

Cisco Euro-DOCSIS/DOCSIS Transponder

Installation and Operation Guide

Explanation of Warning and Caution Icons

Avoid personal injury and product damage! Do not proceed beyond any $\bigtriangleup \oplus \bigstar$ 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:

 $\angle ! ackslash$ 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.

 $(\underline{\Gamma})$ You may find this symbol affixed to the product. This symbol indicates a protective ground terminal.

A You may find this symbol affixed to the product. This symbol indicates a chassis terminal (normally used for equipotential bonding).

<u>/</u><u>%</u>\ 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 intensitymodulated 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.

Trademark Acknowledgments

- Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1009R)

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 Cisco and/or its affiliates. All rights reserved. Printed in the People's Republic of China.

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 Sa	afety Instructions	vi
Preface		xiiv
About this (Guide	xiiv
	Introduction	xiiv
	Purpose	xiiv
	Who Should Use This Guide	xiiv
	Qualified Personnel	xiiv
	Scope	xiiv
	Document Version	xiiv
Chapter 1	Introduction	
Description		1-2
	General Description	1-2
	Features	1-2
	Part Number List	1-2
Transponde	er Overview	
	Transponder Diagram	
Connector S	Summary	
	Connector Summary	
Chapter 2	Installation	
Before You	Begin	2-2
	About the USB Driver	2-2
	Important Concepts	2-2
	To Install the USB Driver	2-2
Mounting		
	To Mount the Transponder	2-4
	To Connect the Transponder to Your Computer	2-5
	To Reset the Trasponder's IP Address	2-5
Checking th	re LEDs	
5	LED Overview	
	LED Status Summary	2-9

Contents, Continued

Chapter 3	Operation	
Preparation.		
	Before You Begin	
	To Configure CMTS for the Transponder	
Telnet Conse	ole Interface	
	About Telnet Console Interface	
	To Obtain Telnet Access	
Web UI Ove	rview	
	About Web UI	3-5
	User Accounts	3-5
Login Mana	gement	
	To Log in to the Web UI	
Status Inform	nation	
	Introduction	
	General Information	
	Connection Information	
	Constellation	
	Interpreting QAM Constellation Data by Visual Inspection	
	Trend Track	
	Event Log	
Transponde	r Configurations	
	Introduction	
	Configuration Data	
	Device Files	
	Firmware Upgrade	
	DOCSIS Mode	
	Security	
HSIA Diagn	ostics	
	Introduction	
	To Perform the Diagnostics	

Contents, Continued

Device Confi	gurations
	Introduction
	Identification
	Alarm
	Device Setting
	Forward RF
	Optical Receiver
	Reverse RF
	Optical Transmitter
	Device Log
ROSA Eleme	nt Management System
	About the ROSA Element Manager
	To Build Connection with the ROSA Element Manager
Chapter 4	Trouble Shooting
Transponder	signaling
_	To troubleshoot from the LEDs
Further Assis	-4-2
	Contact Cisco for Support4-2
Chapter 5	Customer Support Information
If You Have	Questions

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 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. Refer to this equipment's data sheet for details about regulatory compliance approvals.

\land WARNING:

Avoid electric shock! Opening or removing the equipment cover may expose you to dangerous voltages. 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.
- Only qualified service personnel are allowed to remove equipment covers and access any of the components inside the chassis.

Important Safety Instructions

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

\rm 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 Installation

🗥 WARNING:

Avoid 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.

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 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 main, 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.

Important Safety Instructions, Continued

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 the equipment cover may expose you to dangerous voltages. Refer all servicing to qualified service personnel only.

🔥 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 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 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.

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.

About This Guide

Introduction

The Cisco Euro-DOCSIS/DOCSIS Transponder offers both online and local monitoring and control capabilities for Cisco compact amplifiers and nodes deployed in the Euro-DOCSIS/DOCSIS network.

Purpose

This guide provides instructions for installing, configuring, setting up, and troubleshooting the Cisco Euro-DOCSIS/DOCSIS Transponder.

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

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

Preface

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

Scope

This guide discusses the following topics.

- Description
- Installation
- Operation
- Troubleshooting
- Customer Support Information

Document Version

This is the first release of this guide.

Chapter 1 Introduction

Overview

This chapter provides an overview of this guide and of the Cisco Euro-DOCSIS/DOCSIS Transponder for Cisco compact amplifiers and nodes, including general descriptions, transponder overview, and connector summary.

In This Chapter

Topic	See Page
Description	1-2
Transponder Overview	1-3
Connector Summary	1-4

Description

General Description

The Cisco Euro-DOCSIS/DOCSIS transponder offers monitoring and control capabilities for Cisco compact amplifiers and nodes deployed in Euro-DOCSIS/DOCSIS networks.

Features

The transponder has the following features.

- Network Environment: Works in Euro-DOCSIS/DOCSIS 2.0 networks, and also works in Euro-DOCSIS/DOCSIS 1.0, and 1.1 environments.
- Network Management: Complies with the Euro-DOCSIS/DOCSIS 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 Euro-DOCSIS/DOCSIS 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:** Only 2.5-w power consumption for whole transponder.

Part Number List

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

Description	Part Number
Euro-DOCSIS/DOCSIS Transponder for Cisco Compact Amplifiers and Nodes	4038498

Transponder Diagram

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



Connector Summary

The following tables and diagrams show all the connector interfaces of the Euro-DOCSIS/DOCSIS 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.



Mini-USB

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



Chapter 2 Installation

Overview

Introduction

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

In This Chapter

Topic	See Page
Before You Begin	2-2
Mounting	2-4
Checking the LEDs	2-8

Before You Begin

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

- Prepared the installation site
- Prepared the Cisco device to install the transponder
- Install the device 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 Windows XP, Windows Server 2000/2003, and Linux. For any other system, please consult your system administrator before operating.

Note: The USB driver supports Window 7 under XP mode. For computers with Windows 7 operating system, download and install the windows XP mode installation package

from http://www.microsoft.com/windows/virtual-pc/download.aspx

and attain complete instructions from the page to attach the transponder to the virtual PC before installation.

Important Concepts

The following items have been defined in this guide.

- **Device**: A device is defined as a Cisco compact amplifier or node with the Euro-DOCSIS/DOCSIS transponder installed. Refer to the data sheets of your own device to verify whether it supports the Euro-DOCSIS/DOCSIS transponder.
- **Transponder**: The Euro-DOCSIS/DOCSIS transponder.

To Install the USB Driver

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://software.cisco.com/download/release.html?mdfid=281510184&flowid= 34262&softwareid=284174356&release=USB_Driver_0.0.1&relind=AVAILABLE &rellifecycle=&reltype=latest
- 3. Download the USB driver software.

Before You Begin

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.

Mounting

To Mount the Transponder

Mounting Steps:

1. Insert the transponder in the Transponder Module Slot of the desired device. Make sure to position the transponder in the correct direction before installation, by matching its PCB edge into the PCB Slot.

(Cisco Compact Dual Amplifier taken as the device for example)



Important Note: Make sure that the transponder is inserted in the correct slot.

Note: If the transponder is mounted to the device in an operating CMTS system, certain LEDs will flash to display the startup process, the upstream and downstream status. See the **Checking the LEDs** section, on page 2-8 for details.

2. Push down on the transponder until it clicks into the connectors of the device.

Note: For Cisco Compact Segmentable Node A90200 and A90201, the following mounting bracket is used for installing the transponder.



Follow the steps below to mount the bracket.

- a) Insert the transponder and push down till it clicks into connectors.
- b) Insert the mounting edge into the mounting bracket slot on the design print.

Transponder

Mounting Bracket Slot



- d) Using a screw driver to tighten the mounting screw.
- 3. When the transponder is connected to the desired device, and power is applied, the LED "POWER" starts to blink.

To Connect the Transponder to Your Computer

Mounting Material: 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.
- Connect the mini-USB port of the USB cable to the transponder. (Cisco Compact Segmentable Node is taken as the device for example)



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.



Mounting, Continued

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.

上 Local Area Connection Properties	? X		
General Advanced			
Connect using:			
Intel(R) 82567LM Gigabit Network Co Configure			
This connection uses the following items:			
Particle Protocol (IEEE 802.1x) v3.7.4.0 Network Monitor Driver Internet Protocol (TCP/IP)			
Install Uninstall Properties			
Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks. Show icon in notification area when connected Notify me when this connectivity has limited or no connectivity.			
Show icon in notification area when connected Notify me when this connective has limited or no connective	tu		
Show icon in notification area when connected Notify me when this connective has limited or no connective	ty		
Show icon in notification area when connected Notify me when this connective has limited or no connective OK Car	ty		

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.)

nternet Protocol (TCP/IP) Properties			
General			
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.			
Obtain an IP address automatica	lly		
🕞 Use the following IP address: —			
IP address:	192 . 168 . 100 . 105		
Subnet mask:	255.255.255.0		
Default gateway:	· · ·		
C Obtain DNS server address automatically			
─● Use the following DNS server ad	dresses:		
Preferred DNS server:	· · ·		
Alternate DNS server:	· · ·		
	Advanced		
	OK Cancel		

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

LED Overview

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

Item	Description	
LED Indicators	The transponder includes six LEDs:	
	• POWER (Green)	
	• DS (Green)	
	• US (Green)	
	ONLINE (Green)	
	• USB (Green)	
	• STATUS (Red)	
	These indicate transponder status.	

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 on page 2-24 for more details

Chapter 3 Operation

Overview

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

Topic	See Page
Preparation	3-2
Telnet Console Interface	3-3
Web UI Overview	3-4
Login Management	3-5
Status Information	3-7
Transponder Configurations	3-18
HSIA Diagnostics	3-23
Device Configurations	3-24
ROSA Element Management System	3-33

Preparation

Before You Begin

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

\triangle 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 Eoro-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 Eoro-DOCSIS and DOCSIS root certificates.

The document is stored in the following address on Cisco.com: <u>http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_docs.html#w</u> <u>p1217174</u>

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 factory trained 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 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

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**.

🙋 Certificate	Error: Navigation Blocked - Windows Internet Explorer provided by Cisco		_ 8 ×
OO-	http://192.168.100.1/	💌 🐓 🗙 🚼 Google	
File Edit V	ew Favorites Tools Help		🗙 🍕转换 🔹 🔂 选择
🔆 Favorites	Certificate Error: Navigation Blocked	🏠 • 🗟 - 🗆 🖶 •	Page • Safety • Tools • 🕢 •
8	There is a problem with this website's security certificate.		×
	The security certificate presented by this website was not issued by a trusted certificate authority. The security certificate presented by this website was issued for a different website's address.		
	Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.		
	We recommend that you close this webpage and do not continue to this website.		
	Click here to close this webpage.		
	Continue to this website (not recommended).		
	More information		
		Internet	✓ ● 100% ▼ //

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.

Status	Transponder	HSIA [Device
cisco	Statu Gene	JS ral Information	
General Information	This pa	ge displays information o	n the current system.
Connection	Informati	on	
	Standard	Specification Compliant	DOCSIS 2.0
Constellation	Hardward	e Version	R2
Trend Track	Software	Version	0.01.04
	DOCSIS	VIAC Address	18:59:33:ff:c2:c6
Event Log	HSIA MA	C Address	00:10:18:de:ad:09
	DOCSIS	Serial Number	ffc2c6
	CM certi	ficate	Installed
	Status		
	System U	lp Time	0 days 18h:31m:25s
	Network	Access	Allowed
	DOCSIS	P Address	10.1.4.2

©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.

Status	Transponder	HSIA		Device						
cisco	Status Connectio	n								
General Information	This page dis	plays info	rmatior	n on the s	tatus of th	эca	ble modem's HF	C and IP	network	connectivity.
Connection	Startup Proced	ure								
	Procedure		5	Status	Comme	nt				
Constellation	Acquire Downs	tream Ch	annel	543.00 MH	z Locked					
Trend Trends	Connectivity St	tate	0	OK	Operatio	nal				
Irend Irack	Boot State			OK	Operatio	nal				
Event Log	Configuration I	ile		OK	platinum	.cm				
	Security			Enabled	BPI+	_				
	Downstream Cl Lock Status	nannel	Locked	i Mod	lulation		QAM64			
	Channel ID		3	Sym	bol rate		5056.941 Ksym/	sec		
	Downstream Fr	equency	543.00	MHz Dow	nstream l	eve	I-19.3 dBmV	_		
	SNR		26.8 dE	3			Ì			
	Upstream Chan	inel	icked	Modulat	ion)PSL				
	Chappel ID	1	icheu	Symbol		100				
	Unstream Fred	Leney 12	20 MH 2	Unstrea	m Level 6	200.	NBm\/			
	CM IP Address	Duration	i 100 M: 00	Ex S: 00 Th	pires u Feb 23 0	3:34	:24 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.

General Information	Cons This p	stel age	lati sho	on ws	Ma dow	p /nsti	rear	n co	onst	ella	tion	ma	p.					
Trend Track		_	_	_	_	_					_	_	_	_			Downstream	Data
	•	÷	•		*	+	+	*	•	*	•	••	*	-	*	8	Frequency	594.00
Event Log				×	*		*	*	*		•	*	*	•	*	× 1	Level	21.30 d
									+								SNR	43.30 d
								•	+								MER	42.15 d
																	BER interval	60 sec
																	Pre FEC BER	9.03450
																	Post FEC BEF	R 7.21553
									•									
							•	•	•									
			*			•		-	•									
					•			•	•							·		
		1		8		-	1	*	*	۰.	•	*	*	*	*			

 \circledcirc 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.

Shape	Focus	Impairment	Description
	Individual cells	Coherent Interference	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.
	Individual cells	Gaussian Noise	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.
	Entire QAM constellation	Phase Noise	QAM constellation consists of smeared, concentric, circular patterns.
	Entire QAM constellation	Gain Compression	QAM constellation looks uniformly square, but the outside corners appear to be smashed toward center of grid (compression in the RF plant).
	Entire QAM constellation	I-Q Imbalance in the Modulator	Overall appearance of QAM constellation is rectangular rather than the desired square shape (square inequality).



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

w	Ð	٠	٠	•	•	٠	•	*	٠	•	۵	*	۰	•	٠
•	•	۵	٥	•	3	*	٩	*	•	•	•	٠	۰	•	٠
•	•	•	•	4		۰	٠	•	*	٠	•	٠	•	•	e
×	s.	٠		•	•	*	•	*	٠	•	÷	÷	۰	•	•
٠	•	*	*		•	•	•	ĸ	a	•	÷	4	٠	•	۰
•	•	٠	•	÷	*	9	٠	٠	*	٠	•	٠	•	•	•
۴	+	٠	٠	•	•	•	٠	•	*	÷	9	٠	•	•	•
w	¢.	٠	•	٠	•	٠	•	*	٠	•	٩	۰	٥	•	٠
٩	+	÷	٠	•	•	•	٠	•	٠	Ŷ	9	*	•	•	•
v	5	٠	•	٠	•	*	•	*	٠	٠	٩	۰	۰	•	٠
۰	+	٠	٠	•	•	•	e	•	٠	÷	9	٠	•	•	•
٠	•	•	•	٠	*	•	٠	۰	*	٠	•	٠	•	•	•
٠	•	6		÷	*		٠	٠	*	٠	•	٠		٠	•
w	Ð	٠	•	•	•	•	•	*	•	•	٥	۰	۰	•	٠
٠	٠	•		4	*	٩	٠	۰	*	٠	•	٠		•	e
٠	•	6	•	٠	*	9	٠	٠	٠	٠	•	٠	•	٠	•



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

		藻	÷	÷	\$	÷		Ġ	ŝ	\$\$	\$	豪	ŝ	S.	灏	*
	No.	()	88	戀	978 1979		靈	25	變	缬	¢۶	\$\$\$	33	1	ŵ	-@j
	-	瘘	Ť	Ŵ	Ø.	ø	÷	戀	ŝ.	¢		÷.	ŝ,	窭	儆	勜
		ŝ.	\$	÷	ē.	ŵ		٢	ŝ		\$	嶽	Ş	Ŵ		
1 1	ŝ	Ť		Ś	÷.	1	*	19 19	S.	*		19	÷	*	戀	勮
1 1	Ť	¢.	88	戀	6je		촣	$\tilde{g}_{2}^{i};$	ŝ	÷	÷.	\$	\$	3	÷	13
1 1	ŝ	瘘	Ŵ	ŝ.	¢.	ø	ŝ.	戀	ŝ.	¢	瘤	-	ŝ,	癫	鬱	勜
(a) (ald's a	de.	635	65	180	- 	10.0	企	-	- 28	錦	22	<i>.</i>	59		2
3 3 4 5	25.5	1.0	100	1.1	20	.076		65	4.94	10.60		145		- A	E.S.a.	24.1
30 30 <td< th=""><th>5 (S)</th><th>199 199</th><th>ŵ</th><th>- </th><th>\$\$ \$</th><th>- Car</th><th>1</th><th>5 35</th><th>容</th><th>1990 1990</th><th>Ż</th><th>÷.</th><th></th><th>\$\$</th><th>89 10</th><th>÷</th></td<>	5 (S)	199 199	ŵ	- 	\$\$ \$	- Car	1	5 35	容	1990 1990	Ż	÷.		\$\$	89 10	÷
3 3 3 5	(学校) (学校) (学校) (学校) (学校) (学校) (学校) (学校)		~ *	2 22 22	\$ \$			80 (B)		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	》 登 禄	10 10 10 10 10 10 10 10 10 10 10 10 10 1	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	2 **	40 40 40 40 40
30 30 40 30 40 50 <td< th=""><th>四 離 影 感</th><th>39 19 19 19</th><th>~ 會 你 你</th><th></th><th></th><th></th><th></th><th>5 8 8 3</th><th></th><th></th><th>* 8 8 8 8</th><th>127 登 祭 彩</th><th></th><th></th><th>· 祭 谷 谷</th><th>00 00 00 00 00</th></td<>	四 離 影 感	39 19 19 19	~ 會 你 你					5 8 8 3			* 8 8 8 8	127 登 祭 彩			· 祭 谷 谷	00 00 00 00 00
(a) (a) <th></th> <th></th> <th>> @ @ @ @</th> <th>- 務 会 物 落</th> <th></th> <th></th> <th></th> <th>8 8 8 8 8</th> <th></th> <th>\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$</th> <th>8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8</th> <th>20 18 18 18 18 18</th> <th></th> <th></th> <th></th> <th>00 00 00 00 00 00 00 00 00 00 00 00 00</th>			> @ @ @ @	- 務 会 物 落				8 8 8 8 8		\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8	20 18 18 18 18 18				00 00 00 00 00 00 00 00 00 00 00 00 00
35 35 45 36 36 36 37 48 <			* * * * * *	- 谷谷				8 8 8 8 8 8			* * * * * * * * *	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2				
***								8 8 9 9 8 8 8 8			* * * * * * * * * * * * * * *	20 20 20 20 20 20 20 20 20 20 20 20 20 2				
											* * * * * * * * * * * * * * * * * * *	20 登 登 登 登 登				
								8 8 8 9 9 9 8 8 8 8 8			 ● ● ● ●	28 88 88 88 88 88 88 88 88 88 88 88 88 8				



100	107	NOT	12.	-38	01)x	$p_{\rm gal}$	4727	490	12th	1925	ser -	(\$5)	聖	Q.	÷.
1 ⁵¹	107	ŵ	151	725	12.52	-	-	11.97	*	1525	1860	\$ 2	÷.	ŧę.	÷2
is.	i	107	¥	183	4	1251	1215	49	75.55	÷ų.	ήL	٩ <u>د</u>	÷1	ð	÷2
5	#	10	at .	10	4	-	1950	rtav	49	ú <u>p</u>	12	ų,	<i>е</i> ц.	\$	5
3	12.	NOT	\$	152	enter .	1925	125	-49-	-en	3	52	ŧĿ.	¢۴.	8	8
\$	1	ş	÷	1	1071	- 10	18	day	490	52	1	ir.	4	ş	ŝ
10	ş	1	ŝ	ģ	2	1071	1925	-	52	8	100	ş	1942	8	õ
ngu.	ŵ	164	õ	Ŷ	127	ō.	43	¢.	1071	ŵ	100	Ŷ	ulu.	ş	1075
ģ	up.	ş	15.W	alar.	ş	afar.	*	\$	ş	ata.	ş	ct.w	÷	16.01	ŵ
ş	ş	ą	ş	Ę.	4	÷.	19.5%	-490	107	Et.	4	Ę.	4	10	ų
12.0	ų.	9	ø	2	÷.	-	*	15.97	- 192	all a	200 ²	15	2	4	10.0
¥0)-	5	ş	÷.	Đ	×4	12.51	1925	4	7932	1 ²⁷	1 ⁵¹	ø	15	×0-	\$
8		é	9	Ø.	ġ,	-	89×	18.97	*	15	ø	155	de la	45	8
ϕ_{ℓ}	ġ	ŧ.	1021	75.71	alu:	7975	19.32	\$	1925	P	1571	19,5%	1 ²⁰	15	15
$\hat{\ell}_{\vec{k}}$	n.	ŧĘ.	ų.	-05	140	1820	-	rigy.	~	1975	142	-	1 ¹	157	ist.
62	ŧ,	62	еş-	~***	01)k	1944	19.55	-	12/1V	1025	x9 -	$(\vec{x}; \vec{y})$	151	157	100

Sample QAM Constellation – Circular Smear (Phase Noise)



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

	9	٠	•	۰	٠	•	•	*	٠	•	4	۰	•	•	•
•	٠	۰	•	•	•	•	٩	٠	•	•	•	•	۰	•	•
	٠	٠		•	٠	0	٠	٠	٠	٥	٠	•	•	•	•
•	Ð.	•		٠	•		•	*		•		۰	•	•	•
		٠	٠	્ય	٠	•	۰	×	٠	٠	÷	4	٠	•	•
	٠	•			٠	٩	٠	٠	٠	٥		٥	•	•	•
٠	•	٠	٠		•	•	٠		٠	۰	٠		•	•	•
	Ð	٠		٥	•	*	•	•	*	•	٥	۰	•	•	•
٠	*	٠	٠		٠	•	٠	•	٠	ه			•	•	
	ъ.	٠	•		•	•	•	•		٠	4	•	•	•	•
	٠	٠	٠	•	•	•	•	•	٠	٠	9	٠	•	٠	•
٠	٠	•	•	•	٠	٠	٠	٠	٠	٠	٠	٠		•	۰
	•	•		•		٠	•	•	٠	٠	•	٠		•	•
	0	•		٠		•	•		٠	•	4	۰	•	•	٠
٠	•							•		٠		•			•
•	•	٠	•	•		•		•	•	٠	٠	٠		•	•





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



Sample QAM Constellation – Twisted or Skewed (Quadrature Distortion)

										•	4	•		•	
-		-	-		-								1.1		
•	•	•	۰	•	2	*	•	•	•	•	•	•	4		
	•	•		٠		٩	•	•	•	۰	•	۰			•
	Ð			٠	•		•	•	•	•	٥	۰	۰	•	۰
				з	•	•		÷	*	•	3	4		•	ø
•	•	•	•			٠	•	•	٠	۰	•	٠	•	٠	•
٠	+	٠	٠	•	•	•			٠	۰		٠	•	•	•
	¢	٠		٠		•	•	•	٠	•	4	•	۰	٠	٠
		•	•		•	•	•		٠	ه		•	•	•	•
	Ð	٠		٠				*			4	۰	۰	•	٠
			•				e		٠	e	9	•	•	٠	•
						٠	•	•	٠	•	•	٠	•	٠	•
						ę.	•		•	•	•	٠	•	•	•
	Ð	•		•			•		•	•	4	•	•		•
	•				*			•	٠	•	•	*		•	۰
						9			•	•	•	•	đ	•	٠



Trend Track

- 1. Click **Status** on the main menu.
- 2. Click **Trend Track** in the left panel.
- 3. **Result**: The trend chart is displayed. The trend chart displayed is based on the default settings.



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.

Tre	nd Recording Configuration
Sample Interval	0 Days 0 Hours 1 Mins
Sample Enabled	Yes 🕶
Log Server IP	192.168.100.11
Log Filename Prefix	trend/log_
Log Interval (Number of Points)	10
Log Upload Enabled	Yes 🕶
Log Upload Status (<u>Refresh</u>)	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

Apply Upload All 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 T	ransponder HSIA		Device
alah			
CISCO	Status		
General Information	SNMP Event	Log	
Connection	This page displ	ays the	contents of the SNMP event log.
Constellation			
Trend Track	Time Tue Jap 17 15:09:00	Priority	Description
Event Log	2012	(3) Oritical	response.
	Time Not Established	(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	Telnet login failed from 10.75.196.18.
	Thu Jan 12 14:23:53	Critical	Telnet user logged out.
	Thu Jan 12 14:17:44	Critical	Telnet user logged in from IP address
	Wed Jan 11 23:33:21	Critical	DHCP WARNING - Non-critical field invalid in
	Wed Jan 11 23:31:10	Critical	Received Response to Broadcast Maintenance
	Wed Jan 11 23:18:15	Critical	DHCP WARNING - Non-critical field invalid in
	Wed Jan 11 23:18:04	Critical	Received Response to Broadcast Maintenance
	2012 Wed Jan 11 23:09:01	(3) Critical	DHCP WARNING - Non-critical field invalid in
	2012 Wed Jan 11 23:08:50	(3) Critical	response. Received Response to Broadcast Maintenance
	2012 Wed Jan 11 23:05:48	(3) Critical	Request, But no Un DHCP WARNING - Non-critical field invalid in
	2012 Wed Jan 11 23:05:38	(3) Critical	response. Received Response to Broadcast Maintenance
	2012 Wed Jan 11 23:03:46	(3) Critical	Request, But no Un DHCP WARNING - Non-critical field invalid in
	2012 Wed Jan 11 23:03:35	(3) Critical	response. Received Response to Broadcast Maintenance
	2012 Wed Jan 11 22:58:40	(3) Critical	Request, But no Un DHCP WAPNING - Non-critical field invalid in
	2012	(3) Critical	response.
	2012	(3)	Received Response to Broadcast Maintenance Request, But no Un
	Wed Jan 11 22:57:57 2012	(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	DHCP WARNING - Non-critical field invalid in
		x-7	
	Clear Log		

©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.

Status	Transponder	HSIA	Device
cisco	Trans Configur	oonder ation Data	
Configuration	This page	allows editing of	finstallation data for the cisco DOCSIS-based transponder.
Device files (Firmware Upgrade)			Apply
DOCSIS Mode	Information	า	
	Name		Cisco DOCSIS Transponder
Security	Location		
Restore Default	Serial Num	iber E	3VAR0MN
	Model Nun	nber 7	700000
	Mode		IEP -
	TFTP Serv	er 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.

Transponder Configurations, Continued

Configuration Device files (Firmware Upgrade DOCSIS Mode Security	Transponder Device Files This page allows manage Current used file : File Name COMPACT_SEG_NODE	version
Configuration Device files Firmware Upgrade DOCSIS Mode Security	Device Files This page allows manage Current used file : File Name COMPACT_SEG_NODE	Version
Configuration Device files Firmware Upgrade DOCSIS Mode Security	This page allows managed of the second secon	Version
Device files (Firmware Upgrade) DOCSIS Mode Security	Current used file : File Name COMPACT_SEG_NODE	Version 0.3
(Firmware Upgrade) DOCSIS Mode Security	File Name COMPACT_SEG_NODE	Version 0.3
DOCSIS Mode Security	COMPACT_SEG_NODE	0.3
Security		
(Security		
Restore Default	Information	
	File	Browse Download
	Files stored in flash: 2 fil	es in all
	2:COMPACT_SEG_NODE 1	/er0.3 Size15349 Application ID2071
	Upload Upload All	Delete Format Reset
	Flash Information : (KByt	e)
	Size	960
	Used	21
	Available	938

©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.

Status	Transponder HSIA Device
cisco	Transponder Firmware upgrade
Configuration	This page allows firmware upgrade.
Device files	
Firmware Upgrade	Image 1 Version: 0.00.11 Image 2 Version: 0.00.12
DOCSIS Mode Security	Upgrade Image Section Select:
Restore Default	Information
	Software Image Browse Download

©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 <u>http://www.cisco.com/cisco/software/navigator.html?mdfid=281510329&i=r</u> <u>m</u>
- 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.

Configuration Configuration Device files Printware Upgrade OCCSIS Mode Security Security Current downstream channel mode: Undetermined(Not connected) OCCSIS OCCSIS Betore Default This field allows to set the start frequency of the scanning sequence during initialization and registration. Enter a start frequency in MHz and restart transponder to make it takes effect. Start Frequency(MHZ) Bestore Start Frequency	Configuration Device files mware Upgrade DCSIS Mode Here allows to select DOCSIS mode. Current downstream channel mode: Undetermined(Not connected) • DOCSIS • DOCSIS • Euro DO	Status Transponder	HSIA Device
Configuration Device files firmware Upgrade DOCSIS Mode Corrent downstream channel mode: Undetermined(Not connected) Security ODCSIS Restore Default RF This field allows to set the start frequency of the scanning sequence during initialization and registration. Enter a start frequency in MHz and restart transponder to make it takes effect. Start Frequency(MHZ) Bestore Start Frequency	Configuration Apply Device files mware Upgrade POCSIS Mode Here allows to select DOCSIS mode. Current downstream channel mode: Undetermined(Not connected) © DOCSIS © DOCSIS © DOCSIS © Euro DOCSIS Natio RF This field allows to set the start frequency of the scanning sequence during initialization and registration. Enter a start frequency in MHz and restart transponder to make it takes effect. Start Frequency(MHZ)	cisco	Transponder
Device files DOCSIS Mode Firmware Upgrade Here allows to select DOCSIS mode. DOCSIS Mode Current downstream channel mode: Undetermined(Not connected) Security DOCSIS Restore Default Euro DOCSIS RF This field allows to set the start frequency of the scanning sequence during initialization and registration. Enter a start frequency in MHz and restart transponder to make it takes effect. Start Frequency(MHZ) #58.25 Restore Start Frequency	Device files mware Upgrade POCSIS Mode Here allows to select DOCSIS mode. Current downstream channel mode: Undetermined(Not connected) Security DOCSIS DOCSIS DOCSIS DOCSIS DOCSIS DOCSIS DOCSIS DOCSIS DOCSIS Current downstream channel mode: Undetermined(Not connected) DOCSIS DOCSIS <th>Configuration</th> <th>Apply</th>	Configuration	Apply
DOCSIS Mode Current downstream channel mode: Undetermined(Not connected) Security ODCSIS Image: Euro DOCSIS Restore Default FF This field allows to set the start frequency of the scanning sequence during initialization and registration. Enter a start frequency in MHz and restart transponder to make it takes effect. Start Frequency(MHZ) 858.25 Bestore Start Frequency	DOCSIS Mode Current downstream channel mode: Undetermined(Not connected) Security DOCSIS Euro DOCSIS Nestore Default RF This field allows to set the start frequency of the scanning sequence during initialization and registration. Enter a start frequency in MHz and restart transponder to make it takes effect. Start Frequency(MHZ) 858.25	Device files (Firmware Upgrade	DOCSIS Mode
RF This field allows to set the start frequency of the scanning sequence during initialization and registration. Enter a start frequency in MHz and restart transponder to make it takes effect. Start Frequency(MHZ) 858.25 Bestore Start Frequency	Restore Default RF This field allows to set the start frequency of the scanning sequence during initialization and registration. Enter a start frequency in MHz and restart transponder to make it takes effect. Start Frequency(MHZ) 858.25	DOCSIS Mode Security	Here allows to select DOCSIS mode. Current downstream channel mode: Undetermined(Not connected) ODOCSIS Euro DOCSIS Auto
RF This field allows to set the start frequency of the scanning sequence during initialization and registration. Enter a start frequency in MHz and restart transponder to make it takes effect. Start Frequency(MHZ) 858.25 Bestore Start Frequency	RF This field allows to set the start frequency of the scanning sequence during initialization and registration. Enter a start frequency in MHz and restart transponder to make it takes effect. Start Frequency(MHZ) 858.25	Restore Default	
Start Frequency(MHZ) 858.25 Restore Start Frequency	Start Frequency(MHZ) 858.25		RF This field allows to set the start frequency of the scanning sequence during initialization and registration. Enter a start frequency in MHz and restart transponder to make it takes effect.
Restore Start Frequency			Start Frequency(MHZ) 858.25
	Restore Start Frequency		Restore Start Frequency

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

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.)

Transponder Configurations, Continued

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.

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
cisco	Transponder Restore Default	
Configuration	I his page restore defaults to	o the device parameters and transponder configurations.
Device files		
Firmware Upgrade	A WARNING:	
DOCSIS Mode Security	Reset Device Param all configured paramet may terminate transpo any other system insta	eters and Reset All Settings restore ters to factory default. The operations inder and device connection, or cause ibilities.
Restore Default	Reset All Settings re of all accounts to facto disconnect the target of uninvited access, and change them to your of	stores the WEB UI logon passwords ry default. It's highly recommended to device before operation to prevent any once the passwords are restored, wn immediately.
	 I have read through all the risks, I still wat all the risks, I still wat risks, I still wat all the risks all t	the warning above and understand ant to continue.

©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, and check I have read through the warning above and understand all the risks, I still want to continue box.
- 2. Click Reset Device Parameters or Reset All Settings.

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.

Security

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

Result: The security management window is displayed.

ale ale	
cisco	Transponder
	Security
Configuration	This page allows configuration of administration access privileges and the ability to restore factory defaults to the
Device files	
(Firmware Upgrade)	Current Authorized Level Administrator
DOCSIS Mode	Password Change User ID
Security	New Password
	Re-Enter New Password
Restore Default	Current User ID Password
	Restore Factory Defaults ○ Yes ● No
	Apply

©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.

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.

Status	Transponder HSIA Device High Speed Internet Access Diagnostics Ping	
Ping	This page provides ping diagnostics to help with IP connectivity problems.	
	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 Start Test Abort Test	
	Results Pinging 192.168.100.1 Reply from 192.168.100.1: bytes=1518 seq=0 time < 10ms IIL=64 Reply from 192.168.100.1: bytes=1518 seq=1 time < 10ms IIL=64 Reply from 192.168.100.1: bytes=1518 seq=2 time=1 ms IIL=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. Cisco Compact EGC Segmentable Node A90200 is used in this guide for example. The following contents are applicable based on the assumption that the necessary components are successfully installed on your device. For example, the **Optical Transmitter** section on page 3-30 becomes inapplicable if the device is not successfully installed with an optical transmitter. For any uncertainties, refer to the installation and operation guide of your device.

Identification

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

Result: The identification window is displayed.

Status	Transponder	HSIA	Device
cisco	Devic Identifi	e cation	
Identification	This pag	e displays the	data of Device.
Alarm			
	Item		Value
Setting	Devfile Rev	/ision	0.4
Forward RF	Name		90200
Optical Receiver	Description	1	COMPACT EGC SEGMENTABLE NODE
	Product Ty	ре	EGCNODE
Reverse_RF	Serial Num	ber	23456
	Software N	umber	SCN_1.03.05
(Optical_Transmit1)	Software ID)	2071
Log	Time In Se	rvice	27
	Hardware	/ersion	0
	Production	Date	2008/12/22

The identification tab displays device identification information including its device revision, name, product type, production date ...etc.

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 temperature, tamper status, local craft connection, and the status of Automatic Gain Control (AGC) Module and Reverse Transmitter (RTX). (compromised, intact)

Alarm	
attention: red for alarm	, white for normal
Parameter	Value
Summary Status	Major Alarm
TamperStatus	Compromised
CraftStatus	Connected
AGC1	Error
AGC2	Error
RTX1	Normal
RTX2	Normal

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 node temperature, transmitter power, and receiver power and so on.

Properties Alarm											
attention: red for major ala	rm, yellow fo	r minor alarr	n, white for	norm	al						
			Арр	bly							
h		Current	Major Lo	w	Minor Lo	w	Minor H		Major H		
Item	Status	Value	Value	On	Value	On	Value	On	Value	On	Hysteresis
Node Temperature(C)	Normal	36	-40	•	-15	•	85		90		2
OPT Transmitter Power1 (mW)	Normal	2.0	0.5	•	0.7		4.5		6.0	•	0.1
OPT Transmitter Power2 (mW)	Normal	4.0	0.5	•	0.7		4.5		5.0		0.1
OPT Receiver Power1(mW)	Major Low	0.0	0.1	•	0.4		1.7	•	2.5		0.1
OPT Receiver Power2(mW)	Major Low	0.0	0.1		0.3	•	1.7	•	2.5		0.1
Remote Power(V)	Normal	0	35		40		99		108		5
24V DC(V)	Normal	24.3	23.2		23.8		24.5		25.0		0.1
7V DC(V)	Normal	6.9	6.0		6.5		7.2	•	7.5		0.3
5V DC(V)	Minor Low	5.0	4.5		4.8	•	5.2		5.5		0.3

- 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.

Device Setting

- 1. Click **Device** on the main menu.
- 2. Click **Setting** in the left panel.
- 3. **Result**: The device setting window is displayed.

Status	Transponder HSIA	Device	
cisco	Device		
Identification	Setting This page displays	the data of Device	
Alarm Setting	A.	nghy .	
Forward_RF	ltem	Value	
Optical Receiver	RX1 Optical AGC	AGC OK	
Reverse_RF	RX1 Reference Level(dBm)	-0.3	
Optical_fransmit1	RX2 Optical AGC	AGC OK	
Optical_Transmit2	RX2 Reference Level(dBm)	-4.2	
	Remote Power Connection	Not Connected	
	Display Module	Mounted	
	Forward Mode	Segmentation 💌	
	Reverse Mode	Segmentation 💌	
	TP signal on FwdPath	On_FwdPathA 💌	
	TP signal on TX	On_TX1 💌	
	TP signal Setting	Manual 💌	
	Forward RX Select	force to RX1 💌	
	Number of Return Lasers	2	
	Number of Optical Receivers	2	

The device setting window displays device settings and enables you to configure the forward/reverse mode, Test Point (TP) settings and the forward receiver (RX) option.

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

- 1. Click on the following drop-down box and choose the intended right option.
- a) Click on the drop-down box below to choose the forward and reverse modes.

Forward Mode	Segmentation 💌
Reverse Mode	Segmentation Bedundancy
TP signal on FwdPath	Single
TD signal on TV	

b) Click on the drop-down boxes below to separately choose the TP signal on forward path and transmitter.

TP signals on forward path:

TP signal on EwdPath	On_FwdPathA 💌	
TP signal on TX	On_FwdPathA On_FwdPathB	
TP signal Setting		
Forward RX Select		

TP signals on transmitter:

TP signal on TX	On_TX1 💌		
TP signal Setting	On_TX1		
Forward RX Select		1 🗸	
Number of Return			
Lasers]	

c) Click on the drop-down boxes below to set TP signal setting automatically or manually.

TP signal Setting	Manual 💌
Forward RX Select	Manual (1 🔽
Number of Return Lasers	
Number of Ontical	

d) Click on the drop-down box below to set forward receiver preferences.

Forward RX Select	force to RX1 💌
Number of Return	force to RX1 force to RX2
Number of Optical	prefer RX1 prefer RX2
Receivers	

2. Click **Apply**.

Forward RF

- 1. Click **Device** on the main menu.
- 2. Click **Forward RF** in the left panel.

Result: The Forward RF setting window is displayed.

- Modem Device: Data-Page2 - V	windows Incernet Explorer provided	by Lisco						
🕒 💽 🗢 🙋 https://192.168.1	00.1/HMSDataPage2.asp		T	Certificate Error	* ×	Google		₽ •
File Edit View Favorites Too	ls Help							- "
🔶 Favorites 🛛 🏀 Modem Device: D	ata-Page2				<u>ि</u>	- 🔝 - 🖃 🖶 - Page -	 Safety • 	Tools - 🔞 - "
Status T	ransponder HSIA	Device						^
ahaha	Device							
cisco	Forward_RF							
Identification	This page displays th	e data of Device.						
Alarm		Apply						
Setting	Item	Value						
Forward_RF	FWD BW	862MHZ 💌]					
Optical Receiver	FWD EQ A(dB)	1.0						
	Level Adjust A(dB)	-22.0						
[Reverse_RF]	Power Saving A	On 💌]					
Optical_Transmit1	FWD EQ B(dB)	0.5						
Optical_Transmit2	Level Adjust B(dB)	-22.0]					
	Power Saving B	Off 💌]					
Log								
								-
Jone						😜 Internet	· 6	€ 105% ·

The forward RF setting window enables you to configure the forward bandwidth, forward EQ, level adjust and power saving of the forward RF ports A and B.

Follow the steps below to configure the forward RF settings.

- 1. Click on the drop-down box after FWD BW to choose the forward bandwidth.
- 2. Input the desired value in the textboxes after FWD EQ and Level Adjust.
- 3. Click on the drop-down box after Power Saving to enable or disable power saving mode on the forward RF ports A and B.
- 4. Click **Apply**.

Optical Receiver

- 1. Click **Device** on the main menu.
- 2. Click **Optical Receiver** in the left panel.
- 3. **Result**: The optical receiver setting window is displayed.

🕒 🕑 💌 🕐 https://192.188.100.1/H%D0#aBeg83.asp	P -
File Edit View Favorites Tools Help	
🏫 Favorites 🏽 🍘 Modem Device: Data-Page3	ety 🔹 Tools 👻 🔞 👻 🎽
Status Transponder HSIA Device	_
dulu Device	
CISCO	
Optical Receiver	
Identification This page displays the data of Device.	
Alarm	
Item Value	
Optical Receiver A Present Present	
Optical Receiver A State Off	
Optical Receiver B Present Present	
Reverse_RF Optical Receiver B State Off	
Optical_Transmit1	
opaca_transmiz_	
Log	_
Done Contraction Contra	• •

The optical receiver setting window displays the current status of the optical receiver A and B.

Reverse RF

- 1. Click **Device** on the main menu.
- 2. Click **Reverse RF** in the left panel.

Result: The reverse RF setting window is displayed.

CModem Device: Data-Page4 - Wi	indows Internet Explorer provided l	by Cisco			_ 8 ×
	0.1/HM5DataPage4.asp		💌 😵 Certificate E	irror 🛛 😽 🗙 🚼 Google	P •
File Edit View Favorites Tools	Help				
🔆 Favorites 🔘 Modem Device: Dal	ta-Page4			🏠 🔹 🔂 🖌 🖃 👘 🔹 Page 🕶	Safety + Tools + 🔞 + 🎽
Status Ti	ransponder HSIA	Device			<u>*</u>
cisco	Device				
	Reverse_RF				
Identification	This page displays th	e data of Device.			
Alarm		Apply			
Setting	Item	Value			
Forward_RF	Tri-State Switch A	0dB 💌			
Ontical Pacaivar	Tri-State Switch B	OdB 💌			
Optical Receiver	REV ATT A(dB)	0.0			
Reverse_RF	REV ATT B(dB)	0.0			
Optical_Transmit1					
Optical_Transmit2					
Log					
					-1
(3 items remaining) Downloading picture h	https://192.168.100.1/btn_bottom_right.	gif		Noternet	🖓 • 🔍 110% • 🏾

The reverse RF setting window enables you to configure 3-state switch and reverse attenuator of the reverse RF port A and B.

- 1. Click on the drop-down box after Tri-State Switch A/B to choose attenuation value in dB.
- 2. Input the desired reverse attenuation value in the textboxes after REV ATT A/B in dB.

Note: The above values are defined by the tri-state switch and the reverse attenuator, thus only specified values are allowed as below.



3. Click **Apply**.

Optical Transmitter

- 1. Click **Device** on the main menu.
- 2. Click **Optical Transmitter 1** or **Optical Transmitter 2** in the left panel.

Result: The optical transmitter setting window is displayed.

menv Pavontes 10	us nep	1		N		
5 GModern Device:	Data-Page5			⊡ *6] - 📑 🗰 - Page -	 Safety + Tools
cisco	Device					
	Optical_Transmit1					
dentification	This page displays the d	ata of Device.				
Alarm	A	pply				
Setting	Item	Value				
orward_RF	Model Number ID	90083.101310				
	Serial Number ID	061126F3852				
tical Receiver	Software Number	530383				
Reverse_RF	Pilot Generator	On 💌				
	Transmitter RF BW(MHz)	200				
cal_Transmit1	Electrical Sensitivity (dBuV)	60				
cal_fransmitz	Factory Bias(mA)	30				
Log	Attenuator(dB)	5.5				
	Pilot Setting(dB)	-10.0				
	Pilot Level(dBuV)	40.0				
	Pilot Frequency(MHz)	5				
	Pilot Reference(dB)	-1.0				
	Laser Status	OK				
	Laser Control	On 🔻				

The optical transmitter setting window enables you to view the settings configure the pilot settings, attenuator and laser control of the optical transmitters.

- 1. Click on the drop-down box after Pilot Generator to enable or disable the pilot generator.
- 2. Input the desired values in the textboxes after Attenuator, Pilot Setting in dB.
- 3. Input the desired values in the textboxes after Pilot Level in dBuV.
- 4. Click on the drop-down box after Laser Control to enable or disable the laser control.
- 5. 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.

Status	Transponder	HSIA	Device			
CISCO	Devic Log	e				
Identification	This page	e displays informa	tion on the Device log.			
Alarm						
Setting	Time Tue Feb 21	04:48:05 2012	OID 1.3.6.1.4.1.5591.1.5.5.1.2.1	Value 0	type LOLO (5)	
Forward_RF	Tue Feb 21	04:47:33 2012	1.3.6.1.4.1.5591.1.5.5.1.2.1	0	NOMINAL (1)	
Optical Receiver	Clear Log	Upload Log				
Reverse_RF	I					
Optical_Transmit1						
Log						

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

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**.

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.

Logs Operator Alarms Reports Window View Mode Help					
10_75_196_19 (System)					
	Time Synchronization Apollo	configuration Alarm Bufferir	a Persistence IP Cor	fig SecondNIC Routing	IPSec Services
— 🛁 Nod001 (Node)	Paging Service Email Servi	ce SMS Service Operat	r HEC.Plant.Monitoring	Debug Device Backup	Device-Polling Config Backup
— 🔜 Nod000 (Node)	Properties Alarm Processing	1 System License Clie	nt Connections SNMD	Notification Information N	otify Group Member Information
— insaemio (IO)	Properties Hidrifferfocessing	j System Electrise Cite	in connectiona Shawin	Notification_Information	ony_oroup member_mormation
	Parameter	Value			
	Currently Routed Subnet	265 265 265 0			
	Current Overboad Gateway	10.75.106.20			
	New Routed Subnet	10 200 10 0			
	New Routed Subnet Mask	255.255.255.0			
	New Overhead Gateway	10.75.196.20			
	New Route Apply Changes				

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**.



ROSA Element Management System, Continued

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.

🕌 Change Parameter Dialog 🛛 🗙				
Device: 10_75_196_19				
Parameter: New Routed Subnet Mask				
This is the new subnet mask of the subnet to which you can route on the second NIC. This new subnet mask will only become active after clicking on New Route Apply Changes and choosing Apply.				
255.255.255.0				
Execute Cancel				

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**.

🛓 Change Parameter Dialog 🛛 🗙				
Device: 10_75_196_19				
Parameter: New Overhead Gateway				
This is the new overhead gateway to which you can route on the second NIC. This new overhead gateway will only become active after clicking on New Route Apply Changes and choosing Apply.				
10.75.196.20				
Execute Cancel				

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

🛓 Change Parameter Dialog	×
Device: 10_75_196_19	
Parameter: New Route Apply Changes	
Choose Apply to program the new route on the second NIC.	
Apply	
Execute Cancel	

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.

Chapter 4 Troubleshooting

Overview

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

In This Chapter

Topic	See Page
Transponder Signaling	4-2
Further Assistance	4-4

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	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	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	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	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.

Problem Description	Solution
The LED Status is ON	Check if certain specs or properties exceeded the limit of the alarm status of your transponder. See Alarm section on page 3-24 for details.
The LED USB is OFF	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.

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*.

Chapter 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.

. . | . . . | . . CISCO .

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

This document includes various trademarks of Cisco Systems, Inc. Please see the Notices section of this document for a list of Cisco Systems, Inc., trademarks used in this document. Product and service availability are subject to change without notice.

© 2013 Cisco Systems, Inc. All rights reserved. December 2013 Printed in United States of America

Part Number OL-31165-01