface or rack where necessary to protect against damage due to any disturbance and subsequent fall.
- Ensure the mounting surface or rack is appropriately anchored according to manufacturer's specifications.
- Ensure the installation site meets the ventilation requirements given in the equipment's data sheet to avoid the possibility of equipment overheating.
- Ensure the installation site and operating environment is compatible with the equipment's International Protection (IP) rating specified in the equipment's data sheet.

Connecting to Utility AC Power

Important: If this equipment is a Class I equipment, it must be grounded.

- If this equipment plugs into an outlet, the outlet must be near this equipment, and must be easily accessible.
- Connect this equipment only to the power sources that are identified on the equipment-rating label, which is normally located close to the power inlet connector(s).
- This equipment may have two power sources. Be sure to disconnect all power sources before working on this equipment.
- If this equipment **does not** have a main power switch, the power cord connector serves as the disconnect device.
- Always pull on the plug or the connector to disconnect a cable. Never pull on the cable itself.

Connection to Network Power Sources

Refer to this equipment's specific installation instructions in this manual or in companion manuals in this series for connection to network ferro-resonant AC power sources.

AC Power Shunts

AC power shunts may be provided with this equipment.

Important: The power shunts (where provided) must be removed before installing modules into a powered housing. With the shunts removed, power surge to the components and RF-connectors is reduced.



CAUTION:

RF connectors and housing seizure assemblies can be damaged if shunts are not removed from the equipment before installing or removing modules from the housing.

Grounding (Utility AC Powered Equipment in Pedestals, Service Closets, etc.)

This section provides instructions for verifying that the equipment is properly grounded.

Safety Plugs (USA Only)

This equipment is equipped with either a 3-terminal (grounding-type) safety plug or a 2-terminal (polarized) safety plug. The wide blade or the third terminal is provided for safety. Do not defeat the safety purpose of the grounding-type or polarized

Important Safety Instructions

safety plug.

To properly ground this equipment, follow these safety guidelines:

- **Grounding-Type Plug** - For a 3-terminal plug (one terminal on this plug is a protective grounding pin), insert the plug into a grounded mains, 3-terminal outlet.

Note: This plug fits only one way. If this plug cannot be fully inserted into the outlet, contact an electrician to replace the obsolete 3-terminal outlet.

- **Polarized Plug** - For a 2-terminal plug (a polarized plug with one wide blade and one narrow blade), insert the plug into a polarized mains, 2-terminal outlet in which one socket is wider than the other.

Note: If this plug cannot be fully inserted into the outlet, try reversing the plug. If the plug still fails to fit, contact an electrician to replace the obsolete 2-terminal outlet.

Grounding Terminal

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

Safety Plugs (European Union)


- **Class I Mains Powered Equipment** – Provided with a 3-terminal AC inlet and requires connection to a 3-terminal mains supply outlet via a 3-terminal power cord for proper connection to the protective ground.

Note: The equipotential bonding terminal provided on some equipment is not designed to function as a protective ground connection.

- **Class II Mains Powered Equipment** – Provided with a 2-terminal AC inlet that may be connected by a 2-terminal power cord to the mains supply outlet. No connection to the protective ground is required as this class of equipment is provided with double or reinforced and/or supplementary insulation in addition to the basic insulation provided in Class I equipment.

Note: Class II equipment, which is subject to EN 50083-1, is provided with a chassis mounted equipotential bonding terminal. See the section titled **Equipotential Bonding** for connection instructions.

Equipotential Bonding

If this equipment is equipped with an external chassis terminal marked with the IEC 60417-5020 chassis icon () , the installer should refer to CENELEC standard EN 50083-1 or IEC standard IEC 60728-11 for correct equipotential bonding connection instructions.

General Servicing Precautions



WARNING:

Avoid electric shock! Opening or removing this equipment's cover may expose you to dangerous voltages.



CAUTION:

These servicing precautions are for the guidance of qualified service personnel only. To reduce the risk of electric shock, do not perform any servicing other than that contained in the operating instructions unless you are qualified to do so. Refer all servicing to qualified service personnel.

Be aware of the following general precautions and guidelines:

- **Servicing** - Servicing is required when this equipment has been damaged in any way, such as power supply cord or plug is damaged, liquid has been spilled or objects have fallen into this equipment, this equipment has been exposed to rain or moisture, does not operate normally, or has been dropped.
- **Wristwatch and Jewelry** - For personal safety and to avoid damage of this equipment during service and repair, do not wear electrically conducting objects such as a wristwatch or jewelry.
- **Lightning** - Do not work on this equipment, or connect or disconnect cables, during periods of lightning.
- **Labels** - Do not remove any warning labels. Replace damaged or illegible warning labels with new ones.
- **Covers** - Do not open the cover of this equipment and attempt service unless instructed to do so in the instructions. Refer all servicing to qualified service personnel only.
- **Moisture** - Do not allow moisture to enter this equipment.
- **Cleaning** - Use a damp cloth for cleaning.
- **Safety Checks** - After service, assemble this equipment and perform safety checks to ensure it is safe to use before putting it back into operation.

Electrostatic Discharge

Electrostatic discharge (ESD) results from the static electricity buildup on the human body and other objects. This static discharge can degrade components and cause failures.

Take the following precautions against electrostatic discharge:

- Use an anti-static bench mat and a wrist strap or ankle strap designed to safely

Important Safety Instructions

ground ESD potentials through a resistive element.

- Keep components in their anti-static packaging until installed.
- Avoid touching electronic components when installing a module.

Fuse Replacement

To replace a fuse, comply with the following:

- Disconnect the power before changing fuses.
- Identify and clear the condition that caused the original fuse failure.
- Always use a fuse of the correct type and rating. The correct type and rating are indicated on this equipment.

Batteries

This product may contain batteries. Special instructions apply regarding the safe use and disposal of batteries:

Safety

- Insert batteries correctly. There may be a risk of explosion if the batteries are incorrectly inserted.
- Do not attempt to recharge 'disposable' or 'non-reusable' batteries.
- Please follow instructions provided for charging 'rechargeable' batteries.
- Replace batteries with the same or equivalent type recommended by manufacturer.
- Do not expose batteries to temperatures above 100°C (212°F).

Disposal

- The batteries may contain substances that could be harmful to the environment
- Recycle or dispose of batteries in accordance with the battery manufacturer's instructions and local/national disposal and recycling regulations.



廢電池請回收

- The batteries may contain perchlorate, a known hazardous substance, so special handling and disposal of this product might be necessary. For more information about perchlorate and best management practices for perchlorate-containing substance, see www.dtsc.ca.gov/hazardouswaste/perchlorate.

Modifications

This equipment has been designed and tested to comply with applicable safety, laser safety, and EMC regulations, codes, and standards to ensure safe operation in its intended environment. Refer to this equipment's data sheet for details about regulatory compliance approvals.

Do not make modifications to this equipment. Any changes or modifications could void the user's authority to operate this equipment.

Modifications have the potential to degrade the level of protection built into this equipment, putting people and property at risk of injury or damage. Those persons making any modifications expose themselves to the penalties arising from proven non-compliance with regulatory requirements and to civil litigation for compensation in respect of consequential damages or injury.

Accessories

Use only attachments or accessories specified by the manufacturer.

Electromagnetic Compatibility Regulatory Requirements

This equipment meets applicable electromagnetic compatibility (EMC) regulatory requirements. Refer to this equipment's data sheet for details about regulatory compliance approvals. EMC performance is dependent upon the use of correctly shielded cables of good quality for all external connections, except the power source, when installing this equipment.

- Ensure compliance with cable/connector specifications and associated installation instructions where given elsewhere in this manual.

EMC Compliance Statements

Where this equipment is subject to USA FCC and/or Industry Canada rules, the following statements apply:

FCC Statement for Class A Equipment

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 this 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.

Important Safety Instructions

Industry Canada - Industrie Canadienne Statement

This apparatus complies with Canadian ICES-003.
Cet appareil est conforme à la norme NMB-003 du Canada.

CENELEC/CISPR Statement with Respect to Class A Information Technology Equipment

This is a Class A equipment. In a domestic environment this equipment may cause radio interference in which case the user may be required to take adequate measures.

1

Introduction

Overview

The Cisco DOCSIS/EuroDOCSIS Transponder for GainMaker offers both online and local monitoring and control capabilities for Cisco GainMaker Nodes deployed in the DOCSIS/EuroDOCSIS network.

Purpose

This guide provides instructions for installing, configuring, setting up, and troubleshooting the DOCSIS/EuroDOCSIS Transponder for GainMaker.

Who Should Use This Document

This document is intended for authorized service personnel who have experience working with similar equipment. The service personnel should have appropriate background and knowledge to complete the procedures described in this document.

Qualified Personnel



WARNING:

Allow only qualified and skilled personnel to install, operate, maintain, and service this product. Otherwise, personal injury or equipment damage may occur.

Only appropriately qualified and skilled personnel should attempt to install, operate, maintain, and service this product.

Scope

This guide discusses the following topics.

- Description of the transponder
- Installing and configuring the transponder
- Operating the transponder
- Troubleshooting the transponder
- Customer support information

Document Version

This is the first release of this guide.

In This Chapter

- Description..... 3

Description

This chapter provides an overview of this guide and of the Cisco DOCSIS/EuroDOCSIS Transponder for GainMaker Nodes, including general descriptions, transponder overview, and connector summary.

Features

The Cisco DOCSIS/EuroDOCSIS transponder for GainMaker Nodes offers monitoring and control capabilities for Cisco GainMaker Nodes deployed in DOCSIS/EuroDOCSIS networks, has the following features:

- **Network Environment:** Works in DOCSIS/EuroDOCSIS 2.0 networks, and also works in DOCSIS/EuroDOCSIS 1.0, 1.1 and 3.0 environments.
- **Network Management:** Complies with the DOCSIS/EuroDOCSIS Standard to monitor the devices in a CATV network.
- **Firmware Upgrade:** Supports firmware download for new features and applications, either locally or remotely.
- **Configurable:** Supports local control of the transponder parameters via an embedded web server.
- **Compatible with Other Transponders:** Complies with SCTE's HMS standard for monitoring devices in HFC networks and allows seamless integration with existing HMS management systems. Upgrade of existing deployments with DOCSIS/EuroDOCSIS transponders is fully supported.
- **Hot-pluggable:** Supports hot-plugging during system operation.
- **LED Indications:** Supports full indications of power, upstream/downstream active, online, USB and status with 6 LEDs.
- **High Performance:** Fully-integrated broadband tuner is optimized for high performance data application in a DOCSIS network. The transponder is temperature-hardened allowing for operation in outdoor conditions.
- **Power-saving:** Less than 3 W power consumption for whole transponder.

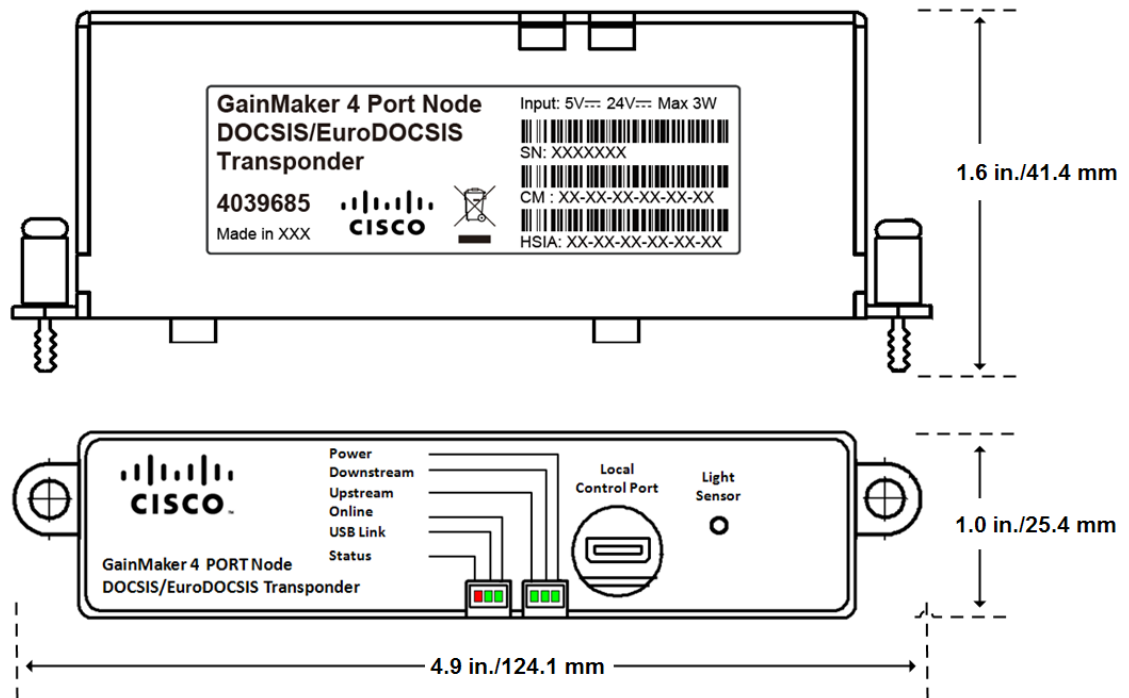
Part Number List

For the latest DOCSIS/EuroDOCSIS Transponder available part number, contact your customer service representative for details.

Description	Part Number
DOCSIS/EuroDOCSIS Transponder for GainMaker 4-Port Node	4039676
DOCSIS/EuroDOCSIS Transponder for all other GainMaker Nodes	4039677

Transponder Diagram

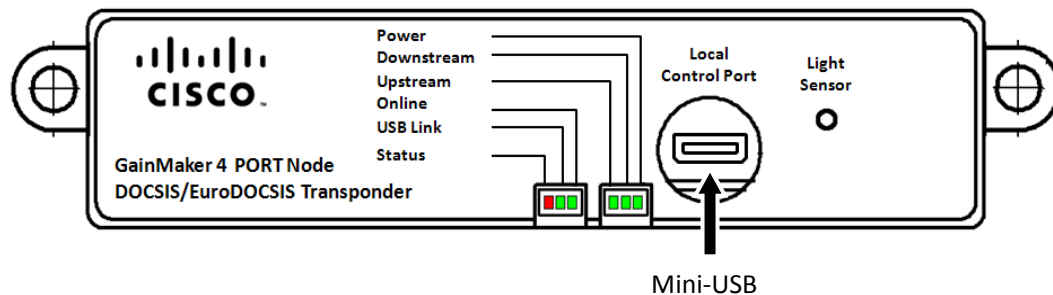
The following diagram shows an overview of the DOCSIS/EuroDOCSIS transponder including its dimensions.



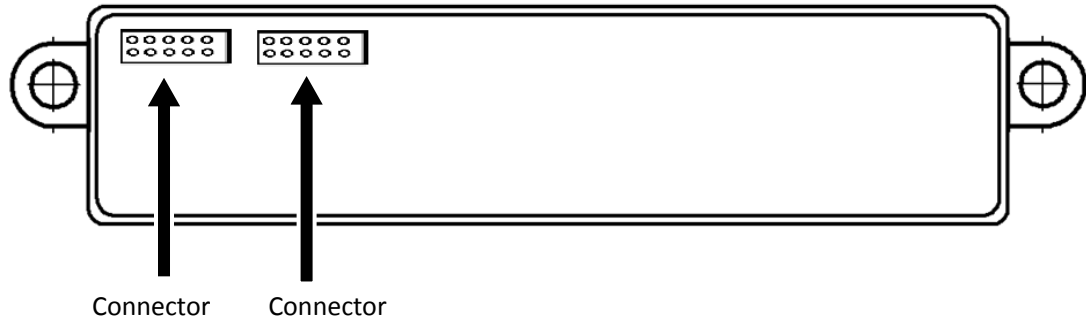
Connector Summary

The following tables and diagrams show all the connector interfaces of the DOCSIS/EuroDOCSIS transponder.

Connector	Description
Mini-USB	The Mini-USB port provides a local, physical connection to the transponder. In addition, the Mini-USB port is a fully functional virtual Ethernet port capable of providing all the functionality of any standard Ethernet connection.



Connector	Description
INTERFACE CONNECTOR	The Interface Connector is the physical connection point at which the transponder is installed in the device.



2

Installation and Configuration

Introduction

This chapter provides instructions for installing the transponder in the node and verifying the connection status through checking the LEDs.

In This Chapter

- Before You Begin..... 8
- Mounting..... 12
- Checking the LEDs 16

Before You Begin

The procedures in this chapter assume that you have completed the following:

- Prepared the installation site
- Prepared the Cisco GainMaker Node to install the transponder
- Install the node correctly

About the USB Driver

The USB driver is a Cisco standard driver which enables your computer to build virtual Ethernet connection with the transponder.

Before you start, make sure that you have installed the USB driver.

System Compliance

The USB driver is tested to support the operating system including 32-bit Windows XP, Windows 2000, Windows Server 2000/2003, and Linux. For Windows 7, a standard driver for Remote NDIS Compatible Device can be used. For any other system, please consult your system administrator before operation.

Important Concepts

The following items have been defined in this guide.

- **Transponder:** The DOCSIS/EuroDOCSIS transponder.

To Install the USB Driver

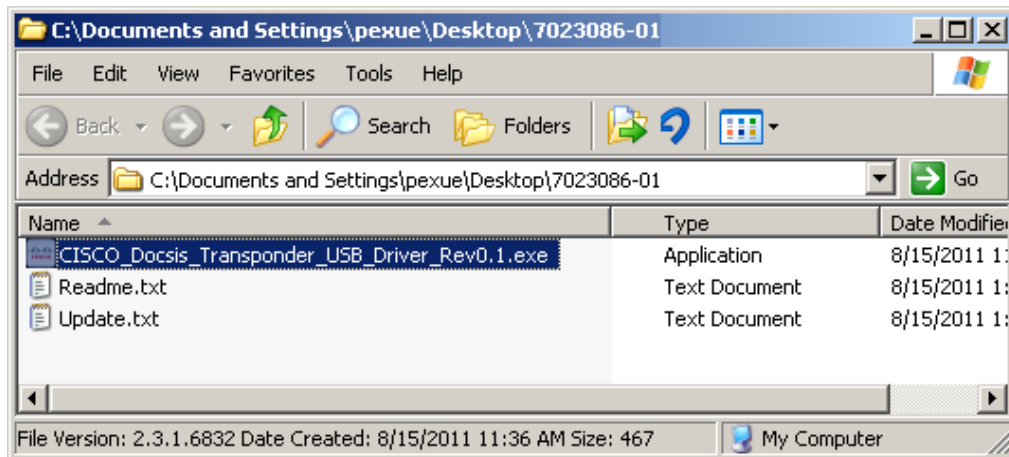
For 32-bit Windows XP, Windows 2000, and Windows Server 2000/2003, follow the steps below to install the USB driver.

1. Register or use the existing account to log on to Cisco.com.
2. Click on the following address to find the USB driver

[http://www.cisco.com/cisco/software/navigator.html?mdfid=281510329&i=r
m](http://www.cisco.com/cisco/software/navigator.html?mdfid=281510329&i=r
m)

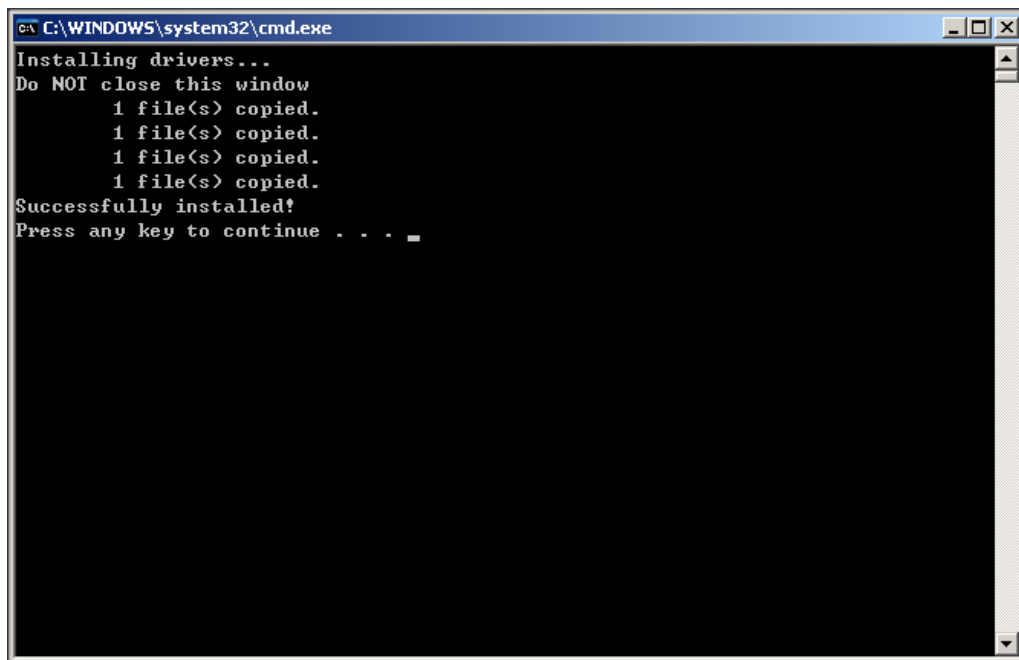
3. Download the USB driver software.
4. Double click on the execution file to install the USB driver software.

Note: System administrator privilege is required to install the driver.



5. Wait for several seconds to finish the installation.

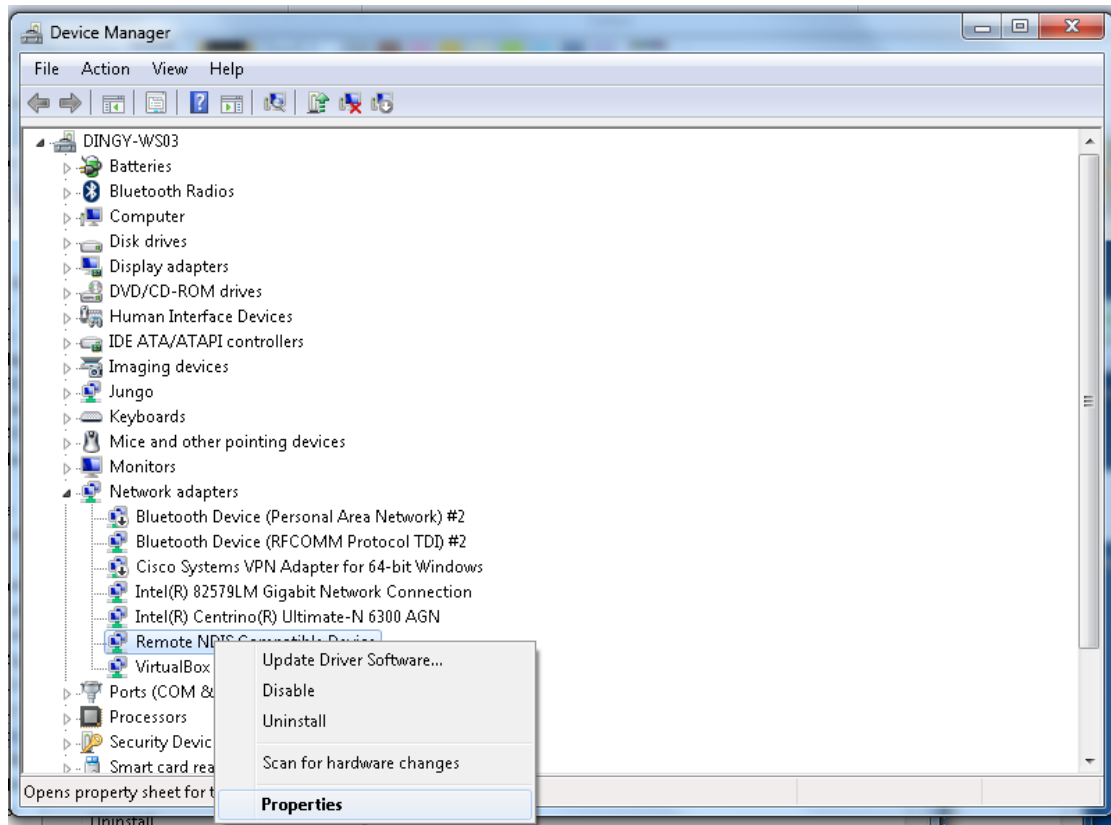
Result: The following successful installed page is displayed.



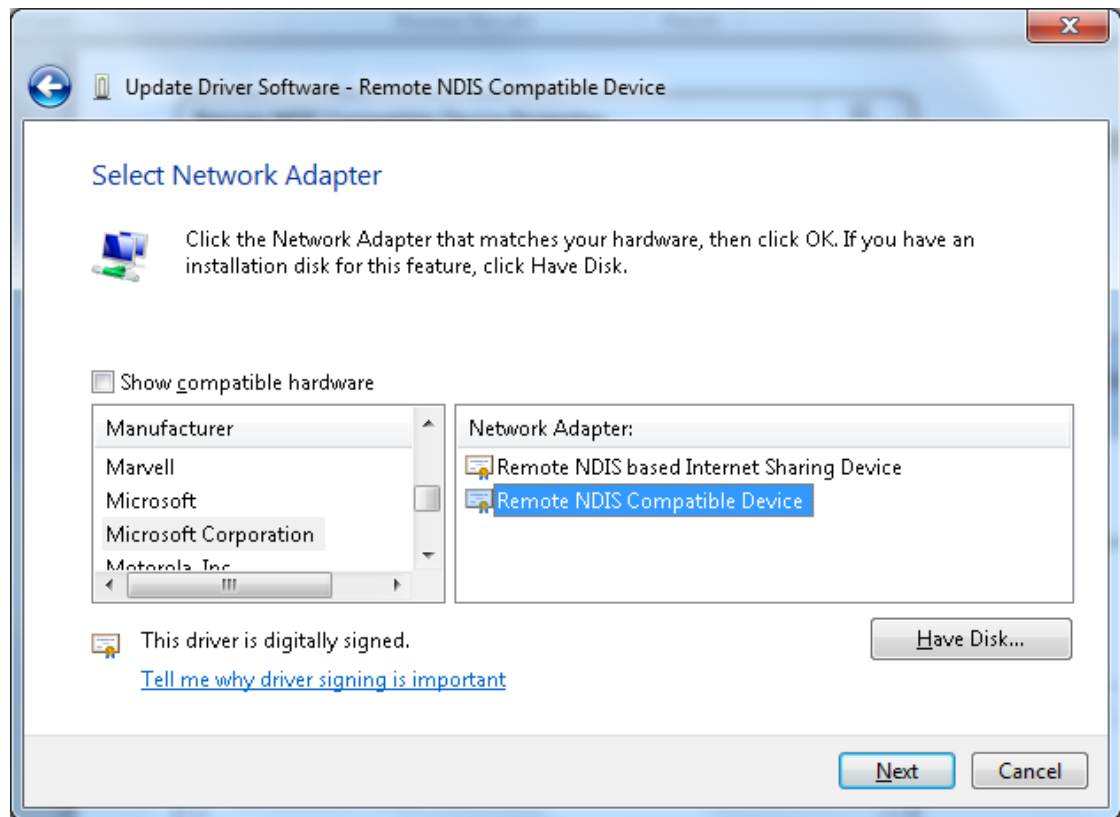
6. Proceed to the next step.

For Window 7, follow the steps below to install the USB driver:

1. Go to Device Manager (Right click on **My Computer**, select **Properties** from the menu, and click on **Device Manager** on the left).
2. Expand Network adapters. And right click on the Remote NDIS Compatible device (DOCSIS transponder USB driver), select **Properties**.



3. Click **Update Driver** under Driver tab, and select **Browse my computer for driver software**, then select **Let me pick from a list of device drivers on my computer**.
4. Uncheck the **Show compatible hardware** checkbox. Select **Microsoft Corporation** in Manufacturer. And select **Remote NDIS Compatible Device** in Network Adapter. Click the **Next** button.

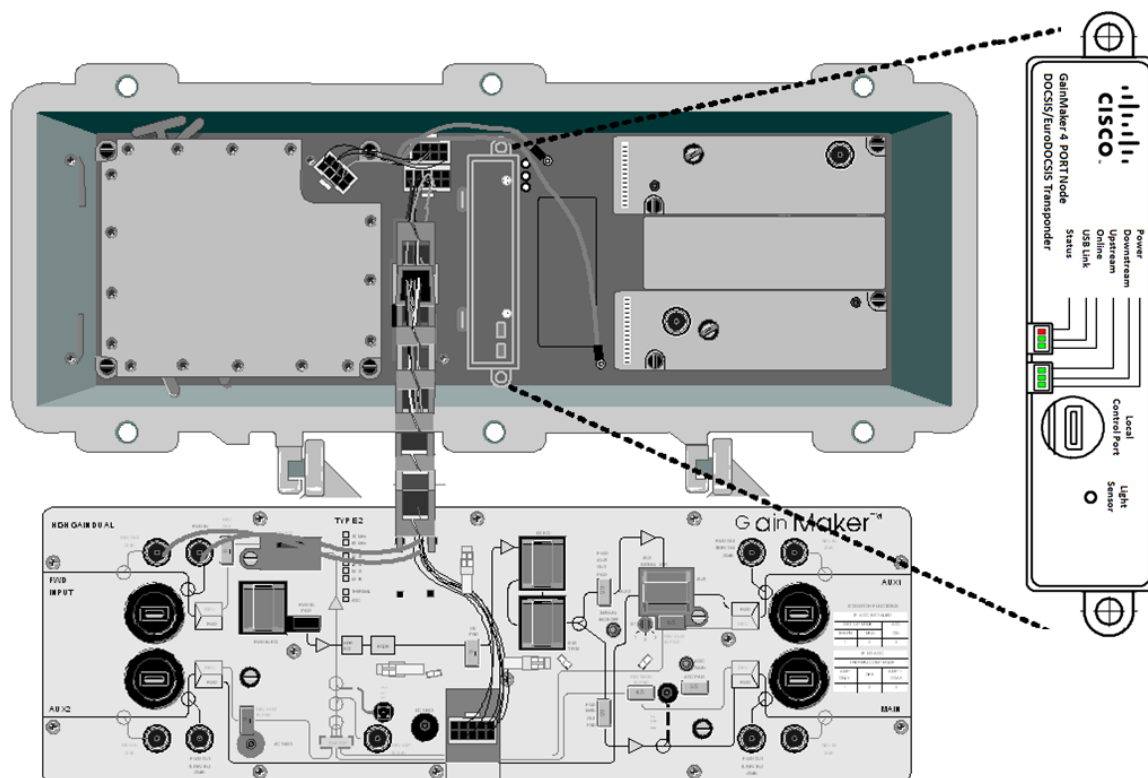


5. Click **Yes** to upgrade the driver.
6. Wait for several seconds to finish the installation.

Mounting

Transponder Mounting Location

The transponder module mounts in the lid of the GainMaker node housing. The transponder mounting location is shown below.



Note: You must mount the transponder module in the GainMaker Node housing before you can configure the transponder module.



WARNING:

Confirm the correct transponder type for your GainMaker Node before installation! Damage may be caused by mounting the wrong type of transponder!

To Mount the Transponder

Mounting Steps:

1. Open the GainMaker node housing. Note the position and orientation of the transponder in the lid of the housing.

**WARNING:**

Protect yourself from electric shock and your system from damage. Take precautions when working with this equipment. Certain components can deliver electrical shock or cause burns.

2. Position the transponder module with the Cisco label facing you. Align the connectors on the other side of the transponder module with the mating connectors on the interface board. Use the two tabs on the other side of the transponder as a guide to position the transponder module correctly.

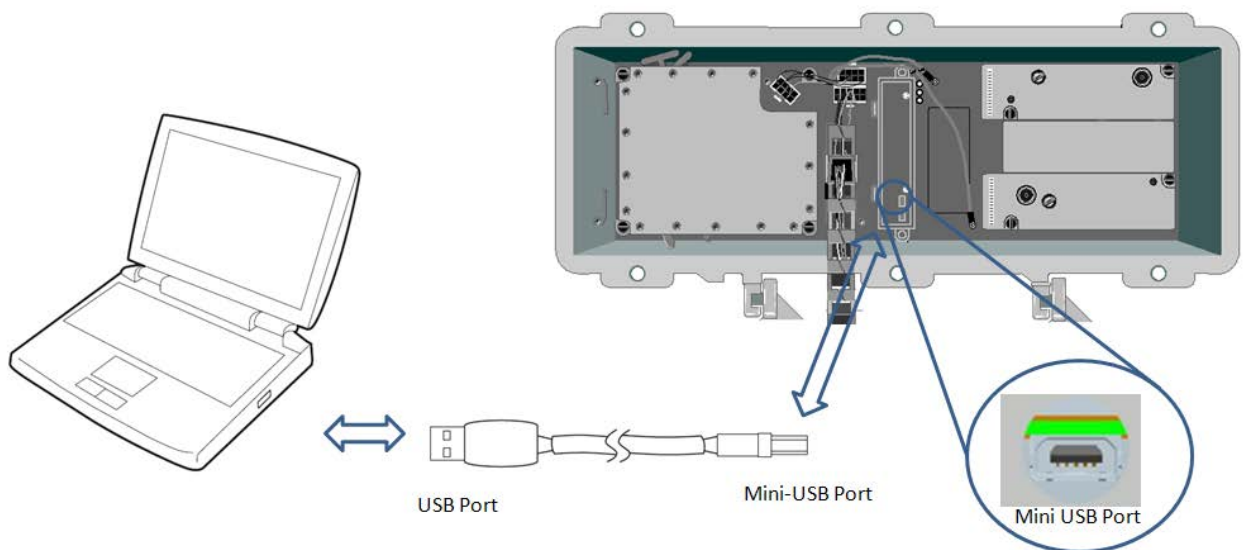
Note: If the transponder is mounted to the GainMaker in an operating HFC system, certain LEDs will flash to display the startup process, the upstream and downstream status. See the **Checking the LEDs** section the I&O Guide for details.

3. Push down on the module of the transponder module until it clicks into place.
4. Tighten the two module retaining screws on the transponder to 6.2 in-lb (0.7 Nm).

To Connect the Transponder to Your Computer

Required Tools: Prepare the USB cable as the following diagram. One end of the cable is USB port and the other end is mini-USB port.

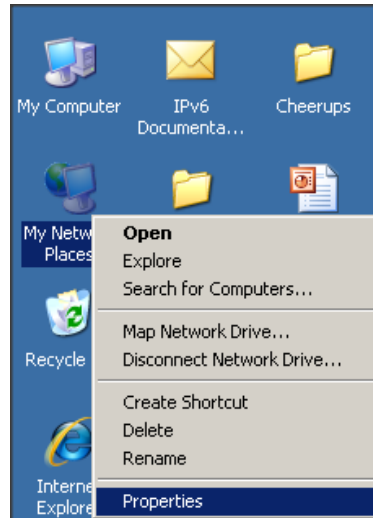
1. Connect the USB port of the USB cable to your computer.
2. Connect the mini-USB port of the USB cable to the transponder.



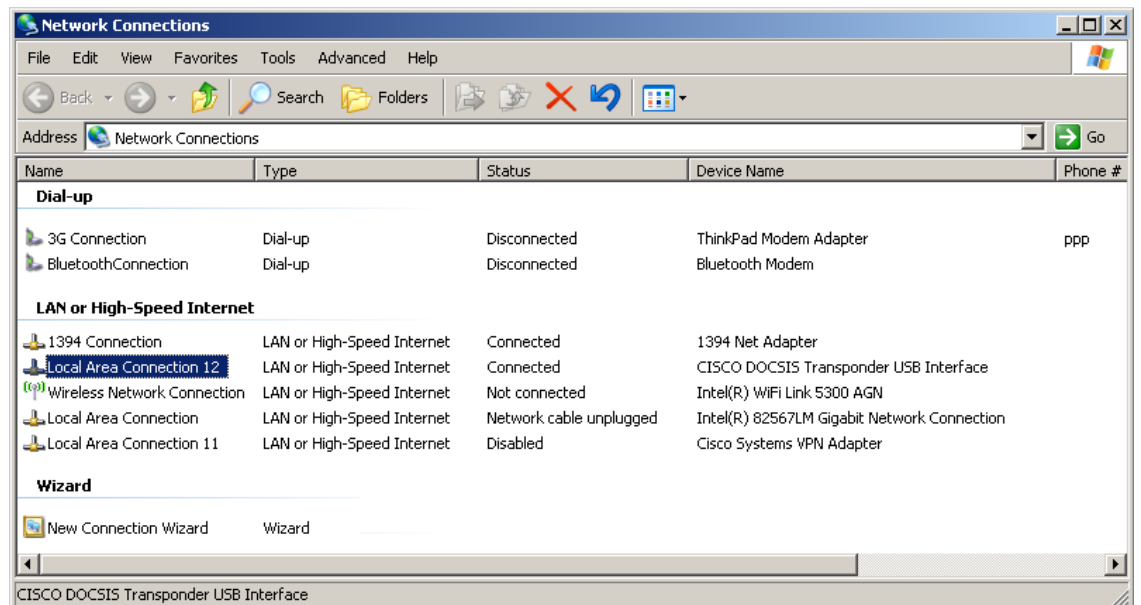
To Reset the Transponder's IP address

The following steps are recommended in order to set and record the IP address of the network adapter.

1. Right click on **My Network places** on your desktop.

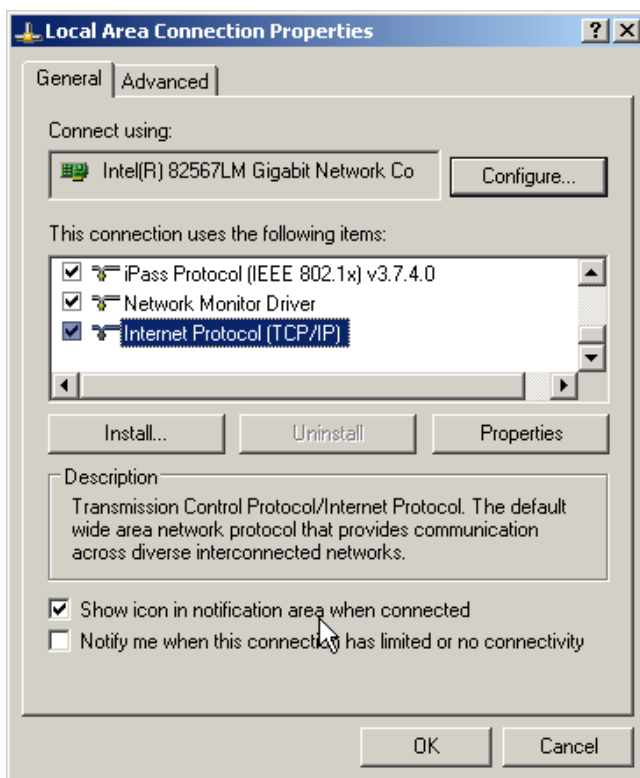


2. Click the **Properties** tab to open the **Network Connections** interface.

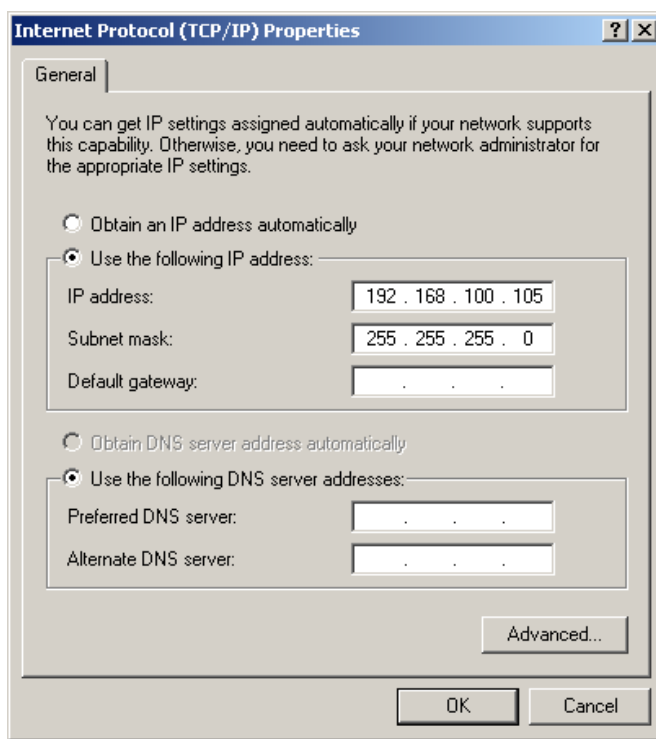


3. Double click on the local area connection with the device name “CISCO DOCSIS Transponder USB Interface”.

Result: The local area connection properties page is displayed.



4. Scroll down and double click on **Internet Protocol (TCP/IP)**.
5. Reset the IP address of the network adapter to the same address field with the transponder. (The default address of the transponder is 192.168.100.1.)



6. Click **OK** and proceed to the next step.

Checking the LEDs

LED Overview

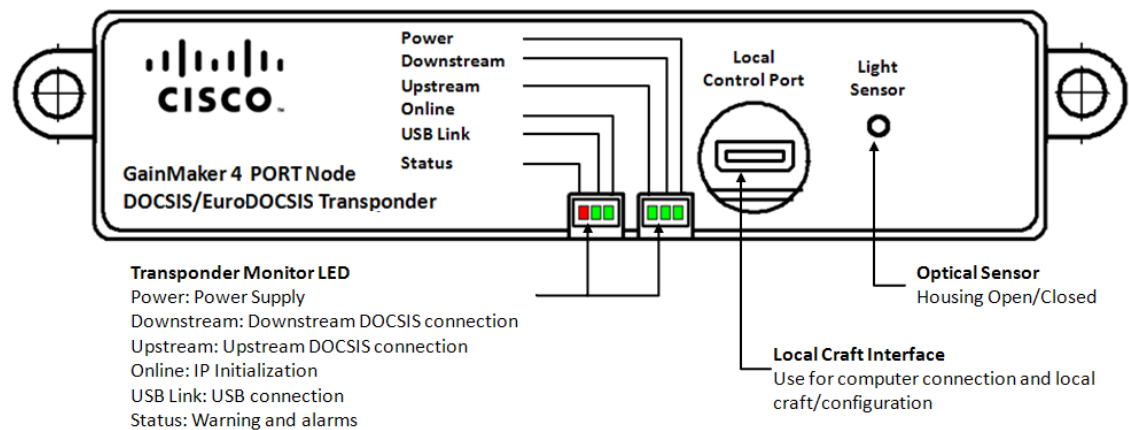
The DOCSIS/EuroDOCSIS transponder includes 6 LEDs on its monitoring interface:

Item	Description
LED Indicators	<p>The transponder includes six LEDs:</p> <ul style="list-style-type: none"> • POWER (Green) • DS (Green) • US (Green) • ONLINE (Green) • USB (Green) • STATUS (Red) <p>These indicate transponder status.</p>

On initial power up, the LEDs will remain off for several seconds after which time the DS, US, and Online LEDs will blink in unison six times. After this sequence completes, the LEDs indicate the status.

The POWER, DS, US, ONLINE, USB and STATUS LEDs conform to the DOCSIS OSSI specification.

The front-panel LEDs indicate the transponder operating condition.



LED Status Summary

The following table summarizes the meaning of the status LEDs.

LED	Function	State	Description
-----	----------	-------	-------------

POWER	Power LED	OFF	The transponder is switched off or is not functioning.
		ON	The transponder is powered on.
DS	Downstream LED Status of downstream scanning and synchronization	Blinking	The transponder is scanning for a downstream DOCSIS channel.
		ON	The transponder has locked onto and synchronized with a downstream DOCSIS channel.
US	Upstream LED Status of downstream scanning and synchronization	Blinking	The transponder is scanning for an upstream DOCSIS channel.
		ON	The transponder has locked onto and synchronized with an upstream DOCSIS channel.
Online	Online LED: Status of the IP initialization process	Blinking	The transponder is currently requesting IP address.
		ON	The transponder has completed the IP initialization process and is operational.
USB	USB LED: Status of the USB connection	Blinking	The transponder is sending or receiving data.
		OFF	The USB is disconnected.
STATUS	STATUS LED: Status of the specifications and properties of the transponder This LED is red to highlight warnings.	OFF	The transponder is currently working in normal status.
		ON	The transponder's specs or properties exceeded certain restrictions and certain alarms are triggered. Note: The status LED is turned on automatically for both major and minor alarms. See the Alarm section for more details.

3

Operation

Introduction

This section provides information on how to configure the transponder via its internal management system using a laptop or PC. Through configuring the transponder, you are able to observe and/or configure the transponder settings, perform the High Speed Internet Access (HSIA) diagnostics and view and/or set the settings of the device.

In This Chapter

■ Preparation	20
■ Telnet Console Interface	21
■ Web UI Overview	22
■ Login Management.....	23
■ Status Information	25
■ Transponder Configurations.....	36
■ HSIA Diagnostics.....	45
■ Device Configurations	46
■ Monitored and Controlled Parameters.....	50
■ ROSA Element Management System.....	52

Preparation

Before You Begin

Before you begin, it is important to review and understand the following information.



CAUTION:

Make sure the device is connected to a working CMTS and receiving proper input signals before you configure the transponder.



CAUTION:

For SNMP access, UDP ports 161 and 162 must not be blocked.

To Configure CMTS for the Transponder

Before you begin, make sure you have downloaded the Euro-DOCSIS/DOCSIS root certificate and configured your CMTS successfully.

Refer to the **Downloading the DOCSIS Root Certificate to the CMTS** section in the document *DOCSIS 1.1 for the Cisco CMTS* of the profile *Cisco CMTS Feature Guide* to configure your CMTS before installing the transponder in the CMTS network. The above document is applicable for both Euro-DOCSIS and DOCSIS root certificates.

The document is stored in the following address on Cisco.com:

http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_docs.html#wp1217174

Telnet Console Interface

About Telnet Console Interface

Telnet is a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communications facility using a virtual terminal connection over the Transmission Control Protocol (TCP).

Cisco Euro-DOCSIS/DOCSIS transponder allows to build TCP/IP connection for local area network craft configuration through telnet connections through the transponder's embedded telnet server.

Transponder receives telnet access through port 23.



CAUTION:

Telnet access is only intended for use by advanced technicians. Thus access is allowed only for authorized users.

Any other users please ignore this section and see the Web UI section on the full configuration of the transponders and devices.

To Obtain Telnet Access

Telnet access supports a number of commands that are used for troubleshooting and debugging purposes. Providing a list and description of all of the available commands would exceed the scope of this manual. For additional information about the use of the console commands, contact Technical Support using the contact information provided in *Technical Contact Information* (on page 5-1).

Web UI Overview

About Web UI

The transponder firmware integrates the Web User Interface (UI) into the web browser as its internal management system.

The Web UI contains the interface to view and configure all the transponder configurations including the IP addresses of the transponder and the server, the status data...etc, of the devices.

System Compliance

The web UI is tested to support the internet explorer applications including Microsoft Windows Internet Explorer (IE) 7.0 and above, Firefox Mozilla 10.0 and above. For any other explorer, please consult your system administrator before operating.

User Accounts

The Web UI includes user account privileges of Administrator, user and viewer. The following table lists the user account privileges of each user account.

Note: In normal cases, user account provides all the necessary functions for operation of the transponder and devices. Thus an administrator account is not given to end users. See *Technical Contact Information* on page 5-1 to request the administrator account privileges from our service consultant for emergent operations. Make sure to switch to account with the required privileges before configuring certain parameters on the transponder or the device with the transponder installed.

Operation	Administrator	User	Guest
Authorize Access	Allowed	Not Allowed	Not Allowed
Reset Password	Allowed	Not Allowed	Not Allowed
Change Password	Allowed	Allowed	Not Allowed
View Transponder's Parameters	Allowed	Allowed	Allowed
Configure Transponder's Parameters	Allowed	Allowed	Not Allowed
View Device Parameters	Allowed	Allowed	Allowed
Configure Device Parameters	Allowed	Allowed	Not Allowed

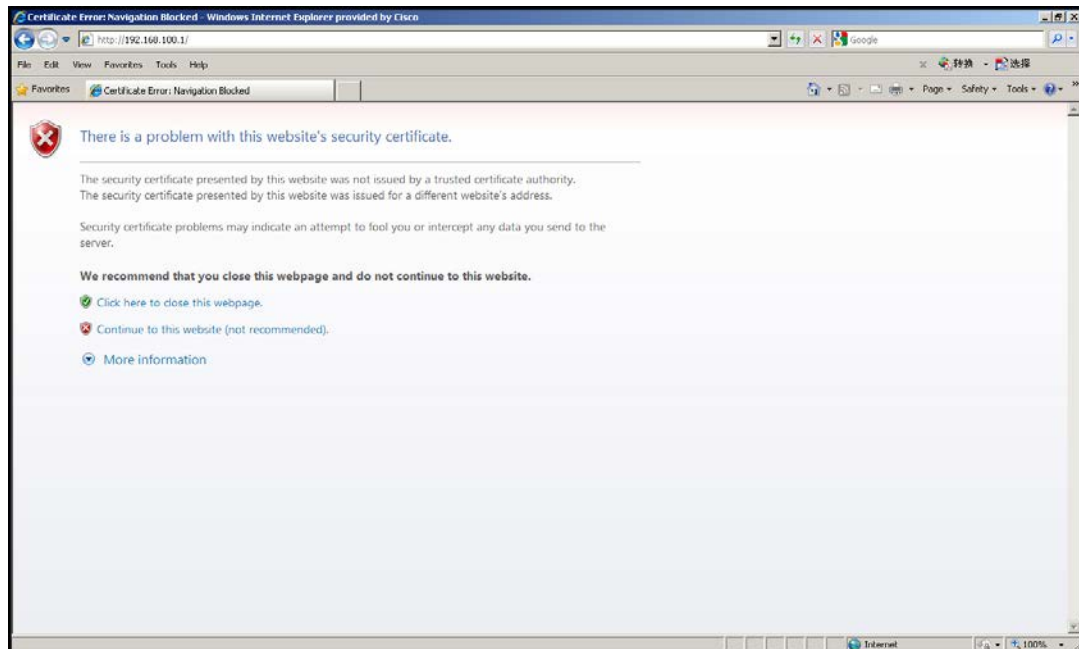
Login Management

To Log in to the Web UI

The following steps describe how to login to the Web UI via the web browser.

1. Refer to the **Mounting** section, on page 2-3 to connect the transponder to your PC with the USB cable.
2. Start the Internet Explorer application.
3. Type the URL `http://192.168.100.1` in the browsing window, which is the default IP address of the transponder.
4. Click **Enter**.

Note: A warning window about security certificate might be displayed. Since this is not relevant, just ignore the warning and click **Continue to This Website**.



Result: The login window is displayed.



5. Type the user name and password in the appropriate text box.

The factory default user accounts for the Web UI are listed as in the following table.

Note: Contact your customer consultant to request admin access and password recovery if you have lost your password.

User Account	User ID	Password
user	user	usercisco
guest	guest	guestcisco

6. Click **OK**.

Result: The status page is displayed. See the **General Information** section on page 3-7 for details.

Status Information

Introduction

The **Status** menu provides a brief overview of the current general and system status.

General Information

1. Click **Status** on the main menu.
2. Click **General Information** in the left panel.

Result: The general information is displayed.

The screenshot shows the Cisco Status Information window. The top navigation bar includes 'Status', 'Transponder', 'HSIA', and 'Device'. The left sidebar contains the Cisco logo and a menu with 'General Information' (highlighted), 'Connection', 'Constellation', 'Trend Track', and 'Event Log'. The main content area is titled 'Status' and 'General Information'. It contains the text: 'This page displays information on the current system.' Below this are two tables.

Information	
Standard Specification Compliant	DOCSIS 2.0
Hardware Version	R2
Software Version	0.01.05
DOCSIS MAC Address	18:59:33:ff:c2:c8
HSIA MAC Address	00:10:18:de:ad:09
DOCSIS Serial Number	ffc2c8
CM certificate	Installed

Status	
System Up Time	0 days 00h:07m:58s
Network Access	Allowed
DOCSIS IP Address	30.20.10.28

©Elements of the software and the display are copyrighted by Cisco System Inc. All rights reserved.

The **General Information** window displays the general information on the current system.

The information tab allows you to confirm system information, including the compliant Euro-DOCSIS/DOCSIS Standard version, hardware/software versions, DOCSIS/HSIA MAC Addresses, and so on.

The status tab allows you to monitor the time for system connection, network access status, and so on.

Connection Information

Log in to the Web UI or

1. Click **Status** on the main menu.
2. Click **Connection** in the left panel.

Result: The connection information is displayed.

The screenshot shows the Cisco Web UI interface. At the top, there is a navigation bar with tabs for Status, Transponder, HSIA, and Device. The Status tab is selected. On the left side, there is a sidebar with a Cisco logo and a menu with options: General Information, Connection (highlighted), Constellation, Trend Track, and Event Log. The main content area is titled 'Status' and 'Connection'. Below the title, there is a text box stating: 'This page displays information on the status of the cable modem's HFC and IP network connectivity.' There are three main sections: 'Startup Procedure', 'Downstream Channel', and 'Upstream Channel'. Each section contains a table with various parameters and their values. At the bottom, there is a table for 'CM IP Address'.

Startup Procedure		
Procedure	Status	Comment
Acquire Downstream Channel	594.00 MHz	Locked
Connectivity State	OK	Operational
Boot State	OK	Operational
Configuration File	OK	performance.bin
Security	Disabled	Disabled

Downstream Channel			
Lock Status	Locked	Modulation	QAM256
Channel ID	2	Symbol rate	5360.537 Ksym/sec
Downstream Frequency	594.00 MHz	Downstream Level	16.2 dBmV
SNR	44.8 dB		

Upstream Channel			
Lock Status	Locked	Modulation	QAM64
Channel ID	1	Symbol rate	5120.000 Ksym/sec
Upstream Frequency	10.00 MHz	Upstream Level	30.7 dBmV

CM IP Address	Duration	Expires
30.20.10.28	D: 04 H: 22 M: 34 S: 00	Tue May 29 14:15:05 2012

©Elements of the software and the display are copyrighted by Cisco System Inc. All rights reserved.

The **Connection** window displays the Hybrid Fiber COAX (HFC) and IP network connection status.

The startup procedure tab displays the self-checking results of during the startup procedure, including the status of configuration file, boot state, connectivity state and so on.

The downstream and upstream channel tabs display the status of downstream/upstream connections, including channel modulation, symbol rate, level, frequency and so on.


Constellation

1. Click **Status** on the main menu.
2. Click **Constellation** in the left panel.
3. Click **Run** to perform the downstream test.

Result: the downstream constellation map is displayed.

Note: Click **Stop** to abort the test.

Status
Transponder
HSIA
Device

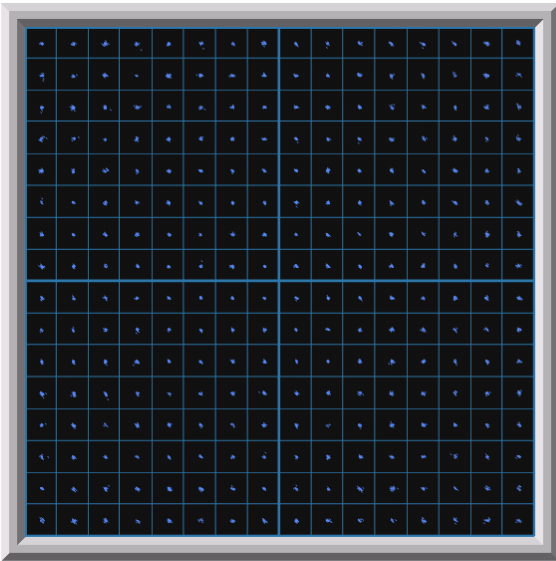


- General Information
- Connection
- Constellation
- Trend Track
- Event Log

Status

Constellation Map

This page shows downstream constellation map.



Downstream	Data
Frequency	594.00 MHz
Level	16.20 dBmV
SNR	44.90 dB
MER	46.90 dB
BER interval	60 sec
Pre FEC BER	2.126871e-06
Post FEC BER	2.197459e-07

Updates remaining 0

©Elements of the software and the display are copyrighted by Cisco System Inc. All rights reserved.

The **Constellation Map** window consists of the constellation map and the constellation specifications table. The constellation map enables you to observe and map including downstream data package, frequency split, level, Signal Noise Ratio (SNR) and so on.

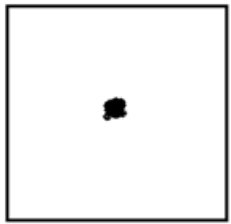

The constellation map is useful in diagnosing line problems that might otherwise go undiagnosed.


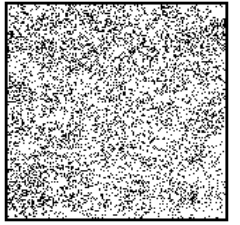
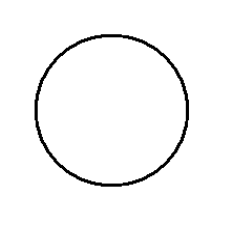
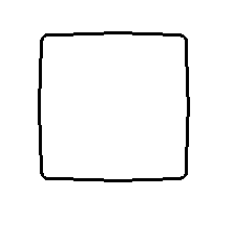
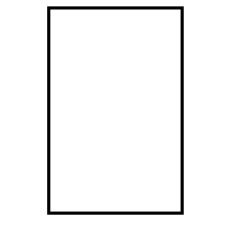
This following table provides useful information on how to interpret the information presented in the table.

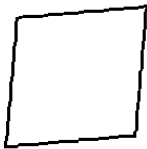
Specification	Description
Frequency	The downstream frequency given in Hz
Power	The downstream power given in dBmV
SNR	The downstream signal quality. Signal Noise Ratio (SNR)
MER	The downstream signal quality. Modulation Error Ratio (MER) Note: The MER value displayed are subject to the transponder itself and varies from the field test results tested from the test points of amplifier and nodes.
CER Interval	The intervals of each CER check. Codeword Error Rate (CER) refresh rate.
Pre FEC CER	Codeword error rate (CER) before forward error correction is applied.
Post FEC BER	Codeword error rate (CER) after forward error correction is applied.

Interpreting QAM Constellation Data by Visual Inspection

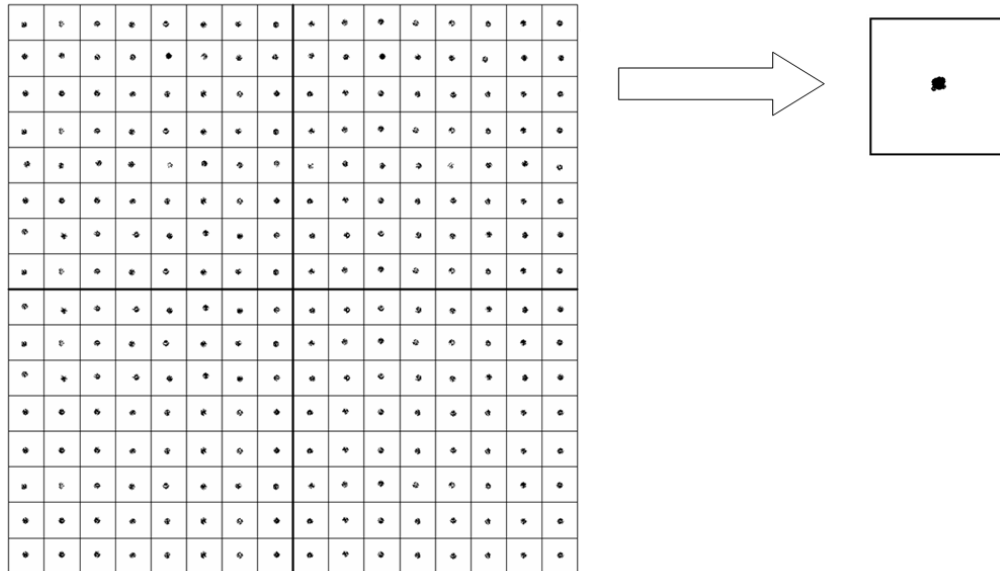
The usefulness of the QAM constellation comes in the ability to recognize common shapes and configurations within the map. The following table summarizes the shapes commonly visible in the RF Constellation page. Examples of these shapes are illustrated in the figures that follow.

Shape	Focus	Impairment	Description
	Individual cells and entire QAM constellation	Normal	Dots are centered in the individual QAM quadrants. The QAM constellation has a uniform square shape.
	Individual cells	Low CNR and/or Low MER	Individual cells of QAM constellation contain a fuzzy and diffused pattern.

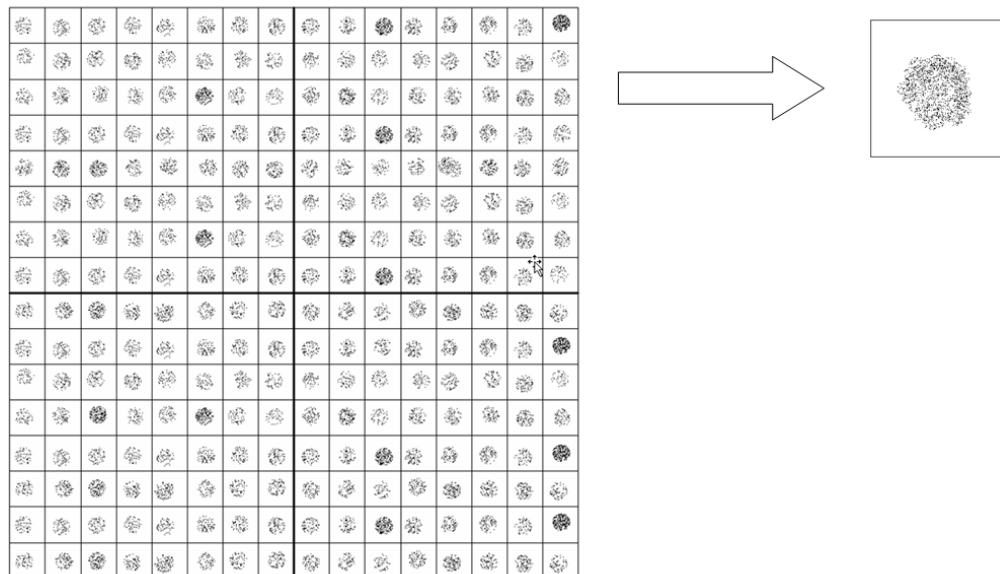
	<p>Individual cells</p>	<p>Coherent Interference</p>	<p>Individual cells of QAM constellation contain diffused hollow circles or doughnuts. This indicates an interfering carrier and shows the effect of not allowing the carrier to ever reach the proper point in the target range.</p>
	<p>Individual cells</p>	<p>Gaussian Noise</p>	<p>Individual cells contain a complete and fairly uniform smear up to all decision boundaries, and are usually caused by improper system setup, too many amplifiers in a cascade, damaged/overheated hardware, and/or low power.</p>
	<p>Entire QAM constellation</p>	<p>Phase Noise</p>	<p>QAM constellation consists of smeared, concentric, circular patterns.</p>
	<p>Entire QAM constellation</p>	<p>Gain Compression</p>	<p>QAM constellation looks uniformly square, but the outside corners appear to be smashed toward center of grid (compression in the RF plant).</p>
	<p>Entire QAM constellation</p>	<p>I-Q Imbalance in the Modulator</p>	<p>Overall appearance of QAM constellation is rectangular rather than the desired square shape (square inequality).</p>

	Entire QAM constellation	Quadrature Distortion	Overall appearance of QAM constellation has a twisted or skewed parallelogram shape.
---	--------------------------	-----------------------	--

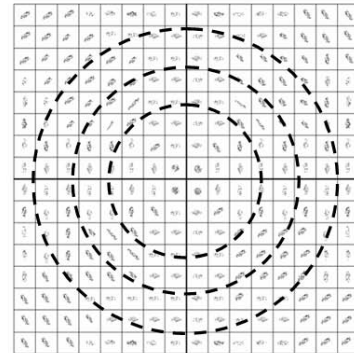
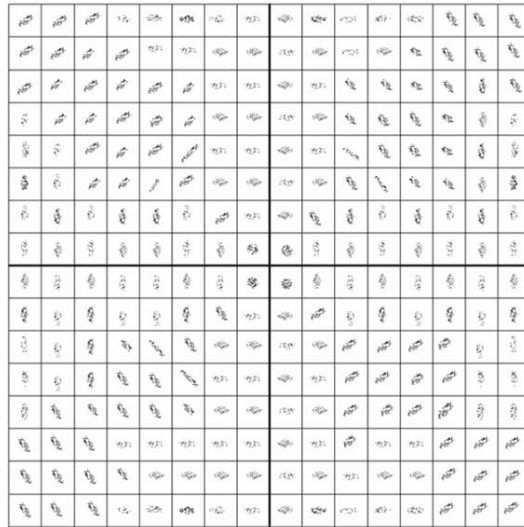
Sample QAM Constellation—Normal Centered Dots (Good Sound Quality)



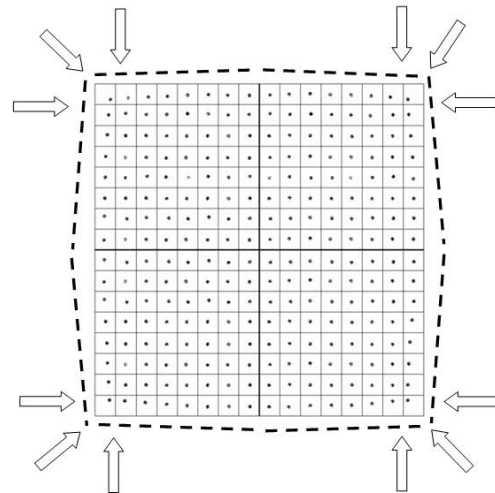
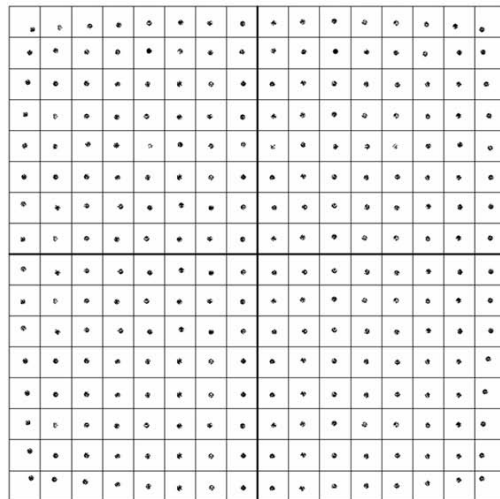
Sample QAM Constellation—Fuzzy (Low CNR and/or Low MER)



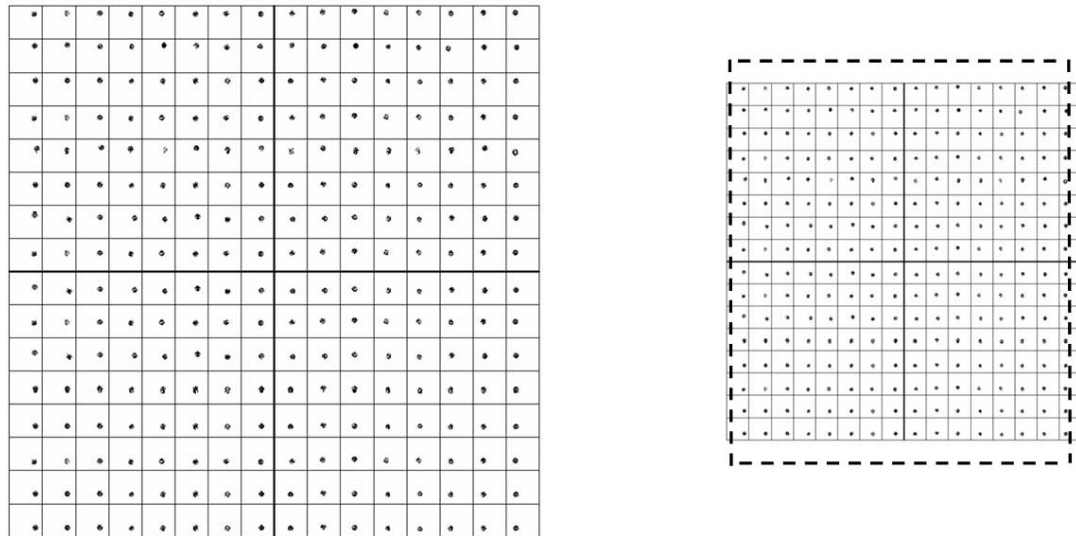
Sample QAM Constellation—Circular Smear (Phase Noise)



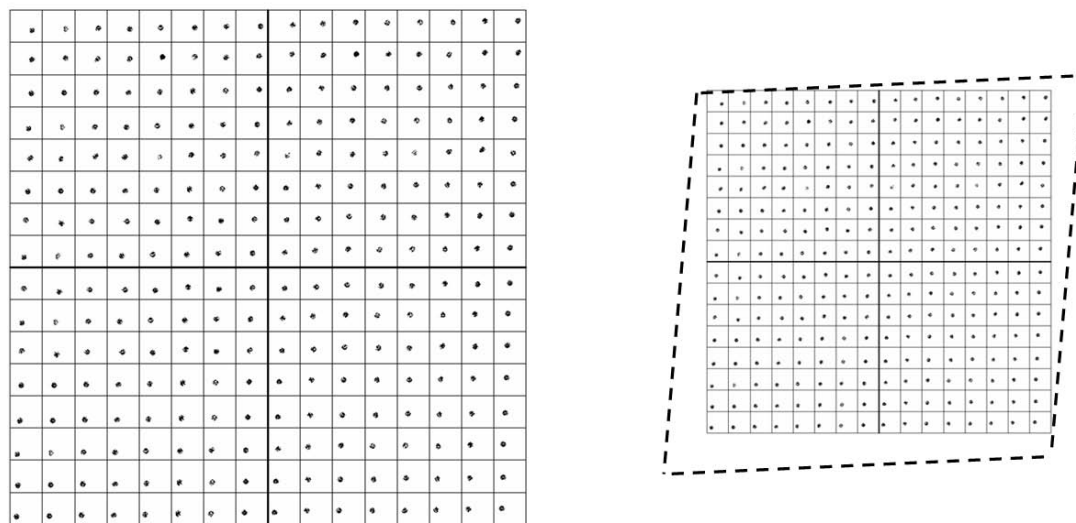
Sample QAM Constellation—Corners Squeezed to Center (Gain Compression)



Sample QAM Constellation—Rectangular vs. Square (I-Q Imbalance)



Sample QAM Constellation—Twisted or Skewed (Quadrature Distortion)



Trend Track

1. Click **Status** on the main menu.
2. Click **Trend Track** in the left panel.

Result: The trend chart is displayed. The trend chart displayed is based on the default settings.



General Information

Connection

Constellation

Trend Track

Event Log

Status

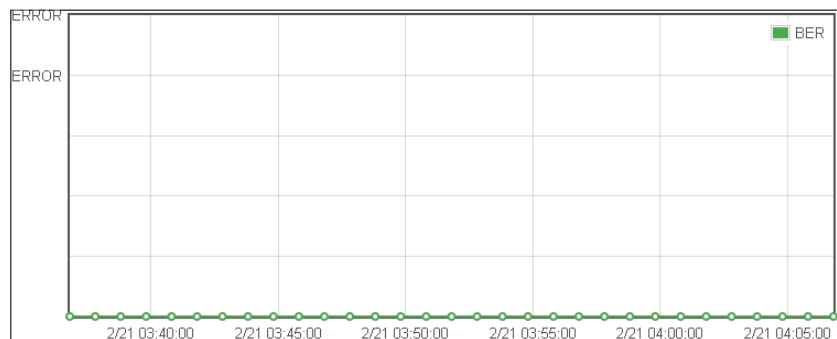
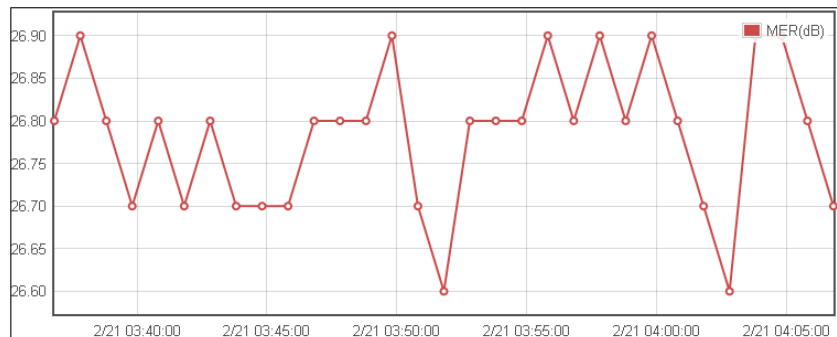
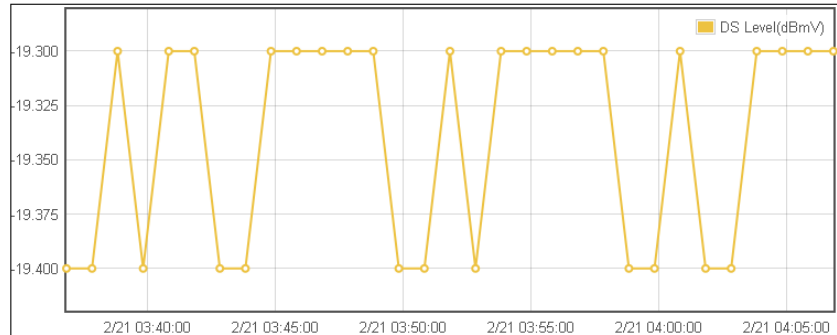
Trend Track

This page shows trend track of downstream channel parameters.

Auto Refresh

(NOTE: Auto refresh will reset viewpoint to show entire track. Any zoom/pan operation will disable auto refresh.)

Last successful data update: Tue Feb 21 2012 13:07:39 GMT+0800 (China Standard Time)



The trend chart tab shows the Downstream (DS) level, the Modulation Error Ratio (MER) and the Bit Error Ratio (BER) of the transponder. Click the checkbox before Auto Refresh to enable automatic update of the chart. Move your mouse to the points displayed in the trend chart enables you to view the detailed value of the specific time point.

The trend recording configuration tab allows you to configure the interval for taking each sample, and the IP address of the TFTP server to store the log files. The interface also includes the option to enable/disable the log upload, the most recent log upload record and the Refresh button to refresh the upload record.

Trend Recording Configuration	
Sample Interval	<input type="text" value="0"/> Days <input type="text" value="0"/> Hours <input type="text" value="1"/> Mins
Sample Enabled	Yes <input type="button" value="v"/>
Log Server IP	<input type="text" value="192.168.100.11"/>
Log Filename Prefix	<input type="text" value="trend/log_"/>
Log Interval (Number of Points)	<input type="text" value="10"/>
Log Upload Enabled	Yes <input type="button" value="v"/>
Log Upload Status (Refresh)	Last log transmission is failed. Happened at Tue Feb 21 04:06:56 2012 Last successful log upload: Tue Feb 21 03:45:50 2012
<input type="button" value="Apply"/> <input type="button" value="Upload All"/> <input type="button" value="Clear Trend Data"/>	

1. Input the desired time interval for taking sample charts after Sample Interval. 1 minute per sample in the above case.

Note: Time interval is automatically converted into hours or days. For example, the input of 70 minutes will be converted to 1 hour and 10 minutes automatically. The max sample interval is 2880 minutes (2 days).

2. Click on the drop-down box after Sample Enabled to enable/disable taking samples for the trend track.
3. Verify the IP address of the TFTP server displayed after Log Server IP. Refer to the **Configuration Data** section on page 3-18 to update the IP address if necessary.

4. Verify the default filename after Log Filename Prefix or input a new file name for the log.

Note: Use different file names to avoid overwriting the previous log records.

5. Verify the default interval of each log in time points (every sample interval time) or input a desired value after Log Interval. 10 minutes per log in the above case.

Note: The max number of time points is 1000.

6. Click on the drop-down box after Log Upload Enabled to enable/disable the trend log upload.

Note: You can also click **Upload All** to upload all logs to the server, or click **Clear Trend Data** to remove all the trend logs stored.

7. Click **Apply** to apply the configuration.

Input your desired value in each textboxes and click **Apply**.

Event Log

1. Click **Status** on the main menu.
2. Click **Event Log** in the left panel.

Result: The SNMP event log is displayed.

Status

SNMP Event Log

This page displays the contents of the SNMP event log.

Time	Priority	Description
Tue Jan 17 15:03:00 2012	Critical (3)	DHCP WARNING - Non-critical field invalid in response.
Time Not Established	Critical (3)	DHCP FAILED - Discover sent, no offer received
Mon Jan 16 00:25:57 2012	Critical (3)	Received Response to Broadcast Maintenance Request, But no Un...
Sun Jan 15 00:01:30 2012	Critical (3)	DHCP WARNING - Non-critical field invalid in response.
Fri Jan 13 00:15:59 2012	Critical (3)	Received Response to Broadcast Maintenance Request, But no Un...
Thu Jan 12 17:18:49 2012	Critical (3)	Started Unicast Maintenance Ranging - No Response received - ...
Thu Jan 12 15:10:38 2012	Critical (3)	DHCP WARNING - Non-critical field invalid in response.
Thu Jan 12 15:10:27 2012	Critical (3)	Received Response to Broadcast Maintenance Request, But no Un...
Thu Jan 12 15:02:29 2012	Critical (3)	DHCP WARNING - Non-critical field invalid in response.
Thu Jan 12 14:26:21 2012	Critical (3)	Telnet login failed from 10.75.196.18.
Thu Jan 12 14:23:53 2012	Critical (3)	Telnet user logged out.
Thu Jan 12 14:17:44 2012	Critical (3)	Telnet user logged in from IP address 10.75.196.18
Wed Jan 11 23:33:21 2012	Critical (3)	DHCP WARNING - Non-critical field invalid in response.
Wed Jan 11 23:31:10 2012	Critical (3)	Received Response to Broadcast Maintenance Request, But no Un...
Wed Jan 11 23:18:15 2012	Critical (3)	DHCP WARNING - Non-critical field invalid in response.
Wed Jan 11 23:18:04 2012	Critical (3)	Received Response to Broadcast Maintenance Request, But no Un...
Wed Jan 11 23:09:01 2012	Critical (3)	DHCP WARNING - Non-critical field invalid in response.
Wed Jan 11 23:08:50 2012	Critical (3)	Received Response to Broadcast Maintenance Request, But no Un...
Wed Jan 11 23:05:48 2012	Critical (3)	DHCP WARNING - Non-critical field invalid in response.
Wed Jan 11 23:05:38 2012	Critical (3)	Received Response to Broadcast Maintenance Request, But no Un...
Wed Jan 11 23:03:46 2012	Critical (3)	DHCP WARNING - Non-critical field invalid in response.
Wed Jan 11 23:03:35 2012	Critical (3)	Received Response to Broadcast Maintenance Request, But no Un...
Wed Jan 11 22:58:40 2012	Critical (3)	DHCP WARNING - Non-critical field invalid in response.
Wed Jan 11 22:58:30 2012	Critical (3)	Received Response to Broadcast Maintenance Request, But no Un...
Wed Jan 11 22:57:57 2012	Critical (3)	Started Unicast Maintenance Ranging - No Response received - ...
Wed Jan 11 22:53:23 2012	Critical (3)	DHCP WARNING - Non-critical field invalid in response.
Wed Jan 11 22:53:12 2012	Critical (3)	Received Response to Broadcast Maintenance Request, But no Un...
Wed Jan 11 22:46:07 2012	Critical (3)	DHCP WARNING - Non-critical field invalid in response.
Wed Jan 11 22:45:54 2012	Critical (3)	Received Response to Broadcast Maintenance Request, But no Un...
Wed Jan 11 22:41:16 2012	Critical (3)	DHCP WARNING - Non-critical field invalid in response.
Wed Jan 11 22:41:06 2012	Critical (3)	Received Response to Broadcast Maintenance Request, But no Un...
Wed Jan 11 22:13:59 2012	Critical (3)	DHCP WARNING - Non-critical field invalid in response.

©Element of the software and the display are copyrighted by Cisco System Inc. All rights reserved.

The **Event Log** window records the system events including the time, priority and event description.

Transponder Configurations

Introduction

The **Transponder** menu enables you to observe and configure the configurations of the transponder including its IP address, device files, firmware upgrade, DOCSIS mode, and security management.

Configuration Data

1. Click **Transponder** on the main menu.
2. Click **Configuration** in the left panel.

Result: The configuration data window is displayed.

The screenshot shows the Cisco Transponder Configuration Data window. The navigation bar at the top includes 'Status', 'Transponder', 'HSIA', and 'Device'. The 'Transponder' tab is selected. The left sidebar contains 'Configuration', 'Device files', 'Firmware Upgrade', 'DOCSIS Mode', 'Security', and 'Restore Default'. The main content area is titled 'Transponder Configuration Data' and includes the text: 'This page allows editing of installation data for the cisco DOCSIS-based transponder.' Below this text is an 'Apply' button. The configuration data is presented in a table with the following fields:

Information	
Name	Cisco DOCSIS Transponder
Location	
Serial Number	NA
Model Number	NA
Mode	stand alone
Device	GM_NODE
TFTP Server IP	192.168.100.101

©Elements of the software and the display are copyrighted by Cisco System Inc. All rights reserved.

The configuration data window enables you to configure the name and location of the transponder and the IP address of the TFTP server.

Note: The TFTP server stores the firmware image and backups all the logs and records of the transponder. For local craft, the TFTP server IP address field displays the IP address of the local craft computer. Thus users can obtain firmware and download/upload logs and records using the local craft computer.

To change the displayed fields, input your desired values and click **Apply**.

Device Files

The transponder stores the device files in its flash memory to record its current configuration information. The device files can be uploaded to a TFTP server for backup and downloaded from the server for restore.

1. Click **Transponder** on the main menu.
2. Click **Device Files** in the left panel.

Note: IEP mode enables identifying the device through device file, while the Standalone mode allows you to manually choose the device.

Result: The device files window is displayed.

The screenshot shows the Cisco Transponder Device Files management interface. The top navigation bar includes Status, Transponder, HSIA, and Device. The left sidebar contains a navigation menu with options: Configuration, Device files, Firmware Upgrade, DOCSIS Mode, Security, and Restore Default. The main content area is titled "Transponder Device Files" and includes the following sections:

- Current used file :** A table showing the file name and version.

File Name	Version
GM_NODE	0.3
- Information:** A section for file management with a "File" input field, a "Browse..." button, and a "Download" button.
- Files stored in flash: 2 files in all**

1:SEGNODE Ver0.2 Size14068 Application ID2071
2:GM_NODE Ver0.3 Size5981 Application ID0
- Flash Information : (KByte)**

Size	960
Used	19
Available	940

At the bottom of the interface, there are buttons for "Upload", "Upload All", "Delete", "Format", and "Reset".

©Elements of the software and the display are copyrighted by Cisco System Inc. All rights reserved.

The device files window displays the device file in use and enables you to download, upload and manage device file.

The current used file tab lists the file name and version of the device file in use for the current configurations.

The Information tab enables you to download, upload and manage the device file.

Follow the instructions below to configure the device file of the transponder.

To Download and Apply the Device File from the TFTP Server:

1. Click **Browse** to open the explorer window and locate the device file previously stored on your computer's hard drive.
2. Click **Download**.

Result: The chosen device file is downloaded and shown in the device files list.

3. Click **Reset**.

Result: The transponder is restarted and the chosen device file is loaded.

To Upload the Device File for backup to the TFTP Server:

1. Click on the correct device file in the stored files list under the information tab.
2. Click **Upload** beneath the list.

Result: The current device file is stored in the computer's hard drive for backup.

Note: Click **Upload All** if you intend to upload all the device files in use. Click **Format** only when you intend to delete all the device files in the current flash memory.

To Remove a Device File:

1. Click on the intended device file in the stored files list.
2. Click **Delete** to remove the chosen device file.

Firmware Upgrade

The transponder firmware integrates the web interface is available on the transponder. Access the interface by typing the cable modem IP address of the transponder into your web browser. The interface includes status data for the cable modem, the HMS section, High Speed Internet Access (HSIA) diagnostics.

1. Click **Transponder** on the main menu.
2. Click **Firmware Upgrade** in the left panel.

Result: The firmware upgrade window is displayed.

The screenshot shows the Cisco Transponder Firmware Upgrade page. The navigation menu on the left includes: Configuration, Device files, **Firmware Upgrade**, DOCSIS Mode, Security, and Restore Default. The main content area is titled "Transponder" and "Firmware upgrade". It states: "This page allows firmware upgrade." Below this, it shows "Image 1 Version: 0.01.05" and "Image 2 Version: 0.01.06". There is a dropdown menu labeled "Upgrade Image Section Select" with the value "2". At the bottom, there is an "Information" section with a "Software Image" field, a "Browse..." button, and a "Download" button.

©Elements of the software and the display are copyrighted by Cisco System Inc. All rights reserved.

The firmware upgrade window displays the current firmware image version and enables you to download the new firmware from the TFTP server.

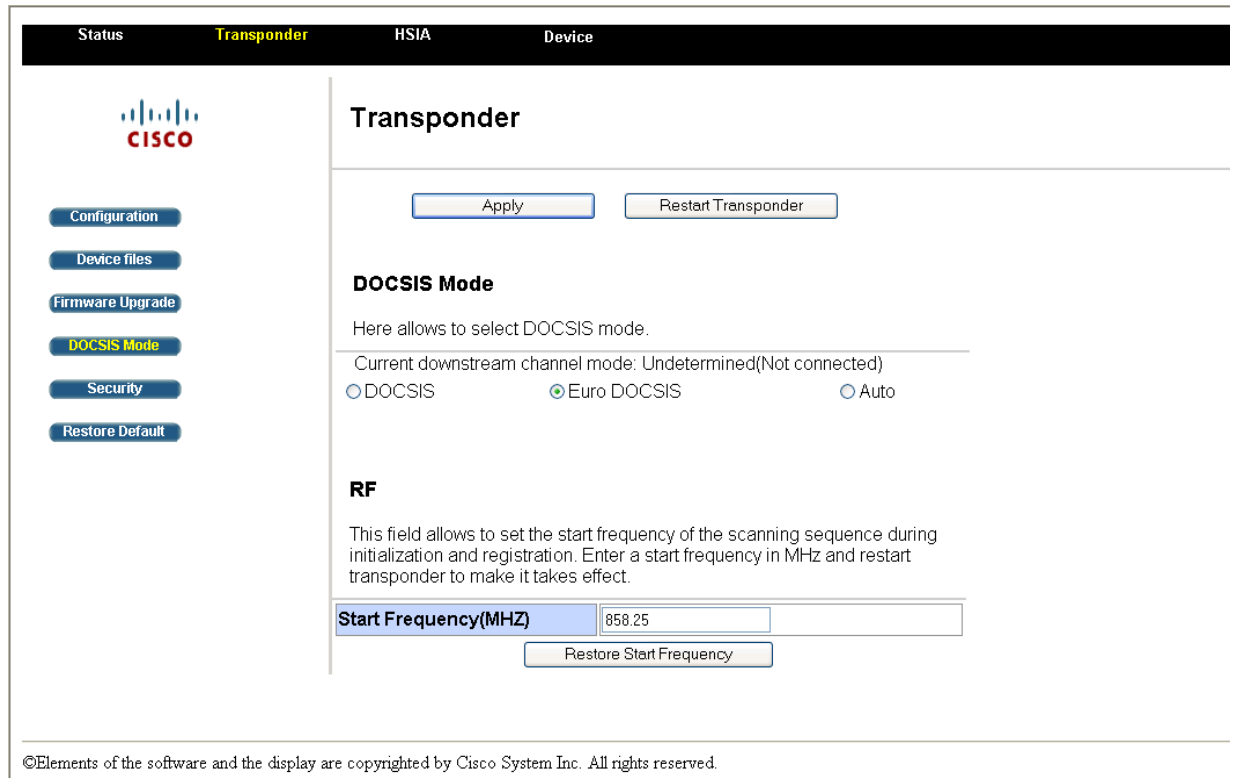
1. Register or use the existing account to log on to Cisco.com.
2. Click on the following address to find the updated transponder firmware
<http://www.cisco.com/cisco/software/navigator.html?mdfid=281510329&i=r>
[m](#)
3. Download the firmware image onto the TFTP server.
4. Click on the drop-down box after Upgrade Image Section Select to choose the desired image for upgrade.
5. Click **Browse** to open the explorer window and locate the firmware file.
6. Click **Download**.

Note: Firmware image is stored on the TFTP server for network configuration or on your local computer for local craft. Refer to the **Configuration Data** section, on page 3-18 to update the TFTP server address when necessary.

DOCSIS Mode

1. Click **Transponder** on the main menu.
2. Click **DOCSIS Mode** in the left panel.

Result: The DOCSIS Mode window is displayed.



The DOCSIS Mode window displays the current DOCSIS mode and enables you to set the DOCSIS mode and RF start frequency.

1. Click the checkbox for DOCSIS or Euro-DOCSIS based on your region. Auto is checked by default to identify the appropriate DOCSIS mode according to your local system settings automatically.

Note: Change the mode only when necessary. Refer to *Technical Contact Information* on page 5-1 to contact our customer consultant if you are not sure on the DOCSIS mode.

2. The scanning sequence will scan for channels below the start frequency. This can be used to reduce the registration time of the transponder to the network. If desired, fill in the start frequency in the **Start Frequency (MHZ)** field. Please refer to the table below for the default, highest, lowest start frequencies and frequency steps under different DOCSIS mode. (Click **Restore Start Frequency** as required to recover the default factory frequency under different DOCSIS mode.)

Mode	Default Start Frequency	Highest Start Frequency	Lowest Start Frequency	Frequency Step
DOCSIS	999.00 MHz	999.00 MHz	93.00 MHz	6.00 MHz
Euro DOCSIS	858.25 MHz	858.25 MHz	112.00 MHz	0.25 MHz
Auto	999.00 MHz	999.00 MHz	93.00 MHz	0.25 MHz

3. Click **Apply** to commit the DOCSIS mode and RF start frequency.
4. Click **Restart Transponder** to restart the transponder. After restart the new mode and/or frequency will take effect.

Result: The transponder DOCSIS mode and RF start frequency are updated.

Security

1. Click **Transponder** on the main menu.
2. Click **Security** in the left panel.

Result: The security management window is displayed.

The screenshot shows the Cisco Transponder configuration interface. At the top, there is a navigation bar with tabs for 'Status', 'Transponder', 'HSIA', and 'Device'. The 'Transponder' tab is active. On the left side, there is a vertical menu with buttons for 'Configuration', 'Device files', 'Firmware Upgrade', 'DOCSIS Mode', 'Security' (highlighted), and 'Restore Default'. The main content area is titled 'Transponder Security' and contains the following text and form elements:

This page allows configuration of administration access privileges and the ability to restore factory defaults to the system.

Current Authorized Level Administrator
 Password Change User ID
 New Password
 Re-Enter New Password
 Current User ID Password

Restore Factory Defaults Yes No

©Elements of the software and the display are copyrighted by Cisco System Inc. All rights reserved.

The security management window enables you to configure the access privileges.

Note: Password change is only available for administrator accounts. See the **User Account** section on page 3-4 for details.

1. Type the user ID in the textbox after Password Change User ID.
2. Type the new password in the textbox after New Password.
3. Type the new password again in the textbox after Re-Enter New Password to confirm.
4. Type the password of the current account in the textbox after the Current User ID Password.
5. Leave the check box before the option **Yes** after Restore Factory Defaults tab default unchecked.
6. Click **Apply**.

To Return to Factory Defaults


1. Click the check box before the option **Yes** after Restore Factory Defaults tab.
2. Click **Apply**.

Restore Default

1. Click **Transponder** on the main menu.
2. Click **Restore Default** in the left panel.

Result: The Restore Default window is displayed.

Status
Transponder
HSIA
Device




- Configuration
- Device files
- Firmware Upgrade
- DOCSIS Mode
- Security
- Restore Default

Transponder

Restore Default

This page restore defaults to the device parameters and transponder configurations.

 **WARNING:**

Reset Device Parameters and **Reset All Settings** restore all configured parameters to factory default. The operations may terminate transponder and device connection, or cause any other system instabilities.

Reset All Settings restores the WEB UI logon passwords of all accounts to factory default. It's highly recommended to disconnect the target device before operation to prevent any uninvited access, and once the passwords are restored, change them to your own immediately.

I have read through the warning above and understand all the risks, I still want to continue.

Reset Device Parameters will:

- Restore device parameters
- Restore alarm properties
- Clear all logs in the device page
- Reboot the transponder immediately

Reset All Settings will:

- Restore device parameters
- Restore alarm properties
- Clear all logs in the device and status pages
- Clear "Location", and "Logical ID" of the transponder
- Restore "Name", "Trap IP", and "Trap Community" of the transponder
- Restore WEB UI logon passwords
- Clear the most recent records of downstream frequency
- Reboot the transponder immediately

©Elements of the software and the display are copyrighted by Cisco System Inc. All rights reserved.

Follow the instructions below to restore the device parameters or all the settings to factory default:

1. Read the warning information carefully and make sure you have understood all the possible risks.

Note: Restore default only when necessary. Refer to *Technical Contact Information* on page 5-1 to contact our customer consultant if you are not sure on the operation.

2. Click the checkbox under the warning.

Result: The buttons **Reset Device Parameters** and **Reset All Settings** are activated.

3. Click **Reset Device Parameters** or **Reset All Settings** by your needs.

Note: **Reset Device Parameters** will restore the operational parameters to factory default, and **Reset All Settings** will reset all the parameters and Web UI logon password to factory default.

HSIA Diagnostics

Introduction

The **HSIA Diagnostics** menu enables you to perform the HSIA ping test to diagnose the IP network connectivity of the transponder.

To Perform the Diagnostics

The HSIA diagnostics provides ping tests to examine the IP connectivity.

1. Click **HSIA** on the main menu.
2. Click **Ping** in the left panel.

Result: The HSIA diagnostics window is displayed.

The screenshot displays the HSIA Diagnostics interface. At the top, there are tabs for Status, Transponder, **HSIA**, and Device. The main content area is titled "High Speed Internet Access Diagnostics" and "Ping". A sub-header reads "This page provides ping diagnostics to help with IP connectivity problems." Below this is the "Ping Test Parameters" section with the following fields:

Target IP address or Name	192.168.100.1
Number of Pings(1-100)	3
Ping Size (64-1518)	1518
Timeout(1000-60000 MSeconds)	5000

Below the parameters are three buttons: "Start Test", "Abort Test", and "Clear Results". The "Results" section shows a terminal window with the following output:

```
Pinging 192.168.100.1...
Reply from 192.168.100.1: bytes=1518 seq=0 time < 10ms TTL=64
Reply from 192.168.100.1: bytes=1518 seq=1 time < 10ms TTL=64
Reply from 192.168.100.1: bytes=1518 seq=2 time=1 ms TTL=64
Ping statistics:
    Pings sent: 3 (1 per second); Replies received: 3 (1 per second)
    Bytes sent: 4554 (2277 per second); Bytes received: 4554 (2277 per second)
```

©Elements of the software and the display are copyrighted by Cisco System Inc. All rights reserved.

1. Click **Clear Results** if previous test results are still recorded in the results tab.
2. Click **Start Test** to initiate the ping test.
Result: The following ping test result is displayed in the results tab.
3. Or Click **Abort Test** to give up the test if you are not intended for the test.

Note: If the ping test shows no reply, troubleshoot your transponder connections according to steps listed in the **Troubleshooting** section on page 4-1.

Device Configurations

Introduction

The **Device Configurations** menu enables you to view and configure the device with the transponder installed, including its alarm setting, forward/reverse RF configurations, optical transmitter settings and so on.

Note: The Device Configurations menu displays different options based on the devices. The Cisco GainMaker 4-Port Node is used in this guide for example.

Status

1. Click **Device** on the main menu.
2. Click **Status** in the left panel.

Result: The Status window is displayed.

Item	Value
Amplifier Type	Gainmaker Node 4-Port

©Elements of the software and the display are copyrighted by Cisco System Inc. All rights reserved.

Alarm

1. Click **Device** on the main menu.
2. Click **Alarm** in the left panel.
3. **Result:** The alarm window is displayed.

The alarm window displays parameter alarms and enables you to configure the property alarms.

The parameter alarms tab lists the device parameters and their status. The parameters include summary status, tamper status and local craft connection status.

Alarm

attention: red for alarm, white for normal

Parameter	Value
Summary Status	Minor Alarm
TamperStatus	Intact
CraftStatus	Not connected

The property alarms tab displays the status and current value of the device properties and enables configure the valve to trigger the alarms. The properties include device temperature, transmitter power, and receiver power and so on.

Properties Alarm

attention: red for major alarm, yellow for minor alarm, white for normal

Item	Status	Current Value	Major Low		Minor Low		Minor H		Major H		Hysteresis
			Value	On	Value	On	Value	On	Value	On	
AC Line voltage(V)	Minor Low	65	35	<input checked="" type="checkbox"/>	70	<input checked="" type="checkbox"/>	99	<input checked="" type="checkbox"/>	108	<input checked="" type="checkbox"/>	5
Node Temperature (C)	Normal	41	-15	<input checked="" type="checkbox"/>	-5	<input checked="" type="checkbox"/>	75	<input checked="" type="checkbox"/>	85	<input checked="" type="checkbox"/>	2
OPT Tx Level1 (mW)	Normal	1.9	1.0	<input checked="" type="checkbox"/>	1.6	<input checked="" type="checkbox"/>	2.4	<input checked="" type="checkbox"/>	3.0	<input checked="" type="checkbox"/>	0.1
OPT Tx Level2 (mW)	Normal	1.9	1.0	<input checked="" type="checkbox"/>	1.6	<input checked="" type="checkbox"/>	2.4	<input checked="" type="checkbox"/>	3.0	<input checked="" type="checkbox"/>	0.1
OPT Rx Level(mW)	Normal	1.2	0.5	<input checked="" type="checkbox"/>	0.6	<input checked="" type="checkbox"/>	1.8	<input checked="" type="checkbox"/>	2.8	<input checked="" type="checkbox"/>	0.1
24V DC(V)	Normal	23.9	22.0	<input checked="" type="checkbox"/>	23.0	<input checked="" type="checkbox"/>	25.0	<input checked="" type="checkbox"/>	26.0	<input checked="" type="checkbox"/>	0.5
15V DC(V)	Normal	14.9	13.0	<input checked="" type="checkbox"/>	14.0	<input checked="" type="checkbox"/>	16.0	<input checked="" type="checkbox"/>	17.0	<input checked="" type="checkbox"/>	0.5
-6V DC(V)	Normal	-5.9	-8.0	<input checked="" type="checkbox"/>	-7.0	<input checked="" type="checkbox"/>	-5.0	<input checked="" type="checkbox"/>	-4.0	<input checked="" type="checkbox"/>	0.5

1. Click the check box after each value to enable alarm on it.
2. Input the desired value after each property to trigger the alarm.
3. Click **Apply**.

Result: Alarms are triggered once the configured major/minor low value and/or the minor/major high value are exceeded.

Note: The gap between the major and minor values can't be smaller than the hysteresis value. Exceeding the limit may cause value returns to the previous setting.

Reverse Switch Configuration

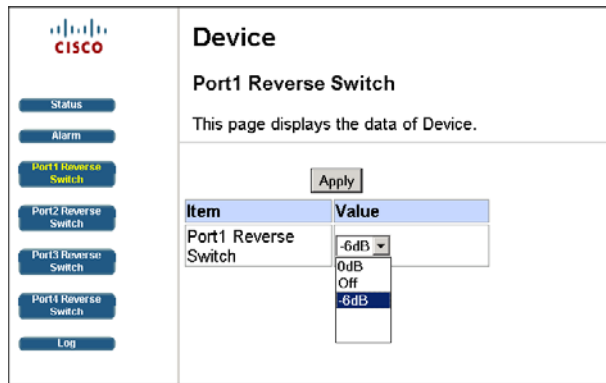
1. Click **Device** on the main menu.
2. Click **Port X Reverse Switch** in the left panel.
3. **Result:** The device reverse switch configuration window is displayed.

The screenshot shows a web interface with a top navigation bar containing 'Status', 'Transponder', 'HSIA', and 'Device' (highlighted in yellow). On the left is a vertical menu with buttons for 'Status', 'Alarm', 'Port1 Reverse Switch' (highlighted in yellow), 'Port2 Reverse Switch', 'Port3 Reverse Switch', 'Port4 Reverse Switch', and 'Log'. The main content area is titled 'Device' and 'Port1 Reverse Switch'. Below the title is the text 'This page displays the data of Device.' and an 'Apply' button. A table with two columns, 'Item' and 'Value', is displayed. The table contains one row: 'Port1 Reverse Switch' with a value of '6dB' shown in a dropdown menu.

Item	Value
Port1 Reverse Switch	6dB

©Elements of the software and the display are copyrighted by Cisco System Inc. All rights reserved.

Follow the steps below to configure the device settings through the web UI.

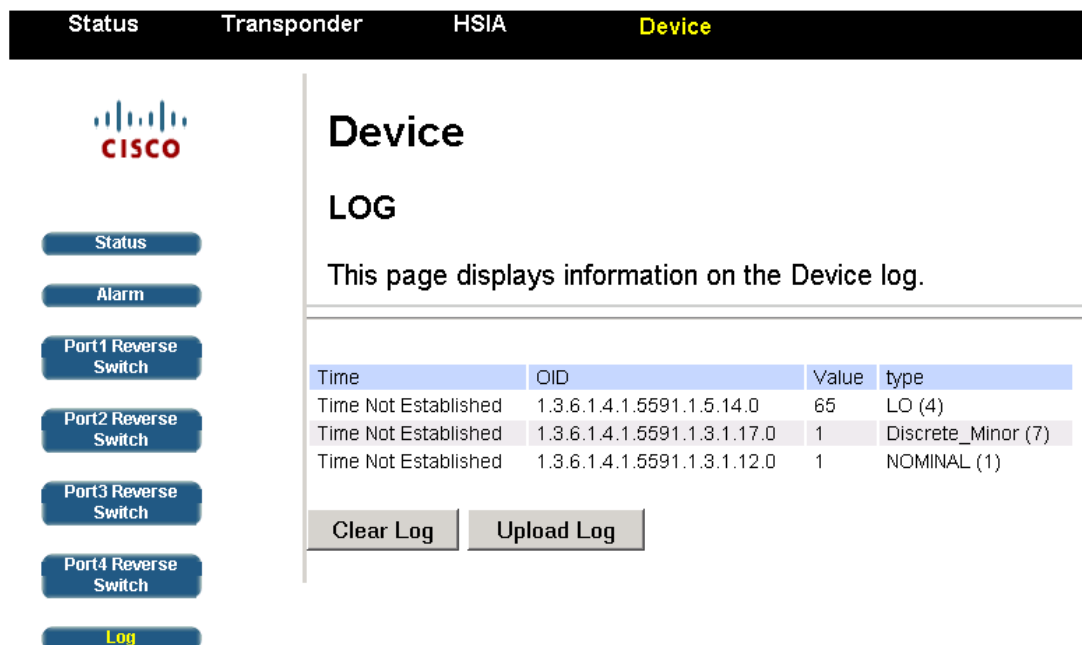


1. Click on the drop-down box in the **Value** column and choose the desired value.
2. Click **Apply**.

Device Log

1. Click **Device** on the main menu.
2. Click **Log** in the left panel.

Result: The device event log window is displayed.



The device event log window records the system events including the time, Object Identification (OID), object value and object type.

The window also enables you to store the device event log into the computer's hard drive by clicking **Upload Log** and remove all the current log information by clicking **Clear Log**.

Monitored and Controlled Parameters

About

The transponder is managed by Management Information Base (MIB). It is recommended for advanced level users only to access and configure the following parameters through MIB loading tools.

Web UI Monitored Parameters

The following table shows the parameters that are monitored by the transponder. Certain alarms may be triggered when the monitored parameters exceeded the normal value.

Monitored Parameters	Description	HMS MIB
DC Power Supply Voltage +24VDC supply +15VDC Supply -6VDC supply	The parameter is monitored on DC power supply: -6V, 15V and 24V.	fnDCPowerTable fnDCPowerIndex (0) fnDCPowerVoltage
Transmitter Optical Output Power	The parameter is monitored in mW for the installed reverse transmitter. The value is in 0.1 mW increments.	fnReturnLaserTable fnReturnLaserOpticalPower in the fnReturnLaser table
Receiver Optical Input Power	The parameter is monitored in mW for the installed optical receiver. The value is in 0.1 mW increments.	fnOpticalReceiverPower in the fnOpticalReceiver table
AC Line Voltage	The parameter is monitored in VAC for the lines power supply status. The value is in 1 VAC increments.	fnLinePowerVoltage1
Tamper Status	The parameter is monitored with 2 states for the status of the anti-tamper device on the node from the in the of the HMS MIBs. The intact(1) represents the unit is closed, and the compromised(2) indicates the unit is open.	commonTamperStatus in the commonAdminGroup

Craft Status	The parameter is monitored with 2 states for the local craft connection status. The disconnected (1) represents the local craft is not connected, and the connected (2) indicates the local craft is connected.	commonCraftStatus in the commonAdminGroup
Device Type	This parameter is monitored with 2 states for the device type. The shown parameter is "Gainmaker Node 4-Port" or "Unknown Launch Amp"/"Invalid Hardware Configuration"	fnDeviceID

Web UI Controlled Parameters

The following table shows the parameters that are controlled by the transponder.

Parameter Number	Parameter	HMS MIB
Port 1 Reverse Switch (1)	The parameter can be changed in 3 attenuation modes: ON, OFF, or -6 dB.	fnRFPortTable in the fnRFPortReverseAttenuationControl
Port 2 Reverse Switch (2)	The parameter can be changed in 3 attenuation modes: ON, OFF, or -6 dB.	fnRFPortTable in the fnRFPortReverseAttenuationControl
Port 3 Reverse Switch (3)	The parameter can be changed in 3 attenuation modes: ON, OFF, or -6 dB.	fnRFPortTable in the fnRFPortReverseAttenuationControl
Port 4 Reverse Switch (4)	The parameter can be changed in 3 attenuation modes: ON, OFF, or -6 dB.	fnRFPortTable in the fnRFPortReverseAttenuationControl

The following table shows configurable states of the above parameters.

Status	Parameter
low (1)	No attenuation in the reverse path
high(2)	Reverse path off
pad(3)	6 dB of attenuation added to reverse path

ROSA Element Management System

About the ROSA Element Manager

The ROSA EM system is specifically designed to cost effectively monitor and control the transmission network in headends, hub sites and HFC outside plants, and transmitter sites.

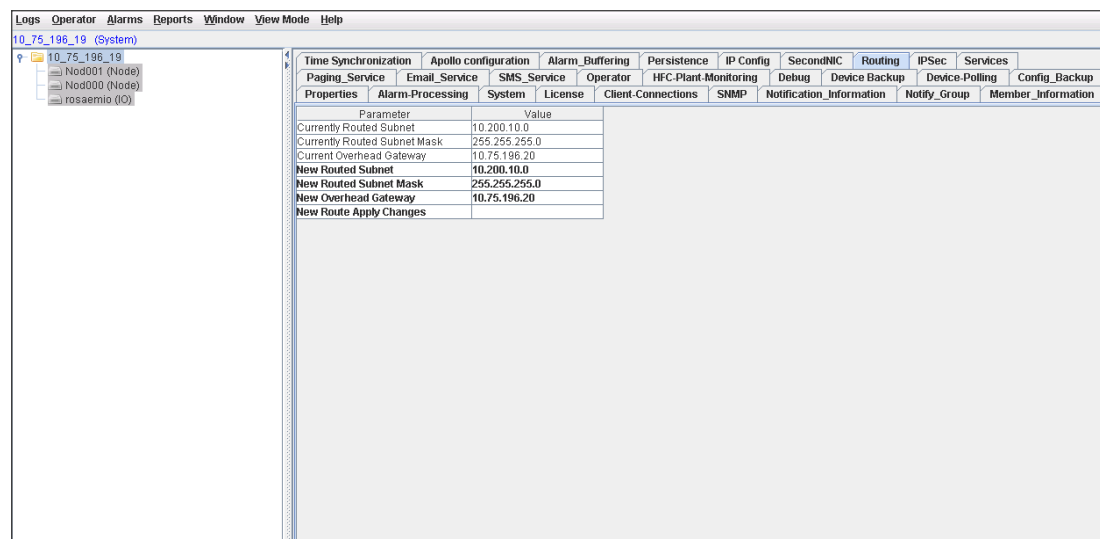
In the CMTS network, transponders are deployed in different address fields. The Cisco ROSA Element Manager enables you to monitor the network management parameters of the transponders in different address fields through building ROSA connections with the transponders.

To Build Connection with the ROSA Element Manager

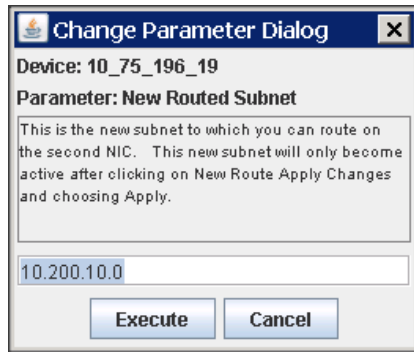
Follow the steps below to build the transponders' connection with the ROSA Element Manager.

1. Log into the ROSA manager.
2. Click on the ROSA EM device (the top node of the device tree).
3. Click **Routing** on the menu displayed.

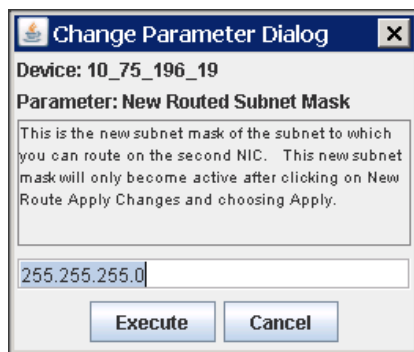
Result: The **Routing** configuration menu is displayed.



4. Click on the value field of New Routed Subnet, type in the address field of the transponders in the Change Parameter Dialog and click **Execute**.



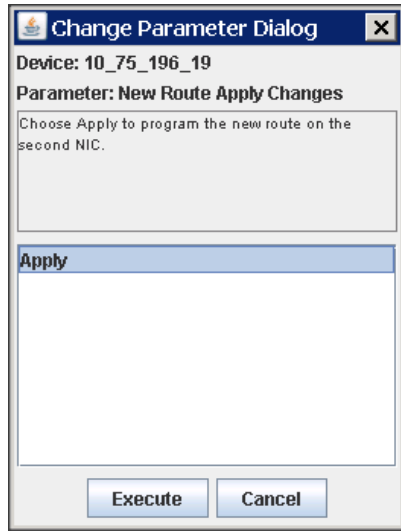
5. Click on the value field of New Routed Subnet Mask, type in the subnet address mask in the Change Parameter Dialog and click **Execute**. 255.255.255.0 is the default subnet mask.



6. Click on the value field of New Overhead Gateway, type in the address of the ROSA EM device in the Change Parameter Dialog and click **Execute**.



7. Double-click on the textbox after New Route Apply Changes, click **Apply** in the Change Parameter Dialog and click **Execute**.



Result: The new routing settings are applied.

For complete information about the installation and operation of the ROSA management, see **ROSA Element Manager User's Guide**, part number 4005743.

4

Troubleshooting

Introduction

This chapter describes the steps you may take to troubleshoot the transponder.

In This Chapter

- Transponder Signaling..... 56
- Further Assistance 58

Transponder Signaling

To Troubleshoot from the LEDs

The following table lists the solutions with regard to the issues shown from the transponder's LED signaling.

Problem Description	Solution
The LED POWER is OFF	<ul style="list-style-type: none"> ■ Verify the power supply of the node or amplifier with the transponder installed. ■ Verify that connectors of the transponder are clicked into the interface connectors in the transponder slot.
The LED DS is OFF	<ul style="list-style-type: none"> ■ Verify the power supply of the node or amplifier with the transponder installed. ■ Verify that connectors of the transponder are clicked into the interface connectors in the transponder slot. ■ Verify the amplifier or node is connected to an operating CMTS.
The LED US is OFF	<ul style="list-style-type: none"> ■ Verify the power supply of the node or amplifier with the transponder installed. ■ Verify that connectors of the transponder are clicked into the interface connectors in the transponder slot. ■ Verify the amplifier or node is connected to an operating CMTS.
The LED Online is OFF	<ul style="list-style-type: none"> ■ Verify the power supply of the node or amplifier with the transponder installed. ■ Verify that connectors of the transponder are clicked into the interface connectors in the transponder slot. ■ Verify the amplifier or node is connected to an operating CMTS. ■ Verify the amplifier or node is connected to an operating DHCP server.
The LED Status is ON	<ul style="list-style-type: none"> ■ Check if certain specs or properties exceeded the limit of the alarm status of your transponder. See Alarm section for details.

Problem Description	Solution
The LED USB is OFF	<ul style="list-style-type: none"><li data-bbox="792 279 1317 338">■ Verify the power supply of the node or amplifier with the transponder installed.<li data-bbox="792 359 1369 449">■ Verify that connectors of the transponder are clicked into the interface connectors in the transponder slot.

Further Assistance

Contact Cisco for Support

If you still cannot find the appropriate solution after performing the recommended solutions in this chapter, contact Cisco for support. Refer to Chapter 5, *Customer Support Information*.

5

Customer Support Information

If You Have Questions

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

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



Americas Headquarters

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

<http://www.cisco.com>
Tel: 408 526-4000
800 553-6387
Fax: 408 527-0883

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL:

www.cisco.com/go/trademarks

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

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Product and service availability are subject to change without notice.

© 2012, 2014 Cisco and/or its affiliates. All rights reserved.

June 2014

Part Number OL-32435-01