

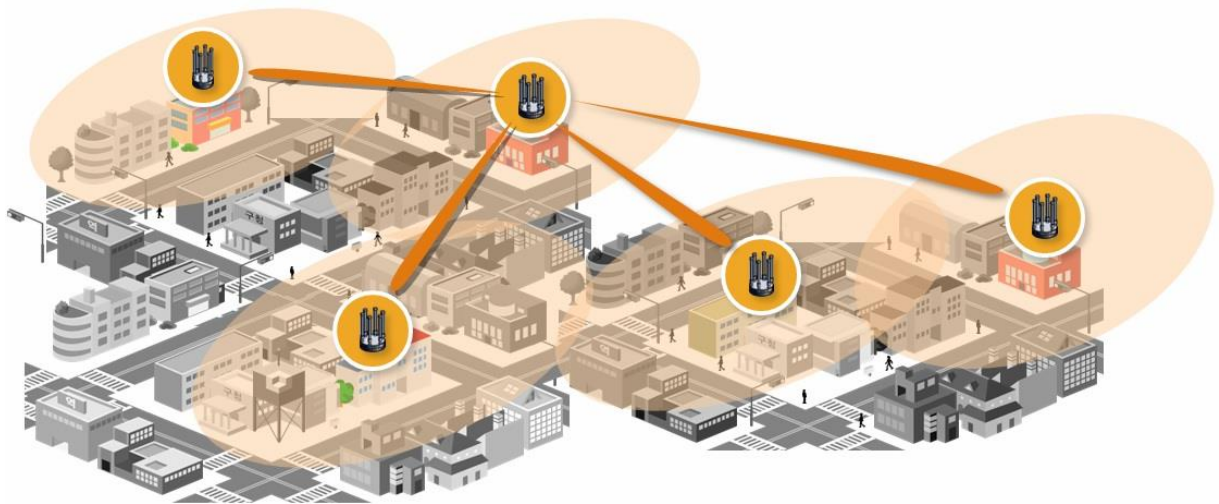


NetBeam Family

Gigabit Ethernet Wireless Solutions

NetBeam Family (M71, M72, 1G1, 1G2, 2G2 and 2G2)

SYSTEM MANUAL



May 2014

This document contains information that is proprietary to Netronics Technologies Inc.

No part of this publication may be reproduced, modified, or distributed without prior written authorization of Netronics Technologies Inc.

This document is provided as is, without warranty of any kind.

Statement of Conditions

The information contained in this document is subject to change without notice.

Netronics shall not be liable for errors contained herein or for incidental or consequential damage in connection with the furnishing, performance, or use of this document or equipment supplied with it.

Information to User

Any changes or modifications of equipment not expressly approved by the manufacturer could void the user's authority to operate the equipment and the warranty for such equipment.

Copyright © 2011 by Netronics. All rights reserved.

READ THIS FIRST!

Important Safety Instructions



Caution

Read and save these instructions. Heed all warnings. Follow all instructions.



Caution

Do not defeat the safety purpose of the grounding. Only use attachments/accessories specified by the manufacturer.



Caution

Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way. For example, if the power-supply cord or plug is damaged, liquid has been spilled on the apparatus, objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, it does not operate normally, or has been dropped.



Warning

There is a risk of personal injury or death if the NetBeam antennas come near electric power lines. Carefully read and follow all instructions in this manual. By nature of the installation, you may be exposed to hazardous environments and high voltage. Use caution when installing the outdoor system.



Warning

This apparatus must be connected to earth ground.



Warning

Do not open the unit. There is a risk of electric shock inside.



Caution

You are cautioned that any change or modification not expressly approved in this manual could void your authority to operate this equipment.



Caution

There are no user-serviceable parts inside. All service must be performed by qualified personnel.



Caution

The Netronics NetBeam can be installed in wet, outdoor locations. Make sure closure caps are installed and all cable connections are securely fastened and waterproofed.



Caution

The Netronics NetBeam can only be used with approved antennas.

Safety and Regulatory Notices

The following are mandatory notices for installation and operation of NetBeam 71-76/81-86 Ghz Wireless Backhaul Link. Indications appearing here are required by the designated government and regulatory agencies for purposes of safety and compliance.

General

Do not install or operate this System in the presence of flammable gases or fumes. Operating any electrical instrument in such an environment is a safety hazard.

European Commission

This product has been designed to comply with CE markings in accordance with the requirements of European Directive 1995/5/EC.

This product has been designed to comply with the requirements of European Directives.

This equipment must be permanently earthed for protection and functional purposes. To make a protective earth connection, use the grounding point located on the System ODU using a minimum amount of 16AWG grounding cable or according to local electrical code.

This apparatus is intended to be accessible only to authorized personnel. Failure to prevent access by unauthorized personnel will invalidate any approval given to this apparatus.

This product is in full compliance with the following standards:

- RF EN 302 217-3 1.3.1
- EMC EN 301 489-4
- Safety IEC 60950
- Operation EN 300 019-1-4 Class 4.1E
- Storage EN 300 019-1-1 Class 1.2
- Transportation EN 300 019-1-2 Class 2.2

About this Document

This document is the Installation and User Manual for the NetBeam family 71-76/81-86 GHz Wireless Link.

This includes the following:

- TDD family (71-76 Ghz):
 - 1G1 and 1G2 (up to 1 Gbps), M71 and M72 (700 Mbps)
 - Two active GbE ports
 - Updated SW version 3.3
- FDD family (71-76/81-86 Ghz):
 - 2G1 and 2G2
 - Four active Gbe ports
 - Updated SW version 5.1.0

Audience

This document assumes a working knowledge of wireless backhaul platforms and their operating environments.

This document is intended for use by all persons who are involved in planning, installing, configuring, and using the NetBeam system.

Conventions

The following conventions are used in this document in order to make locating, reading, and using information easier.

Special Attention



Informs you of a helpful optional activity that may be performed at the current operating stage.



Note

Provides important and useful information.



Caution

Describes an activity or situation that may or will interrupt normal operation of the NetBeam system, one of its components, or the network.

Table of Contents

Chapter 1 Introduction to the NetBeam System	
System Applications.....	13
Main Features.....	15
NetBeam Product Family.....	16
Functional Description.....	18
Licensing.....	19
Management.....	19
Technical Specifications.....	19
Chapter 2 Installing the NetBeam System	
Preparing the Site.....	20
Physical and Environmental Requirements.....	20
Cabling Requirements.....	21
NetBeam Package Contents.....	22
Unpacking the NetBeam.....	22
Required Tools.....	22
Preparing for Installation.....	23
Mounting the NetBeam.....	23
Installing the ODU with a Two Foot Antenna.....	25
Connecting the Cables.....	28
Grounding the NetBeam and Cables.....	29
Power Supply Notes.....	30
Preparing the Cables.....	31
Removing Connectors from the NetBeam ODU.....	32
Connecting the Power.....	32
Connecting Other Interfaces.....	33
Aligning the Antenna.....	33
Setting the ODU to Alignment Mode.....	34
Performing the Alignment.....	34
Performing Initial System Setup.....	36
Chapter 3 Performing Basic Configuration Using the Web EMS	
Connecting to the ODU Using the Web EMS.....	39
Saving Configuration Changes and Resetting the System Using the Web EMS	40
Quick Configuration.....	40
Configuring and Displaying Basic System Information Using the Web EMS.....	41
Configuring System IP Addresses Using the Web EMS	42
Configuring Radio Parameters Using the Web EMS	44
Viewing Modulation Profiles Using the Web EMS.....	47
Configuring Ethernet Interfaces Using the Web EMS.....	47
Configuring SNMP Settings	50
Default VLAN Setting	51
Chapter 4 Performing Basic Configuration using the CLI	
Establishing a CLI Session with the ODU.....	53
Saving Configuration Changes and Resetting the System Using the CLI.....	53
Configuring and Displaying Basic System Information Using the CLI.....	53
Configuring System IP Addresses Using the CLI.....	54
Configuring Radio Parameters Using the CLI.....	56
Displaying Radio Parameters and Status Using the CLI.....	56
Configuring the Radio Parameters Using the CLI.....	58
Viewing Modulation Profiles Using the CLI.....	58

Configuring Ethernet Interfaces Using the CLI.....	59
Configuring Interface Parameters.....	59
Displaying Interface Status.....	60
Default VLAN Setting.....	61
Chapter 5 Commissioning and Acceptance Procedure	
Installation Verification and Testing.....	62
Physical Installation Verification.....	62
RF Link Test.....	63
Link Errors Test.....	63
Ethernet Services Test.....	63
Management Verification.....	63
Recording ODU Configuration.....	63
NetBeam Commissioning and Acceptance Form.....	64
Chapter 6 NetBeam Networking Configuration	
Provider Bridge.....	68
NetBeam Bridging Model.....	69
Configuring VLANs.....	70
Transparent Bridge Mode.....	70
Configuring VLANs Using the Web EMS.....	71
Configuring VLANs Using the CLI.....	72
Single Component Bridge Model.....	74
Model Implementation.....	74
VLAN Configuration.....	75
Configuring Bridge Ports.....	77
Configuring Bridge Ports Using the Web EMS.....	77
Configuring Bridge Ports Using the CLI.....	79
Configuring the Bridging Port.....	79
Configuring Provider Bridge and Advanced VLAN Settings.....	80
Configuring PEP Virtual Ports.....	80
S-VID Translation Table.....	81
C-VLAN Registration Table.....	82
VLAN-to-SNMP ifTable.....	83
Forwarding Data Base (FDB).....	83
Configurable Eth-type.....	84
FDB Address Table.....	85
Chapter 7 Performing Advanced Configuration	
Configuring Quality-of-Service.....	87
QoS Classification.....	88
Metering and Coloring.....	93
QoS Scheduling	94
Weighted Random Early Detection (WRED).....	98
WRED Functionality	98
WRED Parameters	99
CLI	99
Example Measurement.....	100
Configuring CFM (Connectivity Fault Management).....	100
CFM Overview	101
Working with Maintenance Domains	102
Working with Maintenance Associations.....	103
Working with Component Maintenance Associations	104
Working with Maintenance End Points (MEPS).....	105
Working with Peer MEPS	107

Working with CCM Messages	108
Working with Linktrace Messages	108
Sample CFM Configuration	110
Configuring Link OAM.....	117
Enabling Link OAM.....	118
Link OAM Discovery.....	118
Link OAM Loopback.....	119
Configuring Synchronous Ethernet (SyncE).....	120
SyncE Overview.....	121
SyncE Configuration.....	121
Basic SyncE Scenario.....	123
Typical SyncE Scenario.....	124
Electrical 10/100/1000 Ports Setting for SyncE.....	128
SyncE Alarms.....	129
IEEE 1588v2 Transparent Clock (TC).....	129
Configuring Ethernet Ring Protection (ERP).....	131
Supported ERP Features.....	131
ERP Ring Commands.....	132
ERP Administrative Commands.....	133
ERP Timers.....	134
ERP Configuration Example.....	134
Chapter 8 Monitoring the System	
Viewing Active Alarms.....	137
Viewing Alarm History and System Events.....	138
Events Configuration (Masking).....	139
Viewing Radio Statistics.....	140
Viewing Radio Statistics Using the Web EMS.....	140
Viewing a Statistics Summary Using the Web EMS.....	141
Viewing Radio Statistics Using the CLI.....	142
Viewing Radio Statistics Summary Using the CLI.....	143
Viewing VLAN Statistics.....	143
Viewing Queue Statistics.....	144
Viewing Outgoing Queue Statistics.....	144
Incoming Queues Commands.....	145
Viewing Ethernet Statistics.....	146
Ethernet Statistics Attributes.....	146
Viewing Ethernet Statistics Using the Web EMS.....	147
Viewing Ethernet Statistics Using the CLI.....	148
Viewing Bandwidth Utilization Statistics.....	148
Chapter 9 Performing System Administration	
Configuring Encryption.....	151
Loading Encryption License Key.....	151
Setting up a Static Key.....	151
Working with Configuration Files.....	151
Saving Configurations.....	152
Viewing Configurations.....	152
Restoring the Default Configuration.....	152
Rollback Operations.....	153
Configuring Users.....	153
Upgrading the ODU Software.....	155
Upgrading the ODU Software Using the Web EMS.....	155

Upgrading the ODU Software Using the CLI.....	156
Monitoring CLI Sessions.....	158
Viewing System Inventory.....	159
Viewing System Inventory Using the Web EMS.....	159
Viewing System Inventory Using the CLI.....	160
Upgrading the License Key.....	160
Performing Address Translation.....	162
Netronics File System (SFS).....	163
Understanding SFS.....	163
Specifying Files Using URLs.....	163
File System Commands.....	164
SFS Example for Backup/Restore of Configuration file.....	165
History File Transfer.....	166
Command Line Scripts.....	177
Displaying Scripts.....	178
Running Scripts.....	178
Adding Scripts.....	178
Viewing Script Content.....	179
Command Line Scripts using the CLI.....	180
Macro Scripts.....	181
CLI Example.....	181
MAC Table Limitations.....	182
MAC Table Limitation Setting Procedure.....	182
CLI Example.....	182
Configuring NTP.....	183
NTP Configuration.....	183
Viewing User Activity Log.....	184
Access Control List (ACL).....	185
LLDP - Link Layer Discovery Protocol.....	186
DHCP.....	187
Managing SNMP.....	189
SNMP Managers.....	189
SNMP Agent Communities.....	190
SNMPv3 Users Settings.....	191
Tacacs+ / Radius.....	191
Ping (Supported only from CLI).....	193
Traceroute (Supported Only in CLI).....	194
Traceroute CLI Commands.....	194
Chapter 10 Zero Touch	
Zero Touch Feature.....	195
Zero Touch Predefinitions.....	195
Zero Touch System Process.....	196
Configure Zero Touch in the CLI	198
Configure Zero Touch in the WEB EMS.....	199
Chapter 11 NetBeam Diagnostics	
The Troubleshooting and Diagnostics Process	201
NetBeam ODU LEDs.....	202
NetBeam System Alarms and Events	202
NetBeam System Statistics.....	206
RF Statistics.....	207
VLAN Statistics.....	207
Ethernet Statistics.....	208
NetBeam System Loopbacks.....	208

Loopback Diagrams.....	209
Chapter 12 Using the NetBeam CLI	
Invoking the CLI.....	211
CLI Command Syntax.....	212
Basic Conventions.....	213
Common Syntax Rules.....	213
Repeatedly Used Identifiers.....	213
CLI Command Types.....	215
Designating Objects in CLI Commands.....	219
Designating Named Objects.....	219
Viewing the CLI Command History.....	222
Invoking CLI Help and Autocompletion.....	223
CLI Error Messages.....	224
Viewing the NetBeam Statistics History.....	225
Using Statistics Intervals.....	225
CLI Managed Object Reference.....	226
Management Object Attributes.....	227
System Object Attributes.....	227
Physical Inventory Object Attributes.....	230
Physical Inventory Entities.....	237
Radio Object Attributes.....	243
RF Object Attributes.....	243
Radio Statistics.....	245
Encryption Object Attributes.....	247
Connectivity Fault Management (CFM) Object Attributes.....	247
Maintenance Domain (MD) Object Attributes.....	247
Maintenance Association (MA) Object Attributes.....	249
Component MA Object Attributes.....	250
Maintenance End Point (MEP) Object Attributes.....	252
CCM Message Object Attributes.....	260
Peer MEP Object Attributes.....	261
Peer MEP Database Attributes.....	262
LTR Object Attributes.....	265
Network Object Attributes.....	270
Ethernet Interface Attributes.....	270
Ethernet Statistic Descriptions.....	278
Bridge Object Attributes.....	279
Bridging Port Object Attributes.....	280
Outgoing Queue Object Attributes.....	283
Incoming Queue Object Attributes.....	283
IP Object Attributes.....	284
VLAN Common Table Attributes.....	285
VLAN Table Attributes.....	286
C-LAN Registration Table Attributes.....	287
PEP Virtual Port Table Attributes.....	289
S-VID Translation Table Attributes.....	290
SNMP ifTable Attributes.....	292
Forwarding Data Base (FDB) Object Attributes.....	295
FDB Address Table Attributes.....	297
ARP Table Attributes.....	299

Chapter 1

Introduction

Welcome to NetBeam!

Netronics' NetBeam is a carrier-class, high-capacity E-band radio that dramatically lowers the cost of wireless and Ethernet backhaul. The system is uniquely based on an all-silicon design that results in fewer components, greater reliability, and pricing that is up to 80% less than comparable radio systems. Operating in the uncongested and lightly licensed 71-76/81-86 Ghz E-band, TCO (total cost of ownership) is reduced even further to the lowest in the industry.

The following are just some of the highlights of the NetBeam system:

- Operates in the licensed, uncongested, and lightly licensed 71-76/81-86Ghz E-band
- Carrier-grade Gigabit Ethernet radio
- Revolutionary all-silicon-based design, resulting in the industry's lowest TCO
- Priced at as little as one-fifth the cost of available wireless radio alternatives
- Green design providing for extremely low power consumption, small form factor, and easy installation
- Perfect wireless backhaul solution for mobile operators, business service providers, and enterprises



Figure 1-1: NetBeam 1G1 System

System Applications

Wireless Backhaul for 2G, 3G, 4G, LTE, and WiMAX Networks

High-capacity Gigabit Ethernet backhaul at the lowest TCO in the industry enables mobile operators to provide data-intensive services profitably and reliably.

- NetBeam uses the uncongested and interference-free licensed E band 71-76/81-86Ghz wireless spectrum, enabling fast and efficient frequency and network planning and deployment. As a bonus, licensing registration processes for this band are cheaper, simpler, and quicker.
- With 1 Gbps throughput, the NetBeam radio future-proofs the backhaul network to meet the growth in demand for data capacity from 4G, LTE, and WiMAX installations.
- Carrier-class Ethernet provides QoS and OAM with standards-based support for ring, mesh, and multi add-drop topologies, assuring resiliency and high availability.
- NetBeam's bandwidth-aware QoS mechanism differentiates between multiple services, guaranteeing efficient transport of timing, signaling, voice, video, web surfing, and more.
- Advanced timing over packet handling (SyncE, IEEE 1588) enables migration to packet-based backhaul.
- All-outdoor unit eliminates co-location fees and costs associated with indoor installations, and enables fast deployment at any cell-site.
- Low power consumption delivers 80% energy savings.

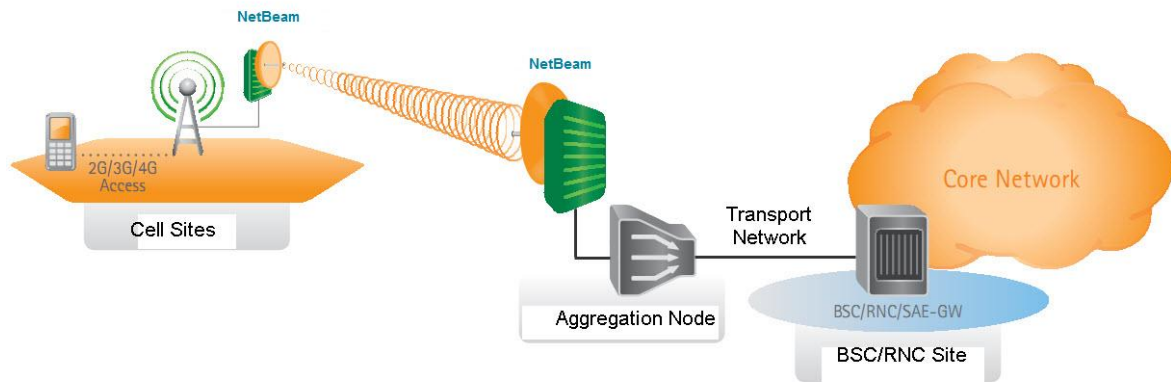


Figure 1-2: Wireless Backhaul for 2G, 3G, 4G, LTE, and WiMAX Networks

Ethernet Wireless Backhaul for Business Services and Enterprise Connectivity

A low cost, high capacity Ethernet wireless solution enables you to rapidly extend your fiber reach beyond your existing fiber footprint or to expand your enterprise network.

- NetBeam operates in the licensed E-band 71-76/81-86Ghz wireless spectrum, with significantly lower licensing fees and simpler and quicker licensing registration processes, for rapid service deployment.
- 1 Gbps throughput delivers enough capacity to support voice, video, and high speed data services.
- NetBeam's advanced Carrier Ethernet capabilities enable differentiated QoS, maintaining diverse SLAs for multiple services and customers.
- NetBeam's all-outdoor unit eliminates the need for a dedicated indoor cabinet and enables rapid roll-out with minimal site preparation.
- NetBeam's zero footprint and flexible installation options enable deployment in any urban, business, or residential environment.
- NetBeam's low power consumption enables the use of standard PoE supplies, connecting the radio with a single cable for both power and data.

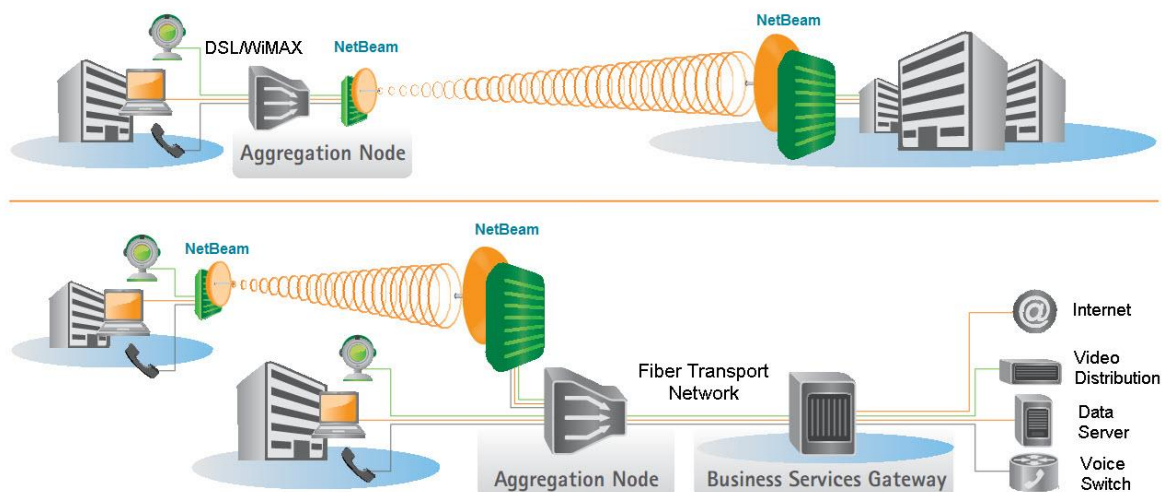


Figure 1-3: Wireless Backhaul for Business Services and Enterprise Connectivity

Main Features

Netronics' NetBeam wireless backhaul radio link operates in the new E-band spectrum, which provides clear technological and economic advantages over the existing lower frequency bands. Taking advantage of the new spectrum, the NetBeam enables easy migration to support Gigabit throughput, enabling operators to enhance bandwidth capacity on a "pay as you grow" basis. Supporting point-to-point, daisy-chain, ring, and mesh configurations, NetBeam system offers carrier class availability and services.

The following are some of the main features of the NetBeam (availability of features depends on platform):

All-Outdoor Packet E-band Radio

- Operates in the licensed 71-76/81-86 GHz E-band
- Up to 1 Gbps throughput
- Asymmetric capacity configuration [TDD version]
- High gain narrow beam-width directional antenna
- Low latency

Highest Spectral Efficiency in E-band Spectrum

- 250 MHz, 500 MHz channel bandwidth
- Advanced hitless/errorless Adaptive Bandwidth, Coding and Modulation (ABCM) for a large dynamic range
- Configurable center frequency across the entire band

Carrier Ethernet Inside:

- Integrated Gigabit Ethernet switch
- Advanced bandwidth-aware QoS capabilities
- MEF compliant services and QoS
- Advanced service management and OAM
- SyncE, optimized transport of IEEE 1588 and IEEE 1588TC
- Ring, mesh, and Link Aggregation (1+1, 2+0) for carrier class availability and resiliency
- Standard-based for seamless integration into existing networks and multi-vendor interoperability
- Seamless software upgrades to MPLS, IP, and beyond

Carrier Grade:

- CLI, SNMP, or web-based local and remote management
- Extremely high reliability with high MTBF
- Designed for ultra-low MTTR without the need for antenna realignment

Green Design:

- Zero footprint, all-outdoor, extremely light weight

- Ultra low power consumption
- Standard IEEE 802.3 at Power over Ethernet (PoE)

Quick and Easy Installation

- Rapid and flexible deployment
- Precise antenna alignment
- Minimal site preparation

Security

- Advanced AES encryption and security
- Narrow and secure beam-width

Adaptive Bandwidth, Coding and Modulation

The NetBeam family implements hitless/errorless adaptive bandwidth, coding and modulation adjustment to optimize the over-the-air transmission and prevent weather-related fading from disrupting traffic on the link. The NetBeam can gain up to 21 dB in link budget by dynamically adapting: Modulation, FEC coding rates, and channel bandwidth dropping the traffic according to the QoS priority (see *Configuring Quality-of-Service* on page 87).

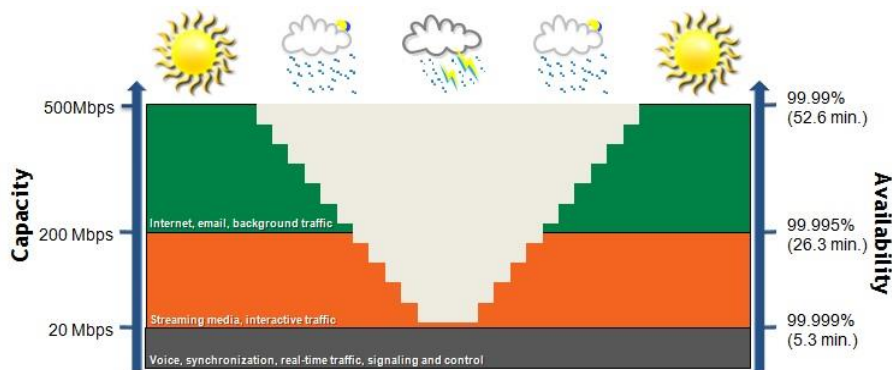


Figure 1-4: Hitless Adaptive Bandwidth, Coding and Modulation

NetBeam Product Family

Feature	NetBeam 1G	NetBeam M7	NetBeam 2G
Frequency	71-76 GHz		71-76/81-86 GHz
Duplexing	TDD		FDD
Modulation Schemes- ABCM	QPSK/QAM16/QAM64	QPSK/QAM16	QPSK/QAM16/QAM64
System throughput	Up to 1000Mbps half-duplex	700Mbps half-duplex	Up to 1000Mbps full-duplex

Traffic Interfaces	2 x GE – combo copper and fiber ports	4xGE - 2xCopper+ 2xFiber ports - 1xCopper+ 3xFiber ports
Antenna	<ul style="list-style-type: none"> Integrated 1ft (26cm) 42dBi antenna gain Integrated 1ft (31cm) 43dBi antenna gain External 2ft (65cm) 50dBi antenna gain 	Integrated 1ft (31cm) 43dBi antenna gain External 2ft (65cm) 50dBi antenna gain
Power specifications	<ul style="list-style-type: none"> PoE+ (IEEE 802.3at) Wide-voltage interface: $\pm 22-60\text{VDC}$ 	
Carrier Ethernet inside	<ul style="list-style-type: none"> VLAN/VLAN stacking (QinQ- IEEE 802.1ad Provider Bridge) IEEE 802.1d Transparent Bridging MAC learning Link state propagation Jumbo frames Traffic management- 802.1p, DSCP & MPLS EXP Scheduler, Shaping, Policing 	
Synchronization	<ul style="list-style-type: none"> Synchronous Ethernet ITU-T G.8261/8262/8264 	<ul style="list-style-type: none"> 1588 TC Synchronous Ethernet ITU-T G.8261/8262/8264
MEF compliant	<ul style="list-style-type: none"> MEF services compliant MEF 9,14 and 21 complaint 	
Security	1. AES 128-bit and 256-bit	
Advanced L2 features	<ul style="list-style-type: none"> Eth OAM (IEEE802.1ag/Y.1731/IEEE802.3ah) G.8032 ERPS 	<ul style="list-style-type: none"> Eth OAM (IEEE802.1ag/Y.1731/IEEE802.3ah) G.8032 ERPS
Management	<ul style="list-style-type: none"> Out of band, Inband management, Embedded WEB GUI, SNMPv2/3 	
Conformance	<ul style="list-style-type: none"> ETSI EN 302 217-4, CE marked, EMC, safety 	
Environmental characteristic	<ul style="list-style-type: none"> Operating Temperature- $-45^{\circ} \div +55^{\circ}\text{C}$ ($-49^{\circ} \div +131^{\circ}\text{F}$) Ingress Protection Rating - IP67 	
Dimensions (H x W x D)	<ul style="list-style-type: none"> 24.5 cm x 22.5 cm x 5 cm ODU + Antenna 31cm(Dia. x Depth)-31 cm x 11 cm 	<ul style="list-style-type: none"> 24.5 cm x 22.5 cm x 7 cm ODU + Antenna 31cm (Dia. x Depth) -31 cm x 13 cm
Weight	<ul style="list-style-type: none"> ODU + antenna (31 cm): 3.5 kg 	<ul style="list-style-type: none"> ODU + antenna (31 cm): 4 kg

Functional Description

The NetBeam ODU consists of four main building blocks: Antenna, RFIC, Baseband modem, and Network processor.

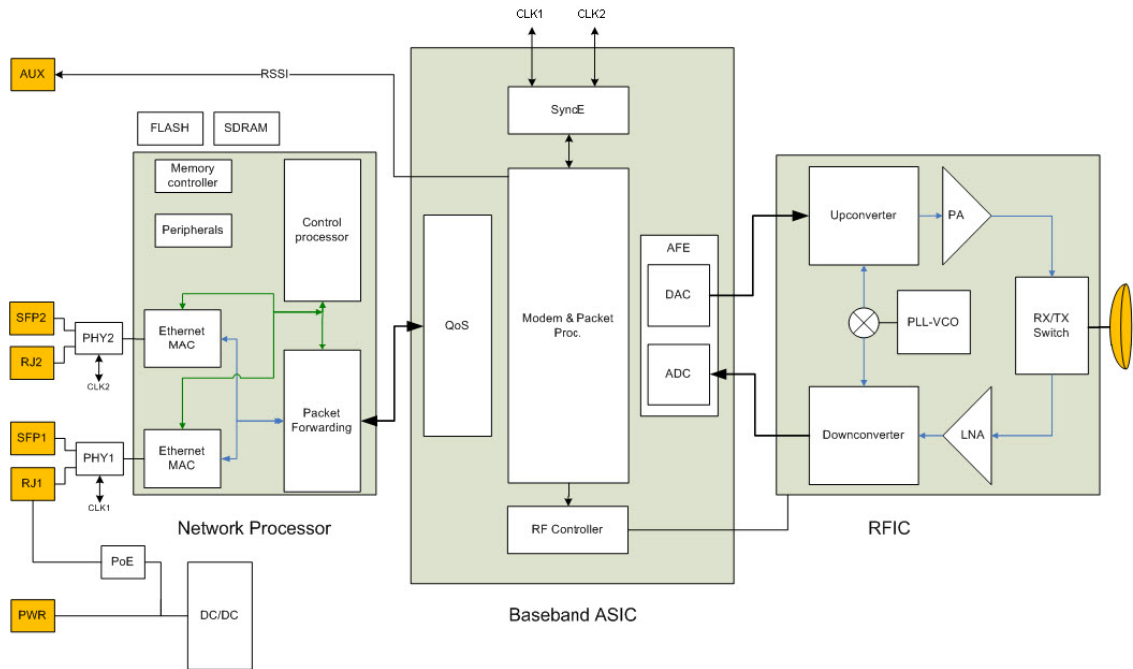


Figure 1-5: NetBeam M7 Functional Block Diagram

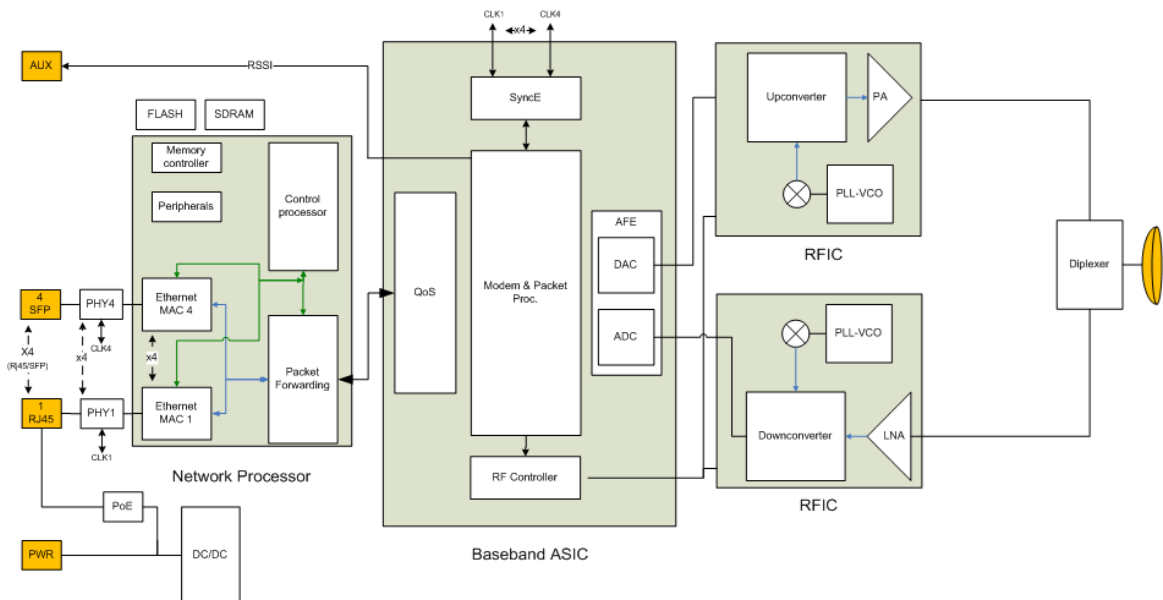


Figure 1-6: NetBeam 2G Functional Block Diagram

- RFIC – Netronics’ integrated Silicon Germanium (SiGe) transceiver operating at 71-76/81-86 Ghz.

- Modem/Baseband ASIC – Netronics’ modem/baseband ASIC includes the modem, FEC engines, and Synchronous Ethernet support.
- Network Processor – The network interface consists of integrated 100/1000 Ethernet MAC I/F. The block is suitable for both copper and fiber interfaces by using the external PHY.

The networking engine is the heart of the high speed bridge/router function. The engine receives packets from both Ethernet interfaces and from the modem. It is responsible for proper forwarding between these four ports.

- Host processor (integrated with the network processor) – The general purpose host processor controls the system, and the antenna alignment system. The processor is integrated with standard peripherals such as memory controller, communication I/F, WD, GPIO, and motor controller.
- Antenna – Netronics’ self-designed, innovative antenna is designed for best price-performance ratio.

Licensing

The NetBeam family provides for easy migration to support Gigabit throughput, enabling operators to enhance bandwidth capacity on a “pay as you grow” basis as well as adding features and capabilities according to their networks evolutions. You can order the following NetBeam software (capacity steps and feature availability depend on your platform):

- Data rates
- Layer 2 networking capabilities – OAM and Resiliency
- Synchronization – Synchronous Ethernet (ITU-T G.8261) and IEE-1588TC
- Encryption

Vlan configuration and Provider-Bridge settings capabilities are enabled by default and do not require a license.

The software licenses are serial number dependent.

Management

You can manage a NetBeam system using a Web-Based Element Management System (Web EMS) or a Command Line Interface (CLI). The CLI is compatible with SNMP.

Advanced network features must be managed using the CLI.

The NetBeam system features a wide range of built-in indicators and diagnostic tools for advanced OAM functionality. The system is designed to enable quick evaluation, identification, and resolution of operating faults. See *NetBeam Diagnostics* on page 201.

Technical Specifications

For detailed technical specifications please refer to the datasheet.

Chapter 2

Installing the NetBeam System

This chapter describes how to install and perform the basic setup for NetBeam antenna outdoor units (ODUs) in a NetBeam wireless network, including:

- Preparing the Site
- NetBeam Package Contents
- Unpacking the NetBeam
- Required Tools
- Preparing for Installation
- Mounting the NetBeam
- Installing the ODU with a Two Foot Antenna
- Connecting the Cables
- Aligning the Antenna
- Performing Initial System Setup



Note

The installation and maintenance of the NetBeam link should only be done by service personnel who are properly trained and certified to carry out such activities.

Preparing the Site

Carefully select and prepare each NetBeam ODU site to make device installation and configuration as simple and trouble-free as possible. During site selection and preparation, always consider the long-term needs of both your network and your applications.

Physical and Environmental Requirements

Each NetBeam ODU site should adhere to the following requirements:

- There must be a clear, unobstructed line-of-sight between ODU nodes.

- You must mount the NetBeam ODU on a fixed, stable, permanent structure. A reinforced steel mounting pole is required, with a diameter measuring from 2-4 inches (5-10 centimeters).



Do not mount the NetBeam device on a structure that is temporary or easily moved. Doing so may result in poor service or equipment damage.

- You must mount the NetBeam ODU in a site that is easily accessible to authorized personnel, and only authorized personnel.
- Operating temperature: between -45° and +55°C.
- Relative humidity: 0 to 100%.
- Maximum altitude: 4,500 m.
- Ingress Protection rating: IP67.

Cabling Requirements

- Ensure that your power connection cable matches the NetBeam power connector pin-outs. See Figure 2 4 for the DC power connector pin-out diagram.
- Install the NetBeam ODU where network connections and optional power cabling are ready for operation and easily accessible.
- All cabling connected to the ODU should be outdoor-grade, with UV protection.
- Use a two-wire cable (14-18 AWG) to connect the power supply to the ODU.
- You should use shielded outdoor Cat5e cables terminated with metallic RJ45 connectors.
- In order to protect indoor equipment, you must install surge protection circuits on all copper cables (DC and Ethernet) on their entrance to the building.
- Install the NetBeam ODU in a location where proper electrical outdoor grounding is readily available. Typically, the grounding connection is attached directly to the mounting pole. If not already present, then suitable structure-to-earth grounding connections must be created before installation. Ground the ODU using a minimum quantity of 16AWG grounding cable or according to local electrical code.



Improper electrical grounding can result in excessive electromagnetic interference or electrical discharge.

Netronics will not be held responsible for any malfunction or damage in the event that the ODU is not properly grounded.

NetBeam Package Contents

A NetBeam link consists of two ODUs and two mounting assemblies.

The NetBeam package includes the following components:

Package	Description	NetBeam 1G1 and M71 Quantity	NetBeam 2G1 Quantity
NetBeam ODU			
	NetBeam ODU (including 1ft antenna and radome)	1	1
	Connecting cable All-Weather shells	3	6
	Connecting fiber All-Weather shells		1
	Unit grounding cable (90 cm)	1	1
	DC cable terminal block connector	1	1
NetBeam mounting assembly			
	NetBeam mounting assembly	1	1

You must examine all NetBeam package contents carefully upon arrival. If a component is missing or damaged, contact your NetBeam distributor before attempting to install the equipment.

Unpacking the NetBeam

When you unpack the components of the NetBeam, it is important to use care so as to avoid damaging or scratching the antenna radome:

- Do not touch the radome when unpacking the ODU.
- Do not rest the ODU face down or touch the radome. It is crucial to prevent contact between the radome and other objects.

Required Tools

Ensure that you have the following tools with you when performing a NetBeam installation:

- Standard handheld digital voltage meter (DVM) with probes
- Standard open-end wrench, 13 millimeter
- Philips screwdriver (medium size head for grounding connection)
- 8mm Allen key for ODU installation with 2 ft antenna
- Cable ties (for securing network and optional power cables)
- Cutter

- Cable labeling

Preparing for Installation

- You must install NetBeam units in pairs, working with two technicians. One technician must be located at each node, in order to align and calibrate each antenna ODU with its remote node pair for best performance.
- You must calculate the expected receive signal strength for each antenna ODU (read from the DVM) prior to installation, based on the network link budget.

Calculating the expected RSSI:

$$\text{RSSI} = P_{\text{tx}} + G_{\text{ant1}} - \text{LFS} - \text{Att}_{\text{atm}} + G_{\text{ant2}}$$

Where:

- P_{tx} – ODU's Tx Power (typically +5dBm)
- G_{ant1} – Gain of antenna 1 (in dBi)
- G_{ant2} – Gain of antenna 2 (in dBi)
- LFS – Loss of Free Space = $92.45 + 20 * \text{Log}(D_{\text{Km}} * F_{\text{GHz}})$
 - D - Link distance in Km
 - F – Frequency in GHz
- Att_{atm} – Attenuation due to Atmospheric gases ($\sim 0.5\text{dB/Km}$) = $0.5 * D_{\text{Km}}$

Mounting the NetBeam 1G1



- These instructions are for mounting a system with a one-foot antenna. For instructions on mounting the NetBeam with a two-foot antenna, refer to *Installing the ODU with a Two Foot Antenna* on page 25.
- Torque level for tightening the nuts and bolts is 8 nm.

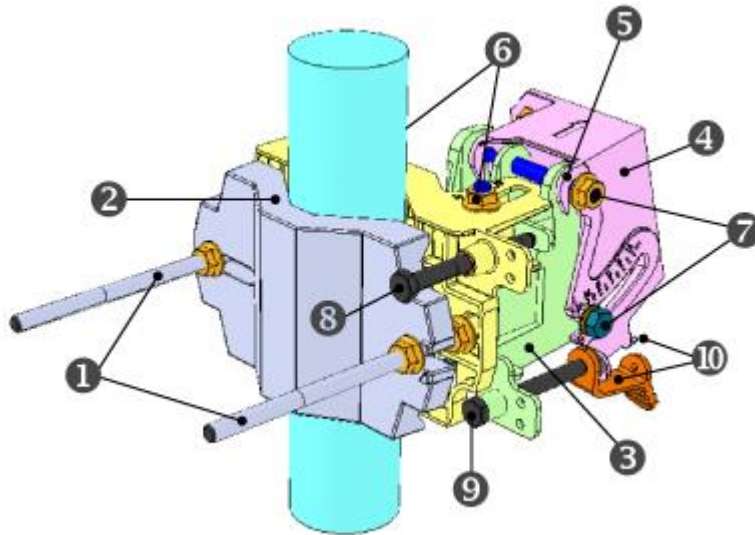


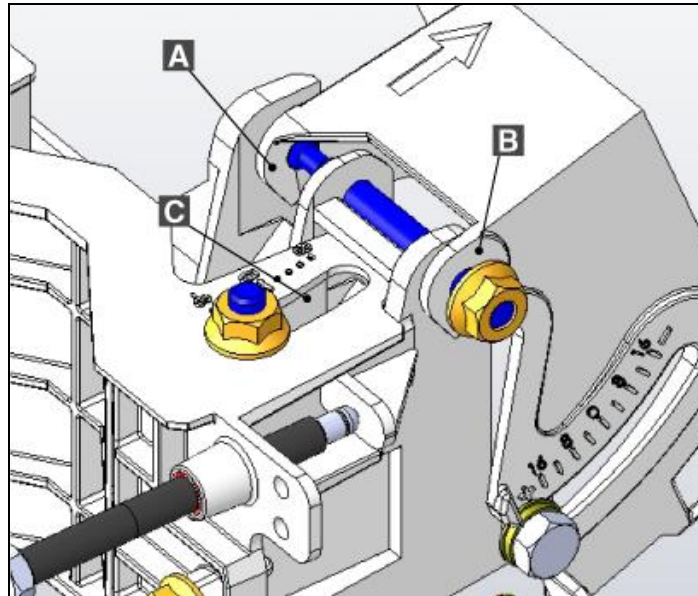
Figure 2-1: Netbeam Mounting Assembly Components

- | | |
|--|---|
| 1. Unit mounting screws and bolts | 6. Azimuth adjustment lock bolts |
| 2. Back mounting bracket | 7. Elevation adjustment lock bolts |
| 3. Front mounting bracket | 8. Azimuth fine adjustment screw ($\pm 8^\circ$) |
| 4. Quick release plate (attached to ODU) | 9. Elevation fine adjustment screw ($\pm 16^\circ$) |
| 5. Quick release hooks | 10. Elevation screw tension band and pin |

1. Prior to mounting, unpack the mounting kit package and attach the two unit mounting screws (1) to the front mounting bracket (3), securing them with mounting bolts.
2. Assemble the back (2) mounting bracket to the front (3) mounting bracket using one bolt and separate them by about 120 degrees so that the assembly can be attached to the mounting pole.
3. Place the assembly on the mounting pole and rotate the front and back mounting brackets to close the assembly on the pole. Replace the unit mounting bolt that was removed.
4. Ensure that both front and back mounting brackets are attached evenly to the pole, and are completely level.
5. Use the 13 mm open wrench to tighten the nuts on both unit mounting bolts. Temporarily tighten the unit mounting bolts at this stage to keep the unit from moving freely.
6. By default, the ODU is delivered with the quick release plate (4) securely attached in a vertical polarization. If necessary, change the ODU polarization to match the orientation of the remote ODU by removing the quick release plate, changing its orientation, and reattaching. For ease of reference, the markings V (vertical) and H (horizontal) are engraved on the back side of the ODU.
7. Examine the position scales of both the Azimuth adjustment lock bolts (6) and the elevation adjustment lock bolts (7), found on the front mounting bracket, and ensure that they are positioned at 0 degrees (in the middle of the scale).
8. Position the quick release hooks (5) onto the top elevation adjustment lock bolt (7) and carefully set the ODU in place on the front mounting bracket and slide it firmly inwards.

Mount the ODU by attaching the interior quick release hook (A) in place **before** attaching the exterior hook (B). The interior hook is the one located farthest from the tightening nut, as shown below.

TIP



A. Interior Quick Release Hook B. Exterior Quick Release Hook C. Elevation Position Slot

Figure 2-2: Quick Release Hooks

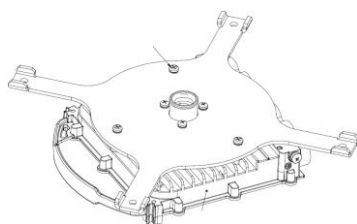
9. **Unlock** the Azimuth adjustment lock bolts (⑥) and the elevation adjustment lock bolts (⑦).
10. Stretch the elevation screw tension band (⑩) slightly and connect it to its mating tension pin, located on the quick release plate.

Installing the ODU with a Two Foot Antenna

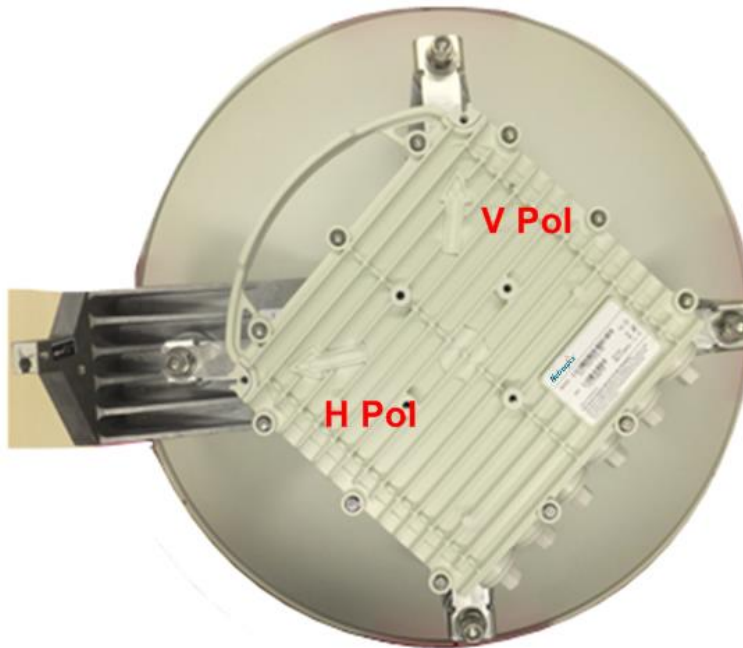
This appendix presents the installation instructions of NetBeam ODU with a two foot antenna.

1. Install the two foot antenna according to the mounting diagram on the next page. Antenna mounting kit installation instructions are also available inside the mounting kit package.
2. Remove the protective tape on the antenna feed.

The two foot ODU is shipped with External ODU adapter attached.



3. Unpack the two foot ODU and remove the protective cap.
4. Attach the ODU to the antenna and tighten the four locking bolts.
5. Make sure you install the ODU with the required polarization (note the polarization arrow on the back of the ODU).



6. Proceed with antenna alignment and ODU setup as described in *section 02, Aligning the Antenna*.

INSTALLATION INSTRUCTIONS FOR MOUNTING KIT

RD43101200C/D

Step: 1

3 Azimuth Lock Bolts (4 PL.)

Bolt 5/16"x1-3/8" UNC
Spring Washer 5/16"
Flat Washer 5/16"
6 PL.

Azimuth Adjustment Bolt 5/16

1 Grease

Hex Nut 5/16 UNC

2 DETAIL A
SCALE 1 : 1.5

Antenna Base Lock

Tilt Antenna Plate Assy

Grease

Hex Nut 5/16 UNC

Elevation Adjustment Bolt 5/16

4

Central Bolts (2 PL.)

Grease Surface Around the Slot from Both Sides

Notes:

- Center the Azimuth Lock Bolts in slot (4 PL.)
- Use tightening torque of 4 Nm on Central Bolts (2 PL.)
- Tool required 1/2" open end or deep socket wrench.
- Use grease in marked recommended places.

Step: 2

Mast 2"-4.5" outer diameter

5

Holder Bracket (2 PL.)

Hex Nut 5/16" UNC
Spring Washer 5/16"
Flat Washer 5/16"
4 PL.

Mounting Lock Bolt 5/16"x6.5" UNC
4 PL.

Tilt Antenna Plate Assy

Pin

Dish Antenna Base

6

Grease

Dish direction

Notes:

- Roughly aim the Mounting Kit Pin perpendicular to Dish direction
- Use tightening torque of 9 Nm on Nut of Mounting Lock Bolt (4 PL.)
- Tool required 1/2" open end or deep socket wrench.
- Use grease in marked recommended places.

Step: 3

7

Elevation Lock Bolt 5/16"x2" UNC
2 PL.

Hex Nut 5/16" UNC
Spring Washer 5/16"
Flat Washer 5/16"
2 PL.

Joint Lock Bolt Hex Head Screw 5/16"x5/8" UNC

Step: 4

8

Joint Lock Bolt must be fastened only when the Dish Antenna Base is in 0 deg Position

Notes:

- **At any time, keep Elevation Adjustment Bolt in parallel to the pole.**
- Adjustment Bolts must be greased at all time.
- After fine adjustment use tightening torque of 4 Nm on Azimuth Lock Bolts (4PL) and 9 Nm on Nut of Elevation Lock Bolts (2PL).
- Tool required 1/2" open end or deep socket wrench.

SHEET 1 OF 1

Connecting the Cables

Figure 2-3 shows the ODU interfaces. There are two or four active Ethernet interfaces, depending on HW configuration.

- NetBeam 1G, NetBeam M7 – two active Ethernet interfaces (Eth1/Eth2). These may be optical (Fiber SFP) or electrical (RJ45) physical interfaces (configurable).
- NetBeam 2G – four active Ethernet interfaces (Eth1/Eth2/Eth3/Eth4).

Ordering options:

- 2xElectrical (RJ45) + 2x optical (Fiber SFP)
- 1xElectrical (RJ45) + 3x optical (Fiber SFP)

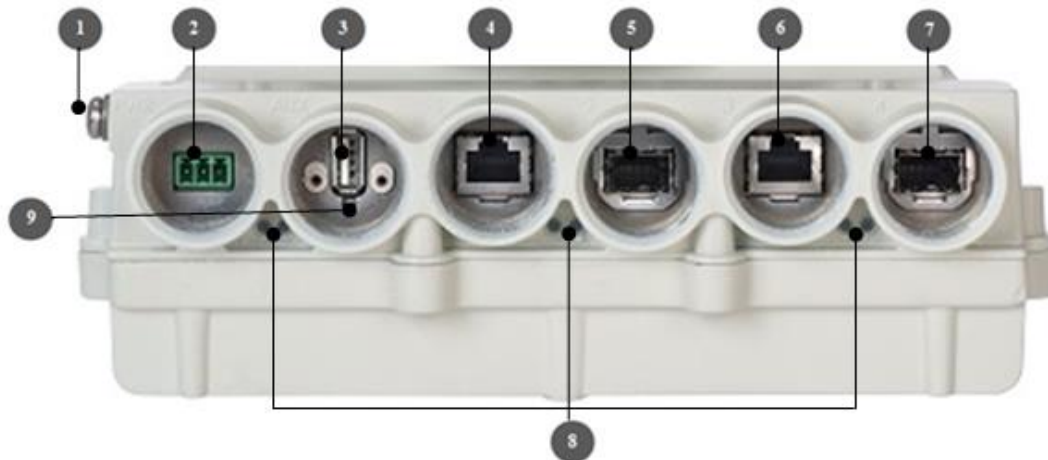


Figure 2-3: NetBeam Connection Panel Details

- | | |
|------------------------------------|---|
| 1. Electrical Ground Outlet (GND) | 6. Ethernet Cable RJ45 Interface |
| 2. Power Connector Interface (PWR) | 7. Fiber Cable SFP Interface (Eth4) |
| 3. DVM Probe Interface (AUX) | 8. System LEDs |
| 4. Ethernet Cable RJ45 Interface | 9. Reset Button (press for more than 8 seconds to restore factory defaults) |
| 5. Fiber Cable SFP Interface | |

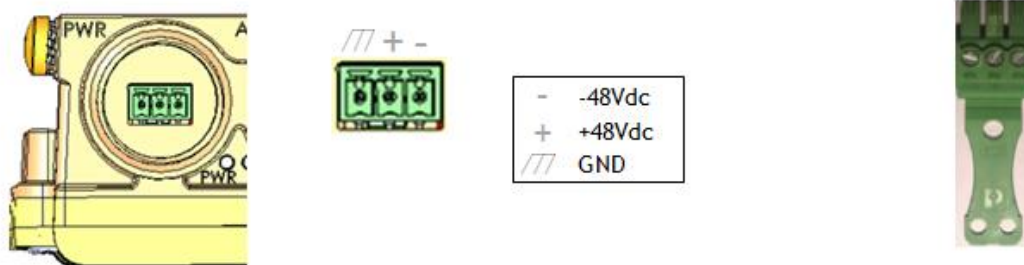


Figure 2-4: NetBeam DC Power Connector Pin-Out Diagram

Grounding the NetBeam and Cables

The location of the electrical ground outlet on the ODU is shown in Figure 2.3.

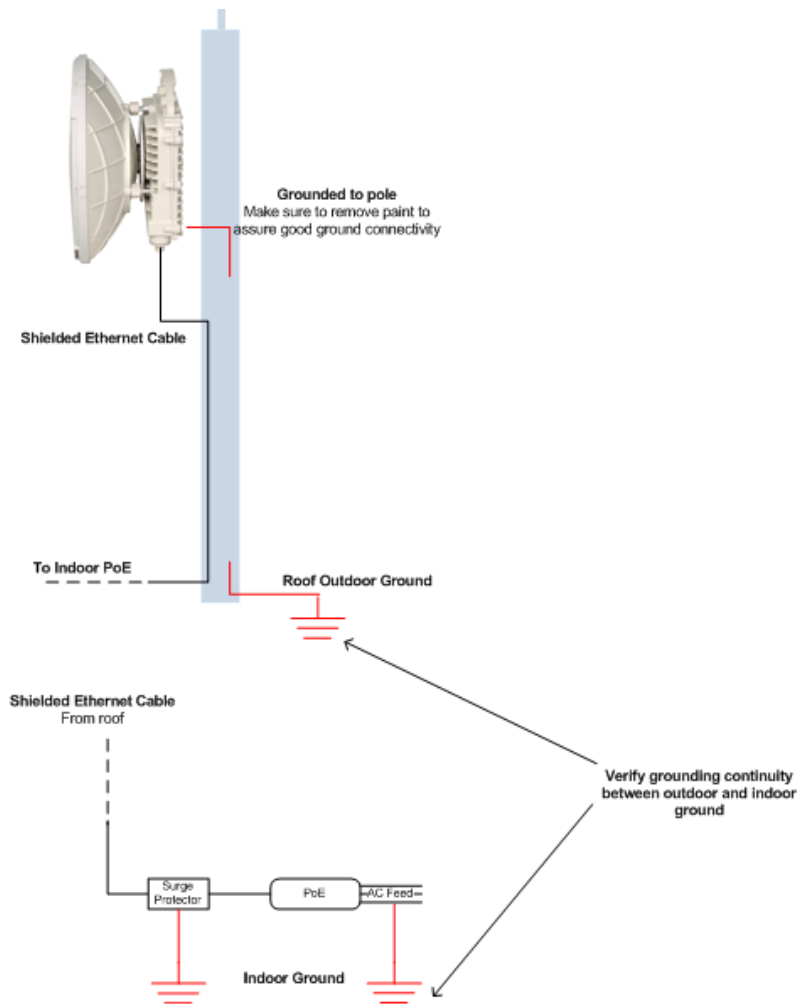
1. Connect one end of the grounding cable to the ground outlet on the left side of the ODU using the grounding cable lug.
2. Tighten the lug securely in place.
3. Connect the opposite end of the grounding cable to the earth connection, typically located on the mounting pole. If the earth connection is out of reach of the grounding cable, install an alternative cable.



Figure 2-5: ODU with Grounding Cable Connected

It is recommended to use Lightning Surge Protector on every Ethernet cable to protect the indoor networking equipment. The Lightning Surge Arrestor should be installed indoor next to the cable's point-of-entry and should be properly grounded.

An example for correct ODU grounding and Lightning Surge Protector installation is shown in Figure 2-3.



Power Supply Notes

The DC power input range of the ODU is 22 - 57 VDC for NetBeam 1G and M7 and 36 - 57 VDC for NetBeam 2G.

- The DC supply should be limited to two ampere to avoid surges and possible damage to the ODU. For that, use limited power supply or circuit breaker (fast-blow fuse). The circuit-breaker is the disconnecting device, and should be readily accessible.
- When connecting the ODU to a MAINS DC distribution system, use a two ampere circuit breaker to enable the central DC system to isolate the ODU in an emergency case.
- Use one poly circuit breaker and should connect it on the live voltage: (+) or (-). The other poly should be grounded.
- Connect the circuit breaker to the (+) or (-) live voltage.

- The DC input is floating, so either (+) or (-) can be connected to the GND on the power supply side. For the sake of consistency with other systems, Netronics recommends that you connect the (+) to the GND.
- Use a two-wire cable (14-18 AWG) to connect the power supply to the ODU. On the ODU DC terminal, connect only the (+) and (-) wires. Do not connect to the ODU's GND input.



Caution

Disconnect all power cables before service!

Preparing the Cables

Before inserting a cable connector into the ODU, you must first enclose the cable connector in a protective All-Weather shell. Three sets of All-Weather shells are provided with the ODU for the ODU interfaces. The protective All-Weather shell assembly is shown in Figure 2-6.

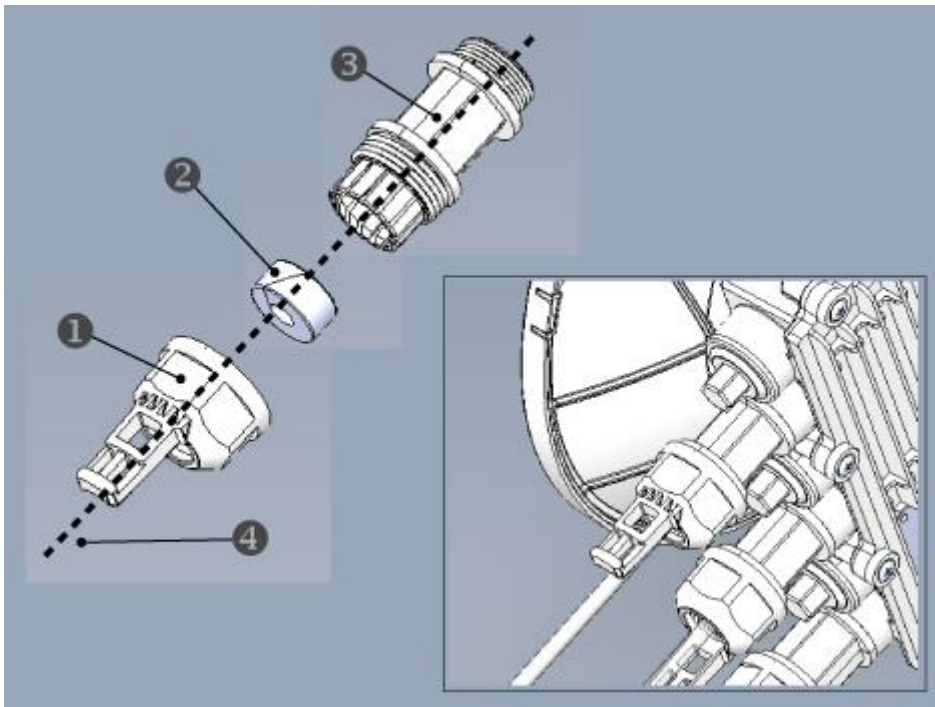


Figure 2-6: All-Weather Connecting Cable Shell Assembly

- | | |
|-------------------------|-----------------------------|
| 1. Cable Inlet Portion | 3. Connector Outlet Portion |
| 2. Rubber Gasket Insert | 4. Ethernet Cable |

Three sets of rubber gasket inserts are provided for different cable diameters:

- 4.2mm inner diameter – for cable diameter 3.5-4.9mm

- 5.8 mm inner diameter – for cable diameter 5.0-6.7 mm
 - 7.9 mm inner diameter – for cable diameter 6.8-9.0 mm
1. For each ODU cable connection, perform the following procedure:
 - a. Disassemble a protective shell by unscrewing its parts and carefully removing the rubber gasket insert (❷) from the cable inlet portion (❶) of the shell.
 - b. Thread the cable connector through the cable inlet portion (❶) of the shell, through the rubber gasket insert (❷) and through the connector outlet portion (❸) as shown in Figure 2.6.
 - c. Connect the cable connector to the ODU interface.
 - d. Screw the connector outlet portion (❸) to the ODU firmly by hand (do not use tools).
 - e. Insert the rubber gasket insert snugly into the connector outlet portion (❸) of the shell.
 - f. Screw the cable inlet portion (❶) to the connector outlet portion (❸) firmly by hand (do not use tools).



Removing Connectors from the NetBeam ODU



To avoid accidental damage to the connector, always use the following order to remove cable connections from the ODU (refer to Figure 2.6).

1. Unscrew the cable inlet portion (❶) of the All-Weather shell to release the gasket seal and then remove tension from the cable connector.
2. Unscrew the connector outlet portion (❸) of the All-Weather shell from its ODU port.
3. Remove the cable connector from its port.

Connecting the Power

1. Carefully screw the connector outlet portion (❸) of the All-Weather shell into the PWR port or alternatively, if a PoE connection is being used, the RJ1 port. Tighten the connector outlet portion securely by hand. **Do not use a wrench.**

2. Insert the power or PoE data connector into the port. The PWR LED color indicator turns red for one second, then blinks green indicating that the ODU is powered on.
3. Screw the cable inlet portion (❶) of the All-Weather shell onto the secured connector outlet portion, taking care not to twist the connecting cable. Tighten the cable inlet portion securely by hand. The rubber gasket insert (❷) will tighten to create a moisture-proof seal. **Do not use a wrench.**
4. Secure the power supply cable into place using a cable tie. Ensure that there is sufficient play in the cabling to allow movement of the ODU during final alignment.
5. Wait for the NetBeam ODU to boot up (about two minutes). When the ODU is fully rebooted, the PWR LED color indicator turns green (during power-up the PWR LED blinks green) and the RF LED color indicator turns off, indicating that the link is down.

Connecting Other Interfaces

For each network connection, perform the following steps:

1. Carefully screw the connector outlet portion (❸) of the All-Weather shell into the appropriate port. Tighten the connector outlet portion securely by hand. Do not use a wrench.
2. Insert the RJ45 or SFP connector into the port.
3. Screw the cable inlet portion (❶) of the All-Weather shell onto the secured top portion, taking care not to twist the connecting cable.
4. Tighten the bottom portion securely by hand. The rubber gasket insert (❷) tightens to create a moisture-proof seal. Do not use a wrench.
5. Secure the network connection cable into place using a cable tie. Ensure that there is sufficient play in the cabling to allow movement of the ODU during final alignment.

Aligning the Antenna

The ODU antenna must be aligned on both local and remote ODUs. You must first perform coarse alignment on each ODU, followed by fine alignment. Accurate alignment of the ODU is critical for achieving the strongest possible receive signal.

To perform antenna alignment, the ODU must be in Alignment mode.

The ODU has three modes of operation:

- Alignment – Carrier Wave transmission. Used for antenna alignment.
- Adaptive – Operational mode used with adaptive bandwidth, code, and modulation.

- Static – Operational mode used with a fixed modulation profile.

ODUs are shipped from the factory in Adaptive mode.

Setting the ODU to Alignment Mode

Switch the NetBeam ODUs to Alignment mode by inserting the DVM probes into the AUX Interface sockets. The RF LED color indicator turns orange, indicating the ODU is in Alignment mode.

The ODU remains in Alignment mode even if the DVM probes are ejected, until the ODU is rebooted.

Performing the Alignment



Note

These instructions are for aligning a one-foot antenna. For instructions on aligning a two-foot antenna, refer to *Installing the ODU with a Two Foot Antenna* on page 25.

These instructions refer to Figure 2-1 NetBeam 1G Mounting Assembly Components

To perform an alignment

1. Verify that the ODU is in Alignment Mode. Refer to *Aligning the Antenna* on page 33.

Coarse Alignment (Azimuth Only)

2. Loosen the unit mounting bolts (❶) slightly to allow the ODU some freedom of movement.
3. Perform a coarse ODU alignment using a line-of-sight visual check with the remote NetBeam ODU. Lock the unit mounting bolts (❶) using the 13mm open wrench.
4. Repeat steps 1 to 3 above on the remote ODU.

Fine Alignment



Note

When aligning an antenna, the antenna in the remote node must remain completely stationary. Perform Fine alignment first on the local antenna, and only afterwards on the remote antenna.

The optimum alignment may require several adjustment iterations between the local and remote antennas.

5. Connect the DVM to the ODU by inserting both red and black probes into their appropriate positions in the AUX port (Figure 2-3).

Throughout the alignment procedure, you must compare the actual receive signal strength indication (RSSI) to the expected RSSI that was calculated during network link budget preparation (refer to Preparing for Installation on page 23).

Read the receive level (RSSI) using the DVM. The voltage reading will be between 0 to 1V, indicating the RSSI in dBms. For example, a DVM reading of 0.45V is equivalent to -45 dBm.

6. Align the fine Azimuth axis. Use the hexagonal wrench to adjust the Azimuth fine adjustment screw (Ⓔ). Be sure to sweep the complete range of the Azimuth in order to determine the maximum received signal strength position.

When the optimum axis is achieved, tighten both Azimuth adjustment lock bolts (Ⓕ).

7. Align the fine elevation axis. Use the hexagonal wrench to adjust the elevation fine adjustment screw (Ⓖ). Be sure to sweep the complete range of the elevation in order to determine the maximum received signal strength position.

When the optimum axis is achieved, tighten both elevation adjustment lock bolts (Ⓗ).

8. Perform steps 6 and 7 for the remote ODU.
9. Repeat steps 6 and 7 for the local ODU.
10. Use the DVM to verify maximum received signal strength on both local and remote ODUs. For best performance, measured RSSI should be within ± 4 dB of the calculated value.
11. Once the optimum position has been achieved for the ODU pair, tighten the Azimuth adjustment lock bolts (Ⓕ) on one ODU (torque of 8 nM), being very careful not to move the ODU while tightening.
12. Tightening the Azimuth adjustment lock bolts will tilt the ODU, so realign the elevation again for optimum position.
13. Once the optimum position has been achieved for the ODU pair, tighten the elevation adjustment lock bolts (Ⓗ) on the ODU (torque of 8 nM), being very careful not to move the ODU when tightening.

14. Repeat steps 11 through 13 for the second ODU.
15. Use the DVM to verify that the received signal strength has not changed on either the local or the remote ODU after final tightening of the brackets.

Antenna alignment is now complete.

Figure 2-7 shows the NetBeam 1G1 after it has been completely installed.

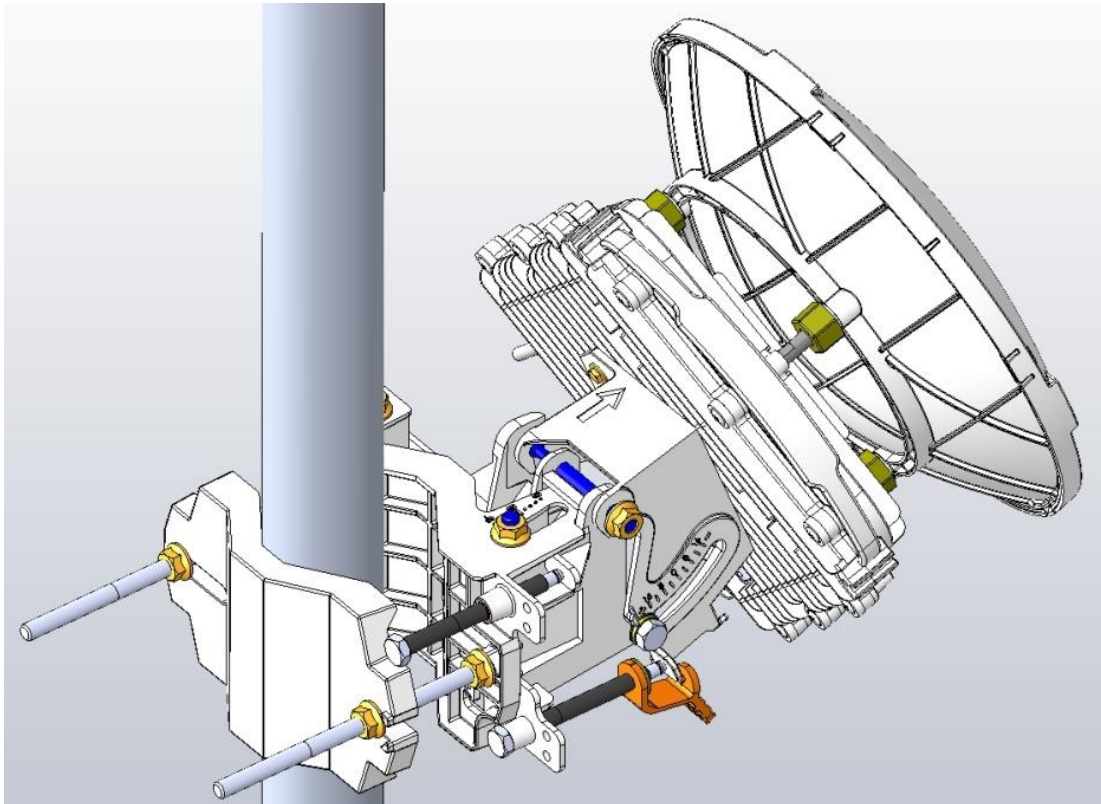


Figure 2-7: Installed NetBeam 1G1 Unit

Performing Initial System Setup



Note

The instructions in this section refer to Figure 2.1.

1. Disconnect the DVM from the ODU by removing the probes from the AUX port (Figure 2-3).
2. Reboot both ODUs by gently pressing the ODU Reset button (Ⓢ). This returns the ODU to **Adaptive mode**. Following this action, and after the ODU has finished rebooting, the RF LED color indicator on both ODUs turns **green**, indicating that the radio link is Up.
3. Carefully re-insert and tighten the AUX port protective seal using the 13mm open wrench.

The NetBeam link can now pass traffic and management between the ports and over the radio link.

Further configuration can be performed using the Web EMS or the CLI.



To perform configuration and monitoring, you must connect your laptop or PC to one of the two Ethernet ports on the ODU.

Chapter 3

Performing Basic Configuration Using the Web EMS

This chapter describes how to perform basic configuration tasks using the Web EMS.

- For instructions how to configure a link using the CLI, refer to *Performing Basic Configuration* using the CLI on page 53.
- For instructions on performing advanced configuration, such as network configuration, synchronization, OAM, and other advanced configuration tasks, refer to *Performing Advanced Configuration* on page 87.

This chapter includes the following topics:

- Connecting to the ODU Using the Web EMS
- Saving Configuration Changes and Resetting the System Using the Web EMS
- Quick Configuration
- Configuring and Displaying Basic System Information Using the Web EMS
- Configuring System IP Addresses Using the Web EMS
- Configuring Radio Parameters Using the Web EMS
- Viewing Modulation Profiles Using the Web EMS
- Configuring Ethernet Interfaces Using the Web EMS
- Configuring SNMP Settings
- Default VLAN Setting



Before you perform basic configuration on the ODU, you must ensure that the ODU is set to either Adaptive or Static mode. The RF LED color indicator on a network-ready ODU is **green**. Refer to Step 2 in *Performing Initial System Setup*, on page 36.

Connecting to the ODU Using the Web EMS

1. Launch an Internet browser and enter the ODU's IP address in the address bar. The default IP address is `https://192.168.0.1`.
2. Wait for the Java Applet to load and enter the username and password (admin, admin). The Web EMS Main screen is displayed:

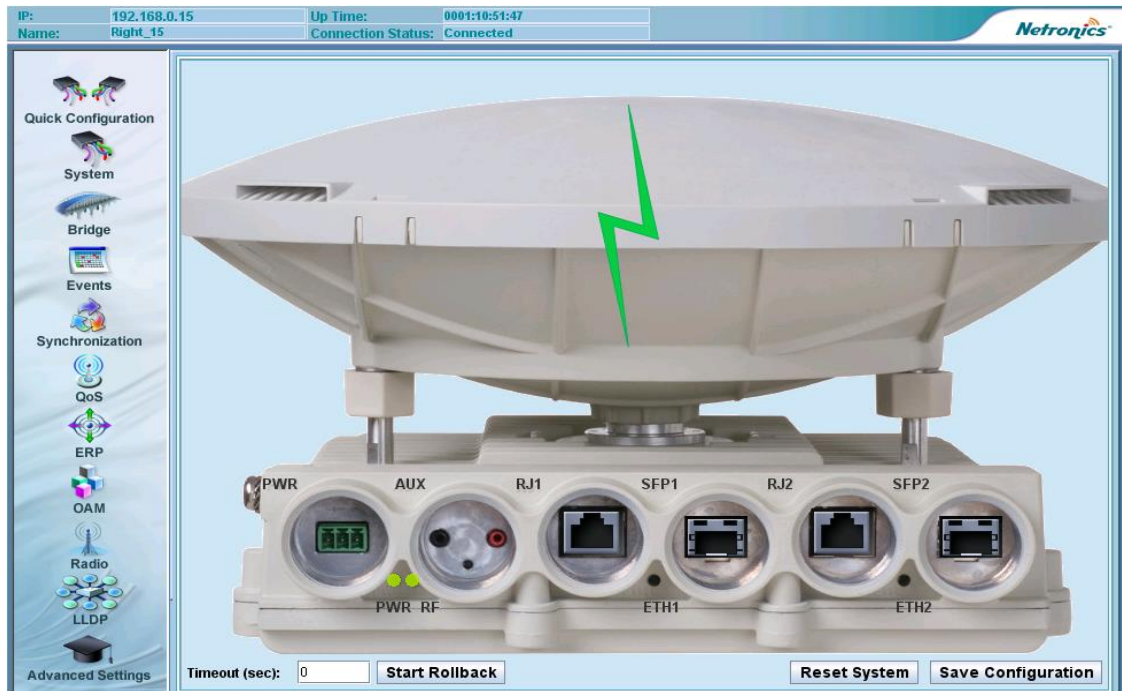


Figure 3-1: Web EMS Main Screen (NetBeam 1G, NetBeam M7)

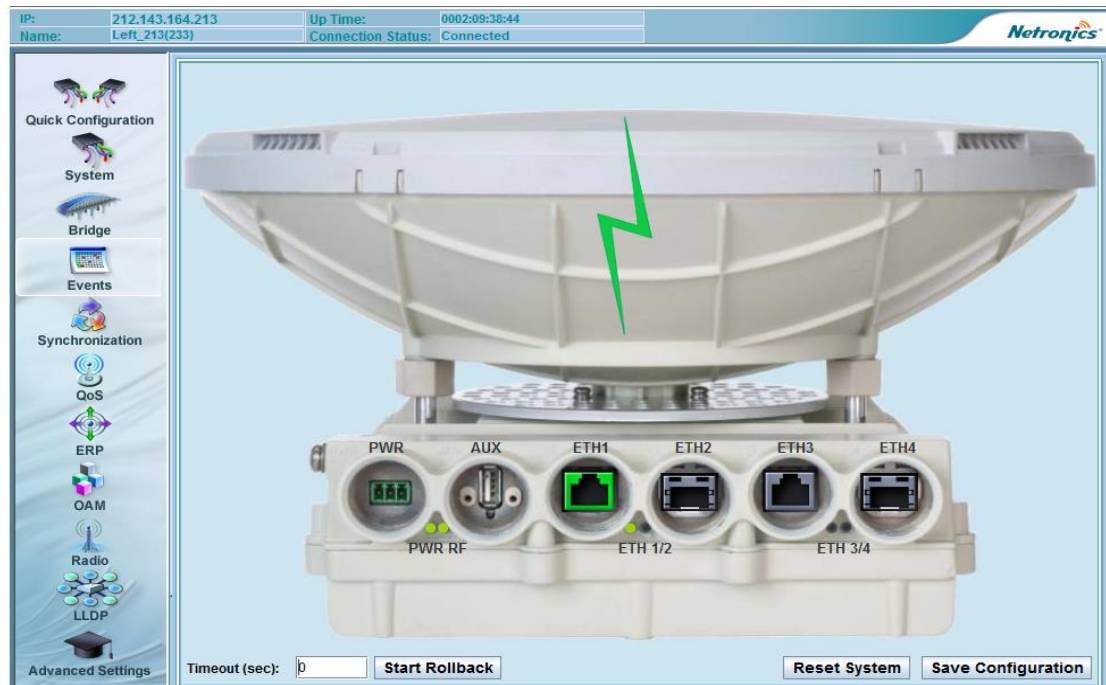


Figure 3-2: Web EMS Main Screen (NetBeam 2G)

Saving Configuration Changes and Resetting the System Using the Web EMS

Whenever you make changes to the ODU configuration using the Web EMS, you must click **Save Configuration** on the Web EMS Main screen to save the configuration changes to the startup configuration. If you do not save the configuration, the changes will be lost the next time the system resets.

To reset the system, click **Reset System** on the Web EMS Main screen.

Quick Configuration

It is recommended to use the Quick Configuration screen to configure the basic ODU parameters. To display the Quick Configuration screen, click **Quick Configuration** on the toolbar on the left.

You can also click specific topics on the toolbar on the left to display and configure more extensive system parameters.

Configuring and Displaying Basic System Information Using the Web EMS

You can view and configure basic system information in the System Information section of the Quick Configuration screen.



System Information	
Name:	NetBeam
Date:	2011.02.17
Time:	09:09:06

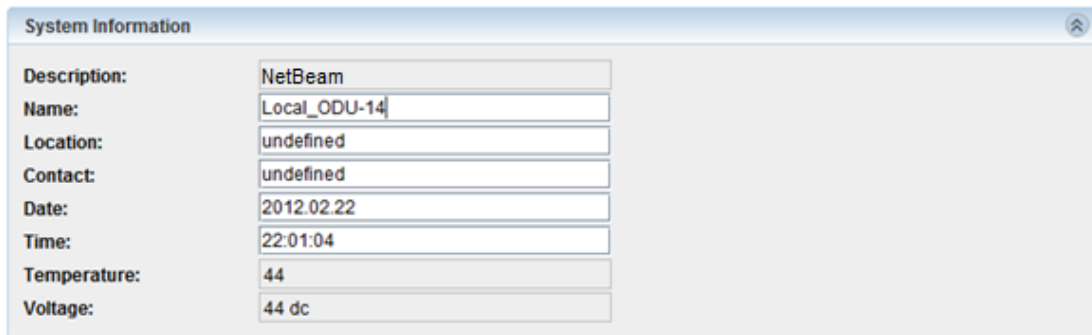
Figure 3-3: Web EMS Quick Configuration Screen – System Information Section

The following are the basic system parameters:

- Name
- Date
- Time

When you are finished, click **Apply**.

To view and configure more extensive system information, click **System** on the Web EMS Main screen. The System screen is displayed.



System Information	
Description:	NetBeam
Name:	Local_ODU-14
Location:	undefined
Contact:	undefined
Date:	2012.02.22
Time:	22:01:04
Temperature:	44
Voltage:	44 dc

Figure 3-4: System Screen – System Information Section

The System Information section of the System screen includes the following system parameters:

- Description
- Name
- Location
- Contact
- Date

- Time
- Temperature
- Voltage (and indication about power source: DC or PoE)

Configuring System IP Addresses Using the Web EMS

You can change and add system IP addresses in the IP section of the Quick Configuration screen, or by clicking **System** on the Web EMS Main screen and clicking the IP section of the System screen.

The NetBeam ODU supports up to four IP addresses that can be on different subnets and associated with different VLANs.

On NetBeam 2G – IP addresses may also be acquired by DHCP (configurable by CLI only).

You can assign a static route to each IP address. Default IP–Gateway is defined as a static route.

By default, one IP address is defined (IP #1):

- IP Address – 192.168.0.1
- IP Prefix Length – 24 (equivalent to Mask 255.255.255.0)
- VLAN – 0 (not defined, meaning the IP is not associated with specific VLAN)

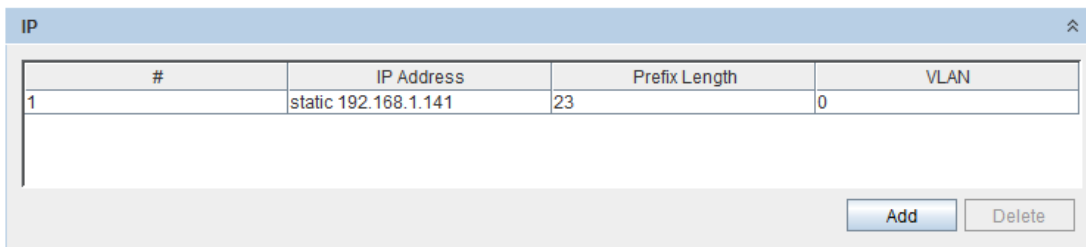


Figure 3-5: IP Section of Quick Configuration and System Screen

To add or change an IP address:

1. Click **Add**. The Add IP window opens.

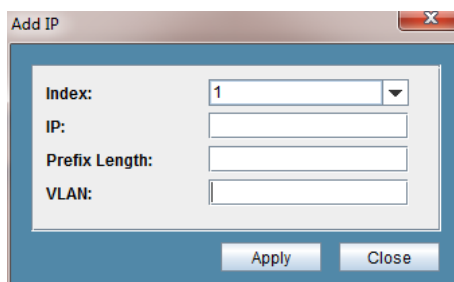


Figure 3-6: Add IP Window

2. In the **Index** field, select the index of the IP you want to add or change.
3. If a single IP is used and you wish to change it, Select **1**.



If you change the default IP address, your connection to the ODU is lost. To re-establish a connection, launch an Internet browser and connect using the new IP address.

4. Click **Apply**.



By default, no static route or default gateway is defined.

You can create or modify the IP Route (and Default Gateway) from the Route section of the Quick Configuration screen or the System screen.

To add or change a Route:

1. Click **Add**. The Add Route window opens.

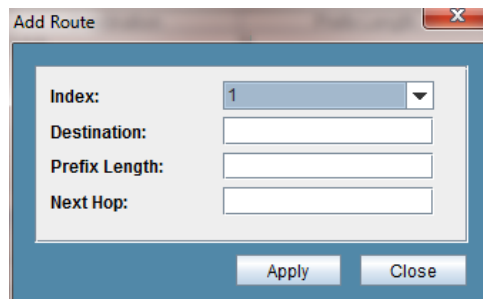


Figure 3-7: Add Route Window

2. In the Index field, select the index of the IP for which you want to add or change a route.
 - a) If you are using a single IP and want to change its route, select **1**.

idx	number 1 to 10
dest	ip address in the form X.X.X.X where X is a decimal number from 0 to 255 (for example, 10.0.15.74).

prefix-len	ip prefix – a number from 0 to 32
next-hop	ip address in the form X.X.X.X where X is a decimal number from 0 to 255 (for example, 10.0.15.74). All IP addresses in the table must be different.

3. Click **Apply**.

The following example shows a single IP configuration with a default gateway:

ODU with IP 192.168.0.17, mask 255.255.255.0 and default gateway 192.168.0.254.

ODU config – IP screen:

- Index – 1
- IP Address – Static 192.168.0.17
- Prefix Length – 24
- VLAN – 0

ODU config – Static Route screen:

- Index – 1
- Destination – 0.0.0.0
- Prefix Length – 0
- Next Hop – 192.168.0.254

Configuring Radio Parameters Using the Web EMS

You can configure radio parameters in the Radio section of the Quick Configuration screen, or by clicking **Radio** on the Web EMS Main screen and going to the Radio section of the Radio screen.

To configure radio parameters using the Web EMS

1. On the Web EMS Main screen, click **Radio**.
2. On the Radio screen, enter the appropriate information in the following fields:

Radio	
Frequency (MHz):	74375
Channel Width (MHz):	500
Role:	auto
Role Status:	slave
Transmit Asymmetry:	50tx-50rx
Tx Link ID:	0
Rx Link ID:	0
Tx Power (dBm):	5
Tx Mute :	disable
Tx Mute Timeout (sec):	60
Oper. Status:	up
Tx State:	normal
Rx State:	normal
Mode:	adaptive
Alignment Status:	inactive
Modulation:	qam64
Sub Channels:	4
Repetitions:	1
FEC Rate:	0.5
Loopback :	disabled
Loopback Timeout (sec):	60
Long Range Mode :	false
RSSI (dBm):	-37
CINR (dB):	21

Figure 3-8: Web EMS System Screen – Radio Section (NetBeam 1G, NetBeam M7)

Radio	
Oper. Status:	up
Tx State:	normal
RSSI (dBm):	-50
Channel Width (MHz):	500
Tx Frequency (MHz):	74375
Role:	master
Mode:	adaptive
Modulation:	qam64
Repetitions:	1
Tx Power (dBm):	7
Loopback :	disabled
Tx Mute :	disable
Tx Link ID:	0
Long Range Mode :	false
Alignment Status:	inactive
Rx State:	normal
CINR (dB):	23
Rx Frequency (MHz):	84375
Role Status:	master
Sub Channels:	4
FEC Rate:	0.5
Loopback Timeout (sec):	60
Tx Mute Timeout (sec):	60
Rx Link ID:	0

Figure 3-9: Web EMS System Screen – Radio Section (NetBeam 2G)

- **Tx Frequency (MHz)** – Select a frequency channel (on NetBeam 2G systems, the Rx Frequency is updated automatically). The default values are 74375/84375.
- **Channel Width (MHz)** – 250 MHz or 500 MHz. The default value is 500.
- **Role** – Determines whether the ODU functions as a master or slave. In a link, one side must be set to Master and the other side must be set to Slave (required for link synchronization). Default value is **Auto**, meaning the role is set automatically by the link. You can check the current set role in the **Role Status** field.

Manually setting the Role is necessary only for asymmetric configurations (TDD systems only).

- **Transmit Asymmetry** – Default value is symmetric configuration: 50% for Tx and Rx (50tx-50rx). For an asymmetric configuration (75%/25% or 90%/10%), you have to

manually configure the Role and set the Master unit to 75tx-25rx (or 90tx-10rx) and the Slave unit to 25tx-75rx (or 10tx-90rx). The default value is 50tx-50rx.

- **Mode** – Select one of the following operation modes:
 - **Alignment** – Carrier Wave transmission. Used for antenna alignment.
 - **Adaptive** – Adaptive Bandwidth, Code, and Modulation.
 - **Static** – Fixed modulation profile. If you select Static, you must select from a list of pre-configured modulation profiles in the Modulation field.
 - Default value is **Adaptive**.
 - **Modulation** – QPSK, 16QAM, or 64QAM.



Max modulation for NetBeam M7 systems is 16QAM.

- **Sub Channels** – From 1 to 4 (occupied bandwidth. For Channel Width 500 MHz: 125-500 MHz)
- **Repetitions** – 1, 2 or 4
- **FEC Rate** – 0.5

When using the system in Static mode, you must select from a pre-defined list of modulation profiles. In Adaptive mode, the ODU switches among the modulation profiles from this list.

To check the available modulation profiles, refer to *Viewing Modulation Profiles Using the Web EMS* on page 47.

- **Tx and Rx Link ID** – You can set unique Link IDs for links installed on the same site to avoid locking on the wrong transmitter.
- **Operational Status** – Displays the radio link status (Up or Down).
- **Tx and Rx State** – Displays the Tx and Rx chains status.
- **RSSI (dBm)** – Displays the Receiver Signal Strength Indicator.
- **CINR (dB)** – Displays the Carrier to Interference + Noise ratio, which indicates the radio link's signal quality. In normal conditions, $CINR \geq 17$ indicates a good signal quality.
- **Tx Power (dBm)** – ODU's transmit power: +5 to -35 dBm (+7 to -5 dBm for NetBeam 2G). Note that it will take the ODU up to 2 minutes to update its Tx power.

Adjust Tx Power so the RSSI at the remote end will not be higher than -35 dBm (overload threshold).

The Tx power value sets the transmit power for the highest modulation profile. In case lower modulation profile(s) has higher max Tx power (based on product's

specs), the Tx power will be increased automatically without indication in RF configuration menu.

- **Tx Mute** – Set to Enable to mute the transmitter.
 - **Tx mute Timeout (seconds)** – Number of seconds for Tx mute enabled
 - **Loopback** – ODU RF loopback. Select the modulation the ODU will be set to in loopback mode. Note that it will take the ODU to stabilize after loopback about 1 minute so set the loopback timeout accordingly (recommended 600 seconds).
 - **Loopback Timeout (seconds)** – Number of seconds the ODU will be in RF loopback.
 - **Long Range Mode** – allows radio link at more than 4500 m (up to 7000 m link). Set to “True” only when path length is over 4500 m.
3. Click **Apply**.

Viewing Modulation Profiles Using the Web EMS

To view the available modulation profiles

1. On the Web EMS Main screen, click **Radio**.
2. On the Radio screen, click the **Modulations** section.

Note that different modulation tables may apply according to product and according to the frequency channel used.

Frequency	Modulation	Sub Channels	Repetitions	FEC Rate	CINR Low	CINR High	Backoff
any	qpsk	1	4	0.5	-128	15	5
any	qpsk	2	2	0.5	11	16	8
any	qpsk	4	1	0.5	12	18	8
any	qam16	4	1	0.5	17	22	8
any	qam64	4	1	0.5	21	127	8

Figure 3-10: WEB EMS Radio Screen – Modulations Section

- **CINR Low** – Lower threshold for stepping down in modulation profile (Adaptive Mode).
- **CINR High** – Upper threshold for stepping up in modulation profile (Adaptive Mode).

Configuring Ethernet Interfaces Using the Web EMS

1. The NetBeam system includes four Ethernet interfaces:
 - **Host** – Management interface
 - **Eth0** – Radio interface
 - **Eth1** – ODU interface, port 1

- **Eth2** – ODU interface, port 2
- **Eth3** – ODU interface, port 3 (NetBeam 2G only)
- **Eth4** – ODU interface, port 4 (NetBeam 2G only)

You can configure Ethernet port parameters in the Port sections of the Quick Configuration screen. Some NetBeam Ethernet port parameters are preset and cannot be modified. This section lists and describes those parameters that can be modified.

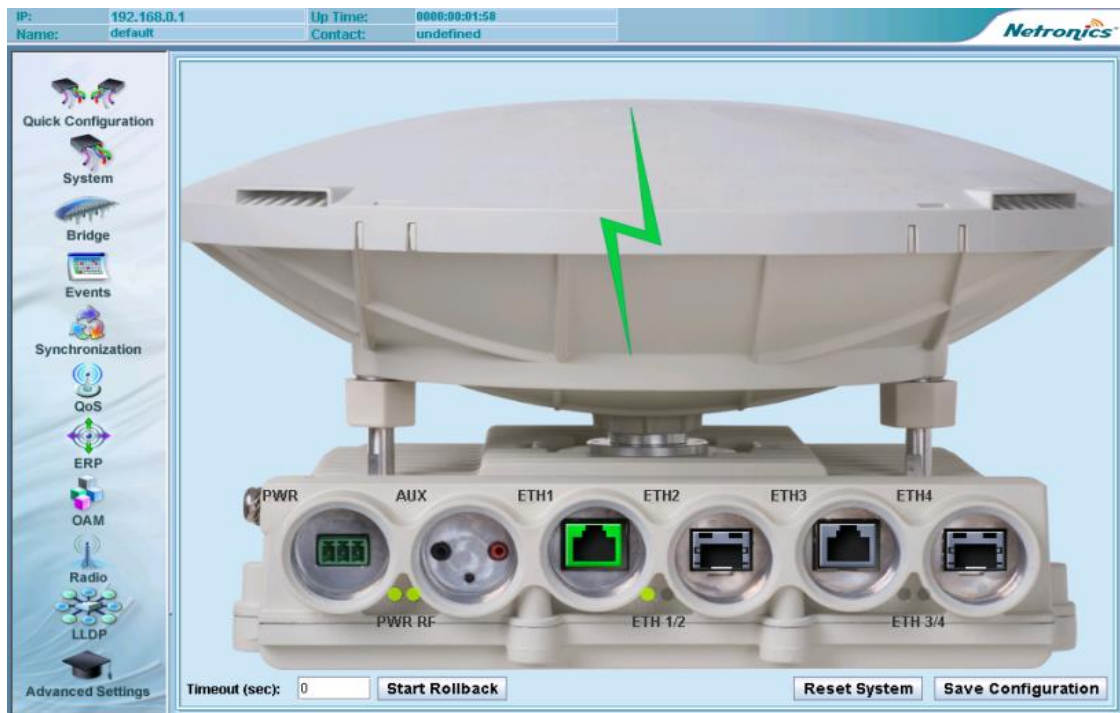


Figure 3-11: Web EMS Quick Configuration Screen – Port Section (Eth1)

You can also configure Ethernet port parameters from the EMS Web Main screen.

To configure Ethernet port parameters from the EMS Web Main screen

1. Click the icon of the interface you want to configure (Figure 3-12).



The Interface screen (Figure 3-13) contains several additional fields.

Figure 3-12: Interface Icons on Web EMS Main Screen

Interface			
Name:	Eth1	Ethernet Type:	1000fd
Description:	Eth 1	Ethernet Actual Type:	100fd
Alias:		Auto Negotiate:	enabled
MAC Address:	00:24:a4:01:4a:88	Loopback Mode:	disabled
MTU:	16384	Loopback Timeout:	60
Admin Status:	up	Alarm Propagation:	disabled
Oper. Status:	up	Network Type:	customer-uni
Last Change:	0002:09:51:04	Classifier Mode:	pcp-dscp
PCP Write Profile ID:	none	Clock:	auto
PFC Mode:	disable	Alarm Suppression:	disable

Figure 3-13: Interface Screen

- **Admin Status** – Determines whether the port is enabled (up) or disabled (down). The Default value is up.
- **Oper. Status** – Displays the operational status of the port – up or down.
- **Auto Negotiation** – Determines whether or not auto negotiation is enabled (enabled) or disabled (disabled). The default value is enabled.
- **Ethernet Type** – When Auto Negotiation is disabled, select the port’s speed manually in this field (10/100/1000, HF/FD). When using the SFP physical port, set this field to 1000xfd. The default value for the Electrical RJ45 ports is 1000fd (1000 Full-Duplex).
- **Ethernet Actual Type** – Displays the port’s actual speed/duplex (after negotiation).



Note

Auto-negotiation and Ethernet Speed/Duplex (in case Auto-neg disabled) must be identical on the ODU port and the end-equipment port.

- **Loopback Mode** – Interface screen only. Options are: Disabled, Internal, Internal-mac-swap, External, and External-mac-swap.
- **Loopback Timeout** – Interface screen only. The loopback timeout (in seconds).
- **Alarm Propagation** – Interface screen only. Used to define system behavior in case of Eth or Radio link failure (port shutdown):
 - **Backward** – Eth port down in case radio link down or Eth port down at the remote.
 - **Forward** – notification is sent to the remote in case Eth port link down.
 - **Both Directions** – Eth port down in case of both radio and Eth link down.
- **Alarm Suppression** – suppress (mask) alarm on port (alarm will not be active on the port).

2. Click **Apply**.

Configuring SNMP Settings

You can configure the SNMP V2 managers trap destination in the SNMP section of the System screen.

Refer to *Managing SNMP* on page 189 for SNMP V3 attributes.

You can define up to five managers, with the following settings:

- **Destination IP Address**
- **UDP Port Number**
- **Security Name (community)**

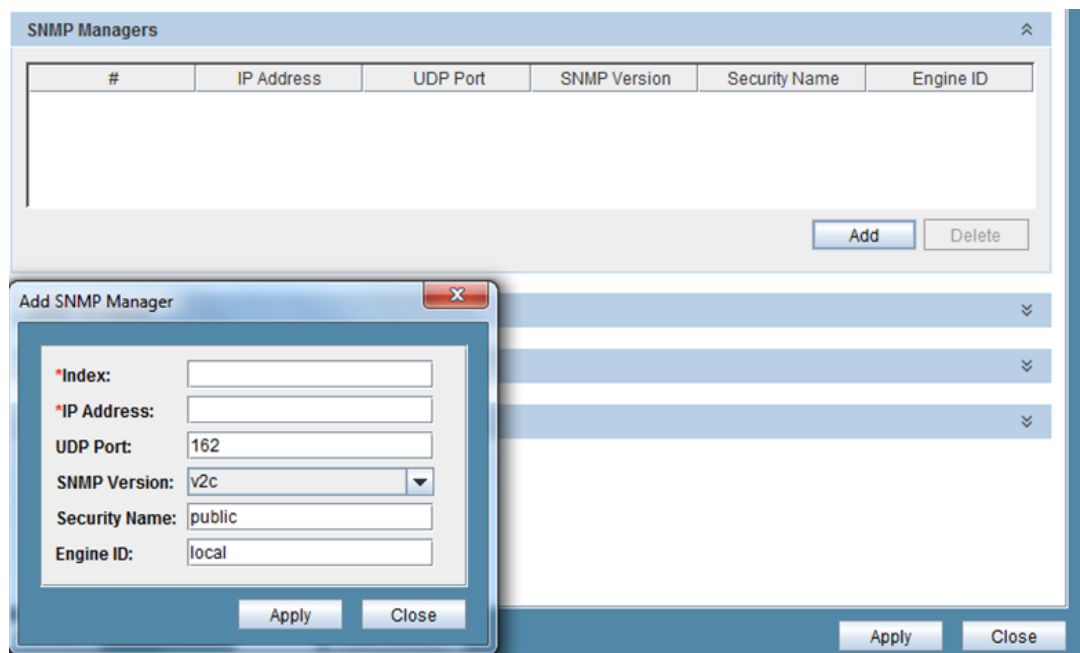


Figure 3-14: Web EMS System Screen – SNMP Managers Section

To add or change managers

1. Click **Add**.
2. Enter an Index and an IP Address.
3. Click **Apply**.



Refer to the Managing SNMP section for SNMPv3 settings.

Default VLAN Setting

NetBeam's Undefined VLAN feature enables transparent forwarding of both tagged and untagged traffic by default. No configuration or license is necessary for this feature, which gives you the flexibility to change your VLANs with no additional configuration necessary in the NetBeam system.

For VLAN configuration options, including the ability to define or block specific VLANs, refer to *Configuring VLANs* on page 70.

Chapter 4

Performing Basic Configuration using the CLI

This chapter describes how to perform basic configuration tasks using the CLI.

- For instructions how to configure a link using the Web EMS, refer to *Performing Basic Configuration Using the Web EMS* on page 38.
- For instructions on performing advanced configuration, such as network configuration, synchronization, OAM, and other advanced configuration tasks refer to *Performing Advanced Configuration* on page 87.

This chapter includes the following topics:

- Establishing a CLI Session with the ODU
- Saving Configuration Changes and Resetting the System Using the CLI
- Configuring and Displaying Basic System Information Using the CLI
- Configuring System IP Addresses Using the CLI
- Configuring Radio Parameters Using the CLI
- Configuring Ethernet Interfaces Using the CLI
- Default VLAN Setting



Before you perform basic configuration on the ODU, you must ensure that the ODU is set to either Adaptive or Static mode. The RF LED color indicator on a network-ready ODU is green. Refer to Step 2 in *Performing Initial System Setup*, on page 36.

Establishing a CLI Session with the ODU

1. Run a standard SSH client. You can use a common, open source SSH client program, such as PuTTY, available for download from the web.
2. Enter the ODU's **default** IP address: **192.168.0.1** (the default Mask is 255.255.255.0), and open the connection.
3. Login with the following criteria:
 - **User: admin**
 - **Password: admin**

When a successful connection is established, the ODU responds as follows:

```
login as: admin
NB2G1, S/N: F323036112, Ver: 5.0.0 9931
admin@192.168.0.1's password:
NB2G1>
```

Saving Configuration Changes and Resetting the System Using the CLI

Whenever you make changes to the ODU configuration, you must save the configuration changes to the startup configuration. If you do not save the configuration, the changes will be lost the next time the system is reset. Use the following command to save configuration changes to the startup configuration:

```
Local_Site> copy running-configuration startup-configuration
```

To reset the system, use the `reset system` command. You must reset the system whenever you exit Alignment mode.

```
Local_Site> reset system
```

Configuring and Displaying Basic System Information Using the CLI

Use the `set system name` command to set the ODU's name. Once you set the ODU's name, a prompt appears with the name you just set, the date, and the time.

```
Default> set system name Local_Site
Local_Site>
```

To set system date & time, use the following command:

```
Local_Site> set system date 2012.12.01 time 15:08:00
```

Use the `show system` command to display basic information about the ODU.

```
Local_Site>show system
```

```
system description      : NB-1G1
system snmpid           : 1.3.6.1.4.1.31926
system uptime           : 0000:00:05:10
system contact          : undefined
system name             : Local_Site
system location         : undefined
system voltage          : 55 dc
system temperature      : 39
system date             : 2012.12.01
system time             : 15:08:06
system cli-timeout      : 15
system auth-mode        : local
system auth-shared-secret : none
system loop-permission  : enabled
```

Configuring System IP Addresses Using the CLI

The NetBeam ODU supports up to four IP addresses that can be on different subnets and associated with different VLANs. You can assign a static route to each IP address. The Default IP-Gateway is defined as a static route.

By default, one IP address is defined (IP #1):

- IP Address – 192.168.0.1
- IP network Prefix – 24 (Mask 255.255.255.0)
- VLAN – 0 (not defined)

By default, no route is defined.

Use the `set ip` command to change or add an IP address. The command must be followed by the index number of the IP address you want to add or change. Use the index number 1 to change the default IP address. For example:

```
set ip <ip-index> ip-addr <value> [prefix-len <value>] [vlan
<value>]
      <ip-index>                : integer 1..4
```

```
Local_Site>set ip 1 ip-addr 192.168.0.11 prefix-len 24
```

If the IP entry does not already exist, the `set ip` command creates it and assigns the attributes specified. If the interface address or the default router address is not explicitly specified, the entry is created with the default value that has been defined for the VLAN.

If the IP entry already exists, the `set ip` command replaces the attributes that are currently defined for the entry with the values specified in the command.

Up to four IP addresses can be specified on the command line.

A `set ip` command fails if the route specified is not within the subnet that has been defined by mask.



If you change the default IP address, your connection to the ODU is lost. To re-establish a connection, launch an Internet browser and connect using the new IP address.

To display all of the currently configured IP addresses and their attributes, use the `show ip` command:

For example: NetBeam 1G, NetBeam M7 Systems

```
Local_Site>show ip
```

```
ip 1 ip-addr           : 192.168.0.11
ip 1 prefix-len        : 24
ip 1 vlan              : 0
```

For example: NetBeam 2G Systems

```
Local_Site>show ip
```

```
ip 1 ip-addr           : static 192.168.0.11
ip 1 prefix-len        : 24
ip 1 vlan              : 0
ip 1 default-gateway   : 192.168.0.254
```

To delete IP entries, use the `clear ip` command:

```
clear ip <index>
```

To create and modify an IP Route and Default Gateway, use the `set route` command:

```
set route <idx> [dest <ip-address>] [prefix-len 0..32] [next-hop
<ip-address>]
```

idx number 1 to 10

`dest` ip address in the form X.X.X.X where X is a decimal number from 0 to 255 (for example, 10.0.15.74).

`next-hop` ip address in the form X.X.X.X where X is a decimal number from 0 to 255 (for example, 10.0.15.74). All IP addresses in the table must be different.

`prefix-len` ip prefix – a number from 0 to 32

By default, no route is defined.

To set a static route, use the following command:

```
Local_Site>set route 1 dest 192.168.0.64 prefix-len 30 next-hop
192.168.0.66
```

To set a single default gateway, use the following command. When single IP is used and a static route is not used, you may configure a default IP gateway. In such case, use 0.0.0.0 as the destination network with `prefix-len 0`.

```
set route 1 dest 0.0.0.0 prefix-len 0 next-hop 192.168.0.254
```

To display all of the currently configured routes and their attributes, use the `show route` command:

```
Local_Site>show route
ip 1 dest      : 0.0.0.0
ip 1 prefix-len: 0
ip 1 next-hop  : 192.168.0.254
```

Configuring Radio Parameters Using the CLI

This section lists and describes the CLI commands you need to configure and display radio parameters.

Use the `set rf` command, followed by the name of the parameter you want to configure, to configure the ODU's radio parameters:

For example:

```
Local_Site>set rf tx-power 3
Local_Site>set rf role auto
Local_Site>set rf mode adaptive
```

Displaying Radio Parameters and Status Using the CLI

Use the `show rf` command to display the ODU's current radio status and parameter settings.

For example: NetBeam 1G, NetBeam M7 Systems

```
Local_Site>show rf
rf operational           : up
rf tx-state             : normal
rf rx-state            : normal
rf cinr                 : 19
rf rssi                 : -43
rf channel-width       : 500
rf frequency           : 74375
rf role                 : auto
rf role-status         : slave
rf mode                : adaptive qam64 4 1 0.5
rf alignment-status    : inactive
rf lowest-modulation   : qpsk 1 4 0.5
rf tx-asymmetry        : 50tx-50rx
rf rx-link-id          : 0
rf tx-link-id          : 0
rf temperature         : 52
rf loopback-timeout    : 60
rf loopback            : disabled
rf tx-power            : 5
rf long-range-mode     : false
```

For example: NetBeam 2G/ Systems

```
Local Site>show rf
rf operational           : up
rf tx-state             : normal
rf rx-state            : normal
rf cinr                 : 24
rf rssi                 : -42
rf channel-width       : 500
rf tx-frequency        : 72375
rf rx-frequency        : 82375
rf role                 : auto
rf role-status         : slave
rf tx-mute             : disable
rf tx-mute-timeout     : 60
rf mode                : adaptive qam16 4 1 0.5
rf alignment-status    : inactive
rf lowest-modulation   : qpsk 1 4 0.5
rf tx-asymmetry        : 100tx-100rx
rf rx-link-id          : 0
rf tx-link-id          : 0
rf tx-temperature     : 44
rf rx-temperature     : 35
```

```

rf loopback-timeout      : 60
rf loopback              : disabled
rf tx-power              : 7
rf long-range-mode      : false
Local_Site>

```

Configuring the Radio Parameters Using the CLI

```

Set rf                    (for NetBeam 1G, NetBeam M7 systems)
  [frequency {71375 | 71875 | 72375 | 72875 | 73375 | 73875 |
74375 | 74875 | 75375}]
Set rf                    (for NetBeam 2G systems)
  [frequency {71375 | 71875 | 72375 | 72875 | 73375 | 73875 |
74375 | 74875 | 75375}]
  [frequency {81375 | 81875 | 82375 | 82875 | 83375 | 83875 | 84375
| 84875 | 85375}]
  [role {master | slave | auto}]
  [tx-mute {disable | enable}]
  [tx-mute-timeout <integer 0..86400>]
  [mode {static <modulation> <subchannels> <repetitions> <fec-
rate> - (from list of modulations) | alignment | adaptive}]
  [lowest-modulation {<modulation> <subchannels> <repetitions>
<fec-rate> - (from list of modulations)}]
  [tx-asymmetry           (for NB1G,NBM7 systems)
    for master use 50tx-50rx, 75tx-25rx, 90tx-10rx
    for slave use 50tx-50rx, 25tx-75rx, 10tx-90rx}]
  [tx-link-id <integer 0..127>]
  [rx-link-id <integer 0..127>]
  [loopback {internal-mac-swap <modulation> <subchannels>
<repetitions> <fec-rate> - (from list of modulations) | disabled}]
  [loopback-timeout <integer 0..86400>]
  [tx-power <integer -35..5>]

```

Viewing Modulation Profiles Using the CLI

Use the show modulation command to display available supported modulation profiles and their parameters.

```

Local_Site>show modulation

frequency  modulation  subchannels  repetitions  fec-rate  cinr-low  cinr-high  backoff
any        qpsk         1            4            0.5      -128     10         5
any        qpsk         2            2            0.5      6        13         8
any        qpsk         4            1            0.5      9        14         8
any        qam16       4            1            0.5      13       127        8

```

- **CINR Low** – Lower threshold for stepping down in modulation profile (Adaptive mode).
- **CINR High** – Upper threshold for stepping up in modulation profile (Adaptive mode).
- **Backoff** – Internal setting controlling the OFDM Tx power backoff.



Note

Modulation parameters are optimized configuration. Do not alter them.

Configuring Ethernet Interfaces Using the CLI

The NetBeam system has four Ethernet interfaces:

- **Host** – Management interface
- **Eth0** – Radio interface
- **Eth1** – ODU interface, port 1
- **Eth2** – ODU interface, port 2
- **Eth3** – ODU interface, port 3 (NetBeam 2G only)
- **Eth4** – ODU interface, port 4 (NetBeam 2G only)

You can change the default values of the ODU interfaces, and display the port status of a specific interface.



Note

The Eth object is always followed by one or more name strings that correspond to ports or devices to be acted upon.

In the commands below, this string is represented as `<eth-list>`.

Configuring Interface Parameters

Use the `set eth` command, followed by the name of the interface (Eth1 or Eth2) to change the default values of an Ethernet interface.

```
set eth <eth-list>
  [admin up | down]
  [alias <string>]
  [eth-type <eth-type-set>]
  [auto-neg {enabled | disabled}]
  [loopback-mode { disabled | external | internal}]
  [loopback-timeout <integer>]
```

```
[alarm-propagation {disabled | backward | forward | both
directions}]
[clock {auto | master | slave | synce}]
```

For NetBeam 2G systems, the following options were added:

```
[network-type provider-nni | customer-uni | customer-nni]
[ieee1588 on | off]
[pcp-write-profile-id none | integer 1..255]
[classifier-mode dscp | pcp-dscp]
```

Displaying Interface Status

Use the `show eth` command, followed by the name of the interface, to display the Ethernet port status for a specific interface.

```
show eth [{<eth-list> | all}
          [{info | description | mtu | mac-addr | admin | operational
          | last-change | name | alias | eth-type | eth-act-type
          | auto-neg | loopback-mode | loopback-timeout | statistics
          | alarm-propagation}]]
```

The following is an example of an Ethernet interface status display:

```
Local_Site> show eth eth1

eth eth1 description      : Netronics
eth eth1 mtu              : 16384
eth eth1 mac-addr        : 00:24:a4:00:06:d2
eth eth1 admin            : up
eth eth1 operational      : up
eth eth1 last-change     : 0000:00:12:11
eth eth1 name             : Eth1
eth eth1 alias            :
eth eth1 eth-type        : 1000fd
eth eth1 eth-act-type     : 1000fd
eth eth1 auto-neg        : enabled
eth eth1 loopback-mode   : disabled
eth eth1 loopback-timeout : 60
eth eth1 alarm-propagation : disabled
eth eth1 clock            : auto
```

The following is an example of an Ethernet interface status display of NetBeam 2G:

```
Local_Site>show eth eth1

eth eth1 description      : Eth 1
```

```
eth eth1 mtu : 16384
eth eth1 mac-addr : 00:24:a4:01:4a:88
eth eth1 admin : up
eth eth1 operational : up
eth eth1 last-change : 0000:03:13:46
eth eth1 name : Eth1
eth eth1 alias :
eth eth1 eth-type : 1000fd
eth eth1 eth-act-type : 1000fd
eth eth1 auto-neg : enabled
eth eth1 loopback-mode : disabled
eth eth1 loopback-timeout : 60
eth eth1 alarm-propagation : disabled
eth eth1 clock : auto
eth eth1 connector-type : rj45
eth eth1 network-type : customer-nni
eth eth1 pcp-write-profile-id : none
eth eth1 classifier-mode : pcp-dscp
eth eth1 pfc-mode : disable
eth eth1 alarm-suppression : disable
```

Default VLAN Setting

NetBeam's Undefined VLAN feature enables transparent forwarding of both tagged and untagged traffic by default. No configuration or license is necessary for this feature, which gives you the flexibility to change your VLANs with no additional configuration necessary in the NetBeam system.

For VLAN configuration options, including the ability to define or block specific VLANs, refer to *Configuring VLANs* on page 70.

Chapter 5

Commissioning and Acceptance Procedure

This chapter presents the recommended commissioning and acceptance procedure to be performed following the installation of each NetBeam ODU.

The commissioning and acceptance procedure verifies the correct installation and the proper, safe, and robust operation of the NetBeam RF link.

This chapter includes the following topics:

- Installation Verification and Testing
- NetBeam Commissioning and Acceptance Form

Installation Verification and Testing

Inspect the following components and confirm their adherence to requirements that are detailed in the accompanying checklist (*NetBeam Commissioning and Acceptance Form* on page 64).



Make copies of the *NetBeam Commissioning and Acceptance Form* on page 64 and use it as a comprehensive guide to RF link commissioning and acceptance.

Physical Installation Verification

This inspection verifies the physical installation of the ODU, in accordance with *Installing the NetBeam* on page 20.

- Pole mount installation

- ODU installation
- Connectors' sealing
- Cables installation
- Grounding

RF Link Test

This inspection verifies the RF link status, in accordance with *Performing Basic Configuration Using the Web EMS* on page 39 and *Performing Basic Configuration using the CLI* on page 53.

- RF LED is green.
- Management/CLI indication: "RF Operational – Up".
- Receive Signal Strength Indication (RSSI) achieved in Alignment mode is within +/-5 dB of the expected value.
- Carrier to Interference + Noise Ratio (CINR) is 17 or higher.
- Link configuration (modulation, mode) is in accordance with plan requirements.

Link Errors Test

This inspection verifies error-free operation of the radio link.

- No errors/loss on the RF Statistics counters (show rf statistics).

Ethernet Services Test

This inspection verifies correct Ethernet services flow and error-free operation.

- Connect PCs on both ends of the link and use software-based utilities to test for packet-loss.
- If available, connect a packet analyzer to the GbE port and verify that no packets are lost.

Management Verification

This inspection verifies proper management of the link.

- Verify correct management/CLI connection to both local and remote ODUs.
- Verify management access from remote NMS stations.

Recording ODU Configuration

Perform the following steps after the NetBeam ODU is commissioned and accepted:

- Copy the Running Configuration (currently active) to Startup Configuration.
- Save the configuration file for future records and backup.

NetBeam Commissioning and Acceptance Form

NetBeam Commissioning and Acceptance Form		
Customer Details		
Customer		
Project/link name		
Physical Installation Verification	<u>Local Site</u>	<u>Remote Site</u>
Site name & address		
Mount type	<input type="checkbox"/> Roof-top <input type="checkbox"/> Mast/Tower	<input type="checkbox"/> Roof-top <input type="checkbox"/> Mast/Tower
ODU mount above ground	meters	meters
Clear line-of-sight	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
ODU safely mounted using Netronics' bracket correctly installed	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
Pole diameter between 2-4"	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
Bracket's mounting bolts securely tightened	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
ODU grounding	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
Cables/Fibers connections <small>(mark all cables connected)</small>	<input type="checkbox"/> Eth1 Cat5 <input type="checkbox"/> Eth1 Fiber <input type="checkbox"/> Eth2 Cat5 <input type="checkbox"/> Eth2 Fiber <input type="checkbox"/> Eth3 Cat5 <input type="checkbox"/> Eth3 Fiber <input type="checkbox"/> Eth4 Cat5 <input type="checkbox"/> Eth4 Fiber <input type="checkbox"/> DC	<input type="checkbox"/> Eth1 Cat5 <input type="checkbox"/> Eth1 Fiber <input type="checkbox"/> Eth2 Cat5 <input type="checkbox"/> Eth2 Fiber <input type="checkbox"/> Eth3 Cat5 <input type="checkbox"/> Eth3 Fiber <input type="checkbox"/> Eth4 Cat5 <input type="checkbox"/> Eth4 Fiber <input type="checkbox"/> DC
Overall cables/fibers length	meters	meters

Cables/Fibers securely routed and fixed properly using cable ties	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
Cables/Fibers are properly weatherproofed using the appropriate glands	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
ODU DC source	<input type="checkbox"/> PoE <input type="checkbox"/> External DC	<input type="checkbox"/> PoE <input type="checkbox"/> External DC
PoE model and manufacturer		
Measured DC power (or CLI/Web reading)	Volts DC	Volts DC
RF Link Parameters		
ODU Model		
ODU P/N		
ODU S/N		
ODU running SW version		
Tx/Rx frequency	MHz	MHz
Channel-width	<input type="checkbox"/> 250MHz <input type="checkbox"/> 500MHz	<input type="checkbox"/> 250MHz <input type="checkbox"/> 500MHz
Role	<input type="checkbox"/> Auto <input type="checkbox"/> Master <input type="checkbox"/> Slave	<input type="checkbox"/> Auto <input type="checkbox"/> Master <input type="checkbox"/> Slave
Tx/Rx Link ID	0 (not used)	0 (not used)
Modulation/Mode <small>Mode: modulation/sub-channel/repetitions/FEC</small>	<input type="checkbox"/> Adaptive _____ <input type="checkbox"/> Static _____	<input type="checkbox"/> Adaptive _____ <input type="checkbox"/> Static _____
UL/DL Configuration	<input type="checkbox"/> Symmetric <input type="checkbox"/> Asymmetric (ratio) _____%	<input type="checkbox"/> Symmetric <input type="checkbox"/> Asymmetric (ratio) _____%
ODU polarization	<input type="checkbox"/> V <input type="checkbox"/> H	<input type="checkbox"/> V <input type="checkbox"/> H
Link distance	meters	

RF Link Tests		
Expected RSSI	dBm	dBm
Measured RSSI	dBm	dBm
Measured CINR	dB	dB
Green "RF" LED	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
RF operational status Up	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
RF Statistics error counters clear	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
Ethernet Services Tests		
Packet-Loss test <input type="checkbox"/> Packet Analyzer <input type="checkbox"/> SW-based	<input type="checkbox"/> No Packet-Loss Test duration _____	<input type="checkbox"/> No Packet-Loss Test duration _____
Eth Statistics dropped-packets counters clear	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
Management		
IP address/Mask		
IP Mask		
Default IP Gateway		
In-band management enabled	<input type="checkbox"/> Yes <input type="checkbox"/> No VLAN ID _____	<input type="checkbox"/> Yes <input type="checkbox"/> No VLAN ID _____
Management of local and remote	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
NMS used	<input type="checkbox"/> Web/CLI only <input type="checkbox"/> Other _____	<input type="checkbox"/> Web/CLI only <input type="checkbox"/> Other _____
NMS management access	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
Traps received in NMS	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
Final Configuration Verification		
Copy running config to startup	<input type="checkbox"/> Done	<input type="checkbox"/> Done

Clear all statistics and logs	<input type="checkbox"/> Done	<input type="checkbox"/> Done
Configuration file saved and stored	<input type="checkbox"/> Done	<input type="checkbox"/> Done
Additional Info / Remarks		
I&C Details		
I&C Date		
Installation team		
Commissioning team		

Chapter 6

NetBeam Networking Configuration

This chapter presents the NetBeam bridge management model and describes the initial procedures for configuring the NetBeam network, including:

- Provider Bridge
- NetBeam Bridging Model
- Configuring VLANs
- Single Component Bridge Model
- Configuring Bridge Ports
- Configuring Provider Bridge and Advanced VLAN Settings

Provider Bridge

The IEEE 802.1ad Provider Bridge, commonly known as QinQ or Provider Bridge, extends the IEEE 802.1Q standard by providing for a second stack of VLANs in a bridged network. The general purpose of Provider Bridge is to enable frames from multiple customers to be forwarded (or tunneled) through another topology (provider network) using service VLANs or S-VLANs. The provider bridge, which may consist of multiple devices in the service provider domain, looks like a simple bridge port to the customer's traffic and maintains the customer's VLANs.

Customer VLANs (referred to as C-VLANs by the IEEE 802.1ad specification) are not used to make any forwarding decisions inside the provider network where customer frames get assigned to service VLANs (S-VLANs). Inside the provider cloud, frames are forwarded based on the S-VLAN tag only, while the C-VLAN tag remains shielded during data transmission.

The S-VLAN tag is removed when the frame exits the provider network, restoring the original customer frame.

The NetBeam incorporates a fully functional integrated Provider Bridge (IEEE 802.1ad).

NetBeam Bridging Model

The Netronics implementation of Provider Bridge is a network of up to seven virtual bridges connected in a cross-like fashion as shown in Figure 6-1 and Figure 6-2.

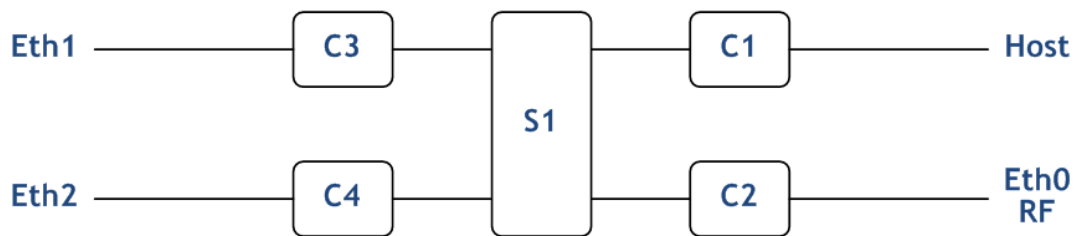


Figure 6-1: NetBeam 1G/M7 Generic Model of the NetBeam Bridge

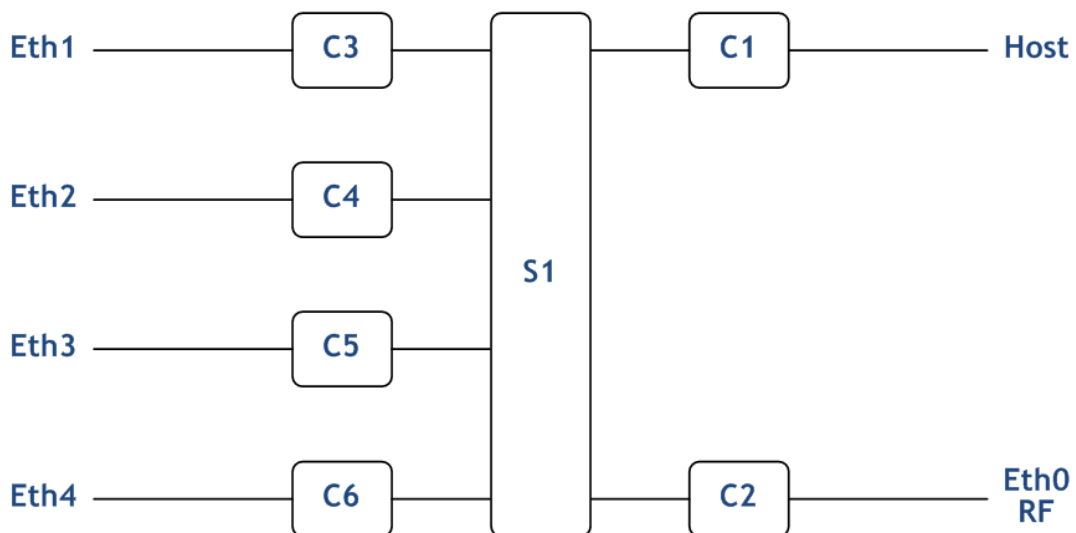


Figure 6-2: NetBeam 2G Generic Model of the NetBeam Bridge

Each component acts as a virtual bridge. A component can have both external and internal ports. An external port name is identical to its interface name. For example, the C-component 1 (C1) external port name is ETH2. An internal port uses the name of its peer component as shown above. For example, when C-component 1 (C1) is connected to the S component, the corresponding internal port is S1.

You can change the default bridge configuration to suit your network by removing or adding the desired bridge components. All components are created, managed, and removed using the CLI or Web EMS.

Configuring VLANs

This section lists the default VLAN and Port settings, and provides instructions for modifying these settings.

By default, the NetBeam system is set to Transparent Bridge (Undefined VLAN) mode. The Transparent Bridge feature enables transparent forwarding of both tagged and untagged traffic by default. No configuration or license is necessary for this feature, which gives you the flexibility to change your VLANs with no additional configuration necessary in the NetBeam system.

In addition to the default Transparent Bridge feature, you can choose to create VLANs, as well as block specific VLANs.

Transparent Bridge Mode

NetBeam's default setting is Transparent Bridge (Undefined VLAN). In this configuration, both tagged and untagged traffic is forwarded transparently. No VLAN configuration is required for Undefined VLAN. This feature gives you the flexibility to change your VLANs with no configuration necessary on the part of the NetBeam system.

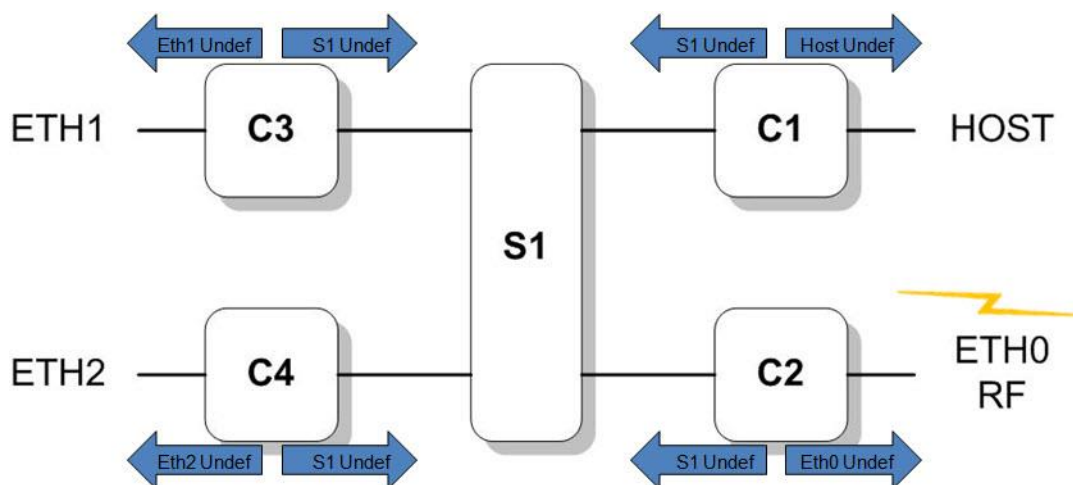


Figure 6-3: Undefined VLAN Implementation

In Transparent VLAN mode, you can use the Eth1 or the Eth2 port for all data and management traffic, included both tagged and untagged data. Alternatively, you can use one of the ports for management, and the other port for data, including both tagged and untagged data.

```
default>show vlan
component-id vid fdb-id egress untagged history
s1 1 1 c1,c2,c3,c4 c1,c2,c3,c4 disable
s1 undef 1 c1,c2,c3,c4 none disable
c1 1 1 host,s1 host disable
c1 undef 1 host,s1 none disable
c2 1 1 eth0,s1 eth0 disable
c2 undef 1 eth0,s1 none disable
c3 1 1 eth1,s1 eth1 disable
c3 undef 1 eth1,s1 none disable
c4 1 1 eth2,s1 eth2 disable
c4 undef 1 eth2,s1 none disable
default>
```

For NetBeam 2G, the following additional config is displayed:

```
c5 1 1 eth3,s1 eth3 disable
c5 undef 1 eth3,s1 none disable
c6 1 1 eth4,s1 eth4 disable
c6 undef 1 eth4,s1 none disable
```

Configuring VLANs Using the Web EMS

To configure VLANs using the Web EMS:

1. In the Web EMS Main screen, click **Bridge**. The Bridge screen is displayed.
2. Click the **VLANs** section of the Bridge screen.

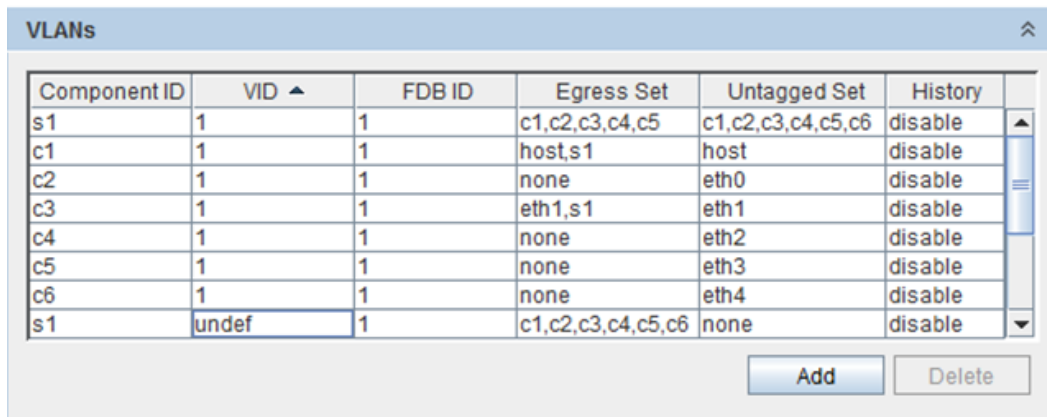


Figure 6-4: Web EMS Bridge Screen – VLANs Section

3. Click **Add**. The Add VLAN window is displayed.

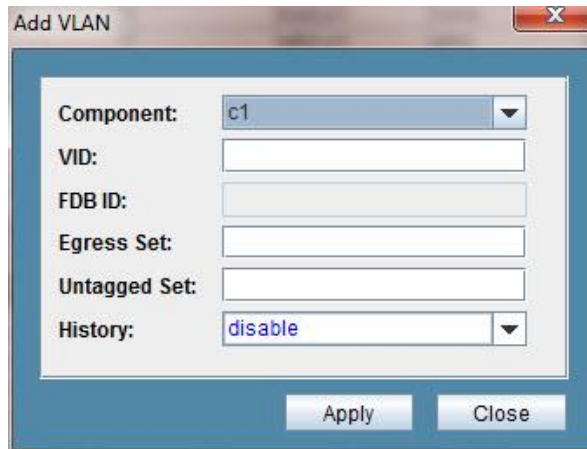


Figure 6-5: Add VLAN Window

4. Configure the following VLAN attributes for the required components:
 - **VID** – C-VLAN Identifier. This can be any number from 1 to 4094, which identifies a particular C-VLAN, or the special value “undef”, which identifies configuration relevant for all VLANs that are not explicitly defined in the VLAN table. To edit an existing VLAN, enter the VID of the VLAN you want to edit.
 - **FDB ID** – Enter **1**. For S-VLANs in Provider Bridge configuration, up to 64 FDBs are available for different S-VLANs.
 - **Egress Set** – A frame which belongs to a VLAN identified by vid can enter the bridge through any port but can only leave through the ports that are included in the egress set (Host – management, Eth0 – radio, Eth1 – ODU port 1, Eth2 – ODU port 2).
 - **Untagged Set** – A subset of the egress set. If a port is a member of the untagged set and a frame leaves the bridge through this port, the C-Tag is removed (untagged). To leave the VLAN tagged when transmitted on all ports in the egress set, enter **none**.
 - **History** – If you want the ODU to collect statistics for this VLAN, select **enable**. Otherwise, select **disable**.
5. Click **Apply** to close the Add VLAN window.
6. Click **Apply** to implement the changes and close the Bridge screen.

Configuring VLANs Using the CLI

Creating and Modifying VLANs

VLAN definitions are stored in a table containing static configuration information for each VLAN that is configured in the device by local or network management. All VLAN table entries are permanent and are restored when the device is reset.

Use the following syntax to create or modify a VLAN:

```
set vlan <comp-id-list> <vid-list>
    [fdb-id <fdb-id>]
    [egress <bridge-port-list>]
    [untagged <bridge-port-list>]
```

Blocking Specific VLANs

You can block specific VLANs from entering the NetBeam system by using the `set vlan` command and setting the `egress` attribute to `none`.

The following example blocks VLAN 333 traffic from entering the NetBeam system:

```
default>set vlan c3 333 egress none untagged none
Set done: vlan c3 333
default>set vlan c4 333 egress none untagged none
Set done: vlan c4 333
default>set vlan c2 333 egress none untagged none
Set done: vlan c2 333
```

```
default>show vlan
component-id vid    fdb-id egress          untagged      history
s1           1      1      c1,c2,c3,c4    c1,c2,c3,c4  disable
s1           undef  1      c1,c2,c3,c4    none          disable
c1           1      1      host,s1        host          disable
c1           undef  1      host,s1        none          disable
c2           1      1      eth0,s1        eth0          disable
c2           undef  1      eth0,s1        none          disable
c3           1      1      eth1,s1        eth1          disable
c3           undef  1      eth1,s1        none          disable
c4           1      1      eth2,s1        eth2          disable
c4           undef  1      eth2,s1        none          disable
default>
```

For NetBeam 2G, the following additional config is displayed:

```
c5           1      1      eth3,s1        eth3          disable
c5           undef  1      eth3,s1        none          disable
c6           1      1      eth4,s1        eth4          disable
c6           undef  1      eth4,s1        none          disable
```

Deleting VLANs

Use the `clear vlan` command to delete VLANs and clear their associated statistics.

Use the following syntax:

```
clear vlan {<comp-id-list> | all} {<vid-list> | all}
    [statistics]
```

Displaying VLAN Details

Use the `show vlan` command to display VLANs and their details.

Use the following syntax:

```
show vlan [{all | <component-id>}
          [{all | <vids>}
          [{info | statistics | fdb-id | egress | untagged}]]]]
show vlan
          [{all | <vids>}
          [{info | statistics | fdb-id | egress | untagged}]]]]
```

Displaying VLAN Common Properties

To display the ODU's VLAN configuration, use the following command:

```
show vlan-common [{<comp-id-list> | all}
                 [{ info | version | max-vid | max-num | curr-num}]]
```

This command displays general information about VLAN bridges that are active in the network.

Single Component Bridge Model

This model is only applicable to version 5 of the NetBeam 2G.

Model Implementation

You can configure the ETH managed object to one of the following port types (network-types) to support both C-VLANs and S-VLANs transmission and to maintain backwards compatibility:

Customer UNI (CEP - Customer Edge Port): C-VLANs port, as per (old) Multi Component Bridge Mode configuration. In such configuration, each port has a C Bridge component.

- Provider NNI (PNP - Provider Network Port): S-VLANs port, as per (old) Multi Component Bridge Mode configuration when the C Bridge component was removed.
- Customer NNI (CNP - Customer Network Port): C-VLANs port, as per (new) Single Component Bridge Mode configuration. It does not have a C Bridge component, but it can carry C-VLANs and map them to S-VLANs using C-VLANs Registration.

By default, all Ethernet ports are configured as Customer NNI ports.

```

set eth host network-type customer-nni
set eth eth0 network-type customer-nni
set eth eth1 network-type customer-nni
set eth eth2 network-type customer-nni
set eth eth3 network-type customer-nni
set eth eth4 network-type customer-nni

```

Figure 6.6: shows the model of the NetBeam Bridge (Single Component Bridge Model).

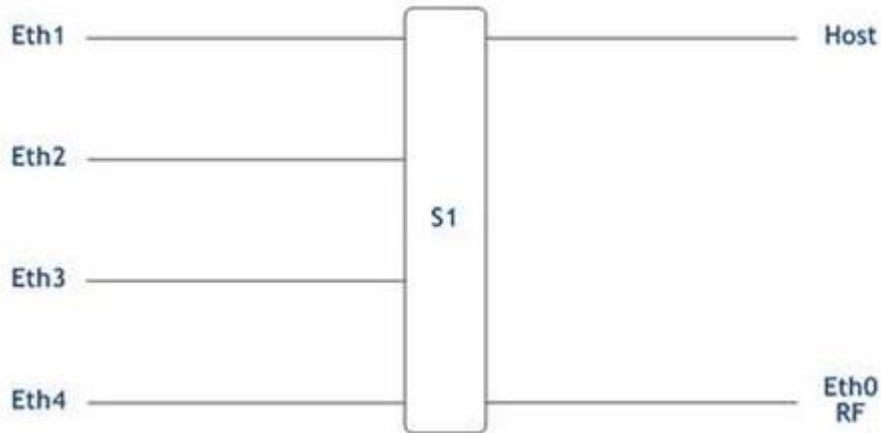


Figure 6-6: Single Component Bridge Model

VLAN Forwarding Based on Network Type

The ability to pass different types of packets depends on the Ethernet port's network type:

- Customer UNI (CEP) can only process C-VLANs (type=8100).
- Provider NNI (PNP) can only process S-VLANs (type=88a8).
- Customer NNI (CNP) can only process C-VLANs (type=8100).

VLAN Configuration

Transparent Bridge

NetBeam's default setting is Transparent Bridge. In this configuration, both C-VLAN tagged and untagged traffic is forwarded transparently (no VLAN configuration is required).

In addition to the default Transparent Bridge feature, you can choose to create VLANs, and block specific VLANs.

Default Configuration

VLAN configuration is available for the S Component only (only S-VLANs can be created).

The VLANs use the C-VLANs Registration to Map the C-VLANs on S-VLANs.

Two configuration lines are used for the S bridge component:

- VLAN 1 – forwarding rule for untagged traffic (no S-VLAN).
- VLAN Undef – forwarding rule for any S-VLAN tagged traffic.

```
# vlan configuring
set vlan s1 1 egress host,eth0,eth1,eth2,eth3,eth4 untagged
host,eth0,eth1,eth2,eth3,eth4 history disable
set vlan s1 undef egress host,eth0,eth1,eth2,eth3,eth4 untagged
none history disable
```

In this configuration, when the Network Type is set to Customer NNI (default configuration):

1. All C-VLAN tagged packets are carried transparently between all ports.
2. All untagged packets are tagged internally with C-VLAN ID 1 (based on the port's PVID) and carried transparently between all ports (the VLAN ID 1 is removed on egress).
3. All S-VLAN tagged packets (with type=88a8) are not recognized by the Customer NNI port, they are, therefore, tagged internally with C-VLAN ID 1 (based on the port's PVID) and carried transparently between all ports (the VLAN ID 1 is removed on egress).

Please note that this default configuration provides transparent connection for all untagged, C-VLAN tagged, and S-VLAN tagged packets.

Basic Configuration Example – Transparent + VLAN Management

The default configuration provides transparent connection for all untagged, C-VLAN tagged, and S-VLAN tagged packets. This includes data and management traffic (going to the Host).

In order to manage the ODU (including in-band management to remote ODUs), it is sufficient to define the management VLAN in the IP configuration. You do not need to configure it in the VLAN table.

For example, VLAN and IP configuration for Transparent Bridge with management over VLAN 100:

```
# vlan configuring
```

```
set vlan s1 1 egress host,eth0,eth1,eth2,eth3,eth4 untagged
host,eth0,eth1,eth2,eth3,eth4 history disable
set vlan s1 undef egress host,eth0,eth1,eth2,eth3,eth4 untagged
none history disable
```

```
# ip configuring
set ip 1 ip-addr static 192.168.24.111 prefix-len 24 vlan 100
```

VLAN Configuration with Network Type = Customer NNI

Use the C-VLANs Registration table to Configure C-VLANs and map them to S-VLANs.

Controlling the forwarding of specific C-VLANs requires mapping them on S-VLANs as only S-VLANs may be defined.

cvlan-reg configuration:

```
set cvlan-reg <component-id> <bridge-port-list> <cvid> [svid
<value>] [untag-cep <value>] [untag-pep <value>]
  <component-id>          : c1 | c2 | c3 | c4 | c5 | c6 | s1
  <bridge-port-list>      : list: | host | eth0 | eth1 | eth2 |
eth3 | eth4
  <cvid>                   : novlan | undef | integer 1..4094
```

- cvlan-reg: An element of the C-VID registration table that contains the mapping between a C-VID and the S-VID which carries the service and determines the handling of untagged frames at the PEP and CEP.
- Untagged CEP: A flag indicating if a C-VID should be carried untagged at the Customer Edge Port. Yes - means untagged.
- Untagged PEP: A flag indicating if a C-VID should be carried untagged at the Provider Edge Port. Yes - means untagged.

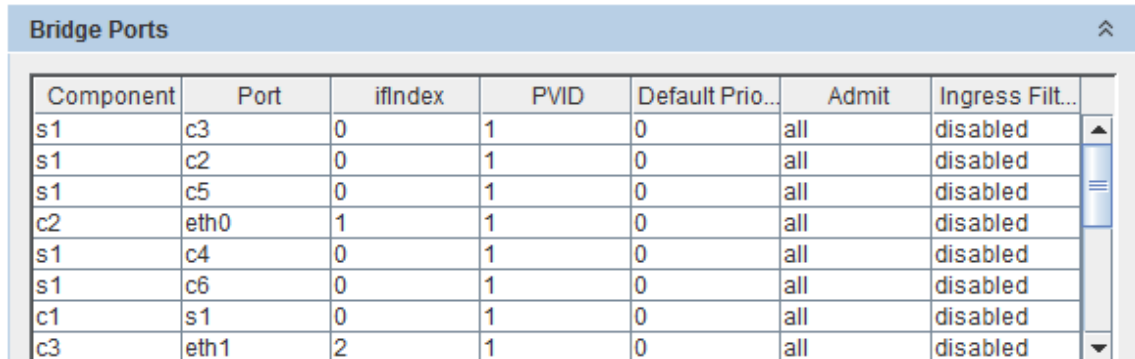
Configuring Bridge Ports

Configuring Bridge Ports Using the Web EMS

To configure ports using the Web EMS:

1. In the Web EMS Main screen, click **Bridge**. The Bridge screen is displayed.

- Click the Bridge Ports section of the Bridge Ports screen.



Component	Port	ifindex	PVID	Default Prio...	Admit	Ingress Filt...
s1	c3	0	1	0	all	disabled
s1	c2	0	1	0	all	disabled
s1	c5	0	1	0	all	disabled
c2	eth0	1	1	0	all	disabled
s1	c4	0	1	0	all	disabled
s1	c6	0	1	0	all	disabled
c1	s1	0	1	0	all	disabled
c3	eth1	2	1	0	all	disabled

Figure 6-7: Web EMS Bridge Screen – Bridge Ports Section

- To edit a port and change its PVID, click **Edit**. The Change Port window is displayed.

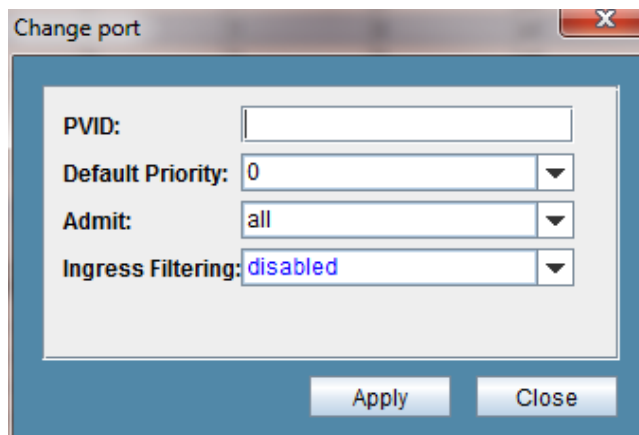


Figure 6-8: Change Port Window

- In the **Port** field, select the port you want to edit.
- Configure the following Port attributes:

pvid A *vid* which will be assigned to an untagged frame or a priority-tagged frame, (the VID is set to 0 indicating that the frame does not belong to any VLAN and only PCP field is relevant), which enters to the bridge through this port. The special value “undef” cannot be used as PVID. By default it is set to 1.

prio The value which is assigned to the PCP field if an untagged frame arrives through this port. For priority-tagged frames this field is irrelevant. By default it is set to 0.

admit This attribute controls what kinds of frames are allowed into the bridge. If it is set to *untagged* then only untagged or priority tagged frames may enter. If it is set to *tagged* then only tagged frames (i.e. those with VID different from zero) may enter. If it is set to *all*, all kinds of frames may enter. By default it is set to *all*.

filter By default the VLAN configuration is essentially asymmetrical. Frames with any VLAN IDs may enter through any port but leave only through a port which is a member in the egress set assigned to a particular VLAN. By setting *filter* to *enabled* symmetry is introduced – in this case a frame can enter through a particular port only if it can leave through this port as well. By default the attribute is set to *disabled*.

6. Click **Apply** to close the Change Port window.
7. Click **Apply** to implement the changes and close the Bridge screen.

Configuring Bridge Ports Using the CLI



Note

The Bridge object is always followed by one or more name strings that correspond to ports or devices to be acted upon.

In the commands below, this string is represented as `<comp-id-list>`.

For more details on this convention, see *Designating Named Objects* on page 219.

Use the following command to assign the bridge device:

```
set bridge <comp-id-list>
```

Use the following command to display bridge parameters:

```
show bridge {[<comp-id-list> | all]
             [{info | mac-addr | num-ports}]}
```

Use the following command to reset all bridge attributes:

```
clear bridge {<comp-id-list> | all}
```

Configuring the Bridging Port

The bridging port provides access to port-wide definitions from the bridge. When using the `bridge-port` commands, you can specify any combination of components and ports. However, only certain combinations will produce a result.

In the current product version, the following usage restrictions exist:

- Component *c1* is strictly associated with the Ports *host* and *s1*.
- Component *c2* is strictly associated with the Ports *eth0* and *s1*.
- Component *c3* is strictly associated with the Ports *eth1* and *s1*.
- Component *c4* is strictly associated with the Ports *eth2* and *s1*.

- Component *c5* is strictly associated with the Ports *eth3* and *s1*.
- Component *c6* is strictly associated with the Ports *eth4* and *s1*.
- The Ports associated with the Component *s1* are dependent on the *c* components that currently exist. For example, if the components *c1* and *c4* already exist, then the Component *s1* is associated with the Ports *eth0*, *eth1*, *c1* and *c4*.

The validity of a specified combination should be tested before command execution.

You can use the `set bridge-port` command to assign the bridging port parameters.

```
set bridge-port <comp-id-list> <bridge-port-list>
    [pvid <vlan>]
    [prio {0..7}]
    [admit untagged | tagged | all]
    [filter enabled | disabled]
```

You can use the `show bridge-port` command to display the bridging port attributes.

```
show bridge-port [[{<comp-id-list> | all}] {<bridge-port-list> |
all}
    [{ info | mac-addr | num-ports | interface | pvid | prio
    | admit | filter | gvrp | vlan-restricted | last-pdu-origin
    | statistics}]]
```

Configuring Provider Bridge and Advanced VLAN Settings

Configuring PEP Virtual Ports

PEP Virtual Ports are used to configure ingress port filtering. PEP table entries define traffic flows from the provider network to the customer edge port. The table is indexed by Component ID and S-VID. You can specify the default C-VID value and default user priority in the PEP table.

Use the following command to create and modify PEP Virtual Port elements:

```
set pep-vp <c-comp-id-list> s1 <vid-list>
    [cpvid <vid>]
    [prio 0..7]
    [admit all | tagged | untagged]
    [filter enabled | disabled]
```

If the PEP Virtual Port entry does not already exist, the `set pep-vp` command creates it and assigns the attributes specified. Upon creation, in the event that an attribute is not explicitly specified, the entry is created with the default value for that attribute.

If the PEP Virtual Port entry already exists, then the `set pep-vp` command replaces the attributes that are currently defined for the entry with those specified in the command.

Note the following conditions for execution:

- The `set pep-vp` command is valid only for those bridge ports which are S component ports.
- The `set pep-vp` command fails if the port specified belongs to an S component and not a C-component.
- The `set pep-vp` command also fails if the S-VID specified is not yet defined in the VLAN table.

Use the following command to display PEP Virtual Port entries:

```
show pep-vp [{<c-comp-id-list> | all}
  [{all | <bridge-port-list>}
  [{all | <s-vid>}
  [{info | cpvid | prio | admit | filter}]]].
```

Use the following command to delete PEP Virtual Port entries:

```
clear pep-vp {<c-comp-id-list> | all} {s1 | all} {<vid-list>
  | all}
```

S-VID Translation Table

The S-VID Translation table is used to maintain bi-directional mapping between a Local S-VID (used in data and protocol frames transmitted and received through a CNP or PNP) and a Relay S-VID (used by the filtering and forwarding process).

Each VID Translation table definition contains Component, Port, Local S-VID values, and the Relay S-VID values for each specified S-VID. If no entry exists in this table for a specified Component, Port, and Local S-VID, then a substitute value is taken from the Relay S-VID that is specified in a frame received on a Local S-VID Port.

All S-VID Translation table entries are permanent and are restored when the device is reset.

Use the following command to create and modify S-VID Translation table entries:

```
set svid-xlat s1 <ext-bridge-port-list> <vid> relay-svid <vid>
```

If the entry does not already exist, the `set svid-xlat` command creates it and assigns the attributes specified. Upon creation, in the event that an attribute is not explicitly specified, the entry is created with the default value for that attribute.

If the entry already exists, then the `set svid-xlat` command replaces the attributes that are currently defined for the entry with those specified in the command.

Note the following conditions for execution of the `set svid-xlat` command:

- The command is valid only for bridge ports that are S-component ports.
- The `set svid-xlat` command fails if the port specified belongs to a C-component and not an S-component.
- The `set svid-xlat` command also fails if the S-VID specified is not yet defined in the VLAN table.

Use the following command to delete S-VID Translation table entries and clear their associated statistics:

```
clear svid-xlat {s1 | all} {<ext-bridge-port-list> | all} {<vid-list> | all}
```

Use the following command to display S-VID Translation table entries:

```
show svid-xlat [{s1 | all}
               [{<ext-bridge-port-list> | all}
               [{<vid-list> | all}
               [info]]]
```

C-VLAN Registration Table

An element of the C-VID registration table is accessed by PB C-VLAN component, Customer Edge Port bridge port number, and C-VID. Each element contains the mapping between a C-VID and the S-VID which carries the service and Booleans for handling untagged frames at the PEP and CEP.

Use the following command to create and modify C-VLAN Registration table entries:

```
set cvlan-reg <c-comp-id-list> <ext-bridge-port-list> <vid-list>
  [svlan <vid>]
  [untag-cep yes | no]
  [untag-pep yes | no]
```

If the entry does not already exist, the `set cvlan-reg` command creates it and assigns the attributes specified. Upon creation, in the event that an attribute is not explicitly specified, the entry is created with the default value for that attribute.

If the entry already exists, then the `set cvlan-reg` command replaces the attributes that are currently defined for the entry with those specified in the command.

Note the following conditions for execution of the `set cvlan-reg` command:

- The `set cvlan-reg` command is valid only for bridge ports that are external C-component ports: `host`, `eth0`, `eth1`, and `eth2`.
- The `set cvlan-reg` command fails if the port specified belongs to an S-component and not a C-component.
- The `set cvlan-reg` command also fails if the C-VID specified is not yet defined in the VLAN table.

Use the following command to display C-VLAN Registration table entries:

```
show cvlan-reg [{<c-comp-id-list> | all}
                [{<ext-bridge-port-list> | all}
                [{<vid-list> | all} [{info | svlan | untag-cep
                | untag-pep}]]]]
```

Use the following command to delete C-VLAN Registration table entries:

```
clear cvlan-reg {<c-comp-id-list> | all} {<ext-bridge-port-list>
                | all} {<vid-list> | all}
```

VLAN-to-SNMP ifTable

Whenever a VLAN is associated with Component `c1`, an entry in the SNMP `ifTable` is automatically created for that VLAN. When the VLAN is deleted, the corresponding `ifTable` entry is also deleted.

Forwarding Data Base (FDB)

The Forwarding Data Base (FDB) enables access to general parameters of the FDB Address table, which specifies configuration and control information for each Filtering Database currently operating on the device.

The system maintains 64 permanent instances of the FDB object.

Use the following command to create and modify FDB entries:

```
set fdb s1 <fdb-id-list> [aging <aging-time>]
```

Use the following command to display FDB entries:

```
show fdb [s1
          [<fdb-id-list>
          [{aging | full-table-counter | num-of-dynamic}]]]
```

Configurable Eth-type

IEEE 802.1ad Provider Bridges (a.k.a Q-in-Q) defines the S-VLAN protocol type as 0x88A8 and lists additional EtherType field values for S-VLAN: 0x8100, 0x9100, and 0x9200 to support backwards compatibility.

Any Eth-type within the range of 0x700..0xFFFF is supported (except for 0x800, 0x806, 0x8809, 0x88CC, and 0x8902).

By default:

- CVID = 0x8100
- SVID = 0x88A8

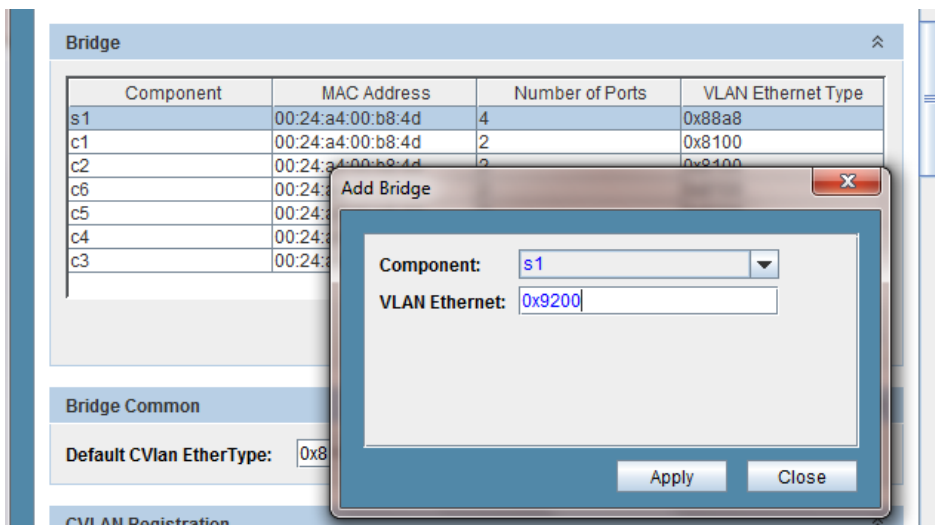


Figure 6-4: Web EMS Ethertype Configuration

The Bridge Common option allows you to configure default CVlan EtherType when handling S-Vlan frames.

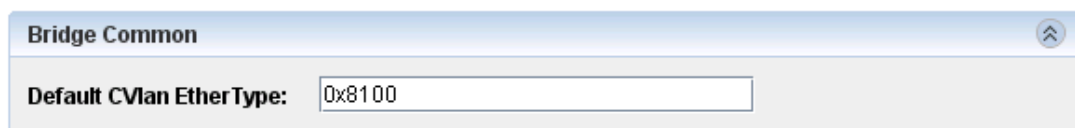


Figure 6-5: Web EMS Bridge Common

EtherType configuration using the CLI:

```
CLI>set bridge c4 vlan-ethertype ?
hex number 0x700..0xFFFF except 0x800, 0x806, 0x8809, 0x88CC,
0x8902
```

Example of setting C4 with Eth-Type of 0x8111:

```
CLI>set bridge c4 vlan-ethertype 0x8111
Set done: bridge c4
CLI>show bridge all vlan-ethertype
bridge s1 vlan-ethertype      : 0x88a8

bridge c1 vlan-ethertype      : 0x8100
bridge c2 vlan-ethertype      : 0x8100
bridge c3 vlan-ethertype      : 0x8100
bridge c4 vlan-ethertype      : 0x8111
bridge c5 vlan-ethertype      : 0x8100
bridge c6 vlan-ethertype      : 0x8100
```

FDB Address Table

The FDB Address table contains information about unicast entries for which the device has forwarding and/or filtering information. This information is used by the transparent bridging function when determining how to propagate a received frame.

Use the following command to create and modify entries in the FDB Address table:

```
set fdb-table s1 <fdb-id-list> <mac-addr> port <bridge-port>
```

If the FDB Address table entry does not already exist, the `set fdb-table` command creates it and assigns the attributes specified. Upon creation, in the event that an attribute is not explicitly specified, the entry is created with the default value for that attribute.

If the entry already exists, then the `set fdb-table` command replaces the attributes that are currently defined for the entry with those specified in the command.

Note that the `set fdb-table` command fails if its port already exists in the FDB with `self` as the assigned status.

Use the following command to display FDB Address table entries:

```
show fdb-table
  [{s1 | all}
  [{<fdb-id-list> | all}
  [{<mac-addr> | all}
  [{info | port | status}]]]
```

Use the following command to delete FDB Address table entries and clear their associated statistics:

```
clear fdb-table {s1 | all} {<fdb-id-list> | all} {<mac-addr>
    | all}
```

Note that the `delete fdb-table` command fails if its port exists in the FDB with `self` as the assigned status.

Performing Advanced Configuration

Configuring Quality-of-Service

Quality of Service (QoS) mechanisms enable service providers to offer different classes of service for different types of traffic or customers. QoS mechanisms are especially important in wireless links with adaptive capabilities, because changing link conditions may require the system to drop some traffic according to a predetermined priority and scheduling scheme.

NetBeam has eight priority queues per interface. Queues are accessed by Strict Priority or Weighted Fair Queuing (WFQ) and Shaper mechanisms.

QoS functions:

- Classifier (COS and EVC)
- Metering (CIR/EIR/CBS/EBS)
- Ingress QOS Marking (Green/Yellow/Red)
- Scheduler (Strict Priority/WFQ/ SP+Shaper /WFQ+Shaper)

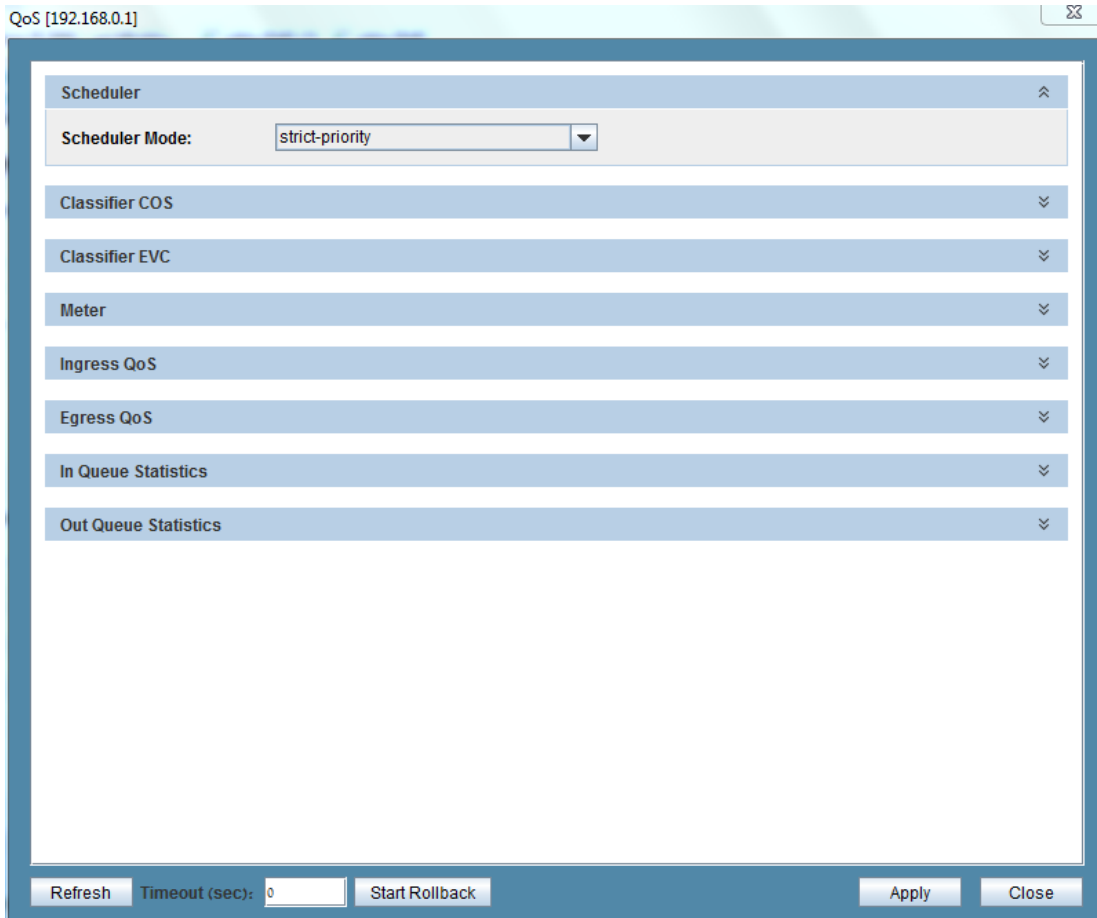


Figure 7-1: QoS Main Screen

QoS Classification

The NetBeam QoS Engine classifies the incoming packets by port, VID, PCP, and/or DSCP (as defined by the IEEE 802.1 Q/p and RFC-2475 standards), or alternatively MPLS EXP bit, and maps them onto {EVC, CoS} pairs.

The classification fields of VID, PCP, and DSCP/MPLS-Exp represent the CoS that determine the egress queue. Classification based on EVC forwards the packets through the meter and the marker.

For NetBeam 1G, DSCP classification is based on 3 MSB bits (8 options).

For NetBeam 2G, two modes are supported:

- PCP-DSCP: classification based on PCP (3 bits) and DSCP (3 bits)
- DSCP: classification based on DSCP (6 bits) only. In this mode classification based on PCP is not available and trying to configure PCP classification will result in error message.

In order to change the classification mode (per interface):

```
Left_11>set eth eth1 classifier-mode
dscp | pcp-dscp
```

The default classification mode is pcp.

Classifier-Cos Settings

Use the following command to configure classifier-cos:

```
set classifier-cos <classifier-id: 1..248> [interface
<host|eth0|
eth1|eth2|eth3|eth4>] [precedence <1..8>] [vid < list
0..4094>] [pcp < list 0..7>] [ip-cos <{{dscp-cos | mpls-exp}
<list of 0..7>}|dont-care>] [cos <0..7>]
```

IP-COS: Priority based on IP header value – DSCP (differentiated services), MPLS-EXP (MPLS experimental bit), or Don't-Care (IP header values ignored).

Precedence: Priority between classifiers. Multiple and overlapping classifiers rules may be configured. In such case, the precedence value will determine the priority between the overlapping classifier rules.

The default system configuration is priority based on Vlan pBits (PCP) on all interfaces:

```
# classifier-cos configuring
set classifier-cos 1 interface host,eth0,eth1,eth2,eth3,eth4
precedence 1 vid 0-4094 pcp 0 ip-cos dont-care cos 0
set classifier-cos 2 interface host,eth0,eth1,eth2,eth3,eth4
precedence 1 vid 0-4094 pcp 1 ip-cos dont-care cos 1
set classifier-cos 3 interface host,eth0,eth1,eth2,eth3,eth4
precedence 1 vid 0-4094 pcp 2 ip-cos dont-care cos 2
set classifier-cos 4 interface host,eth0,eth1,eth2,eth3,eth4
precedence 1 vid 0-4094 pcp 3 ip-cos dont-care cos 3
set classifier-cos 5 interface host,eth0,eth1,eth2,eth3,eth4
precedence 1 vid 0-4094 pcp 4 ip-cos dont-care cos 4
set classifier-cos 6 interface host,eth0,eth1,eth2,eth3,eth4
precedence 1 vid 0-4094 pcp 5 ip-cos dont-care cos 5
set classifier-cos 7 interface host,eth0,eth1,eth2,eth3,eth4
precedence 1 vid 0-4094 pcp 6 ip-cos dont-care cos 6
set classifier-cos 8 interface host,eth0,eth1,eth2,eth3,eth4
precedence 1 vid 0-4094 pcp 7 ip-cos dont-care cos 7
```

Classifier-Cos settings example for management priority (for traffic from ports: Host, Eth2):

```
set classifier-cos 1 interface host,eth2 precedence 1 vid 0-4094 pcp
0-7 ip-cos dont-care cos 7
```

Classifier-Cos settings example for priority based on PCP (pBits) on Eth1, Eth0 with management priority (for traffic from ports: Host, Eth2):

```
# classifier-cos configuring
set classifier-cos 1 interface host,eth2 precedence 1 vid 0-4094 pcp
0-7 ip-cos dont-care cos 7
set classifier-cos 2 interface eth0,eth1 precedence 1 vid 0-4094 pcp
0 ip-cos dont-care cos 0
set classifier-cos 3 interface eth0,eth1 precedence 1 vid 0-4094 pcp
1 ip-cos dont-care cos 1
set classifier-cos 4 interface eth0,eth1 precedence 1 vid 0-4094 pcp
2 ip-cos dont-care cos 2
set classifier-cos 5 interface eth0,eth1 precedence 1 vid 0-4094 pcp
3 ip-cos dont-care cos 3
set classifier-cos 6 interface eth0,eth1 precedence 1 vid 0-4094 pcp
4 ip-cos dont-care cos 4
set classifier-cos 7 interface eth0,eth1 precedence 1 vid 0-4094 pcp
5 ip-cos dont-care cos 5
set classifier-cos 8 interface eth0,eth1 precedence 1 vid 0-4094 pcp
6 ip-cos dont-care cos 6
set classifier-cos 9 interface eth0,eth1 precedence 1 vid 0-4094 pcp
7 ip-cos dont-care cos 7
```

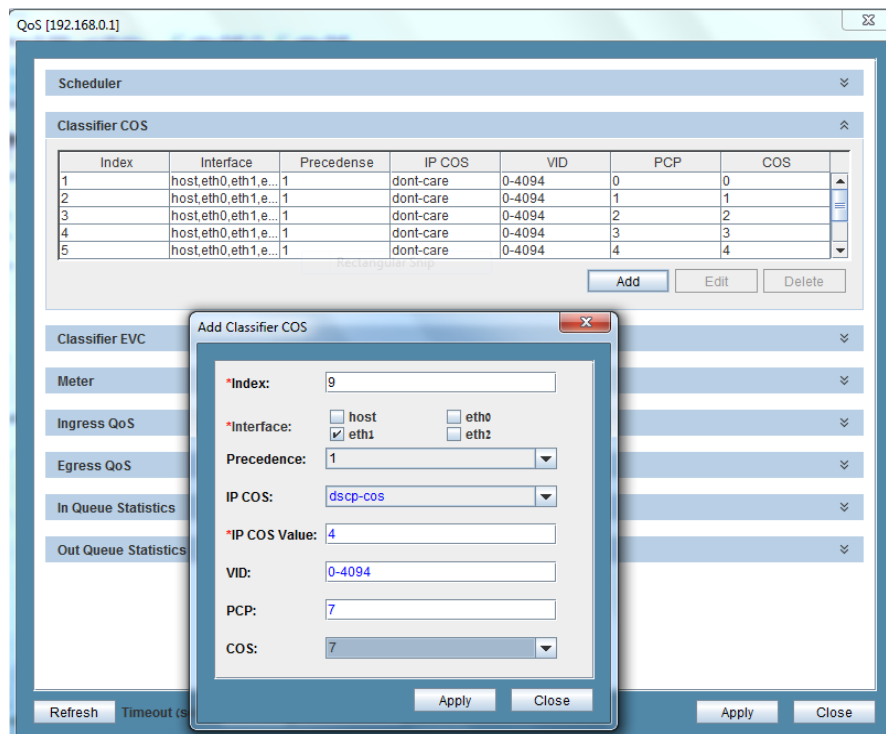


Figure 7-2: Classifier-COS Setup

Classifier-EVC Settings

Use the following command to configure classifier-etc:

```
set classifier-evc <classifier-id: 1..248> [interface <host|eth0|
eth1|eth2>] [precedence <1..8>] [vid < list 0..4094>] [pcp < list
0..7>] [ip-cos <{{dscp-cos | mpls-exp} <list of 0..7>}|dont-care>]
[evc <1..31>]
```

Classifier-EVC settings for priority based on PCP (pBits) on Eth0 and Eth1:

```
# classifier-evc configuring
set classifier-evc 1 interface eth0 precedence 1 vid 0-4094 pcp 0
ip-cos dont-care evc 1
set classifier-evc 2 interface eth0 precedence 1 vid 0-4094 pcp 1
ip-cos dont-care evc 2
set classifier-evc 3 interface eth0 precedence 1 vid 0-4094 pcp 2
ip-cos dont-care evc 3
set classifier-evc 4 interface eth0 precedence 1 vid 0-4094 pcp 3
ip-cos dont-care evc 4
set classifier-evc 5 interface eth0 precedence 1 vid 0-4094 pcp 4
ip-cos dont-care evc 5
set classifier-evc 6 interface eth0 precedence 1 vid 0-4094 pcp 5
ip-cos dont-care evc 6
set classifier-evc 7 interface eth0 precedence 1 vid 0-4094 pcp 6
ip-cos dont-care evc 7

set classifier-evc 8 interface eth0 precedence 1 vid 0-4094 pcp 7
ip-cos dont-care evc 8
```

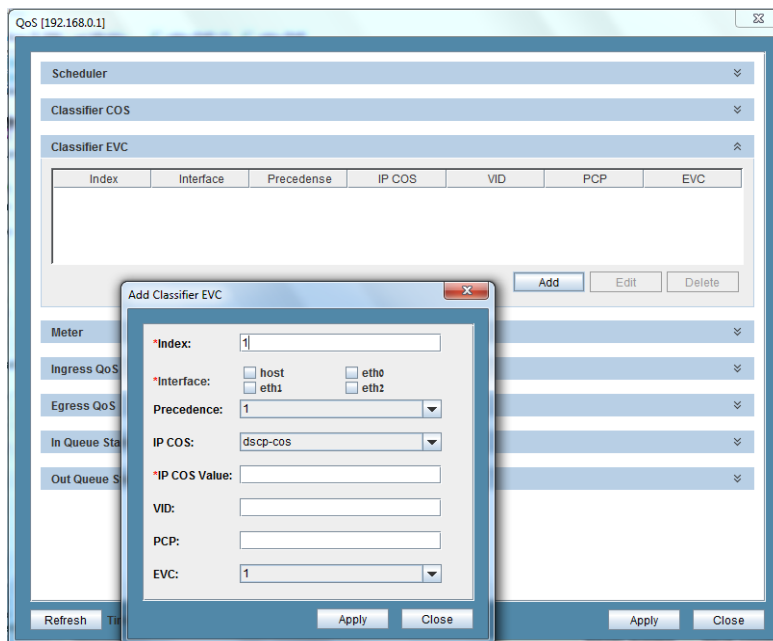


Figure 7-3: Classifier-EVC Setup

PCP Rewrite

PCP Rewriting capability allows you to set the outer PCP value of an outgoing frame as a function of COS. This feature only exists in version 5 of the NetBeam 2G.

The PC-Write-Profile table is a set of profiles where each profile is a single mapping between eight COS values to eight PCP values - so it can be represented by eight values in the range 0-7. Each profile is identified by a profile ID.

In addition, the rewrite-profile attribute is available for each eth. The attribute value can be set to NULL or a valid profile ID. A non-Null value causes a frame's PCP to be written accordingly prior to the frame being sent on an external port. When no value is set the default value is "no profiles defined". The maximum number of profiles is 128.

PCP Rewrite in the CLI:

```
// rewrite PCP on frames going to eth1 with the cos value
set pcp-write-profile 1 0 1 2 3 4 5 6 7 // profile that maps each
cos to the pcp of same numerical value
set pcp-write-profile 1 XX 1 2 3 4 5 6 7 8
set eth eth1 pcp-write-profile-id 1 // let port 1 operate
with PCP rewrite.
```

```
// do not rewrite pcp of frames on eth1
set eth eth1 pcp-write-profile-id none // disable PCP
rewrite on port
```

PCP Rewrite in the Web EMS

1. From the Main screen select **QoS**.
2. Expand the PCP Write Profile area.
3. Select a profile and click **Edit**.
4. In the PCP Mapping field, enter a number from 0–7.
5. Click **Apply**.
6. To add a profile, click **Add**.
7. To delete a profile, select the profile and click **Delete**.

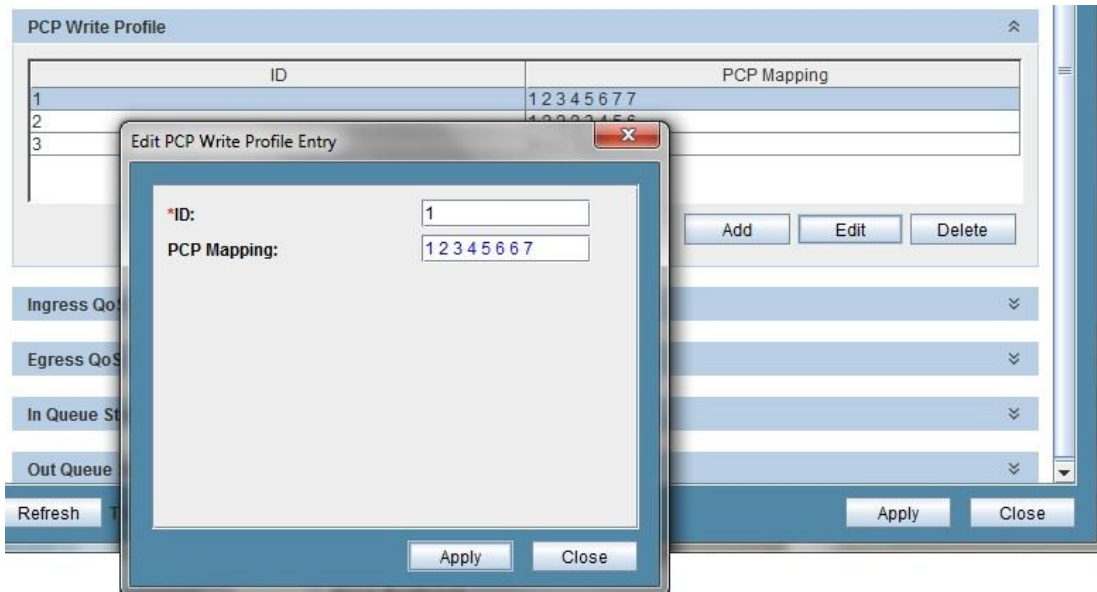


Figure 7-4: PCP Rewrite

8. On the bottom of the QoS window, click **Apply**.

Metering and Coloring

Configuring Meter

This is an optional mechanism (only for use in cases in which classifier-evc is configured) to control and limit the traffic (committed rate and peak rate).

If a meter was defined for the classifier, the packet is internally colored (Green or Yellow) or dropped (Red) based on the following:

- **CIR** – Committed Information Rate [Mbps]. Represents the amount of credit the meter should receive each time interval.
- **EIR** – Excess Information Rate [Mbps]. Exceeding limitations of credits for each time interval.
- **CBS** – Committed Burst Size [bytes].
- **EBS** – Excess Burst Size [bytes].

Color-aware mode is supported for ingress S-VLAN packets only (based on MEF definitions).

Use the following command to configure a meter:

```
set meter <meter-id: 1..248> [cir <0..1000>] [cbs <1522..50000>]
[eir <0..1000>] [ebs <1522..100000>] [color-mode < aware|blind>]
```

The following is an example of configuring a meter with 5 Mbps CIR and 15 Mbps EIR:

```
# meter configuring
set meter 1 cir 5 cbs 9600 eir 15 ebs 100000 color-mode blind
```

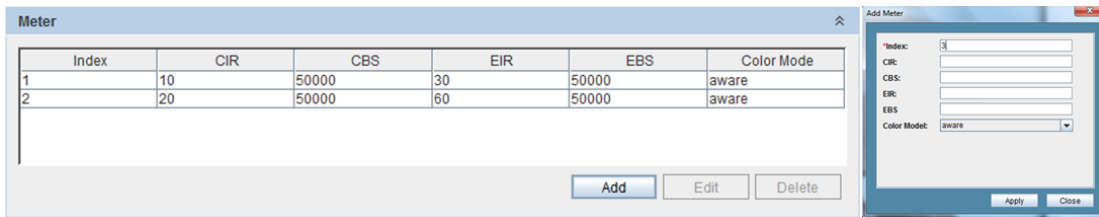


Figure 7-5: Meter Setup

Binding Classifier and Meter

Use the following command to bind specific configured classifier-vc to CoS (queue) and Meter:

```
set ingress-qos <evc-id:1..31> <cos-id:0..7> [meter <id: 0..248>]
[marking <enable|disable>]
```

The following is an example of binding the meter (configured above) to an evc and cos:

```
# ingress-qos configuring
set ingress-qos 5 5 meter 1 marking enable
```

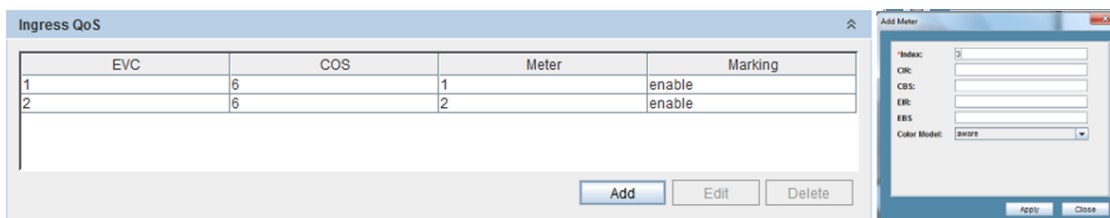


Figure 7-6: Ingress-COS Setup

QoS Scheduling

The NetBeam QoS mechanism operates according to the following scheduling mechanisms:

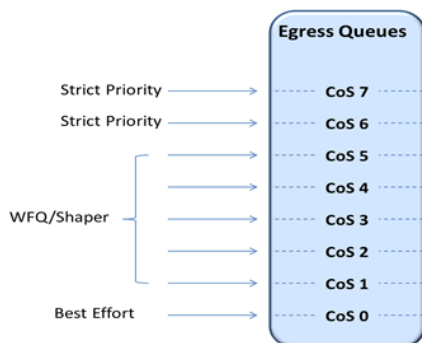


Figure 7-7: Scheduling Mechanisms

- **Strict Priority** – Lower priority packets are served only if all higher priority queues are empty.
- **Weighted Fair Queuing (WFQ)** – Weights can be assigned to the radio queues, assuring fairness between the queues.
- **Shaper** – Sets the CIR (Committed Information Rate, i.e. the maximum rate) of the queues, with Strict Priority or WFQ.

The default scheduling mode is Strict Priority.

When you configure the egress-cos, color-drop blind or aware can be configured.

Weighted Fair Queue (WFQ)

Weighted Fair Queuing (WFQ) can be used to provide different rates to different flows while maintaining fairness in order to avoid starvation. WFQ is a data packet scheduling technique that provides different scheduling priorities to statistically multiplexed data flows.

If the link data rate is R, weights of N data flows are W1,W2,...,Wn, the i'th data flow will achieve an average data rate of:

$$R * W_i / (W_1 + W_2 + \dots + W_n)$$

WFQ explicitly considers data queue, and by regulating the weights dynamically, you can utilize WFQ to control the QoS.

WFQ can only be configured for ETH0 queues 1 through 5. The highest queues, 6 and 7, are Strict Priority queues, and the lowest queue, 0, is on a best effort basis.

Table 7-1 provides an example of WFQ.

Table 7-1: Weighted Fair Queue Example with NetBeam M7

Radio Rate = 320 Mbps				
Stream #	Stream rate	# Queue	Weight	Expected Rate
1	60	SP CoS 7	NA	60
2	60	SP CoS 6	NA	60
3	60	WFQ CoS 5	8	60
4	60	WFQ CoS 4	6	57.1
5	60	WFQ CoS 3	4	38.1
6	60	WFQ CoS 2	2	19.0
7	60	WFQ CoS 1	1	9.5
8	60	BE CoS 0	0	0
Total =	480			

In this example, the introduced load exceeds the radio link rate (480>320 Mbps). The two highest queues (Strict Priority 6 and 7) take precedence over WFQ queues. The remaining bandwidth (320-60-60=200 Mbps) is split among the weighted queues (1 – 5).

The lowest queue (Best Effort 0) gets no bandwidth.

The following is an example of WFQ configuration:

```
# Scheduler mode configuration
set scheduler mode wfq
# egress-qos configuring
set egress-qos eth0 1 color-drop blind weight 1 cir 0
set egress-qos eth0 2 color-drop blind weight 2 cir 0
set egress-qos eth0 3 color-drop blind weight 4 cir 0
set egress-qos eth0 4 color-drop blind weight 6 cir 0
set egress-qos eth0 5 color-drop blind weight 8 cir 0
```

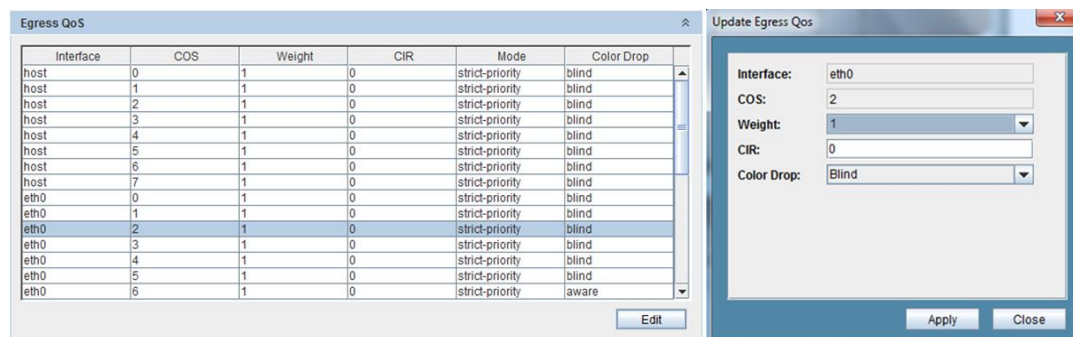


Figure 7-8: WFQ/Shaper Setup

Shaper

Shaper is used to control traffic flows in order to optimize or guarantee performance and improve latency by limiting the maximum bandwidth of certain flows to maintain fairness and to assure SLA.

You must set the Committed Information Rate to a value between 1-1000 Mbps.

Table 7-2 provides an example of Shaper.

Table 7-2: Shaper Example

Radio Rate 320 Mbps				
Stream #	Stream rate	# Queue	CIR	Expected Rate
Stream rate =	60	SP CoS 7	NA	60
Stream rate =	60	SP CoS 6	NA	60
Stream rate =	60	CIR CoS 5	50	50
Stream rate =	45	CIR CoS 4	40	40
Stream rate =	15	CIR CoS 3	30	30
Stream rate =	20	CIR CoS 2	20	20
Stream rate =	40	CIR CoS 1	10	10
Stream rate =	70	BE CoS 0	0	50
Total =	370			

The following is an example of Shaper (Strict Priority) configuration:

```
# scheduler configuring
set scheduler mode priority-shaper

# egress-qos configuring
set egress-qos eth0 1 color-drop blind weight 1 cir 10
set egress-qos eth0 2 color-drop blind weight 2 cir 20
set egress-qos eth0 3 color-drop blind weight 4 cir 30
set egress-qos eth0 4 color-drop blind weight 6 cir 40
set egress-qos eth0 5 color-drop blind weight 8 cir 50
```

Refer to Figure 7-8 WFQ/Shaper Setup for configuration using the Web EMS.

Egress Queues

There are eight egress queues, one queue per CoS. Eight queues for each of the interfaces (Eth0, Eth1, Eth2, Eth3, and Eth4) are served by four queues on the radio (RF).

WFQ and Shaper can only be configured for queues 1 through 5.

Weighted Random Early Detection (WRED)

Weighted Random Early Detection is a queue management algorithm with congestion avoidance capabilities. It is an extension of Random Early Detection (RED) in which a single queue may have several different queue thresholds. Its main purpose is to improve TCP performance. This feature is available for NetBeam 2G systems only.

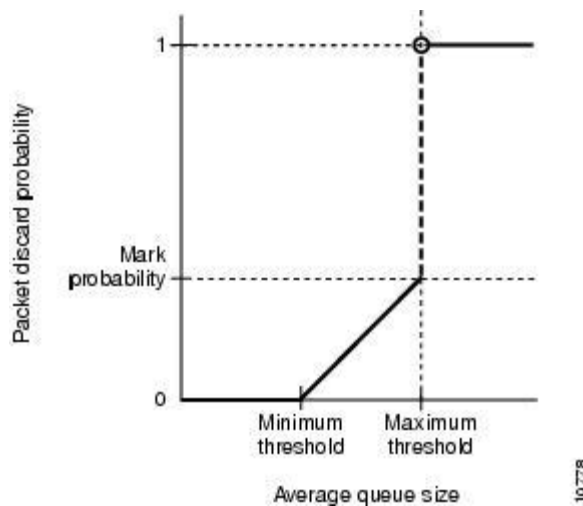


Figure 7-9: TCP Performance

WRED Functionality

When a packet arrives, WRED handles it with the following process:

1. The average queue size is calculated using the following equation:

$$\text{Average} = (\text{old_average} * (1 - 1/2^n)) + (\text{current_queue_size} * 1/2^n).$$
2. The packet is filtered according to its size.
 - If the average queue size is below the minimum queue threshold, the packet is queued normally.
 - If the average queue size is greater than the maximum threshold, the packet is automatically dropped.
 - If the average queue size is between the minimum and maximum queue threshold, the packet is either dropped or queued depending on the packet's drop probability.

WRED Parameters

- **Minimum and Maximum Thresholds** - When the system uses color aware configuration, it requires the use of thresholds per color (green and yellow). When the system does not use color aware configuration (blind mode), it uses one set (the Green set) of thresholds.

The difference between the maximum threshold and the minimum threshold should be large enough to avoid global synchronization of TCP hosts (which can occur as multiple TCP hosts reduce their transmission rates). If the difference is too small, many packets may be dropped at the same time, resulting in global synchronization.

- **“n” the average factor** - “n” is the user-configurable exponential weight factor. The previous average is more important for the higher n values. Peaks and Lows in queue length are smoothed by a high value. Lower n values allow the value of the average queue size to remain similar to the value of the close to the current queue size.

If the value of n is too high, WRED does not react to congestion. Packets are sent or dropped as if WRED is not enabled.

- **Packet Drop Probability** - The mark probability denominator is the fraction of packets dropped when the average queue size reaches the maximum threshold. For example, if the denominator is 512, one out of every 512 packets is dropped when the average queue reaches the maximum threshold.

CLI

bridge-common:

```
bridge-common egress-wred <enable/disable>
```

wred:

```
wred <0-99> min-threshold <UINT32> max-threshold <UINT32 > drop-  
probability <1-1000>
```

egress-qos:

```
egress-qos eth0 <queue> wred <wred-index> wred-green <wred-index>  
wred-yellow <wred-index> wred-n <1-16>
```

Example Measurement

The following images display how the system behaves with and without WRED:

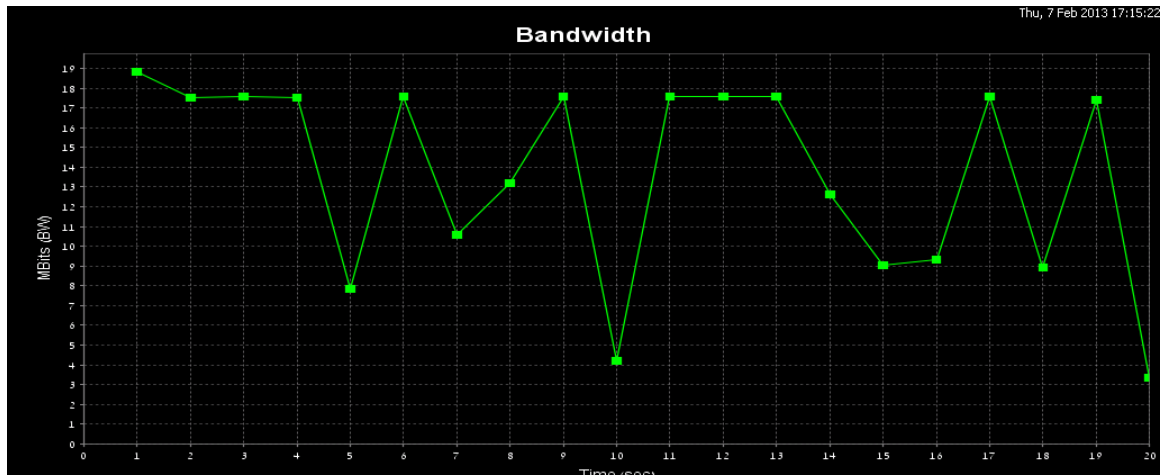


Figure 7-10: System Behavior with WRED

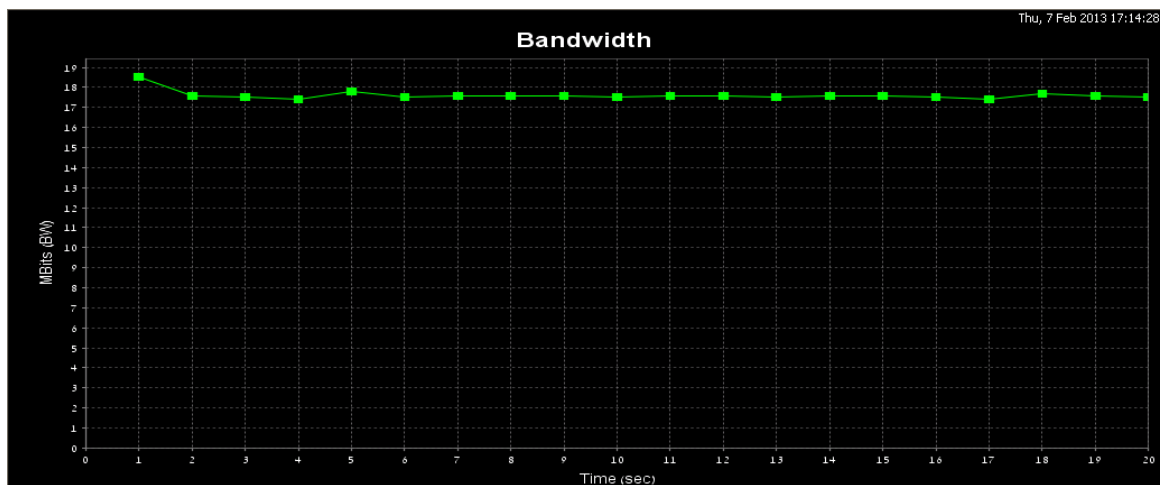


Figure 7-11: System Behavior without WRED

Configuring CFM (Connectivity Fault Management)

This section explains how to configure CFM, and includes the following topics:

- CFM Overview
- Working with Maintenance Domains
- Working with Maintenance Associations
- Working with Component Maintenance Associations
- Working with Maintenance End Points
- Working with CCM Messages

- Working with Peer MEPs
- Working with CCM Messages
- Working with Linktrace Messages
- Sample CFM Configuration

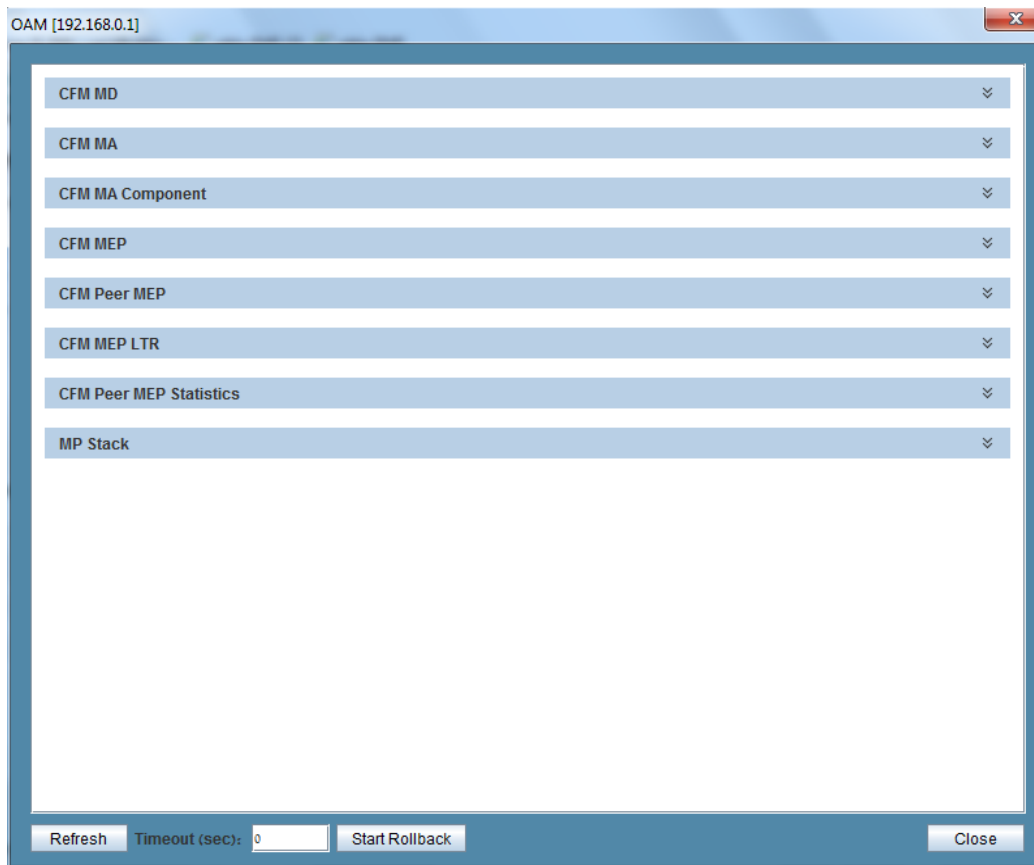


Figure 7-12: CFM (OAM) Main Screen

CFM Overview

Connectivity Fault Management (CFM) is an Ethernet layer operation, administration, and management (OAM) protocol designed to monitor and troubleshoot networks. CFM enables you to detect, verify, and isolate connectivity failures in virtual bridged local area networks.

A Maintenance Domain (MD) is a part of a network that is controlled by a single operator and used to support the connectivity between service access points. There are eight hierarchical Maintenance Domain Levels (MD Level). Each CFM layer supports OAM capabilities independently, with the customer at the highest level, the provider in the middle, and the operator at the lowest level.

CFM is designed to be transparent to the customer data transported by the network and to provide maximum fault coverage. These capabilities are used in networks operated by multiple independent organizations, each with restricted management access to each other's equipment.

CFM entities support an individual service instance as Maintenance Association End Points (MEPs) are configured to create a Maintenance Association (MA). The MA monitors connectivity provided by that instance through the Maintenance Domain. Maintenance Association Intermediate Points (MIPs) are the intermediate points in a specific MA or MD.

The major features of CFM are fault detection, path discovery, fault verification, fault isolation, and fault recovery.

Fault Detection

A Continuity Check protocol detects both connectivity failures and unintended connectivity between service instances (heartbeat). Each MEP can periodically transmit a multicast Connectivity Check Message (CCM) announcing the identity of the MEP and its MA, and tracks the CCMs received from the other MEPs.

Path Discovery

The path is determined by the linktrace (L2 Trace Route). Linktrace messages (LTM) are multicast from the originating MEP to the target MAC (MIP or MEP)/MEP ID. Linktrace Replies (LTR) are unicast from the target (or MIPs on route) to the originating MEP.

Fault Verification and Isolation

A Loopback protocol performs fault verification, typically after fault detection. An MEP can be ordered to transmit a unicast Loopback Message (LBM) to an MEP or MIP in the MA. The receiving MP responds by transforming the LBM into a unicast Loopback Reply (LBR) sent back to the originating MEP.

Fault Notification and Recovery

When an MEP detects a connectivity fault in its MA (CCM is not received or an invalid CCM is received), it sends an SNMP trap and enters a log entry. The network administrator responds to a fault notification by categorizing, isolating, and resolving the connectivity fault. For information on troubleshooting procedures, refer to *NetBeam Diagnostics* on page 201.

Working with Maintenance Domains

A Maintenance Domain (MD) is a part of a network that is controlled by a single operator and used to support the connectivity between service access points. Each of the eight

hierarchical Maintenance Domain Levels (MD Level) supports OAM capabilities independently.

Use the following command to set an MD. Note that the `name` attribute must be unique in the system.

```
set cfm-md <md-idx> [format <md-name-format>] [name <md-name>] [level <md level>] [mhf-creation <mhf creation>] [mhfid-permission <mhf permission>]
```

For example, the following command sets the customer domain at level 2.

```
set cfm-md 2 name string Customer level 2
```

Use the following command to display a particular MD or all MDs.

```
show cfm-md {<md-idx-list> | all} {format | name | level | mhf-creation | mhfid-permission | info}
```

Use the following command to clear a particular MD or all MDs:

```
clear cfm-md {<md-idx-list> | all}
```

For example, the following command clears all the MDs in the system.

```
clear cfm-md all
```

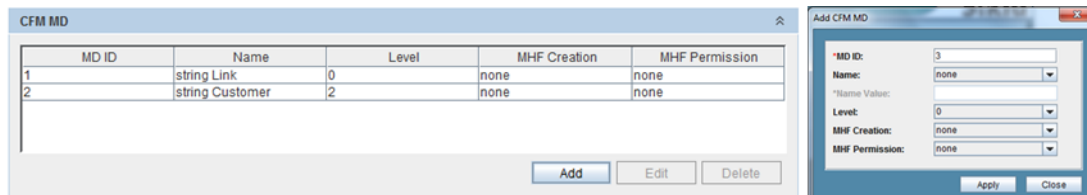


Figure 7-13: CFM MD Setup

Working with Maintenance Associations

A Maintenance Association (MA) is used to monitor connectivity in relation to a specific service instance. All CFM entities that support that service instance are configured as MEPs, with the same Maintenance Association Identifier (MAID) and MD Level.

Use the following command to set an MA. Note that the `ma-name` attribute is mandatory, and must be unique in the system.

```
set cfm-ma <md-idx> <ma-idx> [format <ma-name-format>] [name <ma-name>] [interval <ccm-interval>]
```

Use the following command to display a particular MA or all MAs:

```
show cfm-ma {<md-idx-list> | all} {<ma-idx-list> | all}
{name | component | interval | info}
```

Use the following command to clear a particular MA or all MAs:

```
clear cfm-ma {<md-idx-list> | all} {<ma-idx-list> | all}
```

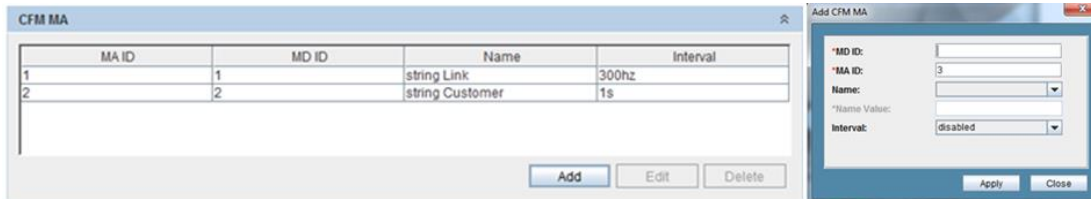


Figure 7-14: CFM MA Setup

Working with Component Maintenance Associations

Use the following command to set a Component MA:

```
set cfm-ma-comp <comp-id> <md-idx> <ma-idx> [vlan <vid>]
[mhf-creation <mhf-creation>] [mhfpermission <mhf-
permission>]
```

Use the following command to display a particular Component MA or all Component MAs:

```
show cfm-ma-comp {<comp-id-list | all> } {<md-idx-list> | all}
{<ma-idx-list> | all} {vlan | mhf-creation | mhfpermission | info}
```

Use the following command to clear a particular Component MA or all Component MAs:

```
clear cfm-ma-comp {<comp-id-list | all> } {<md-idx-list> | all} {<ma-
idx-list> | all}
```

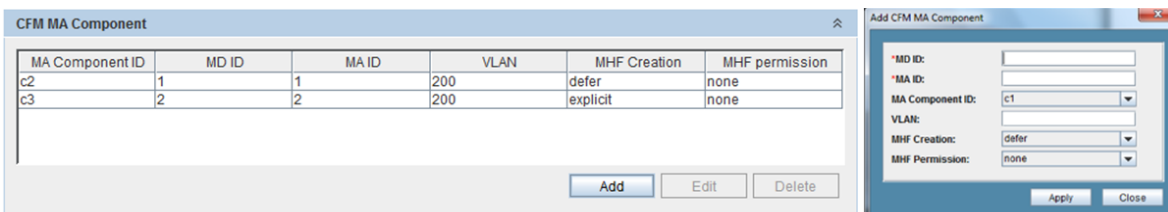


Figure 7-15: CFM MA Setup

Working with Maintenance End Points (MEPs)

A Maintenance End Point (MEP) is a point, on the perimeter of a domain, which sends and receives CFM frames through the domain.

Use the following command to set an MEP:

```
set cfm-mep <md-idx> <ma-idx> <mepid> [interface <ext-bridge-port-list>] [dir {down | up}] [vlan {1..4094}]
[admin-state {active | inactive}] [cci {enabled | disabled}]
[msg-prio {0..7}] [low-defect <low-defect>] [alarm-time {250..1000}]
[reset-time {250..1000}] [lbm-dst-type {mac | mepid}] [lbm-dst-mac <mac addr>]
[lbm-dst-mepid <mepid>] [lbm-tx-num {1..1024}] [lbm-tx-data <hex string>]
[lbm-tx-prio {0..7}] [lbm-tx-drop {enable | disable}] [ltm-dst-type {mac | mepid}]
[ltm-dst-mac <mac addr>] [ltm-dst-mepid <mepid>] [ltm-tx-ttl {0..250}]
]] [lbm-tx-status {tx-pending | tx-idle}] [ltm-tx-status {tx-pending | tx-idle}]
```

Use the following command to display a particular MEP or all MEPs:

```
show cfm-mep [{<md-idx-list> | all} [{<ma-idx-list> | all}
[{{<mepid-list> | all}}]] {interface | dir | vlan | admin-state | cci | msg-prio | low-defect | alarm-time | reset-time | lbm-dst-mac | lbm-dst-mepid | lbm-dst-type | lbm-tx-num | lbm-tx-data | lbm-tx-prio | lbm-tx-drop | ltm-dst-mac | ltm-dst-mepid | ltm-dst-type | ltm-tx-ttl | lbm-tx-status | ltm-tx-status | fng-state | mac | high-defect | defects | ccm-seq-errors | ccm-tx | lbm-tx-result | lbm-tx-sn | lbm-next-sn | lbr-in-order | lbr-out-of-order | lbr-tx | ltm-next-sn | ltr-unexpected | ltm-tx-result | ltm-tx-sn | last-error-ccm | last-xcon-ccm | info}
```

Use the following command to clear a particular MEP or all MEPs:

```
clear cfm-mep {<md-idx-list> | all} {<ma-idx-list> | all}
{<mepid-list> | all}
```

MEP commands include both configurable and read-only attributes.

MEP ID	MD ID	MA ID	Interface	Dir	VLAN	Admin State	CCI	Message P...	Low
1	1	1	eth0	down	200	active	enabled	0	mac
1	2	2	eth1	up	200	active	enabled	0	mac

Add CFM MEP

*MD ID:	<input type="text"/>	Admin State:	<input type="text" value="active"/>
*MA ID:	<input type="text"/>	CCI:	<input type="text" value="enabled"/>
*MEP ID:	<input type="text" value="2"/>	MSG Priority:	<input type="text" value="0"/>
Interface:	<input type="text" value="host"/>	Low Defect:	<input type="text" value="all-def"/>
Direction:	<input type="text" value="down"/>	Alarm Time	<input type="text"/>
VLAN:	<input type="text"/>	Reset Time	<input type="text"/>

LBM Dst. Type:	<input type="text" value="mepid"/>	LBM Tx Num.:	<input type="text"/>
LBM Dst. MAC	<input type="text"/>	LBM Tx Data Len.:	<input type="text"/>
LBM Dst. MEP ID	<input type="text"/>	LBM Tx Priority:	<input type="text" value="0"/>
LBM Tx Status:	<input type="text" value="tx-idle"/>	LBM Tx Drop	<input type="text" value="enable"/>

LTM Dst. Type:	<input type="text" value="mepid"/>	LTM Tx TTL:	<input type="text"/>
LTM Dst. MAC	<input type="text"/>	LTM Tx Status:	<input type="text" value="tx-idle"/>
LTM Dst. MEP ID	<input type="text"/>		

LM:	<input type="text" value="enabled"/>	LM Interval:	<input type="text" value="1s"/>
-----	--------------------------------------	--------------	---------------------------------

DM:	<input type="text" value="enabled"/>	DM Interval:	<input type="text" value="1s"/>
-----	--------------------------------------	--------------	---------------------------------

AIS Generate:	<input type="text" value="enabled"/>	AIS Period:	<input type="text" value="1s"/>
AIS Level:	<input type="text" value="0"/>	AIS Suppress	<input type="text" value="enabled"/>

Figure 7-16: CFM MEP Setup

Working with Peer MEPs

MEPs connected by the NetBeam Provider Bridge feature are known as Peer MEPs. Peer MEPs can be used to measure CCM delay and changes in that delay.

Use the following command to create a Peer MEP entry. This command causes automatic creation of entries in the Peer MEP DB for all MEPIDs that have entries in MEP table and this Peer MEP ID.

```
set cfm-peer-mep-create <md-idx-list> <ma-idx-list> <peer-mepid-list>
```

Use the following command to display Peer MEP information:

```
show cfm-peer-mep-create [{<md-idx-list> | all}] [{<ma-idx-list> | all}] [{<peer-mepid-list> | all}]
```

Use the following command to delete a Peer MEP entry. This command causes automatic deletion of entries in the Peer MEP DB for all MEPIDs that have entries in MEP table and this Peer MEP ID.

```
clear cfm-peer-mep-create {<md-idx-list> | all} {<ma-idx-list> | all} {<peer-mepid-list> | all}
```

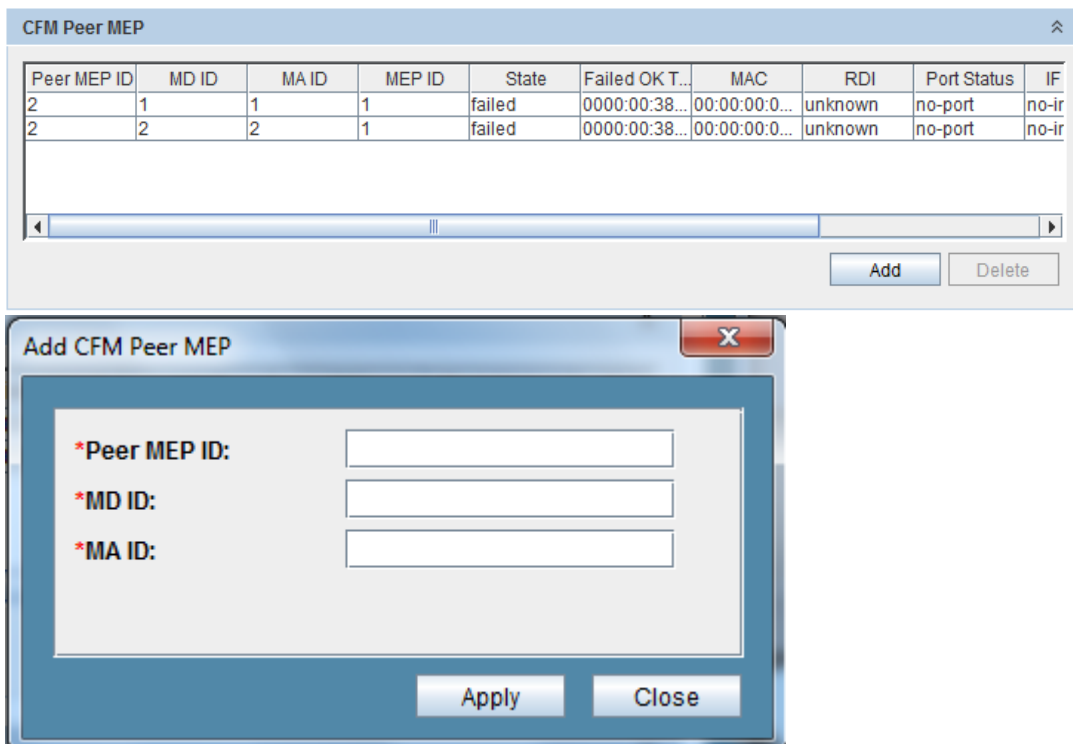


Figure 7-17: CFM Peer MEP Setup

Working with CCM Messages

An MEP can periodically transmit a multicast Connectivity Check Message (CCM) announcing the identity of the MEP and its MA. The MEP also tracks CCMs received from the other MEPs.

The following information is displayed per CCM message stored:

- Eth Source Address
- VLAN Priority (PCP)
- Drop Eligibility
- VLAN ID
- MD Level
- Version
- RDI
- CCM Interval
- Sequence Number
- Counters: TxFCf, RxFCb, TxFCb
- If present:
- Sender Chassis Subtype and ID
- Management Address Domain
- Management Address
- Port Status -- {blocked | up} (according to IEEE 802.1ag Table 21-10)
- Interface Status -- {up | down | testing | unknown | dormant | not-present | lower-layer-down} (according to IEEE 802.1ag Table 21-1)
- Other TLVs: Type, Data as hexadecimal string

To display this information, use the following commands:

```
show cfm-ccm [{{<md-idx-list> | all}} [{{<ma-idx-list> | all}}
[{{<mepid-list> | all}}]]] last-error-ccm
```

and

```
show cfm-ccm [{{<md-idx-list> | all}} [{{<ma-idx-list> | all}}
[{{<mepid-list> | all}}]]] last-xcon-ccm
```

Refer to *Figure 7-17 CFM Peer MEP Setup* for CCM status monitoring.

Working with Linktrace Messages

Linktrace messages are multicast from an originating MEP to a target MAC (MIP or MEP)/MEP ID, to verify the path between the two. Linktrace Reply messages (LTRs) are unicast from the target (or MIPs on route) to the originating MEP. Receipt of an LTR verifies the path.

Arriving LTRs are stored on a per-MEP basis in the LTR database, as shown in Figure 7.18.

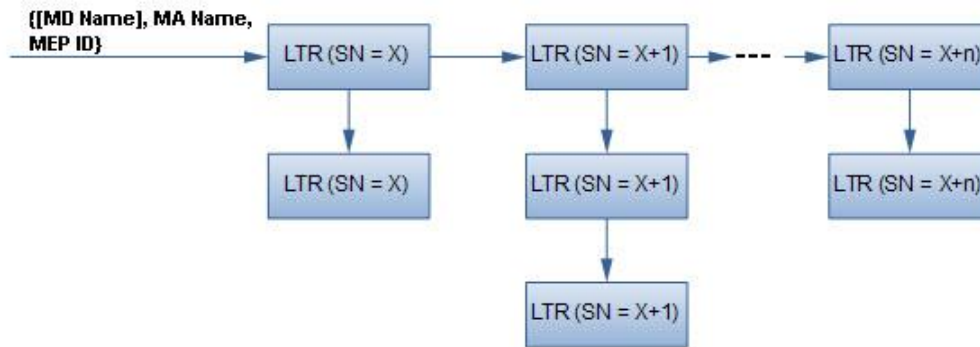


Figure 7-18: Per-MEP LTR Storage Structure

LTRs are stored in ascending sequence number order and LTRs with the same sequence number (i.e. replies to the same LTM) are grouped together.

Since storage is limited, arrival of a new message results in discarding older messages. Entire groups that use the same sequence number are discarded.

Use the following command to display LTR database information:

```
show cfm ltr-db [{"md-idx-list" | all} [{"ma-idx-list" | all} [{"mepid-list" | all} [{"SN-list" | all}]]]]
```

SN stands for the Sequence Number of the LTR message stored. This does not refer to the real sequence number stored in the LTR header, but rather, to the relative SN which is equal to Real SN modulo Maximum Allowed Number of SNs.

For example, if the maximum allowed number of stored LTRs (with different SNs) is 20, then the Real SN = 807 is translated into the Relative SN = 7.

It is possible to specify more than one SN in the command by designating indexed objects.

MD ID	MA ID	MEP ID	SN	Order	Rx TTL	Forward	Relay Action	Chassis ID...	Manag
2	2	1	0	0	63	unknown	fdb	unknown	unknow
2	2	1	0	1	62	unknown	fdb	unknown	unknow
2	2	1	0	2	61	unknown	hit	unknown	unknow

Figure 7-19: Link Trace Status

Sample CFM Configuration

This section provides a sample CFM configuration script.

Configuring the Local ODU

The first step in configuring CFM parameters is to enable the OAM license, which is part of the L2 Networking license. Without an enabled OAM license, the necessary CFM commands are not available.

```
set license oam status enable
```

The next step in this configuration is to configure an MD at level 0:

```
set cfm-md 1 name string Link level 0
```

The following command creates an MA:

```
set cfm-ma 1 1 name string Link interval 300hz
```

The following command creates a Component MA and assigns VLAN 200 as its Service Selector:

```
set cfm-ma-comp c2 1 1 vlan 200
```

The following command creates a Maintenance End Point (MEP):

```
set cfm-mep 1 1 1 interface eth0 dir down cci enabled
```

The following command creates a Peer MEP:

```
set cfm-peer-mep-create 1 1 2
```

The following command creates an MD at level 2:

```
set cfm-md 2 name string Customer level 2
```

The following command creates an MA:

```
set cfm-ma 2 2 name string Customer interval 1s
```

The following command creates a Component MA and assigns VLAN 200 as its Service Selector:

```
set cfm-ma-comp c3 2 2 vlan 200
```

The following command creates a Maintenance End Point (MEP):

```
set cfm-mep 2 2 1 interface eth1 dir up cci enabled
```

The following command creates a Peer MEP:

```
set cfm-peer-mep-create 2 2 2
```

The following command sets the MIP to the lower level:

```
set cfm-ma-comp c3 2 2 vlan 200 mhfc-creation explicit
```

To create MIPs on the radio port (lower level), you must create the Component MA on C3 (Up MEP). If the C3 Component MA is not created on C3, the CFM packets will not enter and pass through the MIP.

The MHF-Creation value, which determines whether MIPs are created, can be on one of two settings:

- **Default** – Creates MIPs on all ports.
- **Explicit** – Creates MIPS only on ports that have MEPs on their lower level.

Configuring the Remote ODU

The first step in configuring CFM parameters is to enable the OAM license. Without an enabled OAM license, the necessary CFM commands are not available.

```
set license oam status enable
```

The next step in this configuration is to configure an MD at level 0:

```
set cfm-md 1 name string Link level 0
```

The following command creates an MA:

```
set cfm-ma 1 1 name string Link interval 300hz
```

The following command creates a Component MA and assigns VLAN 200 as its Service Selector:

```
set cfm-ma-comp c2 1 1 vlan 200
```

The following command creates a Maintenance End Point (MEP):

```
set cfm-mep 1 1 2 interface eth0 dir down cci enabled
```

The following command creates a Peer MEP:

```
set cfm-peer-mep-create 1 1 1
```

The following command creates an MD at level 2:

```
set cfm-md 2 name string Customer level 2
```

The following command creates an MA:

```
set cfm-ma 2 2 name string Customer interval 1s
```

The following command creates a Component MA and assigns VLAN 200 as its Service Selector:

```
set cfm-ma-comp c3 2 2 vlan 200
```

The following command creates a Maintenance End Point (MEP):

```
set cfm-mep 2 2 2 interface eth1 dir up cci enabled
```

The following command creates a Peer MEP/;

```
set cfm-peer-mep-create 2 2 1
```

The following command sets the MIP to the lower level:

```
set cfm-ma-comp c3 2 2 vlan 200 mhf-creation explicit
```

Checking the CCM Status

```
show cfm-peer-mep
```

```

cfm-peer-mep 1 1 1 2 state           : ok
<---ok or failed
cfm-peer-mep 1 1 1 2 failed-ok-time  : 0000:02:22:05
cfm-peer-mep 1 1 1 2 mac             :
00:24:a4:00:01:e1
cfm-peer-mep 1 1 1 2 rdi             : off
cfm-peer-mep 1 1 1 2 port-status     : unknown
cfm-peer-mep 1 1 1 2 if-status       : unknown
cfm-peer-mep 1 1 1 2 chassis-id-subtype : unknown
cfm-peer-mep 1 1 1 2 mng-addr-domain : unknown

```



```

cfm-peer-mep 2 2 1 2 state           : ok
cfm-peer-mep 2 2 1 2 failed-ok-time  : 0000:02:22:05
cfm-peer-mep 2 2 1 2 mac             :
00:24:a4:00:01:e2
cfm-peer-mep 2 2 1 2 rdi             : off
cfm-peer-mep 2 2 1 2 port-status     : unknown
cfm-peer-mep 2 2 1 2 if-status       : unknown
cfm-peer-mep 2 2 1 2 chassis-id-subtype : unknown
cfm-peer-mep 2 2 1 2 mng-addr-domain : unknown

```

Configure the Loopback on the Local ODU

The following set of commands sets up the Loopback on the local ODU. You must set the destination type (mepid or mac) and the destination MEP ID, determine the number of loopback packets to transmit, and enable the Loopback for transmit.

Enter the following commands on the link level:

```

set cfm-mep 1 1 1 lbm-dst-type mepid
set cfm-mep 1 1 1 lbm-dst-mepid 2
set cfm-mep 1 1 1 lbm-tx-num 10
set cfm-mep 1 1 1 lbm-tx-status tx-pending

```

Enter the following commands on the customer level:

```

set cfm-mep 2 2 1 lbm-dst-type mepid
set cfm-mep 2 2 1 lbm-dst-mepid 2
set cfm-mep 2 2 1 lbm-tx-num 10
set cfm-mep 2 2 1 lbm-tx-status tx-pending

```

To view the loopback reply, you must first verify the number for lbr-in-order. You can then transmit the loopback packets, using the following command:

```

set cfm-mep 1 1 1 lbm-tx-status tx-pending

```

Re-check the number for lbr-in-order to verify that all packets were received.

```

show cfm-mep
cfm-mep 1 1 1 interface           : eth0
cfm-mep 1 1 1 dir                 : down
cfm-mep 1 1 1 vlan                : none
cfm-mep 1 1 1 admin-state         : active
cfm-mep 1 1 1 cci                 : enabled
cfm-mep 1 1 1 msg-prio            : 0
cfm-mep 1 1 1 low-defect          : mac-rem-err-xcon
cfm-mep 1 1 1 alarm-time          : 250

```

```

cfm-mep 1 1 1 reset-time           : 1000
cfm-mep 1 1 1 lbm-dst-mac         : 00:00:00:00:00:00
cfm-mep 1 1 1 lbm-dst-mepid      : 2
cfm-mep 1 1 1 lbm-dst-type       : mepid
cfm-mep 1 1 1 lbm-tx-num         : 10
cfm-mep 1 1 1 lbm-tx-data-len    : 0
cfm-mep 1 1 1 lbm-tx-prio       : 0
cfm-mep 1 1 1 lbm-tx-drop       : enable
cfm-mep 1 1 1 ltm-dst-mac       : 00:00:00:00:00:00
cfm-mep 1 1 1 ltm-dst-mepid     : 1
cfm-mep 1 1 1 ltm-dst-type      : mac
cfm-mep 1 1 1 ltm-tx-ttl       : 64
cfm-mep 1 1 1 lbm-tx-status     : tx-idle
cfm-mep 1 1 1 ltm-tx-status     : tx-idle
cfm-mep 1 1 1 fng-state        : fngReset
cfm-mep 1 1 1 mac              : 00:24:a4:00:07:59
cfm-mep 1 1 1 high-defect      : none
cfm-mep 1 1 1 defects          :
cfm-mep 1 1 1 ccm-seq-errors    : 0
cfm-mep 1 1 1 ccm-tx           : 656243
cfm-mep 1 1 1 lbm-tx-result     : ok
cfm-mep 1 1 1 lbm-tx-sn        : 19
cfm-mep 1 1 1 lbm-next-sn      : 20
cfm-mep 1 1 1 lbr-in-order     : 20
cfm-mep 1 1 1 lbr-out-of-order  : 0
cfm-mep 1 1 1 lbr-tx           : 0
cfm-mep 1 1 1 ltm-next-sn      : 0
cfm-mep 1 1 1 ltr-unexpected   : 0
cfm-mep 1 1 1 ltm-tx-result    : unknown
cfm-mep 1 1 1 ltm-tx-sn       : 0
cfm-mep 1 1 1 lm              : disabled
cfm-mep 1 1 1 lm-interval      : 10s
cfm-mep 1 1 1 dm              : disabled
cfm-mep 1 1 1 dm-interval     : 10s
cfm-mep 1 1 1 ais-generate     : disabled
cfm-mep 1 1 1 ais-period      : 1s
cfm-mep 1 1 1 ais-level       : 7
cfm-mep 1 1 1 ais-suppress    : enabled
cfm-mep 1 1 1 ais-defects     : none

cfm-mep 2 2 1 interface       : eth1
cfm-mep 2 2 1 dir             : up
cfm-mep 2 2 1 vlan           : none
cfm-mep 2 2 1 admin-state    : active
cfm-mep 2 2 1 cci            : enabled
cfm-mep 2 2 1 msg-prio      : 0

```

```

cfm-mep 2 2 1 low-defect           : mac-rem-err-xcon
cfm-mep 2 2 1 alarm-time          : 250
cfm-mep 2 2 1 reset-time          : 1000
cfm-mep 2 2 1 lbm-dst-mac         : 00:00:00:00:00:00
cfm-mep 2 2 1 lbm-dst-mepid       : 2
cfm-mep 2 2 1 lbm-dst-type        : mepid
cfm-mep 2 2 1 lbm-tx-num          : 10
cfm-mep 2 2 1 lbm-tx-data-len     : 0
cfm-mep 2 2 1 lbm-tx-prio         : 0
cfm-mep 2 2 1 lbm-tx-drop        : enable
cfm-mep 2 2 1 ltm-dst-mac         : 00:00:00:00:00:00
cfm-mep 2 2 1 ltm-dst-mepid       : 1
cfm-mep 2 2 1 ltm-dst-type        : mac
cfm-mep 2 2 1 ltm-tx-ttl          : 64
cfm-mep 2 2 1 lbm-tx-status       : tx-idle
cfm-mep 2 2 1 ltm-tx-status       : tx-idle
cfm-mep 2 2 1 fng-state           : fngReset
cfm-mep 2 2 1 mac                 : 00:24:a4:00:07:5a
cfm-mep 2 2 1 high-defect         : none
cfm-mep 2 2 1 defects             :
cfm-mep 2 2 1 ccm-seq-errors      : 2
cfm-mep 2 2 1 ccm-tx              : 1948
cfm-mep 2 2 1 lbm-tx-result       : ok
cfm-mep 2 2 1 lbm-tx-sn           : 9
cfm-mep 2 2 1 lbm-next-sn         : 10
cfm-mep 2 2 1 lbr-in-order        : 10
cfm-mep 2 2 1 lbr-out-of-order    : 0
cfm-mep 2 2 1 lbr-tx              : 0
cfm-mep 2 2 1 ltm-next-sn         : 0
cfm-mep 2 2 1 ltr-unexpected      : 0
cfm-mep 2 2 1 ltm-tx-result       : unknown
cfm-mep 2 2 1 ltm-tx-sn           : 0
cfm-mep 2 2 1 lm                  : disabled
cfm-mep 2 2 1 lm-interval         : 10s
cfm-mep 2 2 1 dm                  : disabled
cfm-mep 2 2 1 dm-interval         : 10s
cfm-mep 2 2 1 ais-generate        : disabled
cfm-mep 2 2 1 ais-period          : 1s
cfm-mep 2 2 1 ais-level           : 7
cfm-mep 2 2 1 ais-suppress        : enabled
cfm-mep 2 2 1 ais-defects         : none

```

Configuring the Link Trace

There are five indices. The first three are the MEP, the fourth is the index number of the LTR packet (each LTR is one packet), and the fifth is the number of replies according to their order of arrival. Where several elements answer, you must check the TTL to identify the trace.

Enter the following on the link level:

```
set cfm-mep 1 1 1 ltm-dst-type mepid
set cfm-mep 1 1 1 ltm-dst-mepid 2
set cfm-mep 1 1 1 ltm-tx-status tx-pending
```

```
show cfm-mep 1 1 1 ltr
```

```
cfm-mep 1 1 1 0 0 rx-ttl           : 63
cfm-mep 1 1 1 0 0 ltr-forward      : unknown
cfm-mep 1 1 1 0 0 relay-action     : hit
cfm-mep 1 1 1 0 0 chassis-id-subtype : unknown
cfm-mep 1 1 1 0 0 mng-addr-domain  : unknown
cfm-mep 1 1 1 0 0 ingr-action     : ok
cfm-mep 1 1 1 0 0 ingr-mac        : 00:24:a4:00:07:a9
cfm-mep 1 1 1 0 0 ingr-port-id-subtype : unknown
cfm-mep 1 1 1 0 0 egr-action      : none
cfm-mep 1 1 1 0 0 egr-mac        : 00:00:00:00:00:00
cfm-mep 1 1 1 0 0 egr-port-id-subtype : unknown
cfm-mep 1 1 1 0 0 trm-mep        : unknown
cfm-mep 1 1 1 0 0 last-egr-id     : 00-00-00-24-a4-00-07-59
cfm-mep 1 1 1 0 0 next-egr-id    : 00-00-00-00-00-00-00-00
```

Enter the following on the customer level:

```
set cfm-mep 2 2 1 ltm-dst-type mepid
set cfm-mep 2 2 1 ltm-dst-mepid 2
set cfm-mep 2 2 1 ltm-tx-status tx-pending
```

```
show cfm-mep 2 2 1 ltr
```

```
cfm-mep 2 2 1 0 0 rx-ttl           : 63
cfm-mep 2 2 1 0 0 ltr-forward      : unknown
cfm-mep 2 2 1 0 0 relay-action     : fdb
cfm-mep 2 2 1 0 0 chassis-id-subtype : unknown
cfm-mep 2 2 1 0 0 mng-addr-domain  : unknown
cfm-mep 2 2 1 0 0 ingr-action     : ok
cfm-mep 2 2 1 0 0 ingr-mac        : 00:24:a4:00:07:59
cfm-mep 2 2 1 0 0 ingr-port-id-subtype : unknown
```

```

cfm-mep 2 2 1 0 0 egr-action           : none
cfm-mep 2 2 1 0 0 egr-mac             : 00:00:00:00:00:00
cfm-mep 2 2 1 0 0 egr-port-id-subtype : unknown
cfm-mep 2 2 1 0 0 trm-mep             : unknown
cfm-mep 2 2 1 0 0 last-egr-id         : 00-00-00-24-a4-00-07-5a
cfm-mep 2 2 1 0 0 next-egr-id        : 00-00-00-24-a4-00-07-59

cfm-mep 2 2 1 0 1 rx-ttl              : 62
cfm-mep 2 2 1 0 1 ltr-forward          : unknown
cfm-mep 2 2 1 0 1 relay-action         : fdb
cfm-mep 2 2 1 0 1 chassis-id-subtype  : unknown
cfm-mep 2 2 1 0 1 mng-addr-domain     : unknown
cfm-mep 2 2 1 0 1 ingr-action         : ok
cfm-mep 2 2 1 0 1 ingr-mac           : 00:24:a4:00:07:a9
cfm-mep 2 2 1 0 1 ingr-port-id-subtype : unknown
cfm-mep 2 2 1 0 1 egr-action          : none
cfm-mep 2 2 1 0 1 egr-mac            : 00:00:00:00:00:00
cfm-mep 2 2 1 0 1 egr-port-id-subtype : unknown
cfm-mep 2 2 1 0 1 trm-mep            : unknown
cfm-mep 2 2 1 0 1 last-egr-id         : 00-00-00-24-a4-00-07-59
cfm-mep 2 2 1 0 1 next-egr-id        : 00-00-00-24-a4-00-07-aa

cfm-mep 2 2 1 0 2 rx-ttl              : 61
cfm-mep 2 2 1 0 2 ltr-forward          : unknown
cfm-mep 2 2 1 0 2 relay-action         : hit
cfm-mep 2 2 1 0 2 chassis-id-subtype  : unknown
cfm-mep 2 2 1 0 2 mng-addr-domain     : unknown
cfm-mep 2 2 1 0 2 ingr-action         : ok
cfm-mep 2 2 1 0 2 ingr-mac           : 00:24:a4:00:07:aa
cfm-mep 2 2 1 0 2 ingr-port-id-subtype : unknown
cfm-mep 2 2 1 0 2 egr-action          : none
cfm-mep 2 2 1 0 2 egr-mac            : 00:00:00:00:00:00
cfm-mep 2 2 1 0 2 egr-port-id-subtype : unknown
cfm-mep 2 2 1 0 2 trm-mep            : unknown
cfm-mep 2 2 1 0 2 last-egr-id         : 00-00-00-24-a4-00-07-aa
cfm-mep 2 2 1 0 2 next-egr-id        : 00-00-00-00-00-00-00-00

```

Configuring Link OAM

This section describes how to configure Link OAM.

Link OAM, as defined in IEEE802.3ah, is an Ethernet layer operation, administration, and management (OAM) protocol designed to monitor and troubleshoot networks. Link OAM enables you to detect, verify, and isolate connectivity failures in point-to-point connections.

Enabling Link OAM

Link OAM can be enabled on one of the link interfaces (Eth1, Eth2, Eth3, and Eth4) or the radio interface (Eth0).

To enable Link OAM:

```
set link-oam <eth-list> [admin <value>]
    <eth-list>           : eth0 | eth1 | eth2 | eth3 | eth4
[admin <value: Enabled | disabled >]
default>set link-oam eth0 admin enabled
```

To view Link OAM configuration and status:

```
default>show link-oam

link-oam eth0 admin           : enabled
link-oam eth0 status         : operational
link-oam eth0 mode           : active
link-oam eth0 pdu-size       : 1518
link-oam eth0 revision       : 0
link-oam eth0 functions      : loopback

link-oam eth1 admin           : disabled
link-oam eth1 status         : disabled
link-oam eth1 mode           : active
link-oam eth1 pdu-size       : 1518
link-oam eth1 revision       : 0
link-oam eth1 functions      : loopback

link-oam eth2 admin           : disabled
link-oam eth2 status         : disabled
link-oam eth2 mode           : active
link-oam eth2 pdu-size       : 1518
link-oam eth2 revision       : 0
link-oam eth2 functions      : loopback
```

Link OAM Discovery

Once enabled, the Link OAM will perform discovery of the peer Ethernet port.

To view the discovered peer port (MAC address and other settings):

```
default>show link-oam-peer eth0

link-oam-peer eth0 mac-addr           : 00:24:a4:00:1f:b8
link-oam-peer eth0 vendor-oui         : 00-24-a4
link-oam-peer eth0 vendor-info        : 0
link-oam-peer eth0 mode                : active
link-oam-peer eth0 pdu-size           : 1518
link-oam-peer eth0 revision           : 2
link-oam-peer eth0 functions          : loopback
```

Link OAM Loopback

Link OAM loopback is supported and can be enabled on the Ethernet port. Once enabled, traffic received on the port is looped back to the port that initiated the remote loopback.

To set Link OAM loopback:

```
set link-oam-loopback <eth-list: eth0|eth1|eth2> [status
<value: init|terminate>] [peer-request <value:
ignore|process>]
```

To allow ports to enter loopback state (when receiving remote loopback initiation command) the peer-request status should be set to **process**:

```
default>set link-oam-loopback eth0 peer-request process
```

To initiate loopback on remote port the loopback status should be set to **init**:

```
default>set link-oam-loopback eth0 status init
```

To view loopback settings:

```
default >show link-oam-loopback eth0

link-oam-loopback eth0 status           : remote
link-oam-loopback eth0 peer-request     : process
```

The **status** will change to **remote** on the port that initiated the loopback (i.e. sent the request for loopback) and **local** on the port performing the loopback.

Use reset loopback command to stop the loopback and return to **status: none**;

```
default >reset link-oam-loopback eth0
```

```

default >show link-oam-loopback eth0
link-oam-loopback eth0 status           : none
link-oam-loopback eth0 peer-request    : process
    
```

Configuring Synchronous Ethernet (SyncE)

SyncE Overview

The NetBeam provides Synchronous Ethernet (SyncE) capabilities, receiving a synchronized Ethernet link and providing a synchronized Ethernet link on the other end of the wireless link within the required masks.

SyncE is a link-by-link distribution scheme that uses the Ethernet physical layer to accurately distribute clock frequency. ITU-T standard G.8261 defines various aspects of SyncE, such as the acceptable limits of jitter and wander as well as the minimum requirements for synchronization of network elements.

With SyncE, the receive clock is extracted from the Ethernet Rx by the clock unit and used for transmission on all interfaces, propagating the clock in the path. Every SyncE Network Element contains an internal clock called the Ethernet Equipment Clock (EEC). The EEC locks on the Rx clock and distributes it for transmission on all interfaces, attenuating jitter and wander, and maintaining clock-in holdover. If the Rx clock fails, the local unit switches to holdover and regenerates the clock accurately until the failure is corrected.

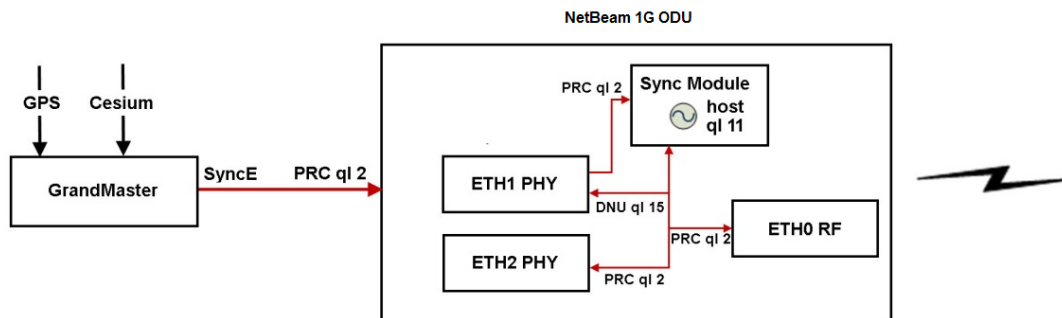


Figure 7-20: SyncE Functional Diagram

Synchronization messages are transported between the SyncE elements using Ethernet Synchronization Message Channel (ESMC). ESMC is similar to SSM (Synchronization Status Message), used in Sonnet/SDH systems. ESMC carries information about the Quality Level (ql) and sync status of the source clock, enabling the NetBeam to determine which clock source of use-based on performance and the need to avoid loops. Quality Level is based on the clock’s holdover performance.

Quality Levels (ql) names:

Quality Level (ql) Names

No.	Name	No.	Name
0	ql-stu	8	ql-ssu-b
1	ql-prs	9	ql-inv9
2	ql-prc	10	ql-eec2
3	ql-inv3	11	ql-eec1
4	ql-ssu-a	12	ql-smc
5	ql-inv5	13	ql-st3e
6	ql-inv6	14	ql-prov
7	ql-st2	15	ql-dnu

SyncE Configuration

SyncE is a licensed feature that requires a license for operation. Before configuring SyncE, verify that the SyncE license key is available and enable the license. Refer to *Upgrading the License Key* on page 160.

You can set the reference clock (ref-clock) per interface (host|eth0|eth1|eth2|eth3| eth4) using the following command:

```
set ref-clock <clk-if> [prio 1..255]
```

The **prio** attribute determines the priority of the reference clock source in the event that there is an equal ql among the interfaces. The priority can be any value from 1 to 255, where 1 is the highest priority. One entry, for host, is always present and cannot be deleted. This entry has the fixed priority 255 (the lowest priority). You cannot configure more than one interface with the same priority. If you configure Eth0, you must give it the highest priority.

For example:

```
set ref-clock eth2 5
```

To clear the reference clock settings, use the following command:

```
clear ref-clock {<clk-if-list> | all}  
For example:clear ref-clock eth2
```

To display the reference clock settings, use the following command:

```
show ref-clock [{<clk-if-list> | all} [{info | prio}]]
```

For example:

```
Default>show ref-clock
ref-clock host prio           : 255
ref-clock host status         : active
ref-clock host ql-actual      : 11
ref-clock host ql-config      : 11
ref-clock host ql-mode        : disable
ref-clock host ssm-cvid       : none
```

where:

- status – active | backup 1/2/3 | down
- ql-actual – The current ql of the active interface.
- ql-config – 0 to 15. Sets the ql of the interface.
- ql mode – Can be Enabled (enable) or Disabled (disable).
- ssm-cvid – the C-VLAN ssm messages are sent over (default untagged).

When ql-mode is disabled, ESMC messages are ignored and the status is determined by the `set ql-config` attribute.

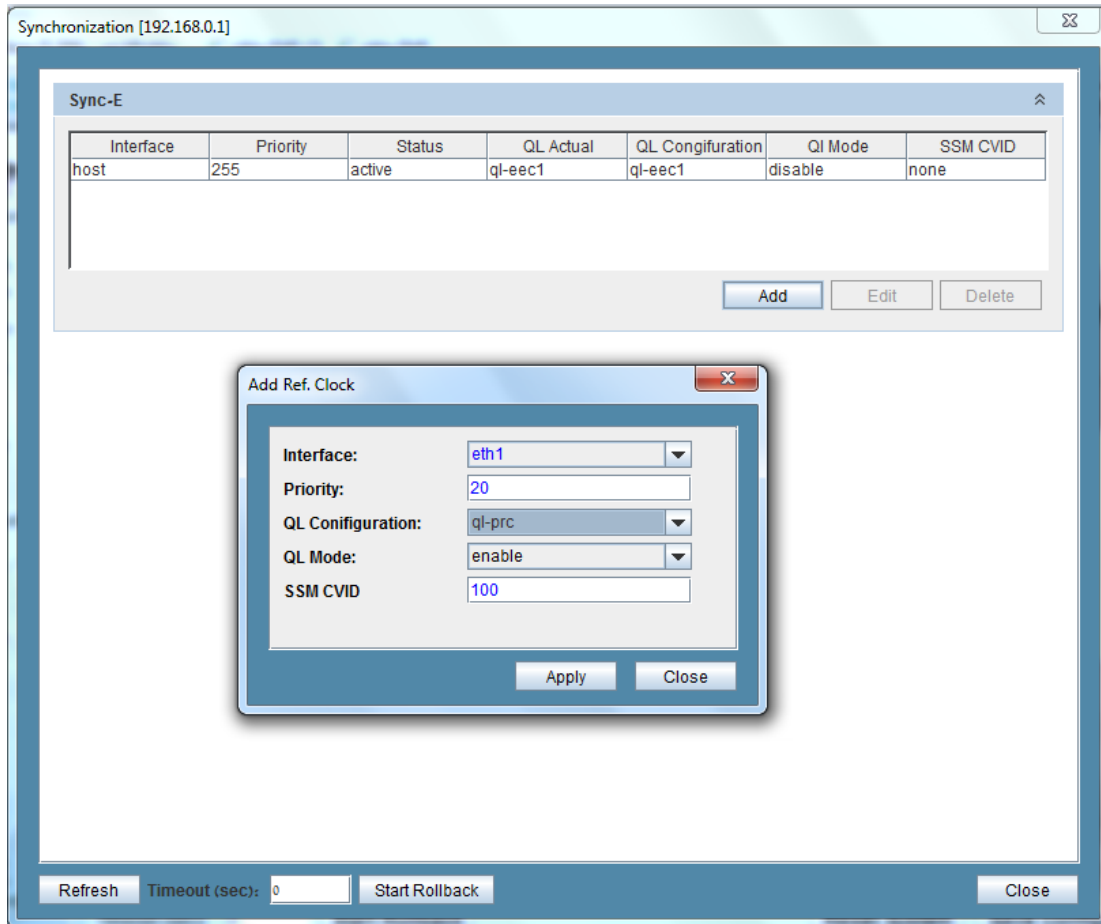


Figure 7-21: SyncE Setup Screen

Basic SyncE Scenario

Syncing both ends of the radio without SyncE on the line interfaces.

- The local NetBeam uses it internal clock (Host)
- The remote NetBeam receives timing information and is locked on Eth0 (RF)

Local NetBeam (default config)

```
Default>show ref-clock
ref-clock host prio           : 255
ref-clock host status        : active
ref-clock host ql-actual     : ql-eecl
ref-clock host ql-config     : ql-eecl
ref-clock host ql-mode       : disable
ref-clock host ssm-cvid      : none
```

Remote NetBeam

```

set ref-clock eth0 prio 100 ql-config ql-eecl ql-mode disable
Default>show ref-clock
ref-clock host prio                : 255
ref-clock host status              : backup-1
ref-clock host ql-actual           : ql-eecl
ref-clock host ql-config           : ql-eecl
ref-clock host ql-mode             : disable
ref-clock host ssm-cvid            : none

ref-clock eth0 prio                : 100
ref-clock eth0 status              : active
ref-clock eth0 ql-actual           : ql-eecl
ref-clock eth0 ql-config           : ql-eecl
ref-clock eth0 ql-mode             : disable
ref-clock eth0 ssm-cvid            : none
    
```

Typical SyncE Scenario

Figure 7-22: illustrates a typical SyncE Scenario in which:

- The local NetBeam receives timing information on Eth1 from PRC (ql 2), and distributes it to all interfaces.
- The remote NetBeam receives timing information and is locked on PRC, via Eth0 (RF).
- DNU (Do Not Use, ql 15) is returned to the source in order to prevent timing loops.

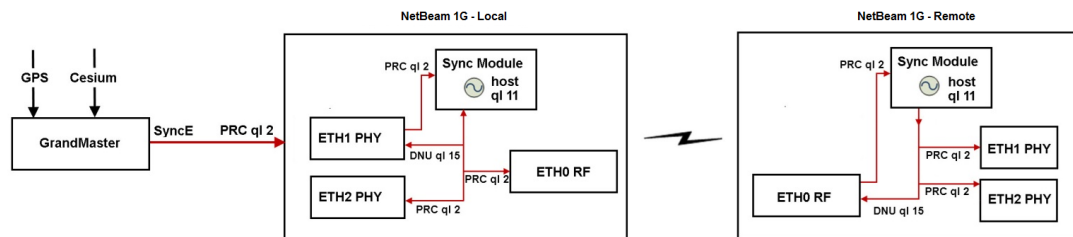


Figure 7-22: Typical SyncE Scenario

The configuration for this scenario is:

Local NetBeam

```

Default>show ref-clock
ref-clock host prio                : 255
ref-clock host status              : backup-1
ref-clock host ql-actual           : 11
ref-clock host ql-config           : 11
    
```

```

ref-clock host ql-mode           : disable
ref-clock host ssm-cvid         : none
ref-clock eth1 prio             : 200
ref-clock eth1 status           : active
ref-clock eth1 ql-actual        : 2
ref-clock eth1 ql-config        : 2
ref-clock eth1 ql-mode          : disable
ref-clock eth1 ssm-cvid         : none

```

Remote NetBeam

```

Default>show ref-clock
ref-clock host prio             : 255
ref-clock host status           : backup-1
ref-clock host ql-actual        : 11
ref-clock host ql-config        : 11
ref-clock host ql-mode          : disable
ref-clock host ssm-cvid         : none
ref-clock eth0 prio             : 100
ref-clock eth0 status           : active
ref-clock eth0 ql-actual        : 2
ref-clock eth0 ql-config        : 14
ref-clock eth0 ql-mode          : enable
ref-clock eth0 ssm-cvid         : none

```

Figure 7-23 illustrates a SyncE scenario in which there is a holdover situation due to radio failure:

- The local NetBeam receives timing information on Eth 1 from PRC (ql 2), and distributes it to all interfaces.
- There is no input on the remote NetBeam because the radio link is down.
- The remote NetBeam switches to holdover mode, maintaining the PRC it received previously and distributing it with its own ql (ql 11).

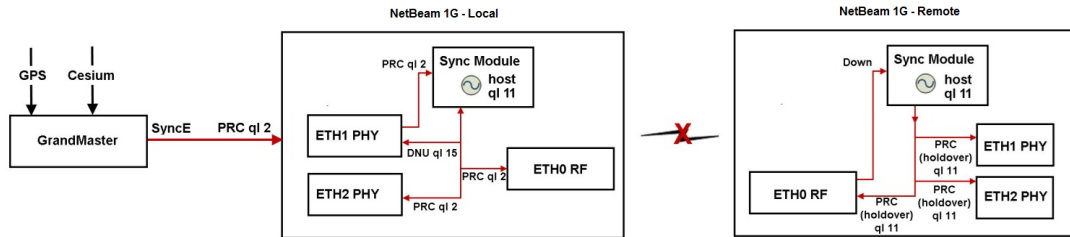


Figure 7-23: Typical SyncE Scenario – Holdover Due to Radio Failure

The configuration for this scenario is:

Local NetBeam

Default>show ref-clock

```

ref-clock host prio           : 255
ref-clock host status         : backup-1
ref-clock host ql-actual      : 11
ref-clock host ql-config      : 11
ref-clock host ql-mode        : disable
ref-clock host ssm-cvid       : none

ref-clock eth1 prio           : 200
ref-clock eth1 status         : active
ref-clock eth1 ql-actual      : 2
ref-clock eth1 ql-config      : 2
ref-clock eth1 ql-mode        : disable
ref-clock eth1 ssm-cvid       : none
    
```

Remote NetBeam

Default>show ref-clock

```

ref-clock host prio           : 255
ref-clock host status         : active
ref-clock host ql-actual      : 11
ref-clock host ql-config      : 11
ref-clock host ql-mode        : disable
ref-clock host ssm-cvid       : none

ref-clock eth0 prio           : 100
ref-clock eth0 status         : down
ref-clock eth0 ql-actual      : 15
ref-clock eth0 ql-config      : 14
ref-clock eth0 ql-mode        : enable
ref-clock eth0 ssm-cvid       : none
    
```

Figure 7-24 illustrates a SyncE scenario in which there is a holdover situation due to line failure:

- Because of the line failure, the local NetBeam does not receive timing information from PRC. The local NetBeam therefore switches to holdover mode, maintains the timing information it received previously over Eth1, and distributes this information with its own ql (ql 11).
- The remote NetBeam receives and is locked on its Eth0 source and distributes timing information from this source to its interfaces.
- DNU (Do Not use, ql 15) is returned to the source in order to prevent timing loops.

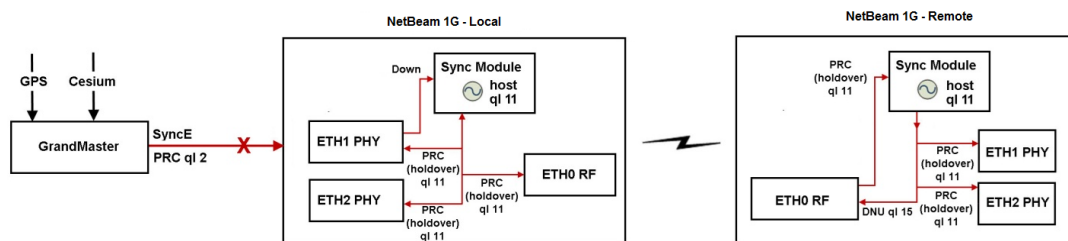


Figure 7-24: Typical SyncE Scenario – Holdover Due to Line Failure

The configuration for this scenario is:

Local NetBeam

```
Default>show ref-clock
```

```
ref-clock host prio           : 255
ref-clock host status        : active
ref-clock host ql-actual     : 11
ref-clock host ql-config    : 11
ref-clock host ql-mode       : disable
ref-clock host ssm-cvid     : none

ref-clock eth2 prio          : 200
ref-clock eth2 status       : down
ref-clock eth2 ql-actual    : 15
ref-clock eth2 ql-config    : 2
ref-clock eth2 ql-mode      : disable
ref-clock eth2 ssm-cvid     : none
```

Remote NetBeam

```
Default>show ref-clock
```

```
ref-clock host prio           : 255
```

```

ref-clock host status           : backup-1
ref-clock host ql-actual        : 11
ref-clock host ql-config        : 11
ref-clock host ql-mode          : disable
ref-clock host ssm-cvid         : none

ref-clock eth0 prio             : 100
ref-clock eth0 status           : active
ref-clock eth0 ql-actual        : 11
ref-clock eth0 ql-config        : 14
ref-clock eth0 ql-mode          : enable
ref-clock eth0 ssm-cvid         : none

```

Electrical 10/100/1000 Ports Setting for SyncE

For Electrical 10/100/1000 ports (RJ45), clock can be set.

```
set eth eth1 clock {auto | master | slave | synce}]
```

Determines the clock flow direction (relevant only when carrying Sync E over 1000BaseT).

When using fibers (SFP), SFPs clock is carried independantely and the clock configuration is not available.

The ports' default is Auto (clock direction determined by the auto-neg protocol).

The relevant Ethernet standards define that two RJ45 ports connected between them **MUST** be configured to one of the automatic modes (auto or sync) or should be configured manually one to master and second to slave.

When using SyncE over RJ45, the Ethernet port's Clock must be set manually as per one of the following options:

1. Option 1: Clock=sync. In this configuration, the clock direction is selected automatically by the SyncE SSMs.
2. Option 2: Clock=Master/Slave. Manually set Clock=Slave on the port that receives the SyncE clock and Clock=Master on the port that transmits the SyncE clock. This mode must be used when no SSMs are used on the network.

SyncE Alarms

Table 7-3: SyncE Alarms

Event	Classification	Default Severity	Destination
Reference Clock Switch	Event	N/A	Trap (ref-clock switch), Log
Reception of QL EEC1 or Worse	Alarm indicating a previous element in the chain is in holdover or failed	Medium	Trap (generic alarm), Log, Active Alarm List
Reception of QL better than EEC1	Event	N/A	Trap (generic alarm), Log, Remove Reception of QL EEC1 and Worse from Active Alarm List.

IEEE 1588v2 Transparent Clock (TC)

In wireless link the compensation of the PDV needs to be done for the entire link including the air interface and not only per node.

Netronics' 1588TC implements one step end to end HW time stamping and distributed TC algorithm to synchronize the two ends of the link. The accuracy level of the synchronization correction field between the two sides is <100ns and complies with the most stringent accuracy level required (accuracy class level 6) on all of the Ethernet ports.

The 1588TC support is part of the outdoor unit and no additional HW is needed. A software license (synchronization) is required to activate this feature.

The 1588TC is supported on NetBeam 2G systems.

CLI example:

(Activated by Sync-E license)

```
set ieee1588 admin up
```

```
default>show ieee1588
```

```
ieee1588 admin : up
```

```

ieee1588 operational          : down
ieee1588 air-delay-correction : 0
ieee1588 air-delay           : 634
ieee1588 air-distance        : 0
ieee1588 modified-packets-counter: 0

```

- `ieee1588 admin` [default down]: enables the 1588 TC stamping
- `ieee1588 operational` [Read Only]: 1588TC status. Will be Up if the 1588 is configured correctly on both sides and both sides time stamp counter are in sync.

Note that it can take up to 5 minutes till sync is achieved and operational status will be Up.

- `ieee1588 air-delay-correction`: Manual correction of air delay (in nSec). Correction may positive or negative.
- `ieee1588 air-delay` [Read Only]: Measured air delay (including modem delay) in nSec. Takes in account `air-delay-correction`.
- `ieee1588 air-distance` [Read Only]: Measured air distance in meters. Takes in account `air-delay-correction` (manually changing the `air-delay correction` affects the `air-distance`)
- `ieee1588 modified-packets-counter`: 0 - Number of 1588 packets which passed through the system and stamped. The counter is cleared upon reset (no option to clear it manually).

For 1588 phase locking, SyncE must be configured (for frequency locking) even in the absence of SyncE signal over the link. Basic SyncE configuration may be applied.

Note that 1588 must be enabled.

Local side (network side) – assuming local clock (Host) is used (no SyncE running):

```
set ieee1588 admin up
```

Remote side (BTS side):

```
set ref-clock eth0 prio 100 ql-config ql-eecl ql-mode disable
set ieee1588 admin up
```

Configuring Ethernet Ring Protection (ERP)

Ethernet Ring Protection (ERP) is a network resiliency protocol defined in ITU-T G.8032. The NetBeam supports ERP G.8032v2, with backwards compatibility to previous versions. ERP support enables protection for any point of failure in the network. This means that network connectivity is maintained in the event that the Ethernet link, the radio link, or even the entire NetBeam fails. This provides resiliency for both Ethernet-Ethernet rings that typically protect single site connectivity and Ethernet-RF rings that typically protect against RF network failure.

ERP is a relatively simple protocol that operates at the network level on the set of nodes that constitute the ring or set of rings. ERP monitors the Ethernet layer to discover and identify Signal Failure (SF) conditions, and prevents loops within the ring by blocking one of the links (either a pre-determined link or a failed link). ERP verifies at all times the ring is closed that frames will not be looped. This is accomplished by taking down a Ring protection Link (RPL) whenever there is no failure in the ring.

Using ERP, NetBeam provides protection and recovery switching within 50 ms for typical rings. The ERP mechanism uses a very small percentage of total available bandwidth.

Figure 7.25: illustrates the basic ERP protection mechanism. In normal ring operation, the RPL is blocked. In a failure condition, the failed link is blocked, R-APS messages are sent from the nodes adjacent to the failed links in order to unblock the RPL, and an FDB flush is performed on all ring nodes as necessary.

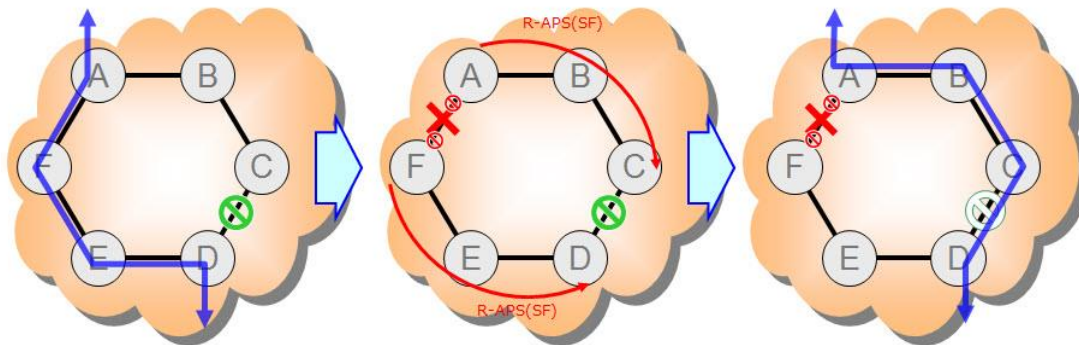


Figure 7-25: Basic ERP Protection Mechanism

Supported ERP Features

Among the ERP features supported by the NetBeam are:

- Backwards compatibility to previous versions
- Revertive and non-revertive behavior
- Flush logic with the Node-ID and BPR (Blocked Port Reference) mechanism
- Administrative commands (manual and forced switch, clear)

- Ability to block RPL at both ends of the link (RPL owner and RPL neighbor)
- Multiple logical ERP instances over a given physical ring
- Link failure detection can be based over CCM's or Physical link down.
- By default the failure detection based on link down detection.

Using CCM's for failure detection required MEP settings 300Hz (every 3.3 ms) for sub 50ms switchover.

ERP Ring Commands

To set a ring, use the following command:

```
Default>set ring
set ring <ring-index-list> [ring-id <value>] [type <value>] [fdb-id
<value>] [role <value>] [cw-port <value>] [acw-port <value>] [raps-md-
level <value>] [raps-svid <value>][raps-cvid <value>] [version <value>]
[revertive <value>] [hold-off-timer <value>] [guard-timer <value>]
[wtb-timer <value>] [wtr-timer <value>] [action <value>]
<ring-index-list>      : <list 1..16>
Default>
```

To display ring statistics, use the following command:

```
Default>show ring all statistics
ring 1 raps-tx          : 1443 <--- ACW-RPL (owner) originate RAPS
ring 1 raps-rx          : 1443 <----- Received RAPS
ring 1 local-sf-cnt     : 0 (Signal Failure)
ring 1 remote-sf-cnt   : 2 (Signal Failure)
ring 1 nr-cnt           : 1 (No request)
ring 1 nr-rb-cnt        : 2 (No request Request blocked)
ring 1 elapsed-time     : 0000:02:00:24
```

To display ring events, use the following command:

```
Default>show log

Jul 5 14:27:21 sw cad: link down eth eth0
Jul 5 14:27:21 sw cad: modulation change qpsk 1 4 0.5
Jul 5 14:27:22 sw cad: local Signal Fail at 1 CW unblocked ACW blocked
Jul 5 14:30:43 sw cad: remote Signal Fail at 1 CW unblocked ACW blocked
Jul 5 14:30:43 sw cad: link up eth eth0
Jul 5 14:30:43 sw cad: modulation change qpsk 2 2 0.5
Jul 5 14:31:43 sw cad: ERP lis ready Role none
```

CLI example for setting failure detection based on CCM's:

```
CLI>set ring 1 cw-mep ?
none | {<md-idx> <ma-idx> <mep-id> <peer-mep-id>}
```

ERP Administrative Commands

The NetBeam provides two commands for blocking a particular ring port:

- **Forced Switch (FS)** – Can be used even if there is an existing condition. Multiple FS commands are supported per ring. FS commands can be used to enable immediate maintenance operations.
- **Manual Switch (MS)** – Not effective if there is an existing FS or SF condition. Also, MS commands are overridden by new FS and SF conditions. New MS commands are ignored.

Additionally, a Clear command can be used to cancel an existing FS or MS command on the ring port. The Clear command can also be used at an RPL owner node to trigger reversion.

The following examples illustrate how to use the administrative commands to control manual switching to the backup and block a particular ring port.

```
Left_Slave> set ring 3 action
cw-ms | acw-ms | cw-fs | acw-fs | clear
Left_Slave> set ring 3 action
```

```
Right_Master>set ring 3 action acw-fs
Set done: ring 3
Right_Master>show log
Aug  4 21:09:39 sw cad: local Forced switch at 200 CW unblocked
ACW blocked
```

```
Right_Master>show ring all state
ring 3 state                : fs
Right_Master>
```

```
Right_Master>set ring 3 action clear
Set done: ring 3
Right_Master>show log
Aug  4 21:09:39 sw cad: local Forced switch at 200 CW unblocked
ACW blocked
Aug  4 21:10:46 sw cad: ERP 200is ready Role acw-rpl
```

```

Right_Master>
Right_Master>set ring 3 action acw-ms
Set done: ring 3
Right_Master>show log
Aug  4 21:43:18 sw cad: local Manual switch at 200 CW unblocked
ACW blocked
Right_Master>set ring 3 action clear
Set done: ring 3
Right_Master>show log
Aug  4 21:43:18 sw cad: local Manual switch at 200 CW unblocked
ACW blocked
Aug  4 21:44:36 sw cad: ERP 200is ready Role acw-rpl
    
```

ERP Timers

Different timers are used to determine the time of fault reports and switching in order to assure only necessary switching for permanent failures.

Table 7-4 ERP Timers

Timer	Description
Hold-off	Timer for ensuring stability of failure before triggering action to avoid reporting a fault in case of intermittent failure. 0..10000 mSec (in 100mSec steps)
Guard	Timer for protecting device against old R-APS messages. 10..2000 mSec (in 10mSec steps)
Wait-to-Block	Timer for delaying switching triggered by administrative command (FS/MS). 5000..7000 mSec (in 100mSec steps)
Wait-to-Restore	Timer for delaying revertive operation. 1..12 minutes

ERP Configuration Example

The following example illustrates an ERP configuration:

```

Left_Master>show ring
ring 1 ring-id      : 1
ring 1 type         : ring

Right_Slave_72>show ring
ring 1 ring-id      : 1
ring 1 type         : ring
    
```

```

ring 1 fdb-id          : 1                ring 1 fdb-id          : 1
ring 1 role            : none             ring 1 role            : acw-rpl
ring 1 cw-port         : eth1             ring 1 cw-port         : eth0
ring 1 acw-port        : eth0             ring 1 acw-port        : eth1
ring 1 raps-md-level   : 7                ring 1 raps-md-level   : 7
ring 1 raps-svid       : none             ring 1 raps-svid       : none
ring 1 raps-cvid       : 100              ring 1 raps-cvid       : 100
ring 1 version         : v2               ring 1 version         : v2
ring 1 revertive       : yes              ring 1 revertive       : yes
ring 1 hold-off-timer  : 0                ring 1 hold-off-time   : 0
ring 1 guard-timer     : 500              ring 1 guard-timer     : 500
ring 1 wtb-timer       : 5500             ring 1 wtb-timer       : 5500
ring 1 wtr-timer       : 1                ring 1 wtr-timer       : 1
ring 1 cw-status-data  : unblocked        ring 1 cw-status-data  : unblocked
ring 1 acw-status-data : unblocked        ring 1 acw-status-data : blocked
ring 1 cw-status-raps  : unblocked        ring 1 cw-status-raps  : unblocked
ring 1 acw-status-raps : unblocked        ring 1 acw-status-raps : blocked
ring 1 state           : idle              ring 1 state           : idle
ring 1 last-state-time : 2011.07.05      ring 1 last-state-time : 2011.06.27
ring 1 idle-percent    : 97.731606       ring 1 idle-percent    : 97.658112
ring 1 protect-percent : 1.249336        ring 1 protect-percent : 1.230652
ring 1 ms-percent      : 0.000000        ring 1 ms-percent      : 0.000000
ring 1 fs-percent      : 0.000000        ring 1 fs-percent      : 0.000000
ring 1 pending-percent : 1.019058        ring 1 pending-percent : 1.111240
ring 1 cw-node-id      : 00:00:00        ring 1 cw-node-id      : 00:00:00
ring 1 cw-bpr          : 0                ring 1 cw-bpr          : 0
ring 1 acw-node-id     : 00:24:a4        ring 1 acw-node-id     : 00:24:a4
ring 1 acw-bpr         : 0                ring 1 acw-bpr         : 0

```

The following example illustrates how to configure ERP on a ring:

```
Left_Slave>
```

```
# ring configuring
set ring 3 ring-id 200 type ring fdb-id 1 role none cw-port eth1
acw-port eth0 raps-cvid 100
set ring 3 raps-md-level 7 version v2 revertive yes hold-off-timer
0 guard-timer 500 wtb-timer 5500 wtr-timer 1
```

```
Left_Slave>
```

```
Right_Master>
```

```
# ring configuring
set ring 3 ring-id 200 type ring fdb-id 1 role acw-rpl cw-port
eth0 acw-port eth1 raps-cvid 100
```

```
set ring 3 raps-md-level 7 version v2 revertive yes hold-off-timer  
0 guard-timer 500 wtb-timer 5500 wtr-timer 1
```

```
Right_Master>
```


Chapter 8

Monitoring the System

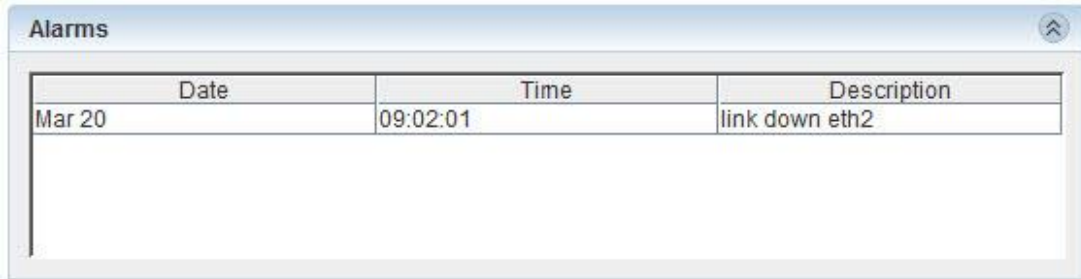
This chapter explains how to monitor system events, status, and statistics, and includes the following topics:

- Viewing Active Alarms
- Viewing Alarm History and System Events
- Events Configuration (Masking)
- Viewing Radio Statistics
- Viewing VLAN Statistics
- Viewing Queue Statistics
- Viewing Ethernet Statistics
- Viewing Bandwidth Utilization Statistics

Viewing Active Alarms

You can display active alarms using the Web EMS or the CLI. For a detailed explanation of NetBeam events and alarms, and instructions for how to use them in diagnosing NetBeam system problems, refer to *NetBeam Diagnostics* on page 201.

To display all active alarms using the Web EMS, click **Events** on the Web EMS Main screen. Active alarms appear in the Alarms section of the Events screen, including the date and time the alarm occurred.



Date	Time	Description
Mar 20	09:02:01	link down eth2

Figure 8-1: Events Screen – Alarms Section

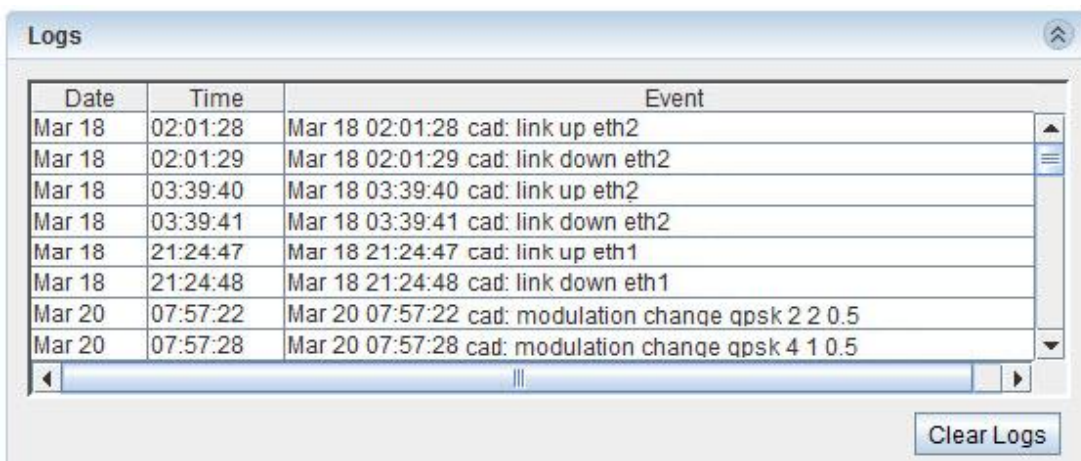
To display all active alarms using the CLI, use the `show alarms` command. All active alarms appear, including the date and time the alarm occurred.

```
2010.7.10  9:45:21    temperature high
2010.7.10  9:50:13    link down eth0
```

Viewing Alarm History and System Events

You can display a log of alarms and system events using the Web EMS or the CLI. For a detailed explanation of NetBeam events and alarms, and instructions on how to use them in diagnosing NetBeam system problems, refer to *NetBeam Diagnostics* on page 201.

To display a log of alarms and system events using the Web EMS, click Events on the Web EMS Main screen. A log of alarms and system events appears in the Logs section of the Events screen, including the date and time the alarm or event occurred.



Date	Time	Event
Mar 18	02:01:28	Mar 18 02:01:28 cad: link up eth2
Mar 18	02:01:29	Mar 18 02:01:29 cad: link down eth2
Mar 18	03:39:40	Mar 18 03:39:40 cad: link up eth2
Mar 18	03:39:41	Mar 18 03:39:41 cad: link down eth2
Mar 18	21:24:47	Mar 18 21:24:47 cad: link up eth1
Mar 18	21:24:48	Mar 18 21:24:48 cad: link down eth1
Mar 20	07:57:22	Mar 20 07:57:22 cad: modulation change qpsk 2 2 0.5
Mar 20	07:57:28	Mar 20 07:57:28 cad: modulation change qpsk 4 1 0.5

Clear Logs

Figure 8-2: Events Screen – Logs Section

To display a log of alarms and system events using the CLI, use the `show log` command. A log of alarms and system events appears, including the date and time the alarm or event occurred.

```
2010.7.10  9:35:11      temperature high
2010.7.10  9:36:13      link down eth0
2010.7.10  9:36:49      link up eth0
2010.7.10  9:40:04      temperature normal
2010.7.10  9:45:21      temperature high
2010.7.10  9:50:13      link down eth0
```

To clear all system logs, use the `clear log` command.

Events Configuration (Masking)

The NetBeam supports masking of individual/group alarms. In case alarm is masked, it is not displayed in the Active Alarms and Event Log and no trap is sent.

By default, none of the alarms are masked.

To mask an alarm, set the event-cfg mask value to yes.

```
set event-cfg <event-cfg-id-list> [mask <value>]
```

Use the following command to view the events configuration:

```
CLI>show event-cfg
event-cfg link-down          mask          : no
event-cfg temperature-high   mask          : no
event-cfg cfm-fault-alarm    mask          : no
event-cfg synthesizer-unlock mask          : no
event-cfg poe-status-low     mask          : no
event-cfg loopback-enabled   mask          : no
event-cfg tx-mute-enabled    mask          : no
event-cfg ql-eecl-or-worse   mask          : no
event-cfg cold-start         mask          : no
event-cfg modulation-change  mask          : no
event-cfg sfp-in             mask          : no
event-cfg ref-clock-switch   mask          : no
event-cfg erp-ready          mask          : no
event-cfg erp-forced-switch  mask          : no
event-cfg erp-manual-switch  mask          : no
event-cfg erp-signal-fail    mask          : no
event-cfg erp-invalid-version mask          : no
```

```

event-cfg rx-ql-eec1                mask                : no
event-cfg poe-incompatible          mask                : no

```



Event	Mask
link-down	<input type="checkbox"/>
temperature-high	<input type="checkbox"/>
cfm-fault-alarm	<input type="checkbox"/>
synthesizer-unlock	<input type="checkbox"/>
poe-status-low	<input type="checkbox"/>
loopback-enabled	<input type="checkbox"/>
tx-mute-enabled	<input type="checkbox"/>
ql-eec1-or-worse	<input type="checkbox"/>
cold-start	<input type="checkbox"/>
modulation-change	<input type="checkbox"/>
sfp-in	<input type="checkbox"/>
ref-clock-switch	<input type="checkbox"/>
erp-ready	<input type="checkbox"/>
erp-forced-switch	<input type="checkbox"/>
erp-manual-switch	<input type="checkbox"/>
erp-signal-fail	<input type="checkbox"/>
erp-invalid-version	<input type="checkbox"/>
rx-ql-eec1	<input type="checkbox"/>
poe-incompatible	<input type="checkbox"/>

Figure 8-3: Events Configuration Screen

Viewing Radio Statistics

You can display radio statistics using the Web EMS or the CLI. Radio statistic counters can be used to identify radio errors. When there are no errors on **In Errored Octets**, **In Errored Packets**, and **In Lost Packets** in the current radio statistics, this indicates that the radio link is operating without errors.

Viewing Radio Statistics Using the Web EMS

To display radio statistics using the Web EMS, click **Radio** on the Web EMS Main screen and click the RF Statistics section.

The RF Statistics section of the Radio screen includes the following two tabs:

- **Current** – Real time statistics counters since the last time the RF statistic counters were cleared.

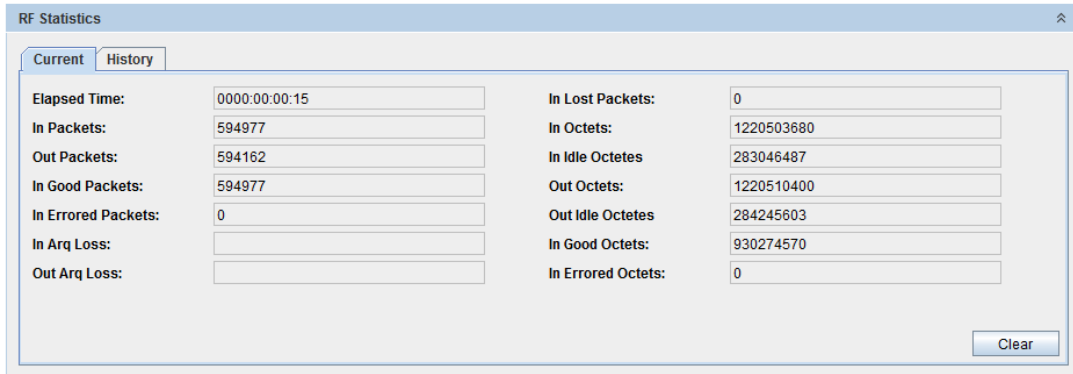


Figure 8-4: RF Statistics Screen – Current Tab

- **History** – Displays 96 intervals of 15 minutes (total 24 hours) of the statistics counters.

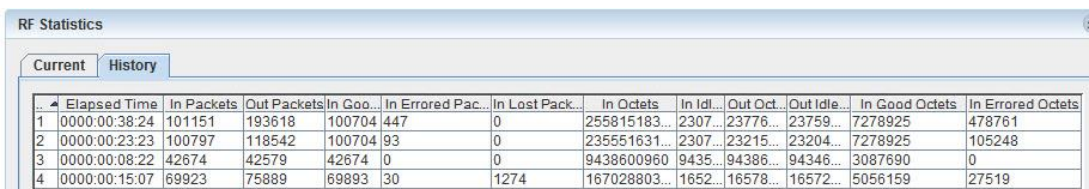


Figure 8-5: RF Statistics–History Screen Tab

For a description of the radio statistics, refer to Table 12-22.

To clear the statistic counters, click **Clear** on the Current tab.

Viewing a Statistics Summary Using the Web EMS

You can display a summary of the ODU’s radio statistics in graph or table format using the Web EMS. To display a summary of the ODU’s radio statistics, click Radio on the Web EMS Main screen and click the Statistics Summary section.

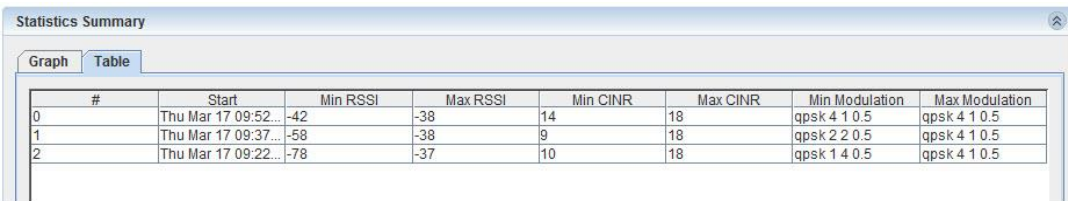


Figure 8-6: Web EMS – Statistics Summary Table

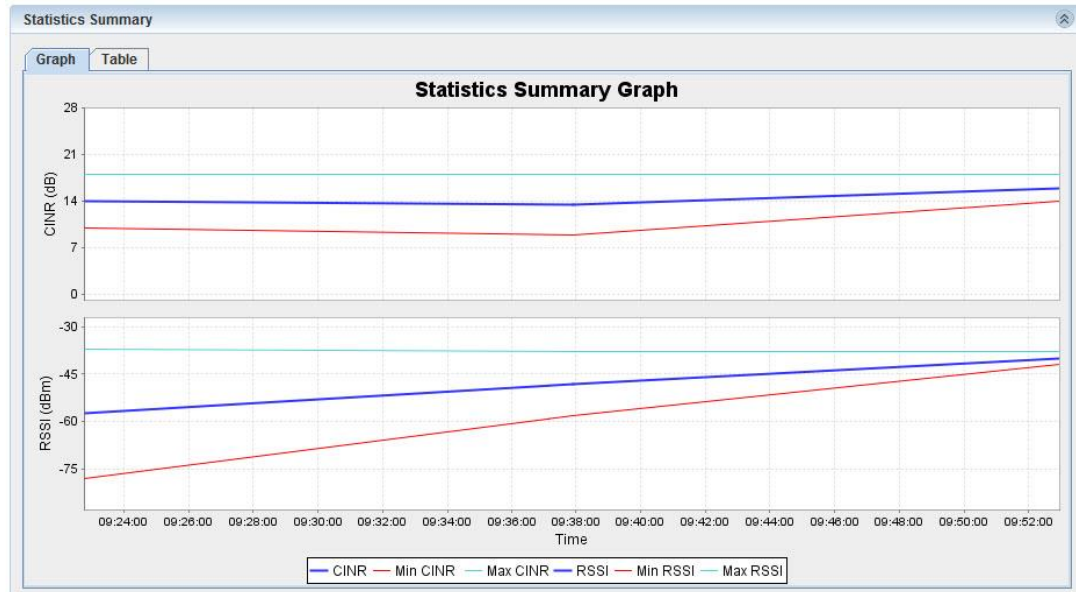


Figure 8-7: Web EMS – Statistics Summary Graph

Viewing Radio Statistics Using the CLI

Use the `show rf statistics` command to display radio statistics using the CLI. Statistics are gathered for 96 intervals of 15 minutes (total 24 hours), recording the minimum and maximum values per interval.

```
Local_Site>show rf statistics
```

```
rf in-octets           : 32535265564
rf in-idle-octets     : 29775780985
rf in-good-octets     : 9370230
rf in-errored-octets  : 0
rf out-octets         : 30552267600
rf out-idle-octets    : 30531707551
rf in-pkts            : 129957
rf in-good-pkts       : 129452
rf in-errored-pkts    : 0
rf in-lost-pkts       : 0
rf out-pkts           : 231519
rf min-cinr           : 13
rf max-cinr           : 18
rf min-rssi           : -56
rf max-rssi           : -33
rf min-modulation     : qpsk 2 2 0.5
rf max-modulation     : qpsk 4 1 0.5
rf elapsed-time       : 0000:00:45:51
```

To clear the statistic counters using the CLI, use the `clear rf statistics` command.

Viewing Radio Statistics Summary Using the CLI

Use the `show rf statistics-summary` command to display a summary of radio statistics using the CLI. Statistics are gathered for 96 intervals of 15 minutes (total 24 hours), recording the minimum and maximum values per interval.

```
Local_Site>show rf statistics-summary 0 95
```

#	start	min-rssi	max-rssi	min-cinr	max-cinr	min-modulation	max-modulation	valid
0	2011.03.17 10:22:58	-76	-33	15	18	qpsk 1 4 0.5	qpsk 4 1 0.5	unknown
1	2011.03.17 10:07:57	-76	-24	-128	-128	qpsk 1 4 0.5	qpsk 1 4 0.5	unknown
2	2011.03.17 09:52:56	-76	-10	-128	-128	qpsk 1 4 0.5	qpsk 1 4 0.5	unknown
3	2011.03.17 09:37:55	-76	-38	9	18	qpsk 2 2 0.5	qpsk 4 1 0.5	unknown
4	2011.03.17 09:22:48	-76	-37	10	18	qpsk 1 4 0.5	qpsk 4 1 0.5	unknown

Viewing VLAN Statistics

You can display VLAN statistics using the Web EMS or the CLI. To display VLAN statistics using the Web EMS, click **Bridge** on the WEB EMS Main screen and click the Statistics section.

VLAN	Port	In-Pkts	Out-Pkts	Drop-Pkts	Elapsed Time
13	eth0	0	0	0	0000:00:58:16
14	eth0	0	0	0	0000:00:58:16
1	eth1	0	2454	0	0000:00:58:20
11	eth1	0	0	0	0000:00:58:16
12	eth1	0	0	0	0000:00:58:16
13	eth1	0	0	0	0000:00:58:16
14	eth1	0	0	0	0000:00:58:16
1	eth2	0	471	0	0000:00:58:20

Figure 8-8: Current VLAN Statistics

Viewing Queue Statistics

You can use the Web EMS or CLI to display statistics for outgoing queues and incoming queues.

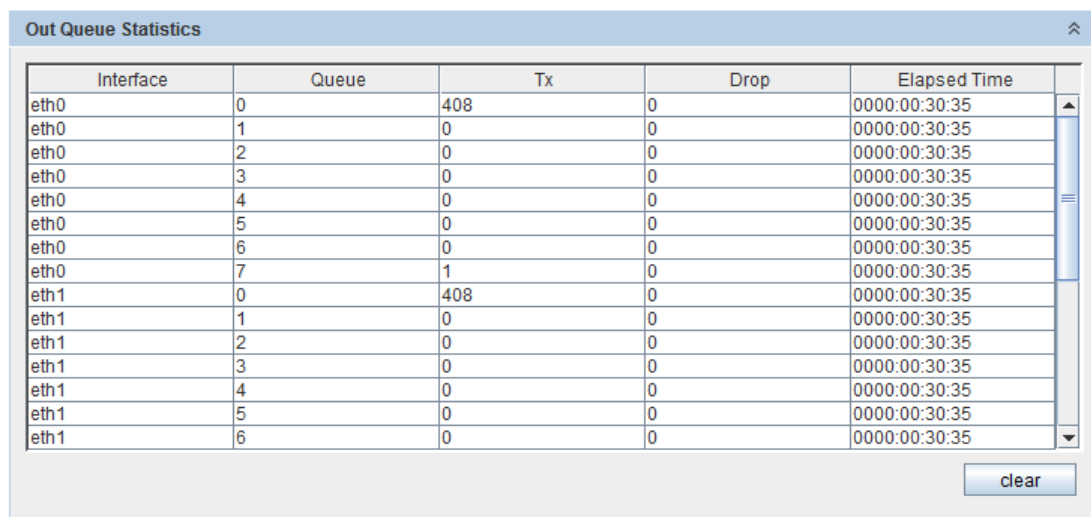
Viewing Outgoing Queue Statistics

Use the following command to display statistics for outgoing queues:

```
show out-queue {{eth0, eth1, eth2,rf} | all} {1..8 | all} statistics
```

Counters of all outgoing queues appear as follows:

```
Default>> show out-queue eth1 all statistics
interface  qid  tx          drop  elapsed-time
eth1      1    1321  3        0001:02:15:09
eth1      2    1543  1        0001:02:15:09
eth1      3    1435  0        0001:02:15:09
eth1      4    2345  0        0001:02:15:09
eth1      5    4563  0        0001:02:15:09
eth1      6    4563  0        0001:02:15:09
eth1      7    6547  9        0001:02:15:09
eth1      8    1256  0        0001:02:15:09
```



Interface	Queue	Tx	Drop	Elapsed Time
eth0	0	408	0	0000:00:30:35
eth0	1	0	0	0000:00:30:35
eth0	2	0	0	0000:00:30:35
eth0	3	0	0	0000:00:30:35
eth0	4	0	0	0000:00:30:35
eth0	5	0	0	0000:00:30:35
eth0	6	0	0	0000:00:30:35
eth0	7	1	0	0000:00:30:35
eth1	0	408	0	0000:00:30:35
eth1	1	0	0	0000:00:30:35
eth1	2	0	0	0000:00:30:35
eth1	3	0	0	0000:00:30:35
eth1	4	0	0	0000:00:30:35
eth1	5	0	0	0000:00:30:35
eth1	6	0	0	0000:00:30:35

clear

Figure 8-9: Ingress-COS Setup

Note that for **rf** there are only four queues. Therefore, only numbers from 1 to 4 (or **all**) are valid for the second ID. If **all** is specified, only four queues are displayed.

Use the following command to clear the outgoing queue statistics:


```
clear out-queue {{eth0, eth1, eth2, rf} | all} {1..8 | all}
statistics
```

Table 8-1: Outgoing Queue Statistics

Attribute	Description	Syntax
Interface Name	Interface name	{eth0 eth1 eth2 rf all}
Queue ID	Queue ID	Range from 1 to 8
Tx Frame Counter	The counter of the per-Q transmitted frames.	tx 0..264
Drop Frame Counter	The counter of the per-Q dropped frames.	drop 0..264

Incoming Queues Commands

Incoming Queues are defined only for rf (note that the rf has only four queues).

Use the following command to display statistics for incoming queues:

```
show in-queue {rf | all} {1..4 | all} statistics
```

Use the following command to clear the incoming queue statistics:

```
clear in-queue {rf | all} {1..4 | all} statistics
```

Interface	QID	Good	Error	Lost	Elapsed Time
rf	0	6183607	17	0	0119:01:34:49
rf	1	0	19	0	0119:01:34:49
rf	2	0	25	0	0119:01:34:49
rf	3	0	15	0	0119:01:34:49

Figure 8-10: Incoming Queue Statistics Screen

Table 8-2: Incoming Queues Commands

Attribute (CLI Attribute Name)	Description	Syntax	Access
Interface Name	Interface name	rf (currently only one, but may be extended in the future)	N/A

Attribute (CLI Attribute Name)	Description	Syntax	Access
Queue ID	Queue ID	Range from 1 to 4	N/A
Good Frame Counter	The counter of the per-Q received good frames.	good 0..264	RO
Erroneous Frame Counter	The counter of the per-Q received erroneous frames.	error 0..264	RO
Lost Frame Counter	The counter of the per-Q lost rx frames.	lost 0..264	RO

Viewing Ethernet Statistics

You can display statistics on NetBeam's Ethernet interfaces using the Web EMS or the CLI.

Ethernet Statistics Attributes

Table 8-3: Ethernet Statistics Attributes

Attribute (CLI Attribute Name)	Description
Incoming Octets (in-octets)	The total number of octets received on the interface, including framing characters.
Incoming Unicast Packets (in-ucast-pkts)	The number of unicast packets received on the interface.
Discarded Incoming Packets (in-discards)	The number of packets which were chosen to be discarded due to RX FIFO full.
Erroneous Incoming Packets (in-errors)	The number of received erred packets.
Outgoing Octets (out-octets)	The total number of octets transmitted out of the interface, including framing characters.
Outgoing Unicast Packets (out-ucast-pkts)	The number of unicast packets transmitted out of the interface.
Discarded Outgoing Packets (out-discards)	The number of outbound packets which were chosen to be discarded due to excessive collision or excessive deferral.

Attribute (CLI Attribute Name)	Description
Erroneous Outgoing Packets (out-errors)	The number of outbound packets that could not be transmitted because of errors.
Incoming Multicast Packets (in-mcast-pkts)	The number of multicast packets received on the interface.
Incoming Broadcast Packets (in-bcast-pkts)	The number of broadcast packets received on the interface.
Outgoing Multicast Packets (out-mcast-pkts)	The number of multicast packets transmitted out of the interface.
Outgoing Broadcast Packets (out-bcast-pkts)	The number of broadcast packets transmitted out of the interface.

Viewing Ethernet Statistics Using the Web EMS

To display Ethernet statistics using the Web EMS, click the icon of the interface for which you want to view statistics on the EMS Web Main screen (Figure 3-12), then click the Statistics section of the Interfaces screen.

The Statistics section includes the following tabs:

- **Current** – Real time statistics counters since the last time the Ethernet statistic counters were cleared.

The screenshot shows a window titled "Statistics" with two tabs: "Current" and "History". The "Current" tab is active and displays a grid of statistics with their corresponding values:

Elapsed Time:	0000:00:31:19	In Broadcast Packets:	196
In Octets:	96310	Out Bcast Packets:	0
Out Octets:	257286	In Discards:	0
In Ucast Packets:	641	Out Discards:	0
Out UCast Packets:	634	In Errors:	0
In Mcast Packets:	52	Out Errors:	0
Out MCast Packets:	0	In No Rule Discards:	0

A "Clear" button is located at the bottom right of the statistics grid.

Figure 8.11: Statistics Screen – Current Tab

- **History** – Displays 96 intervals of 15 minutes (total 24 hours) of the statistics counters.

To clear the statistic counters, click **Clear** on the Current tab.

Viewing Ethernet Statistics Using the CLI

To display Ethernet statistics using the CLI, use the following command:

```
show eth <eth-list> statistics
```

Viewing Bandwidth Utilization Statistics

You can display statistics on radios and Ethernet interfaces bandwidth utilization in 15 minutes intervals using the Web EMS or the CLI.

The total in rate, out rate, and bandwidth utilization (aggregated, meaning Tx and Rx) are displayed.

Bandwidth utilization is displayed as percentage of the aggregated (total Tx and Rx) from the max radio rate per the current modulation.

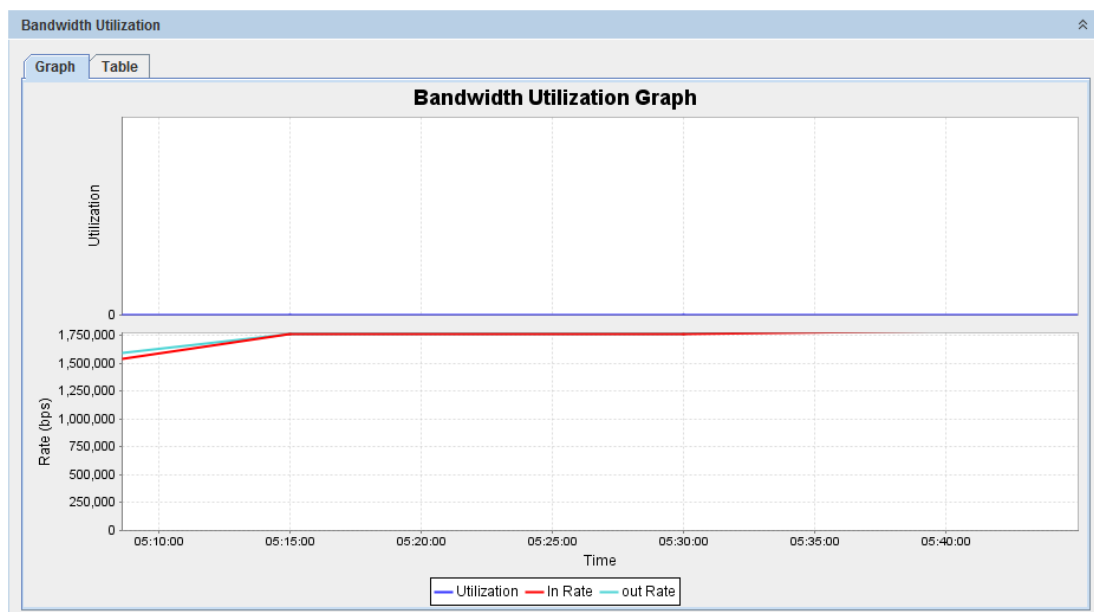


Figure 8-12: Bandwidth Utilization Screen

To display bandwidth utilization Ethernet statistics:

```
show eth <eth-list> statistics-summary
```

#	start		ifc	in-octets	out-octets
in-rate		out-rate		util	
0	2012.12.05	01:01:10	eth0	747984743210	748161700832
1765192		1766392		1 0	

To display the bandwidth utilization history (last 24 hours in 15 minutes intervals):

```
show eth <eth-list> statistics-summary 0 95
```

Chapter 9

Performing System Administration

This chapter describes procedures that involve system administration rather than the network itself, and includes the following topics:

- Configuring Encryption
- Working with Configuration Files
- Configuring Users
- Upgrading the ODU Software
- Monitoring CLI Sessions
- Viewing System Inventory
- Upgrading the License Key
- Performing Address Translation
- Netronics File System (SFS)
- Command Line Scripts
- Macro Scripts
- MAC Table Limitations
- Configuring NTP
- Viewing User Activity Log
- Access Control List (ACL)
- LLDP - Link Layer Discovery Protocol
- DHCP
- Managing SNMP
- Tacacs+ / Radius
- Ping (Supported only from CLI)

Configuring Encryption

The NetBeam supports 128bit and 256bit AES encryption with Static key. This means that the encryption key (32/64 characters long) must be inserted manually into both ends of the link. If there is an encryption mismatch, traffic does not go over the link.

The encryption license must be enabled in order to configure encryption. The NetBeam system supports AES encryption protocol, which is capable of delivering encrypted transmission over the link.

Loading Encryption License Key

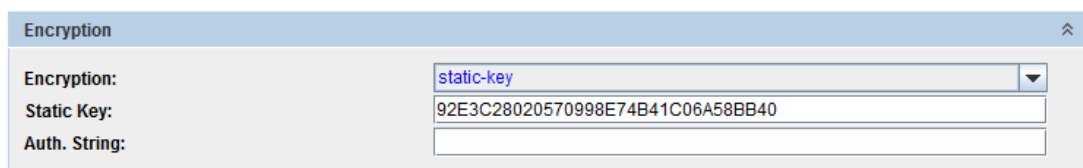
Encryption is a licensed feature that requires a license for operation. Before setting the encryption, verify that the encryption license key is available. Refer to *Upgrading the License Key* on page 160.

Setting up a Static Key

Use the following commands to set up a Static Key:

```
Default > set encryption encryption static-key static-key
0123456789abcdef0123456789abcdef
Set done: encryption
```

The string of either 32 (128bits) or 64 (256bits) hexadecimal digits



Encryption	
Encryption:	static-key
Static Key:	92E3C28020570998E74B41C06A58BB40
Auth. String:	

Figure 9-1: Encryption Screen

Working with Configuration Files

The NetBeam system supports the use of stored network configurations. Generally, a stored configuration is automatically loaded on system startup or following a system reset.

Saving Configurations

A stored configuration is created by saving the currently active (running) configuration as the default configuration.



The running configuration NetBeam is not automatically saved in non-volatile RAM.

If a system reset occurs before a particular configuration is saved, the NetBeam performs a startup using the current stored configuration, or if none exists, the factory default configuration.

To save the running configuration, use the following CLI command or click **Save Configuration** on the Web EMS main screen:

```
Default>>copy running-configuration startup-configuration
running-configuration copied to startup-configuration
```

Viewing Configurations

You can display either the running or the default NetBeam network configuration with the following command:

```
Default>copy running-configuration display
Default>copy startup-configuration display
```

Restoring the Default Configuration

In order to restore the default configuration, the startup-configuration must be removed and the ODU rebooted.

You can clear the startup configuration with the clear startup-configuration command or click Restore to Default in the Commands section of the Advanced Settings screen of the Web EMS:

```
Default>clear startup-configuration
startup-configuration cleared
```

On the next startup after this command is executed, the NetBeam system reverts to the hard-coded factory default parameters.

Pressing the ODU's **reset** push-button on the AUX port for more than five seconds resets the ODU and restores the default configuration.

Rollback Operations

You can roll back system configurations. This is a safety measure to prevent unwanted system changes in the event that a loss of communication occurs while performing configuration activities. The Rollback timeout function reloads the saved startup configuration in the event that no command is entered within a predefined timeout period.

A Rollback timeout is especially recommended when configuring remote elements that are being managed over the link.

To specify the Rollback timeout period, use the following command:

```
set rollback timeout <duration-in-seconds>
```

When Rollback is used, a timer runs (and restarts) whenever a CLI command is entered. In the event that no CLI command is entered within the timeout period, the system automatically resets and wakes up with the saved startup configuration.

Note that the rollback timer resets to zero after each new CLI command. The rollback timer expires when it reaches the value specified by `<duration-in-seconds>`.

To cancel a rollback, use the `clear rollback` command. This command cancels the Rollback function. This means that the System does not automatically roll back to any previous configuration.

You can enter the `clear rollback` command any time before the end of a Rollback timeout period in order to cancel a rollback timeout.

Rollback can also be controlled from the Web-EMS main screen.

Configuring Users

The NetBeam system supports multiple users, and enables you to choose from a selection of user types with different access privileges.

To add a new user:

1. Connect to the ODU. Refer to *Connecting to the ODU Using the Web EMS* on page 39.
2. In the Web EMS Main screen, click **Advanced Settings** and click the Users section.

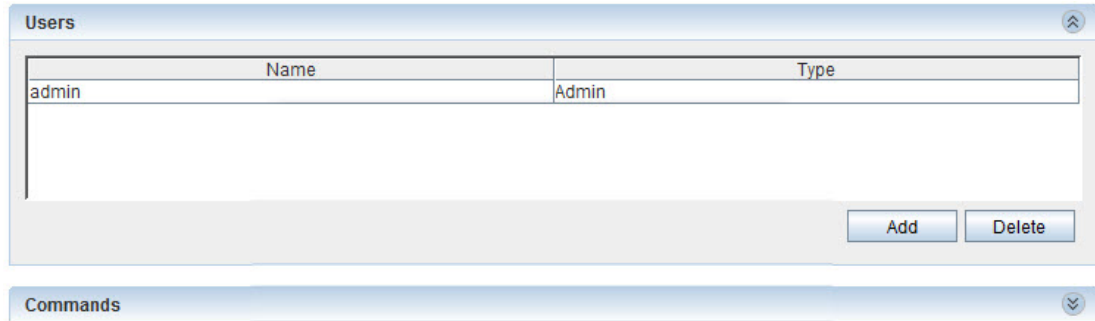


Figure 9-2: Web EMS Advanced Settings Screen – Users Section

3. Click **Add**. The Add User window is displayed.



Figure 9-3: Web EMS – Add Users Screen

4. In the **User Name** field, enter the user name.
5. In the **Password** field, enter a password for the user.
6. In the **Type** field, select from a list of user types. The user type defines the user's access privileges.
 - **User** – Read-only access, but cannot view user names, passwords, and other security settings.
 - **Tech** – Read-only access to configuration settings. Can clear statistics, alarms, and log lists, and run diagnostics.
 - **Super** – Read-write access, but no access to user names, passwords, and other security settings.
 - **Admin** – Full access except for access to debugging tools. A default admin user is built into the system, with the user name **admin** and the password **admin**. Only one admin type user can be defined.
7. Click **Apply** to save the changes.

Upgrading the ODU Software

The NetBeam system supports switching, in real time, between two software versions. NetBeam maintains an active (running) and a standby software version simultaneously. This enables you to upgrade the software with minimal interruption of service.

An external FTP, SFTP, or TFTP server is required for software download. When you download a software version, the downloaded version replaces the standby version.

Figure 9-4 shows the relationship between flash banks and software images in the NetBeam system.

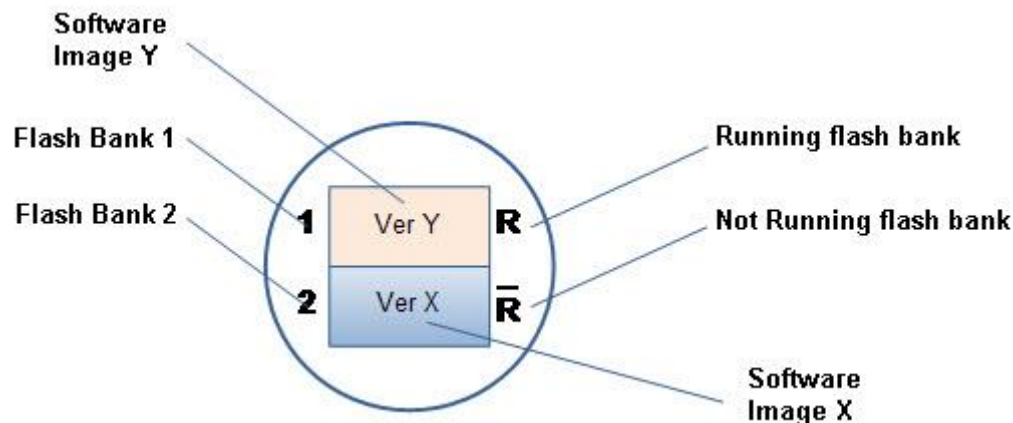


Figure 9-4: Flash Banks and Software Images

You can download and activate a new software version using either the Web EMS or the CLI.

Upgrading the ODU Software Using the Web EMS

To upgrade the ODU software:

1. Connect to the ODU. Refer to Connecting to the ODU Using the Web EMS on page 39.
2. From the Web EMS Main screen, click **Advanced Settings** and click the Software section of the Advanced Settings screen. The Software section displays both the active and the standby software versions.

The software version is followed by the creation date and time of the version. The first digit of the version number represents the major version number, the second digit represents the minor version number, the third digit represents the SVN revision, and the fourth digit represents the version build number.

Software			
Flash Bank	Version	Running	Scheduled to run
1	4.0.0.8484	yes	no
2	4.0.0.8409	no	no

Figure 9-5: Web EMS – Software Section

- Click **Download**. The Software Download window is displayed.

The image shows a 'Software Download' dialog box with the following fields and buttons:

- Username:
- Password:
- IP address:
- File name:
- Buttons:

Figure 9-6: Web EMS – Software Download Window

- In the Software Download window, enter the following details for the FTP, SFTP, or TFTP server from which you are downloading the software:
 - **Username**
 - **Password**
 - **IP address**
 - **File name** – The file name of the software version you want to download.
- Click **Apply** to download the software. The Software Download window closes, and the software is downloaded to the standby flash bank of the ODU.
- Once the software has been downloaded, click **Run SW** in the Software screen. The downloaded software version is activated.

Upgrading the ODU Software Using the CLI

You can use the show sw command to display the active and standby software versions.

```
NB2G1>show sw
```

Flash Bank	Version	Running	Scheduled to run
startup-config			
1 exists	5.0.0.9912 2013-08-27 12:06:30	no	no
2 exists	5.0.0.9931 2013-09-01 10:09:52	yes	no

```
NB2G1>
```

The software version is followed by the creation date and time of the version. The first digit of the version number represents the major version number, the second digit represents the minor version number, the third digit represents the SVN revision, and the fourth digit represents the version build number.

To upgrade the software:

1. Use the command `copy sw <from-url>` to copy a specified software version to the ODU, where `<from-url>` represents the URL of the FTP, SFTP, or TFTP server from which you are downloading the new software version. The software version image is copied from the specified URL to the standby flash bank of the ODU.
2. Use the following command to automatically upgrade the software when a more recent version becomes available:

```
run sw {immediate | next-rst} {<accept-timeout-sec> | no-
timeout} [if-version-differs-from <version>] [convert-
configuration]
run script <script-name> [<arguments>]
      where <arguments> - optional arguments in format
'name=value name=value ...'
run convert-startup

accept sw
```

3. Use the following command to reset the system with the formerly standby software version as the active version:

```
run sw {immediate | next-rst}
      {<accept-timeout-sec> | no-timeout}
```

- If `immediate` is specified as the first parameter on the command line, then a reset is performed immediately. This is the default value.
- If `next-rst` is specified as the first parameter on the command line, then the next system reset that occurs (for whatever reason)

causes the system to wake up with the software version stored in the standby flash bank.

- If `<accept-timeout-sec>` is specified as the second parameter on the command line, then this duration in seconds is used as the safety timeout period in order to manually enter the command `accept sw`.
 - If `no-timeout` is specified as the second parameter on the command line, then the command `accept sw` is not expected and the standby software version automatically becomes the active software version.
4. If the system reactivates after reset with a software version stored in the standby flash bank, use the `accept sw` command to make the standby version the active version. If you do not execute the `accept sw` command before the `accept-timeout-sec` period specified in Step 3 ends, the system resets and wakes up running the software version image stored in the active flash bank. Effectively, this means that the software version rolls back. Note that such a rollback also occurs if a reset occurs (for whatever reason) before the `accept sw` command is entered.

Monitoring CLI Sessions

Use the following command to display active CLI sessions:

```
show loginsession [{my | all}]
```

In response, the software displays the following:

```
Session ID  Session Time
xx          dddd:hh:mm:ss
yy          dddd:hh:mm:ss
```

Where:

`xx` or `yy` is a two-digit integer from 00 to 99, and

`ddd:hh:mm:ss` – days(0000 – 9999):hours(00 – 24):minutes(00 – 60):seconds(00 – 60)

To display only the CLI session of the user entering the command, use the `show loginsession my` command.

To display all active CLI session, use the `show loginsession all` command.

The maximum number of CLI sessions is 10.

Login Sessions	
Session ID	Session Time
00	0000:00:46:55
01	0000:00:34:49

Figure 9-7: Login Sessions Screen

Viewing System Inventory

You can display a system inventory list using the Web EMS or the CLI.

The NetBeam serial number and product type can be viewed under the chassis class in the Web EMS or can be accessed with the following CLI command:

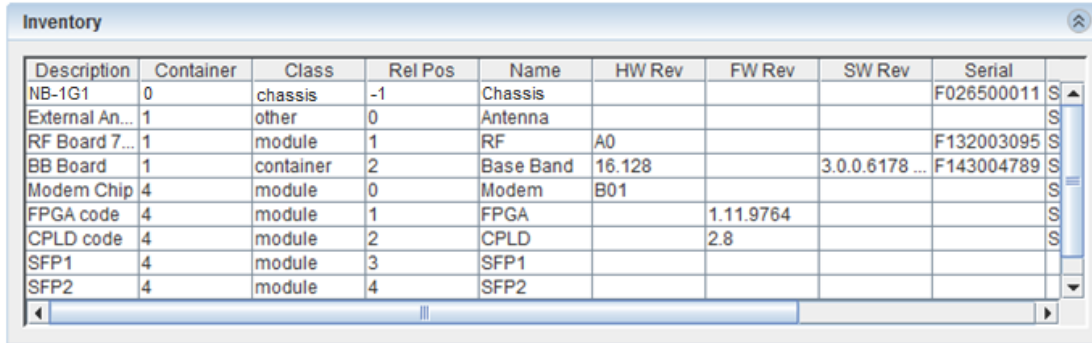
```
default>show inventory 1

inventory 1 desc           : NB-1G1
inventory 1 cont-in       : 0
inventory 1 class         : chassis
inventory 1 rel-pos       : -1
inventory 1 name          : Chassis
inventory 1 hw-rev        :
inventory 1 fw-rev        :
inventory 1 sw-rev        :
inventory 1 serial        : F026500011
inventory 1 mfg-name      : Netronics
inventory 1 model-name    : NB-1G1-ODU-2ft
inventory 1 fru           : true
```

Viewing System Inventory Using the Web EMS

To view the ODU's inventory list using the Web EMS:

1. In the Web EMS Main screen, click **System**. The System screen is displayed.
2. Click the Inventory section of the System screen, which lists parts, sub-parts, and their details.



Description	Container	Class	Rel Pos	Name	HW Rev	FW Rev	SW Rev	Serial	
NB-1G1	0	chassis	-1	Chassis				F026500011	S
External An...	1	other	0	Antenna					S
RF Board 7...	1	module	1	RF	A0			F132003095	S
BB Board	1	container	2	Base Band	16.128		3.0.0.6178 ...	F143004789	S
Modem Chip	4	module	0	Modem	B01				S
FPGA code	4	module	1	FPGA		1.11.9764			S
CPLD code	4	module	2	CPLD		2.8			S
SFP1	4	module	3	SFP1					
SFP2	4	module	4	SFP2					

Figure 9-8: System Screen – Inventory Section

Viewing System Inventory Using the CLI

To display a list and description of the system inventory, use the following command:

```
show inventory [{"<ph-idx-range> | all}
  [{"desc | cont-in | class | rel-pos | name | hw-rev
    | fw-rev | sw-rev | serial | mfg-name | model-name | fru
    | last-change | info}]]
```

Upgrading the License Key

You can order the following NetBeam software licenses (capacity steps and feature availability depends on the platform):

- Data rate (Capacity)
- Layer 2 networking capabilities –OAM, Resiliency
- Synchronization – Synchronous Ethernet (ITU-T G.8261)
- Encryption

Upgrading a license requires loading (using FTP, SFTP, or TFTP) a license key that is generated by Netronics based on your NetBeam serial number.

```
Default>copy license ftp://<ftp_user>:<ftp_password>@<FTP server
IP address>/<license_file_name>
```

...

Finished

- How to activate the licenses keys:

```
set license oam status enable
```

```
set license data-rate status 1000
```



```
set license synce status enable  
set license encryption status enable  
set license resiliency status enable
```

Then save the configuration and then:

```
copy running-configuration startup-configuration
```

Once you have loaded the license file to the ODU, you can activate the license.

- To view the available licenses according to the loaded license file (Permission) and the current configuration (Status):

```
default>show license
```

```
license oam          status      : enable  
license oam          permission  : enable  
  
license synce        status      : enable  
license synce        permission  : enable  
  
license encryption   status      : enable  
license encryption   permission  : enable  
  
license data-rate    status      : 500  
license data-rate    permission  : 1000  
  
license resiliency   status      : disable  
license resiliency   permission  : disable
```

- to activate the license:

```
Default>set license data-rate status 1000
```

```
Set done: license
```



Figure 9-9: Advance Setting Screen – License Section

Performing Address Translation

The ARP table is used to map between IP addresses and physical addresses. Use the following command to create and modify entries in the ARP table:

```
set arp
    [ip-address <mac-address>]
```

If the ARP entry does not already exist, the `set arp` command creates it and assigns the attributes specified. Upon creation, in the event that the interface address or the default router address is not specified, the entry is created with the default value that has been defined for the VLAN.

If the ARP entry already exists, then the `set arp` command replaces the attributes that are currently defined for the entry with the value specified in the command.

Use the following command to display ARP entries:

```
show arp [<ip-address>]
```

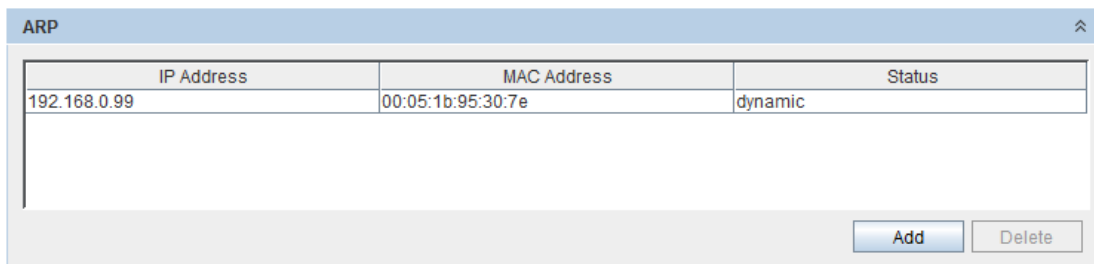


Figure 9-10: ARP Screen

Use the following command to delete ARP entries and clear their associated statistics:

```
clear arp [<ip-address>]
```

Table 12-51 on page 299 lists and describes the ARP table attributes.

Netronics File System (SFS)

Understanding SFS

With SFS, all files can be listed and classified (binary, text file, and so on), including files on remote servers.

SFS minimizes the required prompting for many commands, such as the copy CLI command. You can enter all of the required information in the command line, rather than waiting for the system to prompt you. For example, to copy a file to an FTP, SFTP, or TFTP server, you can specify the specific location on the device of the source file, the specific location of the destination file on the FTP, SFTP, or TFTP server, and the username and password to use when connecting to the FTP, SFTP, or TFTP server. Alternatively, you can enter the minimal form of the command.

SFS enables you to navigate to different directories and list the files in a directory.

Specifying Files Using URLs

Specifying Files on Network Servers

To specify a file on a network server, use one of the following forms:

```
ftp://username:password@Location/subdirectory/filename
```

The *location* can be an IP address or a host name.

The file path (directory and filename) is specified relative to the directory used for file transfers. For example, on UNIX file servers, FTP paths start in the home directory associated with the username.

The following example specifies the file named **mill-config** on the server named **enterprise.netronics-networks.com**. The device uses the username **liberty** and the password **secret** to access this server via FTP.

Since there is currently no DNS, the location is specified as IP Address in the dotted notation.

```
ftp://liberty:secret@127.23.46.17/mill-config
```

Specifying Local Files

Use the `[prefix: [directory/]] filename` syntax to specify a file located on the device specified by prefix. For example, `flash:backup-config` specifies the file named `backup-config` in the `configs` directory of Flash memory. Some devices do not support directories.

Supported Storage Devices

Table 9-1 lists and describes the currently supported file storage devices.

Table 9-1: Supported Support Devices

Device Identification	Description
ftp	FTP server (external server)
sftp	SFTP server (external server)
tftp	TFTP server (external server)
flash	Local flash memory (linux shell /var/netronics/etc).
eprom	RF module ROM. No directories.

The `/scripts` directory resides under flash (`flash:scripts`).

File System Commands

Command List

Table 9-2 lists and describes the file system commands.

Table 9-2: File System Commands

Command	Purpose
<code>dir <device:></code>	Lists files stored at the device; works only for flash and eprom; available to all types of users.

Command	Purpose
copy <from-url> <to-url>	Copy file; root, admin and super are allowed to copy from any device to any device; Tech and user are allowed to copy files from the local devices (namely: flash, ram, eprom) to the network devices (namely ftp) but not vice versa; they are not allowed to copy files between the local devices.
del <url>	Works only for flash; available only for root, admin and super.

Displaying the List of Stored Files

The command dir displays the list of the stored files in table format:

```
<Num>    <Size>    <date>    <time>    <name>
```

Where:

- Num=The sequential number
- size=File size in bytes
- data=Storage data
- time=Storage time
- name=File name

SFS Example for Backup/Restore of Configuration file

Backup the configuration file (startup-configuration.txt) to your PC:

```
CLI>copy flash:/startup-configuration.txt
ftp://user1:pass@192.168.0.222/backup.txt
```

...

finished

Restore the Startup-configuration back into the ODU (from the PC):

```
CLI>copy ftp://user1:pass@192.168.0.222/backup.txt flash:/startup-
configuration.txt
```

...

finished

* FTP server address = 192.168.0.222 (Username = user1 // Password = pass)

```
Default>dir flash:
```

Num	Size	Date	Time	Name
1	2	02.03.2011	14:59:32	demo.txt
2	1035	23.02.2011	09:35:11	finallog
3	6122	24.02.2011	11:06:32	rf.ini
4	8	12.02.2011	21:20:43	rftype_cfg
5	5613	02.03.2011	08:51:19	startup-configuration.txt
6	566	02.03.2011	08:51:19	startup-debug-configuration.txt
7	5688	02.03.2011	16:51:45	scripts/clear_statistics
8	2121	25.02.2011	08:50:24	scripts/qos-dscp
9	2117	24.02.2011	21:07:14	scripts/qos-pcp
10	2078	13.03.2011	09:42:39	scripts/qos-vid
11	5688	02.03.2011	16:51:45	scripts/clear_statistics
12	373	21.03.2011	17:29:05	scripts/system_info

History File Transfer

Data is transferred between the Manager and Network elements through a FTP, SFTP, or TFTP server. This server is controlled by an SNMP mechanism which covers a group of commands using a FTP, SFTP, or TFTP protocol to affect the transfer and SNMP to activate and monitor the transfer. Some data files, such as scripts and logs, are stored on the Ne internal database. Other data types are stored in temporary files generated from statistics history gathering requests, and are sent with a remote name specified by the Manager. At this point, the temporary file is deleted from the system.

This feature is supported on NetBeam 2G system only.

SNMP Request Process

The SNMP Request begins with the manager, who sends the request containing all the parameters needed to start an FTP, SFTP, or TFTP session to the NE (Network Element). The NE then checks the data in the request and sends a SNMP response and prepares a file to send to the Manager. Next, the NE (functioning as a client) opens the FTP, SFTP, or TFTP session to the Manager (who functions as a server). After the session begins, the Manager can use SNMP to request the session status (In Progress or Terminated, and Errors or OK). Note that the NE can open only one session at a time.

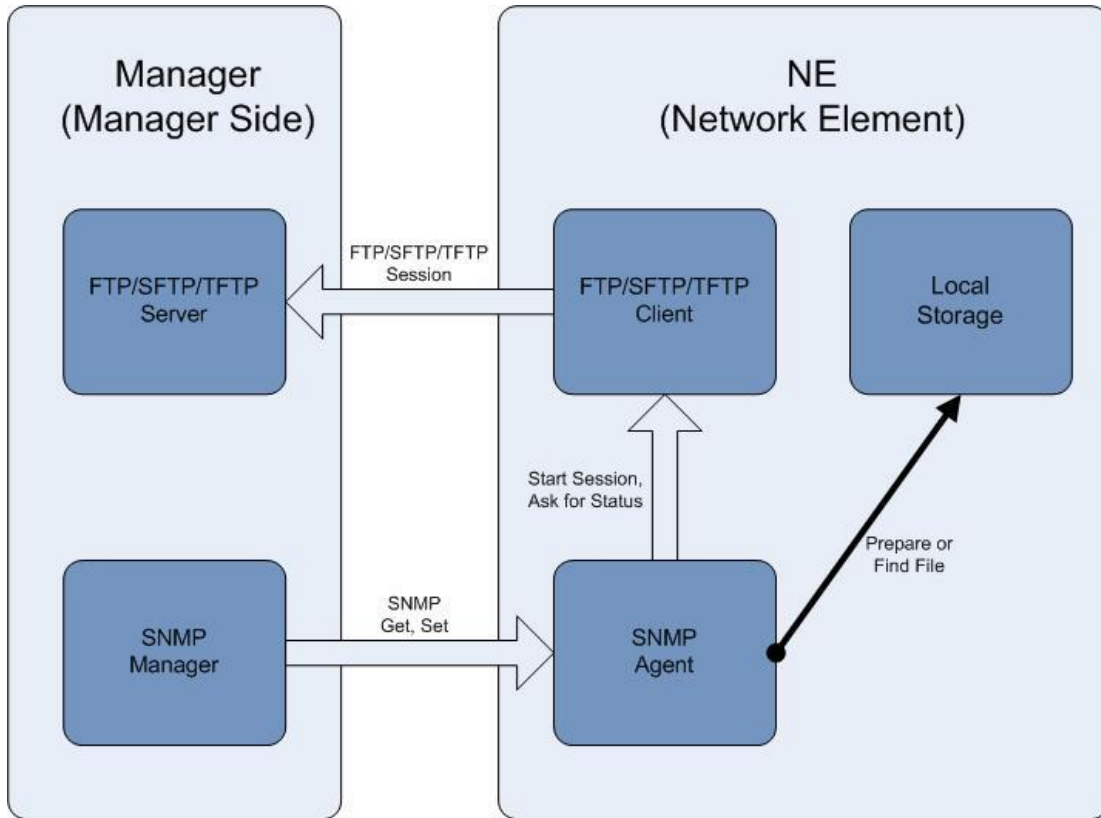


Figure 9-11: SNMP Request Process

SNMP PDU Activation

You can use the following SNMP SET request commands to start a FTP, SFTP, or TFTP session and set the following items:

Table 9-3: SNMP SET Commands

Command	Description
fileSessionProtocol	ftp(1), sftp(2), tftp(3)
fileSessionServer	FTP, SFTP, or TFTP server IP address, string
fileSessionUser	FTP, SFTP, or TFTP server user name, string
fileSessionPassword	FTP, SFTP, or TFTP server password, string
fileSessionRemotePath	URL of file on the Manager side (includes file name). Note, that Manager decides the remote file name and location.

	The NE just uses parameters specified by the Manager to initiate the transfer.
fileSessionLocalParams	The parameter meaning depends on the command type (fileSessionCommand parameter). It can be the name of an actual file in the NE storage or it can be used to generate a temporary file.
fileSessionCommand	copySwFromRemote(1), copyLicenseFromRemote(2), copyFileFromRemoteToLocal(3), ... copyEventLog(9), ... copyInventory(12), copyStatisticsHistory(13)
fileSessionRowStatus	The standard SNMP RowStatus, use the createAndGo(4) value to activate the process.

SNMP PDU Monitoring

You can use the following SNMP GET request commands to monitor a FTP, SFTP, or TFTP session and get the following items:

Table 9-4: SNMP GET Commands

Command	Description
fileSessionState	running(1), terminated-ok(2), terminated-error(3)
fileSessionResult	String. This is useful if an error occurs during the command execution (fileSessionState is terminated-error).
fileSessionRowStatus	

SNMP Activation Request

The following are examples of available activation request commands:

- fileSessionCommand:

copyStatisticsHistory (13)
- fileSessionLocalParams:


```
string: mo='mo-id' from='time' to='time'
```

- mo-id - mandatory parameter in cli format:

```
rf
eth {host | eth0 | eth1 | eth2 | eth3 | eth4}
vlan { c1 | c2 | c3 | c4 | c5 | c6 | s1} {undef |
1..4094}
```

- from - request for history from time in the format <2013.05.22 09:45:00>, optional parameter, if missing then starting from the oldest entry.
- to - request for history until the time in the format <2013.05.22 09:45:00>, optional parameter, if missing then until the latest entry.

File format

CSV is formatted with the following fields:

Table 9-5: CSV File Format

Statistic Type	Available Fields
rf	time, in-octets, in-idle-octets, in-good-octets, in-errored-octets, out-octets, out-idle-octets, in-pkts, in-good-pkts, in-errored-pkts, in-lost-pkts, out-pkts, min-cinr, max-cinr, min-rssi, max-rssi, min-modulation, max-modulation
eth	time, in-octets, in-ucast-pkts, in-discards, in-errors, out-octets, out-ucast-pkts, out-errors, in-mcast-pkts, in-bcast-pkts, out-mcast-pkts, out-bcast-pkts, out-discards, in-no-rule-discards
vlan	time, port, in-pkts, out-pkts, drop-pkts

The “time” field is equal to the interval start time that is displayed by the appropriate CLI show statistics commands.

Enter Settings for Multiple Variable Bindings

To enter fileSessionCommand settings:

1. Double-click the fileSessionCommand row.
2. Enter the following settings:
 - Remote SNMP Agent – The IP address of the ODU connected to the MIB Browser.
 - OID to set - x.x.x.x.x.1 as the next object in table.
 - Value to set – The table number is 13.
3. Click **OK**.

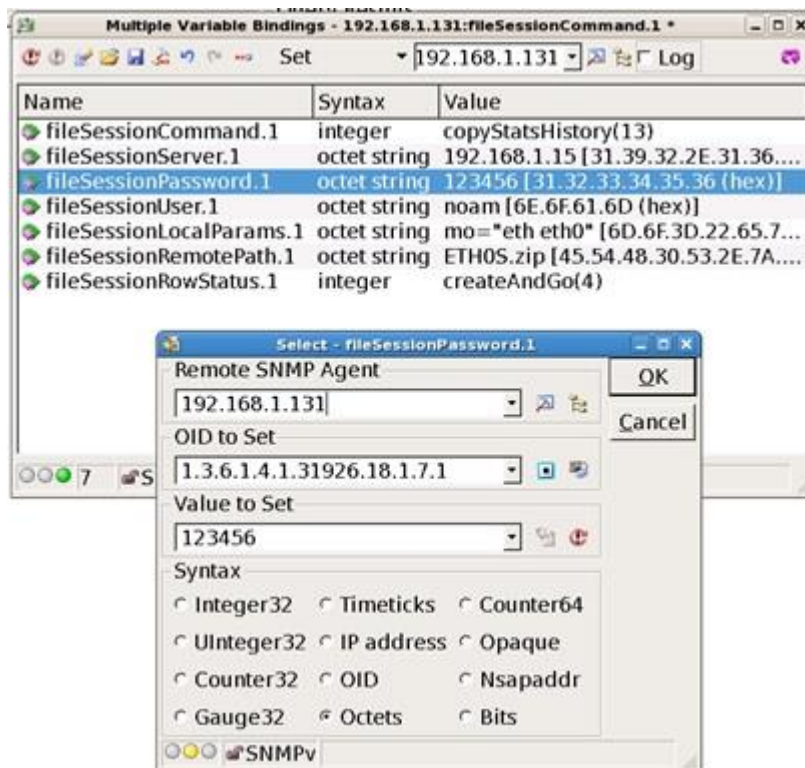


Figure 9-12: fileSessionCommand Settings

To enter fileSessionServer settings:

1. Double-click the fileSessionServer row.
2. Enter the following settings:
 - Remote SNMP Agent – The IP address of the ODU connected to the MIB Browser.
 - OID to set – x.x.x.x.1 as the next object in table.
 - Value to set – The IP address of the FTP, SFTP, or TFTP server.
3. Click **OK**.

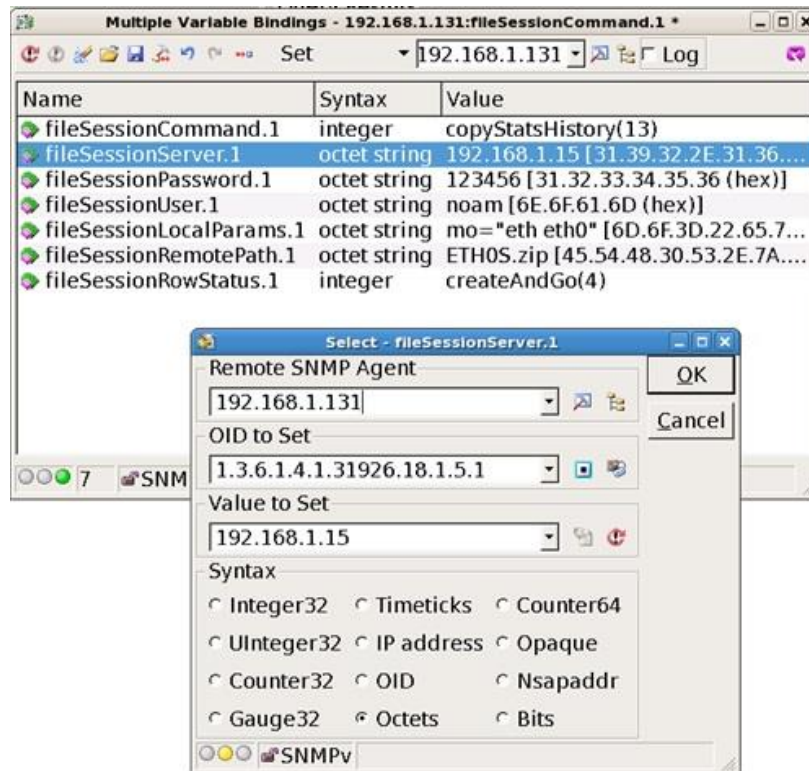


Figure 9-13: fileSessionServer Settings

To enter fileSessionPassword settings:

Note: Only apply these settings if the FTP, SFTP, or TFTP server is password protected.

1. Double-click the fileSessionPassword row.
2. Enter the following settings:
 - Remote SNMP Agent – The IP address of the ODU connected to the MIB Browser.
 - OID to set - x.x.x.x.x.1 as the next object in table.
 - Value to set – The password for the FTP, SFTP, or TFTP server.
3. Click **OK**.

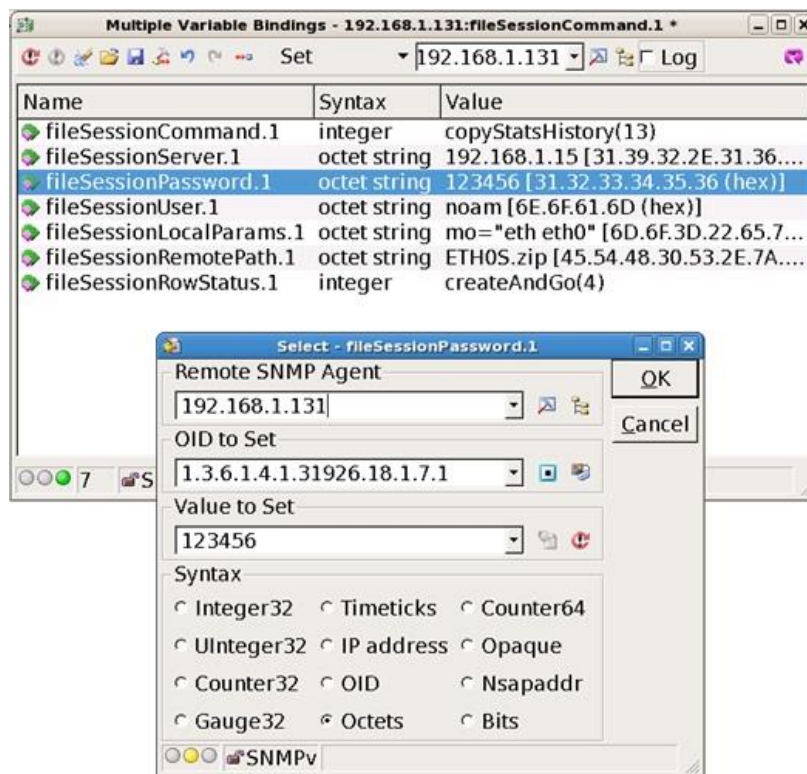


Figure 9-14: fileSessionPassword Settings

To enter fileSessionUser settings:

1. Double-click the fileSessionUser row.
2. Enter the following settings:
 - Remote SNMP Agent – The IP address of the ODU connected to the MIB Browser.
 - OID to set - x.x.x.x.x.1 as the next object in table.
 - Value to set – The username of the FTP, SFTP, or TFTP server.
3. Click **OK**.

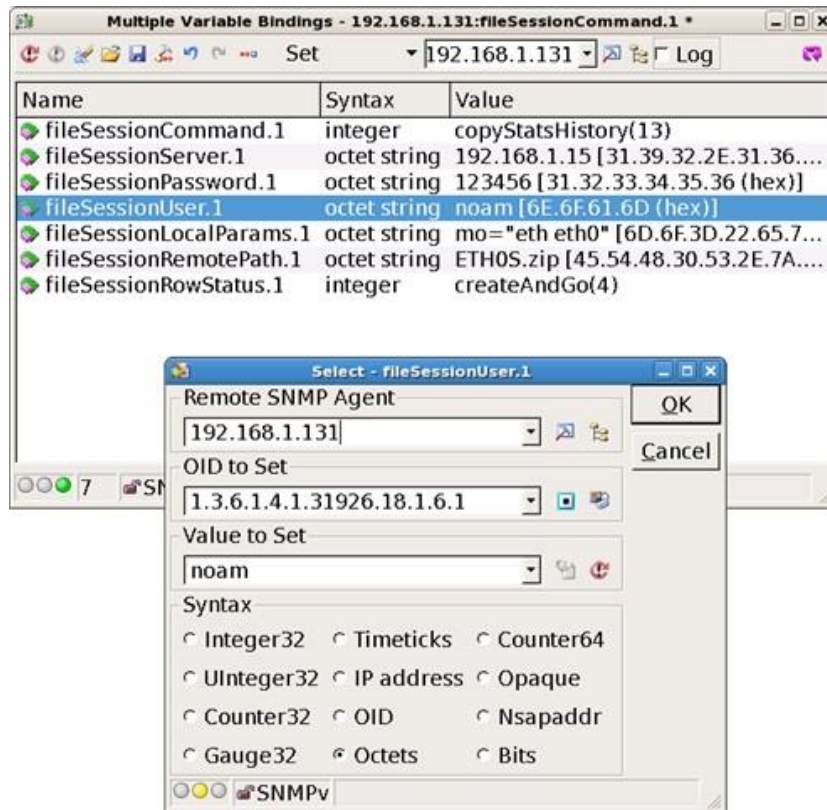


Figure 9-15: fileSessionUser Settings

To enter fileSessionLocalParams settings:

1. Double-click the fileSessionLocalParams row.
2. Enter the following settings:
 - Remote SNMP Agent – The IP address of the ODU connected to the MIB Browser.
 - OID to set - x.x.x.x.x.1 as the next object in table.
 - Value to set – Enter the required MO string:
 - **string:** mo='mo-id' from='time' to='time'

- **mo-id** - Mandatory parameter in CLI format:
 - **rf**
 - **eth {host | eth0 | eth1 | eth2 | eth3 | eth4}**
 - **vlan { c1 | c2 | c3 | c4 | c5 | c6 | s1} {undef | 1..4094}**
- **from** - Request for history from time in the format <2013.05.22 09:45:00>. This parameter is optional. If it is missing, it starts from the oldest entry.
- **to** - Request for history until time in format the <2013.05.22 09:45:00>. This parameter is optional. If it is missing, it goes until the latest entry.

3. Click **OK**.

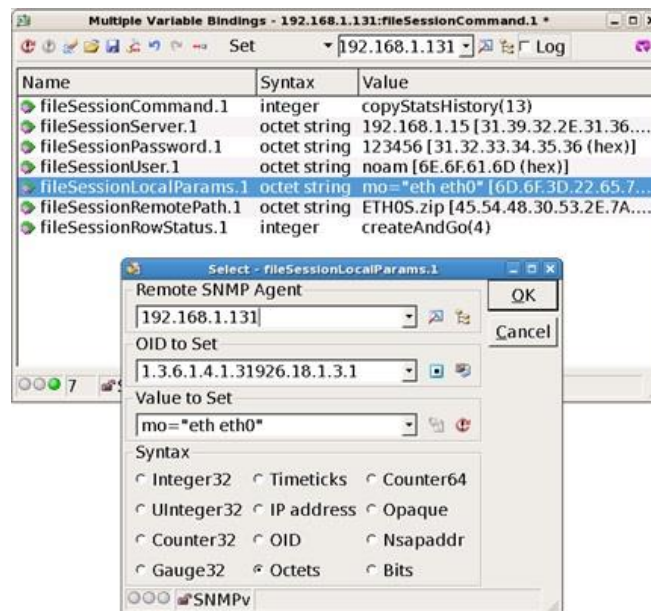


Figure 9-16: fileSessionLocalParams Settings

To enter fileSessionRemotePath settings:

1. Double-click the fileSessionRemotePath row.
2. Enter the following settings:
 - Remote SNMP Agent – The IP address of the ODU connected to the MIB Browser.
 - OID to set - x.x.x.x.1 as the next object in table.
 - Value to set – The file name where the stats are collected to.
3. Click **OK**.

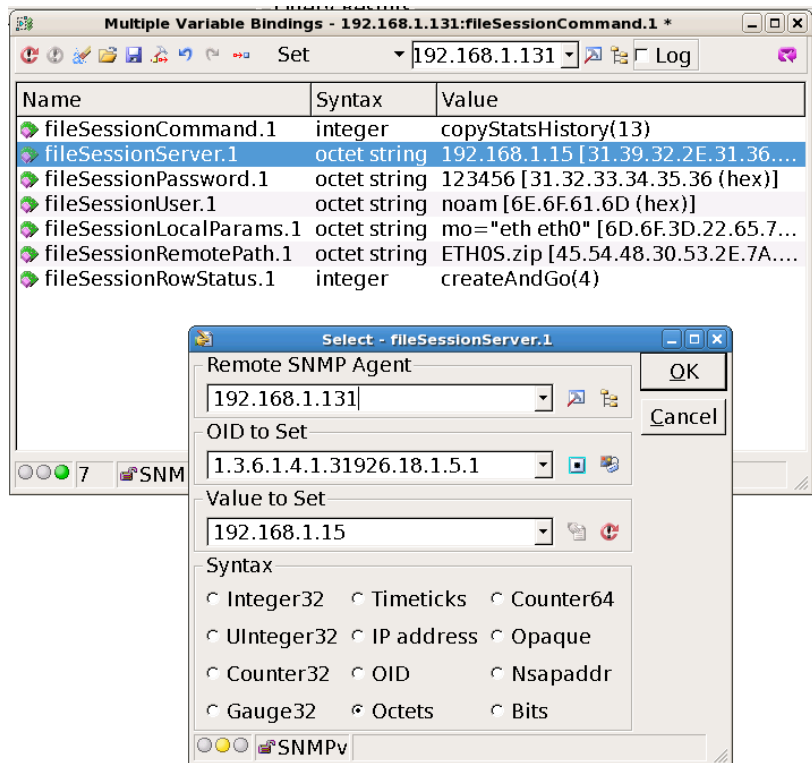


Figure 9-17: fileSessionRemotePath Settings

To enter fileSessionRowStatus settings:

1. Double-click the fileSessionRowStatus row.
2. Enter the following settings:
 - Remote SNMP Agent – The IP address of the ODU connected to the MIB Browser.
 - OID to set - x.x.x.x.x.1 as the next object in table.
 - Value to set – 4 (CreateAndGo). Activate the OID sequence to build the table.
3. Click **OK**.

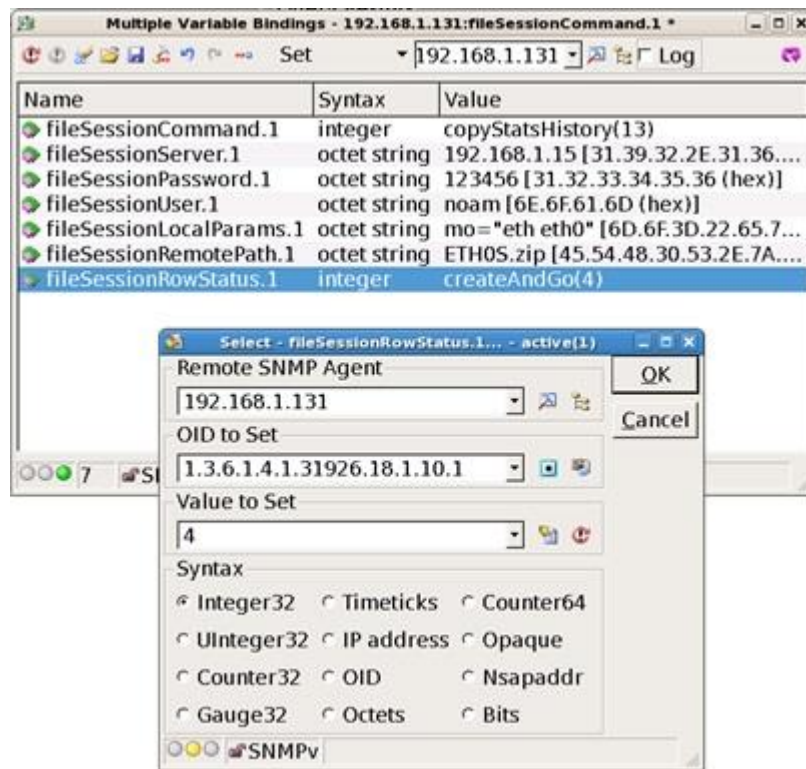


Figure 9-18: fileSessionRemotePath Settings

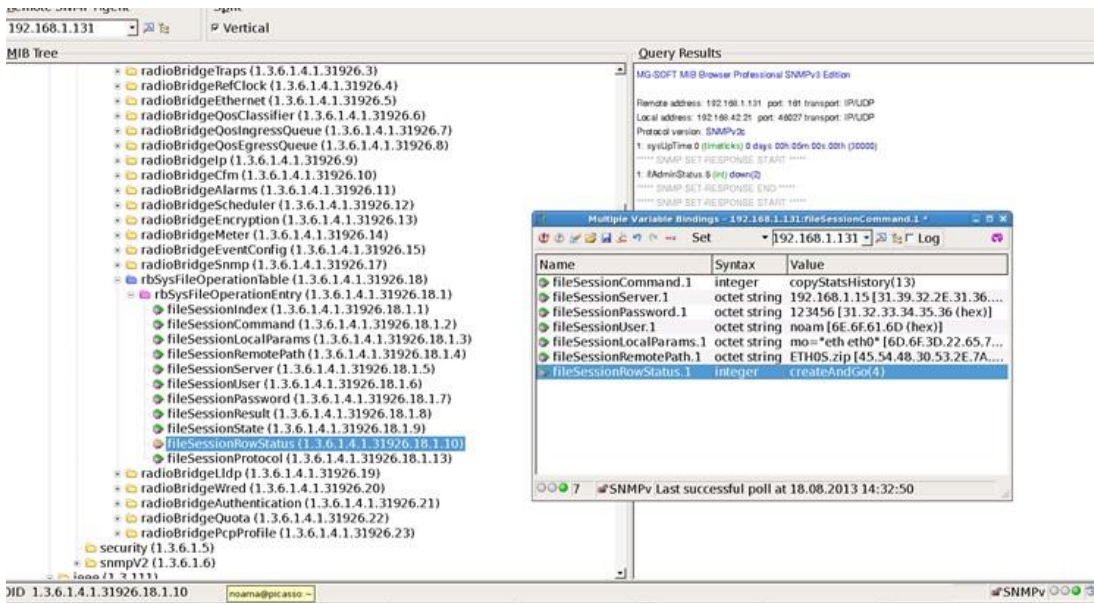


Figure 9-19: MIB Tree

time	in-octets	in-life-oct	in-good-o	in-errored-octets	out-octets	out-life-octets	in-pkts	in-good-pkts	in-errored-in-host-pk	out-pkts	min-cnr	max-cnr	min-rssi	max-rssi	min-modulation	max-modulation	arg-in-loss	arg-out-loss
1	28812456	0	0	0	6240280	6240284	3	0	3	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	1406
2	28736436	0	0	0	6230880	6230880	4	0	4	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	1460
3	30466008	0	0	0	6606000	6606000	8	0	8	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	1415
4	28899944	0	0	0	6240960	6240966	2	0	2	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	1375
5	28887684	0	0	0	6240960	6240960	2	0	2	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	1327
6	28750776	0	0	0	6244560	6244560	4	0	4	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	1285
7	28418960	17	0	0	5726880	5726884	4	0	4	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	1235
8	28852040	0	0	0	6240960	6240960	1	0	1	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	1206
9	28866876	0	0	0	6240960	6240966	8	0	8	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	1164
10	28897032	0	0	0	6241680	6241680	4	0	4	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	1145
11	30030176	7	0	0	6489360	6489360	8	0	8	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	1124
12	28833152	0	0	0	6248880	6248884	3	0	3	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	1083
13	28861180	0	0	0	6240960	6240960	5	0	5	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	1031
14	28937888	0	0	0	6486240	6486240	5	0	5	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	890
15	28317164	0	0	0	5688720	5688720	4	0	4	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	764
16	28807940	0	0	0	6240960	6240960	7	0	7	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	752
17	31211892	0	0	0	6762240	6762240	4	0	4	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	715
18	25993340	0	0	0	5638880	5638880	6	0	6	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	681
19	28779820	0	0	0	6240960	6240960	4	0	4	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	656
20	28743188	0	0	0	6240960	6240960	3	0	3	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	628
21	28800024	0	0	0	6240960	6240966	4	0	4	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	596
22	31075716	0	0	0	6706080	6706080	5	0	5	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	567
23	28769952	0	0	0	6240960	6240960	4	0	4	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	527
24	28905576	0	0	0	6240960	6240964	4	0	4	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	481
25	27854308	0	0	0	5990400	5990400	7	0	7	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	435
26	28814836	4	0	0	6240960	6240966	3	0	3	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	378
27	29489036	6	0	0	6384960	6384960	7	0	7	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	336
28	28826012	0	0	0	6240240	6240244	7	0	7	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	303
29	28817088	18	0	0	6240960	6240960	7	0	7	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	285
30	25993784	15	0	0	5621760	5621756	4	0	4	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	257
31	29807980	0	0	0	6450480	6450484	6	0	6	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	240
32	29197332	0	0	0	6328800	6328796	7	0	7	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	203
33	29803020	0	0	0	6486160	6486154	6	0	6	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	162
34	27900548	0	0	0	5810400	5810400	8	0	8	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	122
35	30750096	0	0	0	6645600	6645600	10	0	10	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	89
36	28097944	24	0	0	6059520	6059516	13	0	13	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	60
37	10051216	17	0	0	2174800	2174804	6	0	6	0	-128	-128	200	-200	qpsk 14.0.5	qpsk 14.0.5	0	17

Figure 9-20: History File Transfer Output

Command Line Scripts

NetBeam supports the use of pre-composed, multiple-line command scripts. A script is simply a list of CLI commands, saved in a text file that runs locally on the ODU. Script output is displayed on a script output screen and can be copied and saved.

Displaying Scripts

To display scripts using the Web EMS:

1. In the Web EMS Main screen, click **Advanced Setup**. The Advanced Setup screen is displayed.
2. Click the Scripts section of the Advanced Setup screen.

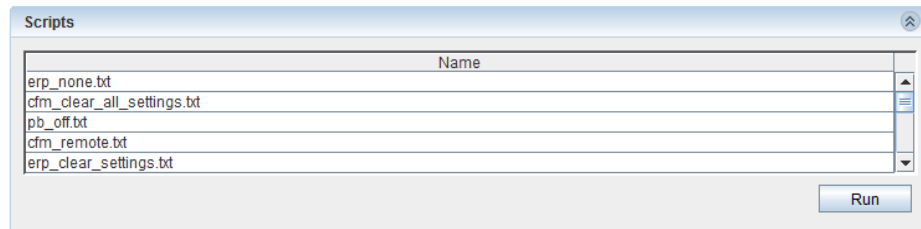


Figure 9-21: Web EMS Advanced Setup Screen – Scripts Section

3. Click **Add**. The Add VLAN window is displayed.

Running Scripts

1. Click the Scripts section of the Advanced Setup screen.
2. Highlight the script and select **Run**. The ODU will run the specified script.

Adding Scripts

You can write scripts in a text file and then copy them to the system. The script must consist of valid CLI commands. To include comments in the script, type # at the beginning of the line. The following is an example of a command line script:

```
# Demo Script
# This script sets the ODU to static mode, saves the
configuration, and resets the system.
set rf mode static qpsk 4 1 0.5
copy running-configuration startup-configuration
reset system
```

To add the script text file to the system, use an FTP, SFTP, or TFTP server to transfer the file to the `scripts` directory under flash (`flash/scripts`). The following example transfers the script `D.txt` to the system.

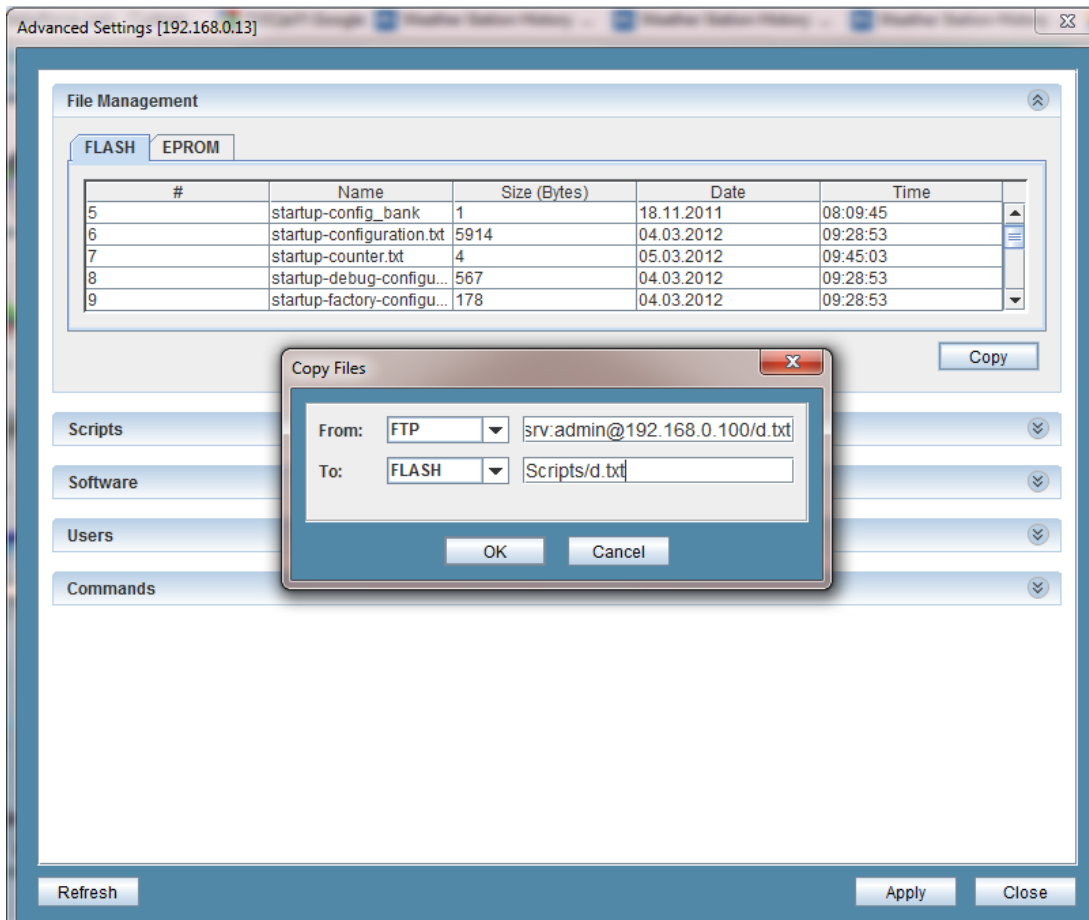


Figure 9-22: Adding Scripts

Viewing Script Content

You cannot display script content directly from the CLI. To view the content of a script, transfer the script to the server and view it with a text editor.

In the same manner, you cannot edit scripts directly on the ODU. To edit a script, transfer the script to the server and edit it with a text editor. Then transfer the new script back to the ODU, overwriting the existing script.

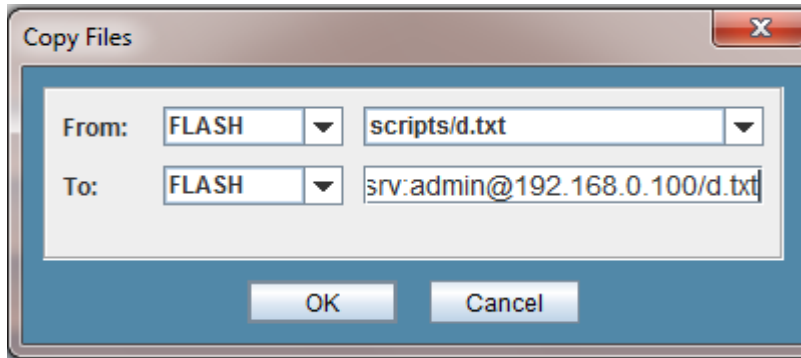


Figure 9-23: Copying Scripts

Command Line Scripts using the CLI

Use the `show script` command to display the names of all script files stored in the local directory.

```
Default>show script
```

Use the `run script` command to execute scripts.

```
Default>run script <script-filename>
```

To add the script text file to the system, use an FTP, SFTP, or TFTP server to transfer the file to the `scripts` directory under flash (`flash:scripts`). The following example transfers the script `DemoScript.txt` to the system.

```
Default>copy ftp://srv:admin@192.168.0.100/DemoScript.txt
flash:scripts/DemoScript.txt
...
Finished
```

You cannot display script content directly from the CLI. To view the content of a script, transfer the script to the server and view it with a text editor.

```
Default>copy flash:scripts/DemoScript.txt
ftp://srv:admin@192.168.0.100/ DemoScript.txt
...
finished
```

Use the `delete` command to delete scripts from `flash:scripts`:

```
Default>del flash:scripts/DemoScript.txt
```

Macro Scripts

This feature allows you to create chunks of CLI command sequences (variables) generic to a particular device. This feature is supported on NetBeam 2G systems only.

The following two methods define CLI variables:

- You can use the SET CLI command to define and use variables anywhere until the command is deleted.
- You can also pass parameters to the CLI script. An existing **run script** `<script-name>` command is extended with additional optional parameters: `run script <script-name> [<parameters-list>]`. Each parameter should be specified as follows: `<variable-name> = <variable-value>` (for example, `run script my_script management-vlan = 5`).

You should define such a variable as part of the script run command and use it until the script ends. It shadows variables with the same name defined previously using the SET command. After the script termination script parameters variables disappear and the global variables (created by SET) with similar names are visible again.

CLI Example

```
NB2G1 >set var ManagmentVID 5
NB2G1 >

NB2G1 >set vlan s1 $ManagmentVID egress eth0,eth1 untagged
eth0,eth1
Substituted: set vlan s1 5 egress eth0,eth1 untagged eth0,eth1

Set done: vlan s1 5
NB2G1 >
NB2G1 >

NB2G1 >set var Contact Netronics

NB2G1 >
NB2G1 >
NB2G1 >show var
Locals:
Globals:
Contact                               : Netronics
```

```
NB2G1 >set system name $Contact
Substituted: set system name Netronics
Set done: system
Netronics>
```

MAC Table Limitations

You can limit the number of learned MAC addresses per PORT/VLAN to the system limitation of 4000 learned MAC addresses based on the configured value.

A smaller table of "secure" MAC addresses is maintained in addition to (and as a subset of) the traditional MAC address table.

This feature is supported on NetBeam 2G1 systems only.

MAC Table Limitation Setting Procedure

1. Configure the FDB-Quota index and size.
2. Configure the Classifier-EVC (VID/Port).
3. Associate the FDB-Quota and the Classifier-EVC.
4. Define the FDB drop /flood mode.
 - **Drop** – Prevents the registration of new MAC addresses (according to the FDB-Quota size).
 - **Flood** – New MAC addresses are registered and one of the old MAC addresses is deleted.

CLI Example

```
# Example
# Set SVID-5 associate to FDB-ID 5, its Egress are ports
Eth3,Eth0
set vlan s1 5 fdb-id 5 egress eth0,eth3 untagged none history
disable
# Set FDB-Quota with size of 2 MAC's.
set fdb-quota 1 size 2
# Set classifier-EVC for ports Eth3/Eth0 for any VID with PCP7
set classifier-evc 1 interface eth0,eth3 precedence 1 vid 1-4094
pcp 7 ip-cos dont-care packet-type all evc 1
# Associate EVC 1 with Quota 1
set fdb-evc-quota 1 evc 1 quota 1
```

```

NB2G1>set bridge-common out-of-quota drop
Set done: bridge-common
NB2G1>
NB2G1>show bridge-common
bridge-common def-cvlan-etype      : 0x8100
bridge-common out-of-quota         : drop
NB2G1>
NB2G1>show fdb-table all all learned

component-id  fdb-id  mac-addr                bridge-port  status
quota
s1            1       f0:de:f1:08:6c:f8      eth1         learned 0
s1            5       00:1f:16:37:1e:15      eth0         learned 0
s1            5       00:24:a4:01:4a:b5      eth0         learned 0

NB2G1>

```

Configuring NTP

The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of network elements over packet-switched, variable-latency data networks.

NTP provides a connectionless service (UDP in the Transport Layer).

The NetBeam has an embeded NTP client. It can synchronize the host clock to any NTP server in the LAN/Internet to deliver accurate and reliable time.

Primary and secondary servers can be defined.

NTP Configuration

Use the following command to configure NTP:

```
set ntp <idx> [server <ip-addr>] [tmz -12..14]
```

Use the following command to display the NTP settings:

```

show ntp [{<idx> | all}][{server | tmz | info}]
* tmz = Time Zone Shift
ntp 1 server                : 192.168.0.222
ntp 1 secondary-server      : 0.0.0.0
ntp 1 tmz                    : 2
Right_Master>

```

Use the following command to clear the NTP settings:

```
set ntp 1 server 0.0.0.0 tmz 0
```

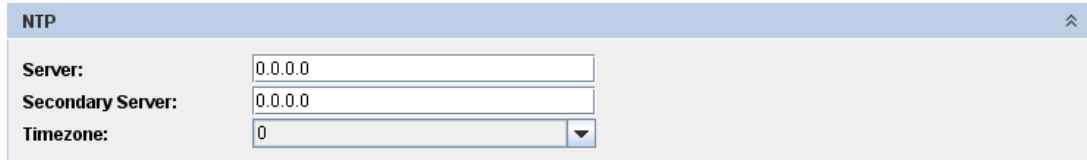


Figure 9-24: NTP Screen

Viewing User Activity Log

The ODU stores a log of all activities performed on the ODU.

Information recorded:

- Date, Time, Type (CLI, SNMP), User Name, and the command.
- Upon execution of each SNMP set request, a CLI command functionally equivalent to the SNMP set request will be constructed and added to the log.
- In case of SNMPv2 the write community name will be put into the log as the user name.
- In case of SNMPv3 the message user name will be put into the log.

Example:

```
Left-13>show user-activity-log
```

```
Dec 23 08:09:44 sw cad: User: cli admin : set rf tx-mute enable
```

```
Dec 23 08:10:05 sw cad: User: cli admin : set rf tx-mute disable
```

```
Dec 23 08:12:24 sw cad: User: cli admin : clear log
```

```
Dec 23 08:16:08 sw cad: User: cli admin : copy sw ftp://192.168.0.254/pub/netronics-  
uimage-40-5444
```

```
Dec 23 08:45:48 sw cad: User: cli tech : run sw immediate no-timeout
```

```
Dec 23 09:06:36 sw cad: User: cli admin : copy running-configuration startup-configuration
```


Dec 23 09:13:09 sw cad: User: cli admin : clear log

Dec 24 02:36:48 sw cad: User: cli admin : set rf mode alignment

Dec 24 02:44:34 sw cad: User: cli admin : set license data-rate status 1000

Access Control List (ACL)

The ACL is list of authorized IP's attached to the Host object and are the only permitted one to access the ODU.

The Max number of IP's in the ACL is eight different IP's.

If no entry is specified, the Host allows access from all IP addresses.

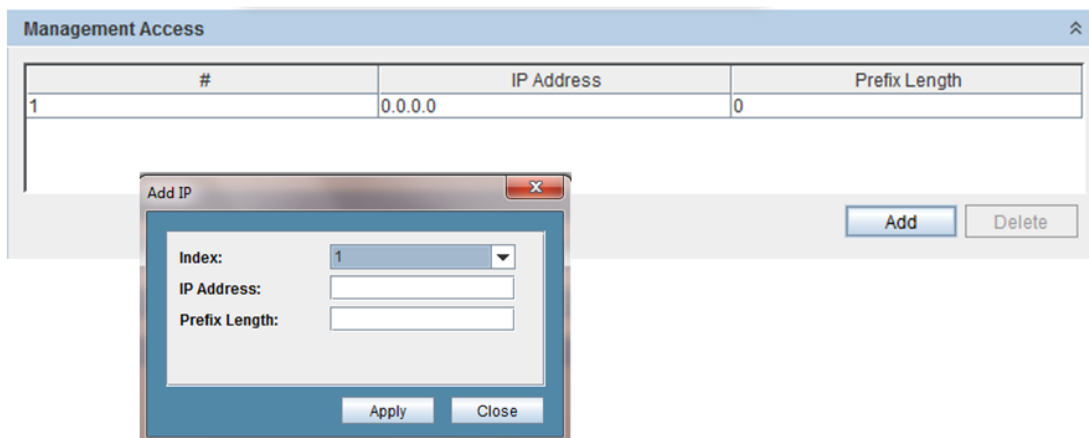


Figure 9-25: Web EMS ACL Window

ACL configuration using the CLI:

```
CLI>show access-list
```

```
access-list 1 ip-addr           : 0.0.0.0
access-list 1 prefix-len       : 0
```

```
CLI>set access-list ?
```

```
set access-list <index> ip-addr <value> [prefix-len <value>]
<index>                  : integer 1..8
```

```
CLI>clear access-list all
```

```
access-list 1 cleared
```

```
CLI>
```

LLDP - Link Layer Discovery Protocol

The Link Layer Discovery Protocol (LLDP) is an unidirectional neighbor discovery protocol. It enables the NetBeam to discover other network elements that are connected to it. This feature enables, among other things, discovery of third-party network elements connected to the NetBeam so that they can be managed.

LLDP performs periodic transmissions of an ODU's capabilities to the adjacent connected stations. LLDP frames are not forwarded, but are constrained to a single link. The information distributed by the protocol is stored in a topology xxxx. This information can be retrieved by the user or network element using CLI in order to describe the network's physical topology and its associated stations.

LLDP enables the discovery of accurate physical network topologies, meaning, which devices are neighbors and through which ports they connect. The user can use this information, especially the retrieved management IP addresses, in order to manage these discovered nodes.

This information can be sent over a VID or Untagged.

The following objects are available from a remote ODU:

- chassis-id (IP address)
- chassis-id-subtype
- port-id (MAC address)
- port-id-subtype : mac-addr port-descr
- sys-name
- sys-descr : NetBeam 1G1

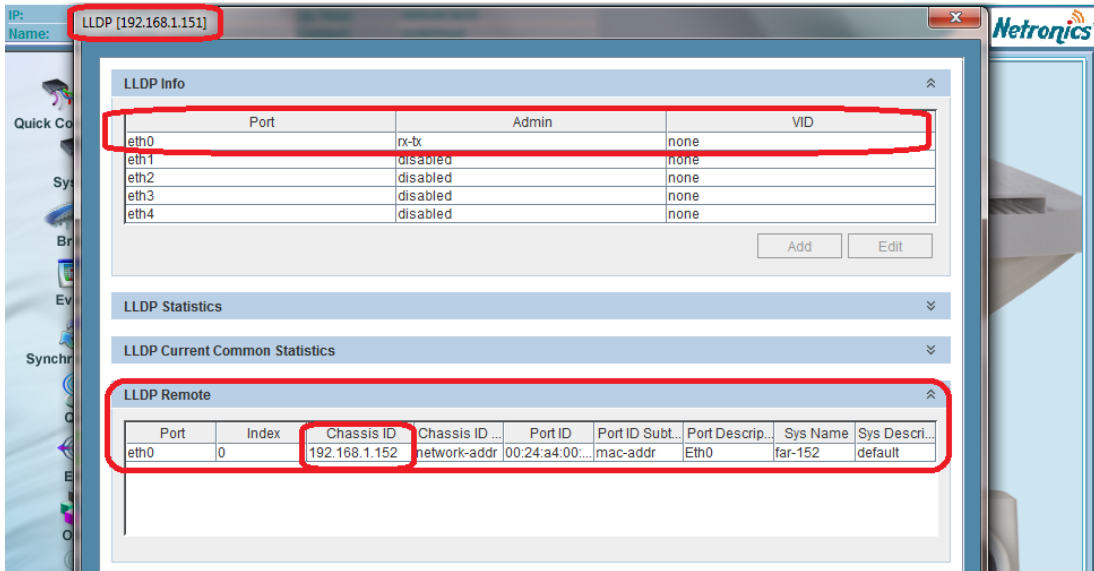


Figure 9-26: Web EMS LLDP Window

LLDP configuration using CLI:

The following is an example of the remote answer of the LLDP-remote (Eth0 = Over the Radio):

```
CLI>set lldp eth0 admin rx-tx
Set done: lldp eth0
CLI>show lldp-remote
```

```
lldp-remote eth0 0 chassis-id           : 192.168.1.152
lldp-remote eth0 0 chassis-id-subtype   : network-addr
lldp-remote eth0 0 port-id              : 00:24:a4:00:b8:74
lldp-remote eth0 0 port-id-subtype      : mac-addr
lldp-remote eth0 0 port-descr           : Eth0
lldp-remote eth0 0 sys-name             : far-152
lldp-remote eth0 0 sys-descr           : NB1G1
CLI>
```

DHCP

The Dynamic Host Configuration Protocol (DHCP) is a computer networking protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network. This protocol reduces system administration workload, allowing networks to add devices with little or no manual intervention.

DHCP is built on a client-server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts. "Client" refers to a host requesting initialization parameters from a DHCP server.

The following is an example of setting STATIC IP&DGW (Via CLI and Web):

```
CLI>set ip 1 ip-addr 192.168.1.151 prefix-len 23 vlan 0
Set done: ip 1
CLI>set route 1 prefix-len 0 next-hop 192.168.1.254
Set done: route 1
CLI>
```

```
CLI>show ip
ip 1 ip-addr           : static 192.168.1.151
ip 1 prefix-len       : 23
ip 1 vlan              : 0
ip 1 default-gateway  : 192.168.1.254
CLI>
```

The following is an example of setting IP&DGW using DHCP server (Currently supported only from CLI):

```
CLI>set ip 2 ip-addr dhcp
```

```
Set done: ip 2
```

```
CLI>show ip 2
```

```
ip 2 ip-addr           : dhcp 192.168.0.36
ip 2 prefix-len       : 23
ip 2 vlan              : 0
ip 2 default-gateway  : 0.0.0.0
CLI>
```

```
CLI>set route 1 prefix-len 0 next-hop 192.168.1.254
Set done: route 1
```

```
CLI>show ip 2
ip 2 ip-addr           : dhcp 192.168.0.36
ip 2 prefix-len       : 23
ip 2 vlan              : 0
ip 2 default-gateway  : 192.168.1.254
CLI>
```

Managing SNMP

The NetBeam supports SNMPv2 and SNMPv3. SNMP managers and users can be configured.

SNMP Managers

The following command sets the SNMP Trap Destination lists:

```
set snmp-mng <ip-addr-list> [udp-port <0..65535>] [security-name  
<string>] [snmp-version {v2 | v3}]  
set snmp-mng <1..5> [ip-addr <value>] [udp-port <0..65535>] [snmp-  
version {v2 | v3}] [security-name <value>] [engine-id <value>]
```

The security name is the same as the trap community name in SNMP2 and it is the same as the user name in SNMP3.

The default **udp-port** is 162.

The default **security-name/trap community** is “public”.

The default **snmp-version** is v2.

Use the following command to view the SNMP manager list:

```
default>show snmp-mng  
snmp-mng 1 ip-addr           : 192.168.0.100  
snmp-mng 1 udp-port         : 162  
snmp-mng 1 snmp-version     : v2c  
snmp-mng 1 security-name    : public  
snmp-mng 1 engine-id       : local
```

Each SNMPv3 agent has an engine ID that uniquely identifies the agent in the device and also the unique identification of the MIB objects within a domain.

In SNMPv3 communication, Engine ID is used as an identifier for an agent among other agents.

When you define get and set commands for an SNMPv3 user, set Engine ID to Local. When you define trap for an SNMPv3 user, set Engine ID to the value of the Engine ID of the remote manager.

Note that get, set, and trap commands should be defined for the same user. The same user should be defined twice: once with `Engin ID=Local` and the second time with the `Engin ID` of the remote manager.

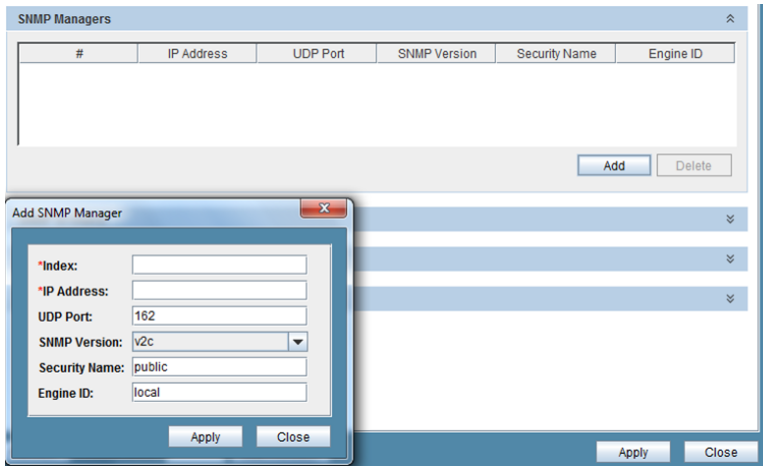


Figure 9-27: Web EMS System Screen – SNMP Managers Section

SNMP Agent Communities

The following command sets the SNMP agent communities:

```
set snmp-agent [read-com <value>] [write-com <value>] [snmp-version <value>]
```

Default **read-com** is public.

Default *write-com* is private.

Default **snmp-version** is v2.

To view the SNMP agent communities:

```
default>show snmp-agent
snmp-agent read-com           : public
snmp-agent write-com          : private
snmp-agent snmp-version       : v2c
```

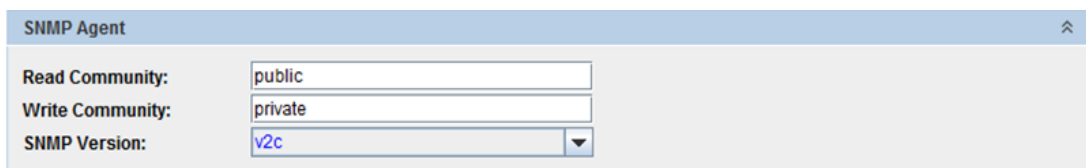


Figure 9-28: Web EMS System Screen – SNMP Agent Section

SNMPv3 Users Settings

The following command sets the SNMP users settings:

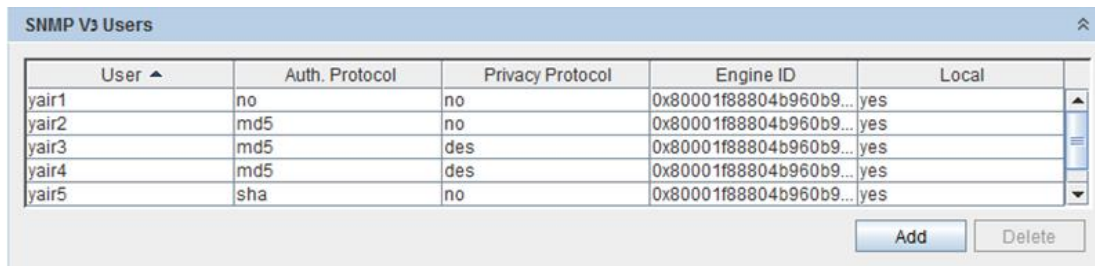
```
set snmp-user <engine-id> <user> <auth> <priv>
    <engine-id> : | local | string
    <auth>      : none | {md5 <passphrase>} | {sha
<passphrase>}
    <priv>      : none | {des <passphrase>} | {aes
<passphrase>}
```

auth-passphrase and privacy-passphrase are ASCII strings. Together with internally calculated Engine ID these strings are used to produce authentication and privacy keys respectively.

If no parameters other than the user name are supplied to the set command, an entry is created for the user identified by the name while privacy and authentication algorithms are set to NULL.

If a privacy algorithm (des or aes) is not supplied, the privacy algorithm is set to NULL.

If a privacy-passphrase is not supplied, the privacy-passphrase is the same as the authentication passphrase.



User ^	Auth. Protocol	Privacy Protocol	Engine ID	Local
yair1	no	no	0x80001f88804b960b9...	yes
yair2	md5	no	0x80001f88804b960b9...	yes
yair3	md5	des	0x80001f88804b960b9...	yes
yair4	md5	des	0x80001f88804b960b9...	yes
yair5	sha	no	0x80001f88804b960b9...	yes

Figure 9-29: Web EMS System Screen – SNMP Users Section

Tacacs+ / Radius

RADIUS (Remote Authentication Dial-In User Service) and TACACS+ (Terminal Access Controller Access-Control System) are AAA mechanisms.

- **Authentication:** Identification of requester profile (username, password, and privilege level) on a per-request basis.

- **Authorization:** Permission/denial of access to a subset of commands subject to authentication success/failure. (The mechanisms of Authorization and authentication are independent of each other.)
- **Accounting:** Reporting of information on requesters (identities, number of access attempts per requester, start and stop times, executed commands, etc.)

This version implements user authentication.

The NetBeam is a Network Access Server (NAS) for requesters.

AAA client passing requester information (e.g. username, password, etc.).

- The AAA Server is responsible for receiving the authentication requests.
- Communication between the NetBeam 1G and the AAA Server are permitted by shared secrets.
- Supporting user authentication with TACACS+ or Radius AAA servers, up to five servers. This is supported in addition to the local authentication.

The settings of Tacacs+ and Radius authentication are supported only in CLI.

How to set the ODU to connect to AAA (Radius/Tacacs+):

1. Configure the Auth-mode and the shared-secret under System.

```
show system
system auth-mode          : local
system auth-shared-secret : testing123
```

2. Configure the Auth-server IP address and its protocol port number.

```
show auth-server
auth-server 1 ip-addr      : 192.168.0.222
auth-server 1 protocol-port : 1812
```

3. Configure the users without a password.

```
show user
name                type
admin               admin
aaa                 tech
```

Every change in the Auth-mode deletes all users (except for the admin user).

You can set up to five separate servers. The Authentication starts from the 1st server and goes down to the 5th.

Setting a user for radius/tacacs is done without a password (The password is in the server). If the server is disconnected – only the Admin local user can connect to the unit.

- **Default Radius port = 1812**

- Default Tacacs port = 49

Ping (Supported only from CLI)

Ping is the basic utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer.

Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP response. In the process, it measures the time from transmission to reception (round-trip time) and records any packet loss. The results of the test are printed in the form of a statistical summary of the response packets received, including the minimum, maximum, and the mean round-trip times.

You can run the ping command with various command line switches to enable special operational modes. Example options include: specifying the packet size used and automatic repeated operation for sending a specified count.

Ping Commands

- **Ping** – Short ping five packets
- **Ping -t** – sending pings continuously until there is a command to stop it.
- **Ping -l** – <packet length 0-5000>
- **.Ping -c** – <number of packets to send 1-32000>

```

CLI>ping 192.168.0.15
PING 192.168.0.15 (192.168.0.15) 56(84) bytes of data.
64 bytes from 192.168.0.15: icmp_seq=1 ttl=128 time=2.77 ms
64 bytes from 192.168.0.15: icmp_seq=2 ttl=128 time=1.01 ms
64 bytes from 192.168.0.15: icmp_seq=3 ttl=128 time=1.07 ms
64 bytes from 192.168.0.15: icmp_seq=4 ttl=128 time=1.07 ms
64 bytes from 192.168.0.15: icmp_seq=5 ttl=128 time=1.04 ms
--- 192.168.0.15 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 1.019/1.398/2.776/0.689 ms

CLI>ping ?
ping [-c <num-packets 1..32000>] [-t] [-l <packet-length 0..5000>]
<host>
-t - ping until stopped by ctrl/c
CLI>ping

```

Traceroute (Supported Only in CLI)

Traceroute is a tool that traces the route that packets of data take from the device that a command originated from to the remote host. Like Ping, it can indicate if a remote host is reachable, but it gives a significantly more detailed report. This feature is supported on NetBeam 2G systems only.

Traceroute CLI Commands

The command `tracert?` displays the three traceroute options:

```
[-h <maximum-hops 1..255>] [-w <timeout, sec, 1..86400>] <host>
```

The `set tracert` command enables you to select one of the above options.

The following is an example of performing a traceroute:

```
NB2G1_Left>tracert 192.168.0.222
traceroute to 192.168.0.222 (192.168.0.222), 30 hops max, 46 byte
packets
 1  212.29.198.122 (212.29.198.122)  1.492 ms  0.710 ms  1.034 ms
 2  * * *
 3  * * *
 4  * * *
 5  *
```

Chapter 10

Zero Touch

This chapter describes the Zero Touch feature and includes the following topics:

- Zero Touch Feature
- Zero Touch Predefinitions
- Zero Touch System Process
- Configure Zero Touch in the CLI
- Configure Zero Touch in the WEB EMS

Zero Touch Feature

Zero Touch enables you to quickly and easily commission the link and complete the startup configuration process. The process begins with the remote and automatic configuration files, which enable the transfer and loading of the software file. The process results in full radio configuration, completed without any need for intervention on your part.

This feature is supported on NetBeam 2G systems only.

Zero Touch Predefinitions

Ensure that the following requirements are in fulfilled in order to enable Zero Touch:

- The system must have an enabled DHCP server and a TFTP server, as well as access to your servers.
- Connectivity to the servers must be verified. The Vlan for Inband management must be set to the correct operator Vlan.
- The operator must set the unit's frequency to the requested or default frequency.

Zero Touch System Process

Predefinition (ODU Side)

1. Enable the Net-config file (`set net-config config-file enable`).
2. Enable the DHCP server (`set ip 1 ip-addr dhcp`).

Zero Touch Procedure

1. The system starts and attempts to run the startup-config file.
2. If the startup-config file does not exist, the system runs the default config file and then the customer_default_config file if it exists on the system.
3. If the DHCP-config file is enabled, the script runs on the DHCP server allocating an IP address to the ODU.
4. The DHCP server points to the TFTP server that contains the user's "zero_touch.txt" configuration file.

In the example below, it changes the system name to NetBeam_SiteA, it then copies a new software version and upgrades the software version if the current version number is not the same as the most recently available version.

```
### Configuration file ###
# Set the system name
set system name NetBeam SiteA
# Copy the following sw and upgrade it if differs from
netronics-uimage-5.0.0-9900
copy sw tftp://192.168.0.222/ netronics-uimage-5.0.0-9931
if-version-differs-from netronics-uimage-5.0.0-9900
run sw immediate no-timeout if-version-differs-from
netronics-uimage-5.0.0-9931
```

- The configuration file is now located on the TFTP server directory.

```

CA> dhcp
Open DHCP Server Version 1.50 Windows Build 1027
Warning: section [80:86:98:01:4a:8d] Invalid subnetmask SubNetMask=255.255.222.0
, option ignored
Warning: section [80:86:98:00:D3:15] Invalid subnetmask SubNetMask=255.255.222.0
, option ignored
IP Address is missing in Static DHCP Host [80:86:98:0e:ef:d9], Entry ignored
Starting DHCP...
DHCP Range: 192.168.0.73-192.168.0.74/255.255.254.0
Server Name: odedo-x200
Detecting Static Interfaces..
Warning: Interface 192.168.42.88 is not Static, not used
Lease Status URL: http://192.168.0.222:6789
Listening On: 10.2.0.1
Listening On: 192.168.0.222
Listening On: 192.168.1.254
DHCP discover for 80:86:98:01:4a:8d (<) from interface 192.168.0.222 received
Host 80:86:98:01:4a:8d (Host808698014a8d) offered 192.168.0.73
DHCP discover for 80:86:98:01:4a:8d (<) from interface 10.2.0.1 received
Host 80:86:98:01:4a:8d (Host808698014a8d) offered 192.168.0.73
DHCP discover for 80:86:98:01:4a:8d (<) from interface 192.168.1.254 received
Host 80:86:98:01:4a:8d (Host808698014a8d) offered 192.168.0.73
DHCP request for 80:86:98:01:4a:8d (<) from interface 192.168.0.222 received
Host 80:86:98:01:4a:8d (Host808698014a8d) allotted 192.168.0.73 for 36000 second
s

CA> tftp
starting TFTP...
alias / is mapped to C:\Program Files (x86)\OpenTFTPServer\
permitted clients: all
server port range: all
max blksize: 65464
default blksize: 512
default timeout: 3
file read allowed: Yes
file create allowed: No
file overwrite allowed: No
thread pool size: 1
detecting Interfaces..
Listening On: 192.168.42.88:69
Listening On: 127.0.0.1:69
Network changed, re-detecting Interfaces..
detecting Interfaces..
Listening On: 192.168.42.88:69
Listening On: 192.168.0.222:69
Listening On: 10.2.0.1:69
Listening On: 192.168.1.254:69
Listening On: 127.0.0.1:69
Client 192.168.0.73:40428 C:\Program Files (x86)\OpenTFTPServer\zero_touch.txt,
1 Blocks Served
Client 192.168.0.73:40428 C:\Program Files (x86)\OpenTFTPServer\nbeam-uimage-5.0
10-9931, 27216 Blocks Served

```

Figure 10-1: Configuration File Location on the TFTP Server

- The ODU output appears as follows (the system name has been changed and the software version has been upgraded):

```

NetBeam_SiteA>show ip
ip 1 ip-addr      : dhcp 192.168.0.73
ip 1 prefix-len  : 23
ip 1 vlan        : 0
ip 1 default-gateway : 192.168.0.1
NetBeam_SiteA>show sw
Flash Bank      Version              Running
Scheduled to run startup-config

```

```

1          5.0.0.9931 2013-09-01 10:09:52    no
no          missing
2          5.0.0.9931 2013-09-01 10:09:52    yes
no          missing

```

7. If any errors occur during the execution of the DHCP script, the error file uploads to the server, restarts the system and sends an SNMP trap.

Configure Zero Touch in the CLI

Begin the configuration with the following command to enable the net-config file. This allows the unit to be configured through the network:

```

default>set net-config config-file enable
Set done: net-config

```

Confirm that the config file was successfully enabled:

```

default>show net-config
net-config config-file          : enable
net-config config-error-restart-delay: 60

```

Then ensure that the DHCP server is enabled:

```

default>set ip 1 ip-addr dhcp
Set done: ip 1

```

Confirm that that the DHCP server was successfully enabled:

```

NB2G1_Left_213>show ip
ip 1 ip-addr          : dhcp 0.0.0.0
ip 1 prefix-len       : 0
ip 1 vlan             : 0
ip 1 default-gateway  : 212.143.164.214
ip 2 ip-addr          : static 212.143.164.213
ip 2 prefix-len       : 30
ip 2 vlan             : 0
ip 2 default-gateway  : 212.143.164.214

```

Move the configured file to the unit through the TFTP Server:

```

Run configuration file /var/sw/etc//customer_default_config.txt

```

If an error occurs in the script, causing the configuration to fail, an error message to the TFTP Server and the unit sends an SNMP trap. The following command allows you to set the delay time before the system restarts the configuration:

```
set net-config [config-file <value>] [config-error-restart-delay <value>]
```

The Show status command shows the status of the net config or the startup-config:


```
default>show status
startup-config | net-config
```

The following response to the prompt to show the net-config status indicates that the Zero Touch configuration is complete:

```
default>show status net-config
NetConfig was successful
```

Configure Zero Touch in the WEB EMS

1. From the Main page select **Advanced Settings**.
2. Expand the **Net Config** section.
3. From the Config File drop-down menu, select **Enable**.
4. In the Config Error Restart Delay field, enter the desired default delay time between config attempts (the system default is 60 seconds).



5. Click **Apply**.

Chapter 11

NetBeam Diagnostics

The NetBeam system's highly reliable and easy-to-use radio link features a wide range of built-in indicators and diagnostic tools designed to enable you to quickly evaluate a link's performance, identify operating faults, and resolve them.

The general diagnostics process for an NetBeam link is to identify whether there is a problem that needs to be addressed, to isolate the root cause of the problem, and to implement the steps that are required to solve the problem.

The following is a partial list of events that can cause system problems:

- End equipment problems (such as connection or device configuration issues)
- External hardware faults
- System level configuration issues
- Hardware faults that require radio link replacement

This chapter describes the NetBeam diagnostics features, and offers basic instructions for how to use these features to isolate and resolve operating faults in the ODU's or in the NetBeam network. The chapter includes the following topics:

- The Troubleshooting and Diagnostics Process
- NetBeam ODU LEDs
- NetBeam System Alarms and Events
- NetBeam System Statistics
- NetBeam System Loopbacks

The Troubleshooting and Diagnostics Process

Follow this step-by-step process whenever you encounter a problem with the link.

Define the Problem

Isolating a problem's symptoms is the first step in corrective maintenance. It is important to define the problem clearly and fully.

Define the problem as either a **customer-impact type** (for example, loss of element management, or no Ethernet services over the link) or a **product-related type** (for example, a link is down or an ODU does not power up).

Check and Gather Relevant Information

Examining the link's status indications will provide both current and historical information regarding the link's performance and alarms.

Indications include ODU LEDs, System Alarms, and System Statistics.

Use these indications to further refine the problem and help to assess possible causes, both physical and logical, in the NetBeam system.

Isolate the Fault

Further isolate and characterize the problem using all available link indications.

Ascertain if the problem is related to:

- End-equipment configuration or an interconnection
- A hardware fault in the link's accessories (such as a cable)
- Configuration settings (this can be verified using the CLI)
- A hardware fault in one of the ODUs
- A result of larger network propagation problem

Note that Loopback indications are especially useful when isolating the fault's component and network location.

Correct the Fault

Once the fault is isolated, implement the necessary corrective actions until resolution of the problem is confirmed.

Whenever possible, it is recommended that you repeat commissioning tests in order to verify that the problem link is now operating correctly.

NetBeam ODU LEDs

The following table lists the possible status of all LEDs, together with a description for purposes of diagnostics.

Table 11-1: NetBeam ODU LEDs

LED	Color	Description
PWR (Power)	Green – Power OK	Blink Green – Device boot
	Red – Power Failure	
	Off – No Alarms	
RF	Green – Link Up	Blink Green – RF activity
	Orange – Alignment Mode	
	Off – Link Down	
ETH1/2/3/4:	Green – Link 1G	Blink Green – 1G activity
	Orange – Link 10/100	Blink Orange – 10/100 activity
	Off – No Link (Carrier)	

NetBeam System Alarms and Events

The following table lists all system alarms and events, together with their severity, possible cause, and corrective actions.

Table 11-1: NetBeam System Alarms and Events

Indication	Classification and Severity	Explanation	Probable Cause	Corrective Actions
Cold Start	Event [Trap, Log]	The ODU is re-initializing due to a Power-Up or Reset action.	N/A	N/A
Link Down	Alarm High [Trap, Log, Active Alarm List]	The communication link (either the RF or one of the Ethernet ports) is not operational.	Ethernet: 1) A cable is disconnected. 2) Configuration	Ethernet: 1) Check the cable connection. 2) Check the CLI

Indication	Classification and Severity	Explanation	Probable Cause	Corrective Actions
			mismatch between the ODU and end-equipment. RF Link: 1) Configuration mismatch between sides (frequency, modulation, RF role, etc.) 2) Line-of-Sight disruption or antennas not aligned. 3) Faulty ODU	configuration and end-equipment configuration. RF Link: 1) Check the configuration. 2) Isolate the problem using loopbacks. 3) Check cable connections and antenna alignment. 4) Replace ODU

Indication	Classification and Severity	Explanation	Probable Cause	Corrective Actions
Link Up	Event [Trap, Log]	The communication link (either the RF or one of the Ethernet ports) is operational.	N/A	N/A
Modulation Change	Event [Trap, Log]	The modulation setting for the RF link (currently in Adaptive mode) has changed.	N/A	N/A
Temperature High	Alarm Medium [Trap, Log, Active Alarm List]	The ODU temperature has exceeded a predefined threshold.	1) The ODU is installed in extreme temperature conditions. 2) Wrong temperature reading in the ODU	1) Check the ODU installation and verify that it is installed in accordance with environmental specifications. 2) Replace ODU
Temperature Normal	Event [Trap, Log]	The temperature of the device has returned to the normal range. This event clears a Temperature High alarm.	N/A	N/A
SFP In	Event [Trap, Log]	SFP inserted	N/A	N/A
SFP Out	Event [Trap, Log]	SFP extracted	N/A	N/A
Reference Clock Source Change	Event [Trap, Log]	The reference clock source for the NetBeam system has changed.	N/A	N/A
CFM Fault Alarm	Alarm High [Trap, Log, Active Alarm]	A maintenance endpoint (MEP) has a persistent defect condition.	Varies	1) Use the reported OID to determine the source of the fault.

Indication	Classification and Severity	Explanation	Probable Cause	Corrective Actions
	List]			
CFM Fault Recovery	Event [Trap, Log]	All MEP defects have been cleared and the alarm has been cleared from the Active Alarm List.	N/A	N/A
Synthesizer Locked	Event [Trap, Log]	The synthesizer has been locked.	N/A	N/A
Synthesizer Unlocked	Alarm High [Trap, Log, Active Alarm List]	The synthesizer has been unlocked.	N/A	N/A
POE Status Low	Alarm High [Trap, Log, Active Alarm List]	The power level being drawn by the ODU from the Ethernet is low.	Problematic PoE, ODU or connection	1) Check voltage and current supply to the PoE 2) Check cable 3) Replace PoE 4) Replace ODU
POE Status Normal	Event [Trap, Log]	The power level being drawn by the ODU from the Ethernet is normal.	N/A	N/A
ERP Ready	Event [Trap, Log]	ERP is ready for operation	N/A	N/A
Forced Switch	Event [Trap, Log]	ERP event	N/A	N/A
Manual Switch	Event [Trap, Log]	ERP event	N/A	N/A
Signal Fail	Event [Trap, Log]	ERP event	N/A	N/A
Invalid version	Event [Trap, Log]	ERP event	N/A	N/A

Indication	Classification and Severity	Explanation	Probable Cause	Corrective Actions
Loopback Enabled	Alarm Low [Trap, Log, Active Alarm List]	User enabled loopback	User action	N/A
Loopback Disabled	Event [Trap, Log]	Loopback cleared	User action	N/A
Tx Mute Enabled	Alarm Low [Trap, Log, Active Alarm List]	User enabled Tx Mute	User action	N/A
Tx Mute Disabled	Event [Trap, Log]	Tx Mute cleared	User action	N/A
Reception of QL EEC1 or Worse	Alarm Low [Trap, Log, Active Alarm List]	SyncE quality received on the link is same or worse than the ODU's internal clock quality	Network changes or sync failure	N/A
Reception of QL better than EEC1	Event [Trap, Log]	SyncE quality restored	N/A	N/A

NetBeam System Statistics

The NetBeam system uses advanced RF and Ethernet counters to provide real-time performance statistics for radio transmission activities, Ethernet ports, and VLAN traffic.

The following statistics enable quick analysis of system and component performance in support of troubleshooting and diagnostics.



For more details on system statistics, refer to *Monitoring the System* on page 137.

RF Statistics

Check RF statistic counters to identify radio errors and check the radio status history. The RF statistics consist of real time statistic counters since the last time the counters were cleared.

The RF transmission quality indicators are `rf in-errored-pkts`, `rf in-lost-pkts`, and `rf-in-errored-octets`. A rise in these indicators indicates radio errors. No errors in these indicators indicate that the radio link is operating without errors.

Radio errors observed in these indicators do not mean necessarily frame-loss on the Ethernet service.

The ARQ (Automatic Repeat Request) algorithm uses selective repeat (retransmission) to eliminate radio BER.

The `arg-in-loss` and `arg-out-loss` indicate frame-loss over the radio that is noticed by the Ethernet service.

For detailed explanations of all RF statistics, refer to *Viewing Radio Statistics* on page 140.

VLAN Statistics

You can display statistic counters of each NetBeam component per VLAN:

```
Default>>show vlan all statistics
component  vlan  port  in-pkts  out-pkts  drop-pkts  elapsed-time
c1          1   host   0         0         0          0000:00:00:32 c1
100  host  96     0         0         0          0000:00:00:32
c2          1   eth0   0         0         0          0000:00:00:32
c2         100  eth0  100        127        0          0000:00:00:32
c2         110  eth0   0        28601        0          0000:00:00:32
c2         120  eth0   0        28601        0          0000:00:00:32
c2         130  eth0   0        57180        0          0000:00:00:32
c3          1   eth1   0         0         0          0000:00:00:32
c3         110  eth1  28601        0         0          0000:00:00:32
c3         120  eth1  28601        0         0          0000:00:00:32
c3         130  eth1  71518        0         0          0000:00:00:32
c4          1   eth2   0         0         0          0000:00:00:32
c4         100  eth2  224         196        0          0000:00:00:32
```

Observe the `in-pkts`, `out-pkts`, and `dropped-pkts` for each VLAN.

Note that packets may be dropped due to traffic exceeding the radio link's maximum bandwidth.

For detailed explanations of all VLAN statistics, refer to *Viewing VLAN Statistics* on page 143.

Ethernet Statistics

You can display Ethernet statistics counters per Ethernet port.

```
Default>show eth all statistics
eth eth0 elapsed-time           : 0000:00:41:17
eth eth0 in-octets              : 18835233
eth eth0 in-ucast-pkts         : 4294967357
eth eth0 in-discards           : 0
eth eth0 in-errors             : 0
eth eth0 out-octets            : 19839102
eth eth0 out-ucast-pkts        : 63
eth eth0 out-errors            : 0
eth eth0 in-mcast-pkts         : 44
eth eth0 in-bcast-pkts         : 247622
eth eth0 out-mcast-pkts        : 247737
eth eth0 out-bcast-pkts        : 0
eth eth0 out-discards          : 0
eth eth0 in-no-rule-discards   : 0
```

Observe the **discard** and **error** counters to evaluate the performance of the Ethernet transmission.

For detailed explanations of all Ethernet statistics, refer to *Viewing Ethernet Statistics* on page 146.

NetBeam System Loopbacks

The NetBeam radio uses Ethernet and RF loopbacks designed to enable fault isolation and Ethernet service performance testing.

- **Ethernet Loopback** – Internal and external loopbacks are performed on the interface, testing the local ODU, the radio link, and the remote ODU.
- **RF (Radio) Loopback** – Internal loopback is performed on the ODU's RF output.



Note

After activating Loopback, it is important to clear all RF and Ethernet statistics in order to receive the most accurate results for analysis.

Use system alarms as well as statistic displays to determine if Loopback testing has passed or failed.

Loopback Diagrams

System Loopback Points

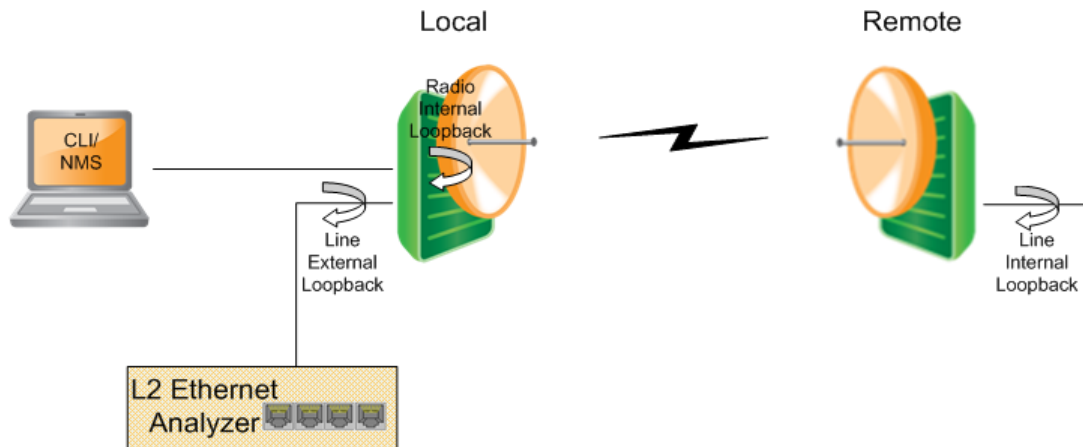


Figure 11-1: NetBeam System Loopback Points

Ethernet External Line Loopback Point

The Ethernet traffic from the customer's end-equipment or Ethernet analyzer is looped on the Ethernet interface (Eth1 or Eth2), enabling testing of the connection (cable/fiber) and the interface between end-equipment and the ODU.

When testing a link from one side (local), an external line loopback should be applied on the local unit.

The loopback can be applied separately for Eth1 and Eth2, and can be set with or without MAC Address swapping.

Set the loopback mode to external for the desired Ethernet port and set the loopback-timeout in seconds:

```
set eth eth1 loopback-timeout 300
set eth eth1 loopback-mode external-mac-swap
```

Use the following command to clear the loopback:

```
set eth eth1 loopback-mode disable
```

RF (Radio) Internal Loopback Point

The Ethernet traffic from a customer's end-equipment or Ethernet analyzer is looped on the ODU's radio output, enabling testing of the connection (cable/fiber), the interface between end-equipment and the ODU and the local ODU.

The loopback should be set with MAC Address swapping and on specific modulation profile.

Set the loopback mode on the RF menu and set the loopback-timeout in seconds:

```
set rf loopback-timeout 300
set rf loopback-mode internal-mac-swap qam64 4 1 0.5
```

Use the following command to clear the loopback:

```
set rf loopback-mode disable
```



For error-free operation at high modulation profiles, no interference should be present. Switch off remote ODU or change its frequency to eliminate risk of interference.

Note

It will take the ODU to stabilize after loopback about 1 minute.

Ethernet Internal Line Loopback Point

An Internal External loop returns the received frames to the radio side, enabling you to test Ethernet traffic across the link.

The Ethernet traffic from the Customer's end-equipment or Ethernet analyzer is looped at the Ethernet interface of the remote ODU, enabling testing of the connection (cable/fiber), the interface between end-equipment and the ODU, both local and remote ODUs, and the radio transmission.

The loopback can be applied separately for Eth1 and Eth2, and can be set with or without MAC Address swapping.

Set the loopback mode to internal for the desired Ethernet port and set the loopback-timeout in seconds:

```
set eth eth1 loopback-timeout 300
set eth eth1 loopback-mode internal-mac-swap
```

Use the following command to clear the loopback:

```
set eth eth1 loopback-mode disable
```

Chapter 12

Using the NetBeam CLI

This chapter describes how to use the NetBeam Command Line Interface (CLI) client to configure and maintain NetBeam devices on your network, and includes the following topics:

- Invoking the CLI
- CLI Command Syntax
- Viewing the CLI Command History
- Invoking CLI Help and Autocompletion
- CLI Error Messages
- Viewing the EtherHaul Statistics History
- CLI Managed Object Reference
- Management Object Attributes
- Radio Object Attributes
- Encryption Object Attributes
- Connectivity Fault Management (CFM) Object Attributes
- Network Object Attributes

Invoking the CLI

1. Run a standard SSH client. You can use a common, open source SSH client programs such as PuTTY.

2. Enter the ODU's IP address and open the connection. The default IP address is [192.168.0.1](#).
3. Login as user **admin**.
4. Enter the password **admin**.

When a successful connection is established, the ODU responds as follows:

```
Netronics-OS
>
Default>
```

NetBeam CLI commands should only be entered at the above prompt.

CLI Command Syntax

After invoking the CLI, you can input commands. Each CLI command is submitted to the NetBeam device for execution, after which a response is typically returned.

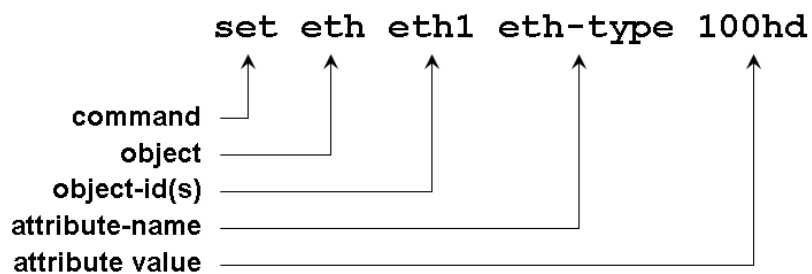
Each command line submitted to the CLI consists of:

1. A unique command that specifies the action(s) to be performed.
2. The object type on which action(s) are performed.
3. The identifier(s) for the object(s) on which action(s) are performed.
4. Zero or more object attributes that typically specify the value or characteristics for each action.

A CLI command line typically uses the following basic form:

```
command object <object-id(s)> [attribute-name <attribute-value>]
```

For example:



Basic Conventions

- CLI commands are not case sensitive.
- You can abbreviate commands and parameters as long as they contain enough letters to be distinguished from any other currently available commands or parameters.
- The commands entered from the CLI can apply to the entire system, to a specific port, or to a specific VLAN.

Common Syntax Rules

This document uses the following notation conventions when presenting CLI usage examples. These syntax conventions are found in commands, index names, objects, and attributes.

Table 12-1: Common Syntax Rules

Syntax	Meaning
{a b c}	One of the specified values must be entered in the command line
<name>	The name of a required attribute, explained in an accompanying or referenced section.
[name]	The name of an optional attribute, explained in an accompanying or referenced section.
n...m	Represents a number or integer series from n to m.

Repeatedly Used Identifiers

This document uses the following identifying conventions when presenting CLI usage examples. These syntax conventions are used primarily to represent various types of objects and lists that are to be specified on the command line.

For more information on using identifiers in the NetBeam CLI, refer to *Designating Named Objects* on page 219.

Table 12-2: Repeatedly Used Identifiers

Convention	Meaning
<comp-id>	A single component ID (one of c1, c2, c3, c4, c4, s1).
<bridge-port>	A single port name (one of host, eth0, eth1, eth2, c1, c2, c3, c4,

Convention	Meaning
	c4, s1).
<fdb-id>	A single FID (number from 1 to 64).
<vid>	A single VID (number from 1 to 4094).
<mac-addr>	A MAC address in the form NN-NN-NN-NN-NN-NN, where N is a hexadecimal number (e.g. 00-AF-DD-1E-2D-A3).
<ip-addr>	A standard dotted notation IP address (e.g. 10.0.15.74).
<ip-mask>	The IP address mask, i.e. the number of bits that constitute the IP network address prefix.
<comp-id-list>	A comma-separated list of the component IDs, e.g. c1, c2, c3, c4, c4, s1. Any combination of the component IDs can be included in the list. For details, refer to <i>Designating Named Objects</i> on page 2199.
<c-comp-id-list>	A comma-separated list of the C-component IDs, e.g. c1, c2, c3, c4, c4. Any combination of the component IDs can be included in the list. For details, refer to <i>Designating Named Objects</i> on page 2199.
<bridge-port-list>	A comma-separated list of port names, e.g. host, eth0, eth1, eth2, c1, c2, c3, c4, c4, s1. Any combination of the names can be included in the list. For details, refer to <i>Designating Named Objects</i> on page 2199.
<eth-list>	A comma-separated list of external port names, e.g. host, eth0, eth1, eth2. Any combination of the names can be included in the list. For details, refer to <i>Designating Named Objects</i> on page 2199.
<ext-bridge-port-list>	A comma-separated list of external port names, e.g. host, eth0, eth1, eth2. Any combination of the names can be included in the list. For details, refer to <i>Designating Named Objects</i> on page 2199.
<vid-list>	A list of ranges of VIDs from 1 to 4094. The notation covers comma-separated lists of the numbers within the specified range, as well a range of numbers separated by a hyphen, e.g. 5-25. For details, refer to <i>Designating Indexed Objects</i> on page 2211.
<fdb-id-list>	A list of ranges of FIDs from 1 to 64. The notation covers comma-separated lists of the numbers within the specified range, as well as a range of numbers separated by a hyphen, e.g. 5-25. For details, refer to <i>Designating Indexed Objects</i> on page 2211.
<comp-id>	A single component ID (one of c1, c2, c3, c4, c4, s1).

Convention	Meaning
<bridge-port>	A single port name (one of host, eth0, eth1, eth2, c1, c2, c3, c4, c4, s1).
<fdb-id>	A single FID (number from 1 to 64).
<vid>	A single VID (number from 1 to 4094).
<mac-addr>	A MAC address in the form NN-NN-NN-NN-NN-NN, where N is a hexadecimal number (e.g. 00-AF-DD-1E-2D-A3).
<ip-addr>	A standard dotted notation IP address (e.g. 10.0.15.74).
<ip-mask>	The IP address mask, i.e. the number of bits that constitute the IP network address prefix.
<qid-list>	A range of numbers from 1 to 8.
<hist-range>	A list of ranges of history interval numbers from 0 to 95. The notation covers comma-separated lists of the numbers within the specified range, as well as a range of numbers separated by a hyphen, e.g. 5-25. For details, refer to <i>Designating Indexed Objects</i> on page 2211.

CLI Command Types

The CLI uses a limited number of commands to create, maintain, and monitor NetBeam configuration.

Table 12-3: CLI Command Types

To perform this operation...	...use this CLI Command:
Create, update, or modify an object	Set
Display the characteristics or values of an object	Show
Reset or delete specified characteristics or values of an object	Clear
Reset the RF or System	Reset

The following sections describe the generic use of these routine CLI commands.

When performing non-routine activities, some additional commands are used, including **copy**, **run**, and **accept**. See, e.g. *Upgrading the ODU Software* on page 160 and *Performing Address Translation* on page 162.



CLI command syntax changes to fit the NetBeam object being managed or displayed. For specific command syntax and execution details, see the information that accompanies a particular object, starting in *CLI Managed Object Reference* on page 226.

Set Commands

The Set command is used to create, update and modify the characteristics of dynamic objects in the NetBeam configuration and values for a chosen object. Examples of dynamic objects are: VLANs, MEPs, and Static MAC Addresses.

The generic form the Set command is:

```
set object-name <object-ids> [attribute-name <value>] ...  
[attribute-name <value>]
```

If a dynamic object does not already exist, the Set command creates it and assigns the attributes specified. Upon creation, in the event that an attribute is not explicitly specified, the entry is created with the default value for that attribute.

If the dynamic object already exists, then the Set command will replace the attributes that are currently defined for the entry with those specified in the command.

If a `set` command is entered in an incomplete or invalid form, when possible, the CLI responds with an execution error message that specifies the reason for the error. For more information on error handling in the CLI, refer to *CLI Error Messages* on page 224.

Show Commands

The Show command is used to display the current characteristics and other values for a chosen object.

The generic form the Show command is:

```
show object-name <object-ids> [attribute-name]
```

If a `show` command is entered in an incomplete form, when possible, the CLI automatically completes missing object-ids with the keyword `all`, and missing attributes with the keyword `info`.

For example:

Table 12-4: Show Commands

When this Command is entered...	...the CLI interprets the Command as:
<code>show system</code>	<code>show system info.</code>
<code>show eth</code>	<code>show eth all info.</code>
<code>show bridge-port</code>	<code>show bridge-port all info</code>
<code>show bridge-port c2</code>	<code>show bridge-port c2 all info</code>
<code>show bridge-port c2 eth0</code>	<code>show bridge-port c2 eth0 info</code>
<code>show vlan</code>	<code>show vlan all info</code>
<code>show vlan s1</code>	<code>show vlan s1 all info</code>
<code>show vlan s1 123-170</code>	<code>show vlan s1 123-170 info</code>

For more information on the NetBeam CLI autocompletion feature, see *Invoking CLI Help and Autocompletion* on page 2233.



Note

The autocompletion mechanism does not enable the omission of object-ids or attributes which are required for correct command interpretation.

For example, `show vlan 123-170` is not correctly autocompleted because it lacks a required reference to the object `s1`.

When a show command is entered with the names or ids of an object that does not exist, the reference to the non-existing object is ignored and the information requested is displayed for all existing objects.

Display Formats

Both line-by-line and table methods are available for displaying attributes. The method used depends upon the object being displayed.

Line-by-line per attribute displays the objects in the form:

```
<object-name> <object-id> <attribute-name>: <value>
```

Note that multiple **<object-ids>** may be displayed using this form.

The Table display method presents the information in blocks and omits the object name and IDs, as in the form:

```
<attribute-name>          <attribute-name>          <attribute-name>
<value>                   <value>                   <value>
```

Clear Commands

The Clear command is used to reset or delete the specified values for a chosen object.

The generic form of the Clear command is:

```
clear object-name <object-ids> [attribute-name]
```

Nearly all **clear** commands require that at least one object identifier follow the object name in the command line. Alternatively, an object identifier may be replaced on the command line with the word **all**, which typically will be interpreted as “the whole range” (or “the whole set”) of identifiers for the specified object.

Reset Commands

There are two Reset commands used in the NetBeam system. Reset commands are used exclusively during initialization or reboot activities.

Reset RF

Resetting the RF returns the radio and modem hardware to its default settings. The command does not change a system configuration.

```
Default>reset rf
```

Reset RF is required whenever an RF Mode change is made from Alignment to Adaptive or Static.



Resetting the RF causes a service disruption of approximately 2 seconds in duration.

Reset System

Resetting the System reboots and reloads the currently saved system startup configuration.

```
Default>reset system
```

Reset System is used for power up and is required after software upgrades.



Resetting the System causes a service disruption of approximately 90 seconds in duration.

Designating Objects in CLI Commands

The CLI requires explicit identifiers to perform operations on the objects in an NetBeam configuration. You can designate a specific object (*e.g.* a bridge) by using its unique identifier.

Two types of object identifiers are used in the CLI:

- Object Names
- Object Indexes

Designating Named Objects

Certain NetBeam CLI objects are identified by symbolic names. These names are static and are always assigned to the same NetBeam object type. Using static names generally makes system configuration much easier and more consistent from network to network.

For example, the designation:

```
eth eth0
```

refers to the *Wireless Port*, while the designation:

```
bridge-port s1 c3
```

refers to *Port c3* on *Component s1*.

The following lists all named objects used in the CLI, together with the NetBeam objects that they reference:

Table 12-5: Named Objects in the CLI

CLI Name	Referenced Object
eth0	Wireless port
eth1	Wired Ethernet port 1
eth2	Wired Ethernet port 2
eth3	
eth4	
host	Internal CPU
s1	S-component 1
c1	C-component 1
c2	C-component 2
c3	C-component 3
c4	C-component 4
c5	C-component 5
c6	C-component 6

The CLI supports specifying a list of named objects by entering multiple comma-separated names.

For example:

```
eth eth0, host, eth1
```

specifies to three **eth** objects: *eth0*, *host*, and *eth1*;

```
bridge c1, c2, s1
```

specifies three bridge components: *c1*, *c2*, and *s1*; and

```
egress host, s1
```

specifies two egress ports: *host* and *s1*.



When using the **show** and **clear** commands, the keyword **all** may be substituted for a list of object names. In this context, “all” means all of the objects.

For example: **eth all** is identical to **eth host, eth0, eth1, eth2, eth3, eth4**.

Multi-Dimensional Object Lists

To specify objects in a multi-dimensional object list, the symbol names (or comma-delimited lists of names) are entered one after another, and are separated by spaces. The generic syntax is as follows:

```
object {<name1>} {<name2>} {<name3>}
```

For example:

```
bridge-port c1 host, s1
```

specifies the bridge ports *c1 host* and *c1 s1*.

Note that not every combination of keywords is valid. For example, the command **bridge-port c1, c2 host** is invalid, because two different C-components cannot be associated with the same port.

Designating Indexed Objects

Countable NetBeam CLI objects are specified by their unique identifying keyword, followed by the object's index number. A VLAN is a typical, countable object. For example:

```
vlan 230
```

refers to the VLAN with the index number 230.

A complete list of indexed objects is specified in a command using a comma-separated series. For example:

```
vlan 230, 330, 430
```

refers to VLANs with the index numbers 230, 330, and 430.

It is also possible to specify a range of indexed objects in a command. For example:

```
vlan 230-270
```

refers to VLANs with the index numbers 230 to 270, inclusive.

Finally, a mixed method may be used for specifying indexed objects in a command, enabling references to both a range of objects and to individual objects. For example:

```
vlan 230-270, 300, 401-410
```

refers to VLANs with the index numbers 230 to 270, VLAN number 300, and VLANs 401 to 410.

Designating indexed objects is valid in all **set**, **show**, and **clear** commands. If the **show** command is executed for indexed objects which do not exist, the non-existing objects are ignored and the command is only executed for existing objects.



When using the **show** and **clear** commands, the keyword **all** may be substituted for an indexed numerical range. In this context, “all” means the entire object range.

For example: `vlan all` is identical to `vlan 1-4094`.

Multi-Dimensional Objects with Indexes

The CLI supports multi-dimensional objects with numerical indexes. If they appear then their indexes (or lists of ranges of indexes) are placed one after another and are separated by spaces. The generic syntax is as follows: `object {<idx1>} {<idx2>} {<idx3>}`.

More specifically: `object 2, 9, 23-25` means the collection of double indexed objects: {2, 23}, {2, 24}, {2, 25}, {9, 23}, {9, 24}, {9, 25}.

For **show** and **clear** commands you can use the word **all** instead of either index. For example: `object 2, 9 all` OR `object all 23-25` OR `object all all`.

Viewing the CLI Command History

The NetBeam CLI maintains a history of the 100 most recent commands. This is especially useful when recalling long, complex or repetitive entries.

To recall commands from the history buffer, you can press the following keys:

Table 12-6: Viewing CLI Command History

Key press	Result
Up Arrow	Recall commands in the history buffer, beginning with the most recent command. Press the key repeatedly to recall successively older commands.
Down Arrow	Return to more recent commands in the history buffer, after recalling one or more commands with the Up Arrow key. Press the key repeatedly to recall successively more recent commands.

Invoking CLI Help and Autocompletion

The NetBeam CLI assists you both actively and passively, as follows:

- You can explicitly request syntax help on the command line.
- You can explicitly request autocompletion assistance on the command line.
- The CLI command interpreter always checks the validity and completeness of a string that is entered on the command line.
 - When a command is determined to be invalid, the CLI responds with a help message. If possible, the command interpreter derives the intended command from the initial entry and explains the syntax of the command and the range of allowed values.
 - When a command is determined to be incomplete (for example, if a required object or attribute is missing), the CLI responds with a choice of variants that represent the possible values, based on your initial entry.

The following table summarizes the ways to invoke CLI help and autocompletion features:

Table 12-7: Invoking CLI Help and Autocompletion Features

Feature	Description
Help <string>	Returns a help line for the requested command and object. For example: Default> help set vlan xxx returns: Default> set vlan <comp-id-list> <vid-list> [fdb-id <fdbid>] [egress <bridge-ports>] [untagged <bridge-ports>] where <bridge-ports> are port names or none fdbid in range 1..64 and relevant for s-vlans only
<string> ?	Returns a detailed list of commands that begin with a particular character string. For example: Default> set vlan? returns: Default> set vlan <comp-id-list> <vid-list> [fdb-id <fdbid>] [egress <bridge ports>] [untagged <bridge ports>] where <bridge ports> are port names or none fdbid in range 1..64 and relevant for s-vlans only Following printout, the CLI prompts you with the command that was input: Default> set vlan xxx

Feature	Description
<string> <tab>	<p>Automatically completes a specific command name. For example:</p> <pre>Default> set vl <tab> Default> set vlan Default> se vl 33 e Default> set vlan 33 egress</pre> <p>If more than one command matches the string that you entered, the CLI indicates that an ambiguous command has been entered.</p> <p>Note that the autocompletion feature does not function for indexes, MAC addresses or IP addresses.</p>
? or Help (without a string)	Returns a list of top-level CLI commands only.

CLI Error Messages

NetBeam CLI issues three types of error messages:

- **%Ambiguous command.** This error occurs when the command entered can only be partially interpreted. If possible, following the error message, a help syntax line is returned to assist you in correcting the command. For example:

```
Default> sh i
%Ambiguous command: sh i
show system, show bridge, show bridge-port, show eth, show
vlan-common, show vlan, show fdb, show fdb-table, show ip,
show rf, show arp, show cvlan-reg, show pep-vp, show svid-
xlat, show cfm-md, show crm-ma, show cfm-mep, show cfm-ccm,
show cfm-peer-mep-db
Default> sh i
```

- **%Invalid input.** This error occurs when the command entered includes an attribute value that is outside of the range allowed. To assist you, the CLI returns the entered command with a question mark (?) added, immediately following the erroneous parameter, as well as the entire command syntax. For example:

```
Default> set vlan cl 5000 egress 1, 3
%Invalid input: set vlan cl 5000 (?) egress 1, 3
set vlan <comp-id-list> <vid-list> [fdb-id <fdbid>] [egress
<bridge-ports>] [untagged <bridge-ports>] where <bridge-
ports> are port names or none fdbid in range 1..64 and
relevant for s-vlans only
```


- **General Execution Errors.** This error occurs when the command entered has correct syntax but cannot be executed for some reason. Such error messages are often application or object dependent.

Viewing the NetBeam Statistics History

The NetBeam CLI enables you to view standard operational and performance statistics for various objects in the system.

View the statistics history using the `show` command:

```
show <object> <comp-id> statistics
      [{<hist-range> | all}]
```

For example:

```
show RF statistics
```



For a complete description of available statistics, refer to Monitoring the System on page 137.

Using Statistics Intervals

You can specify a range of history intervals for the requested object statistics.

When a statistics interval is requested, the CLI returns information in the following format:

Interval	Start	End
<num>	<time>	<time>

Where:

<num> = The interval number, from 0 to 95. Interval 0 is the current interval, while intervals 1 to 95 hold statistics collected from 15 to 1425 minutes ago. The duration time for each interval is 15 minutes.

<time> = The interval time, displayed in a format that is identical to the System Up Time (Table 12-8).

When a history interval is not specified in the command line, the CLI displays the ordinary accumulative counters associated with the object.

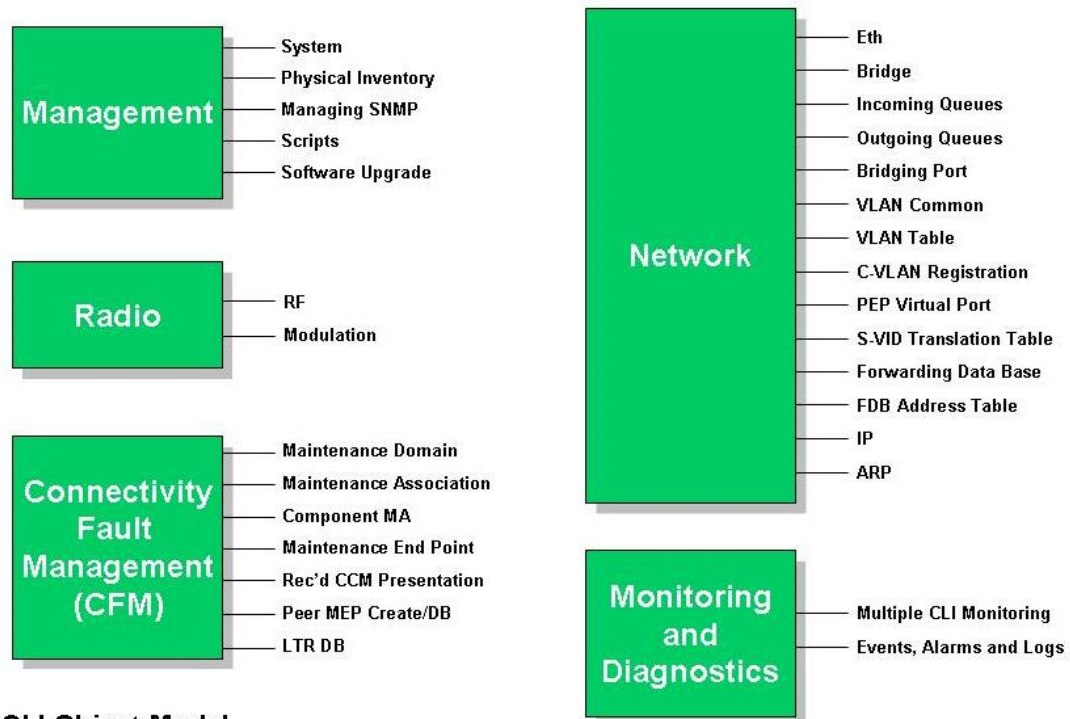


Using the `clear statistics` command erases all accumulative counters as well as the counters for Interval 0.

CLI Managed Object Reference

This section describes all NetBeam System objects that can be created, modified, displayed, or deleted using the command line interface.

Use *Figure 12-1* to quickly identify and locate a specific NetBeam object according to its logical function in the NetBeam System.



CLI Object Model

NetBeam
60/70 Wireless Backhaul Link

Figure 12-1: The NetBeam CLI Object Model

Management Object Attributes

This section lists and describes the attributes of network commands.

System Object Attributes

Table 12-8: System Object Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
System Description (description)	A text string describing the system. Generally includes the full name and version identification of the system's hardware type, operating-system, and networking software.	sysDescr (1.3.6.1.2.1.1.1)	Variable ASCII text	RO	NB 1G1, HW W.X SW Y.Z., where W.X =the HW version Y.Z =the SW version
System Object ID (snmp-id)	The vendor's authoritative identification of the network management subsystem contained in the entity.	sysObiectID (1.3.6.1.2.1.1.2)	1.3.6.1.4.1.31926	RO	1.3.6.1.4.1.31926

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
System Up Time (up-time)	The length of time that has passed since the network management portion of the system was last re-initialized.	sysUpTime (1.3.6.1.2.1.1.3)	ddd:hh:mm:ss, where ddd=decimal integer representing days (it can be an arbitrary number of digits) hh=two-digit decimal integer representing the hours of a day [0..23] mm=two-digit decimal integer representing minutes of an hour [0..59] ss=two-digit decimal integer representing seconds of a minute [0..59]	RO	N/A
System Contact (contact)	A text string identifying the contact person responsible for this managed node, together with information on how to contact this person.	sysContact (1.3.6.1.2.1.1.4)	Up to 256 characters. If no contact information exists, the value returns a zero-length string.	RW	"sysContact undefined"

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
System Name (name)	A name assigned by the administrator to this managed node. Generally, by convention, this is the node's fully-qualified domain name. This value is also used as the system prompt string. If no System Name is assigned the system prompt will read "Default."	sysName (1.3.6.1.2.1.1.5)	Up to 256 characters. If no system name exists, the value returns a zero-length string.	RW	"Default"
System Location (location)	The physical location of this node (e.g. 'telephone closet, 3rd floor').	sysLocation (1.3.6.1.2.1.1.6)	Up to 256 characters. If no system location exists, the value returns a zero-length string.	RW	"sysLocation undefined"
Input Voltage (voltage)	The system input voltage.	NetronicsSysVoltage (1.3.6.1.4.1.31926.1.1)	Integer	RO	N/A
Enclosure Temperature (temperature)	The system enclosure temperature.	NetronicsSysTemperature (1.3.6.1.4.1.31926.1.2)	Integer	RO	N/A
System Date and Time (date, time)	The host's local date and time of day.	hrSystemDate (1.3.6.1.2.1.25.1.2) As defined in RFC 2790	yyyy-mm-dd hh:mm:ss, where: yyyy= year (0 – 9999) mm= month (1 – 12) dd= day (1 – 31) hh= hour (0 – 24) mm= minute (0 – 60) ss= second (0 – 60)	RW	None

Physical Inventory Object Attributes

Table 12-9: Physical Inventory Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	SNMP Syntax	CLI Syntax
Inventory Index	The index for the table entry.	entPhysicalIndex (1.3.6.1.2.1.47.1.1.1.1.1.1)	integer32 (1..2147483647)	integer
Physical Descriptor (desc.)	A textual description of physical entity. This object should contain a string that identifies the manufacturer's name for the physical entity, and should be set to a distinct value for each version or model of the physical entity.	entPhysicalDescr (1.3.6.1.2.1.47.1.1.1.1.1.2)	character string	character string
Contained In (cont-in)	The value of entPhysicalIndex for the physical entity which contains this physical entity. A value of zero indicates this physical entity is not contained in any other physical entity. Note that the set of containment relationships define a strict hierarchy; that is, recursion is not allowed. In the event that a physical entity is contained by more than one physical entity (e.g. double-wide modules), this object should identify the containing entity with the lowest value of entPhysicalIndex.	entPhysicalContainedIn (1.3.6.1.2.1.47.1.1.1.1.1.4)	integer32 (0..2147483647)	integer

Attribute (CLI Attribute Name)	Description	SNMP Object ID	SNMP Syntax	CLI Syntax
Class (class)	An indication of the general hardware type of the physical entity. If no appropriate standard registration identifier exists for this physical entity, then the value 'other(1)' is returned. If the value is unknown by this agent, then the value 'unknown(2)' is returned.	entPhysicalClass (1.3.6.1.2.1.47.1.1.1.1.5)	<pre> INTEGER { other(1), unknown(2), chassis(3), backplane(4), container(5), -- e.g. chassis slot or daughter-card holder powerSupply(6) , fan(7), sensor(8), module(9), -- e.g. plug-in card or daughter-card port(10), stack(11), -- e.g. stack of multiple chassis entities cpu(12) } </pre>	{other, unknown, chassis, backplane, container, power-supply, fan, sensor, module, port, stack, cpu}

Attribute (CLI Attribute Name)	Description	SNMP Object ID	SNMP Syntax	CLI Syntax
Parent Relative Position (rel-pos)	<p>An indication of the relative position of this child component among all its sibling components. Sibling components are defined as entPhysicalEntries that share the same instance values of each of the entPhysicalContainedIn and entPhysicalClass objects.</p> <p>An NMS can use this object to identify the relative ordering for all sibling components of a particular parent (identified by the entPhysicalContainedIn instance in each sibling entry).</p>	entPhysicalParentRelPos (1.3.6.1.2.1.47.1.1.1.1.6)	integer32 (-1..2147483647)	integer
Physical Name (name)	<p>The textual name of the physical entity. The value of this object should be the name of the component as assigned by the local device and should be suitable for use in commands entered at the device's `console`. This might be a text name (e.g. `console`) or a simple component number (e.g. port or module number, such as `1`), depending on the physical component naming syntax of the device.</p> <p>If there is no local name, or if this object is otherwise not applicable, then this object contains a zero-length string.</p>	entPhysicalName (1.3.6.1.2.1.47.1.1.1.1.7)	character string	character string

Attribute (CLI Attribute Name)	Description	SNMP Object ID	SNMP Syntax	CLI Syntax
Physical Hardware Revision (hw-rev)	<p>The vendor-specific hardware revision string for the physical entity. The preferred value is the hardware revision identifier actually printed on the component itself (if present).</p> <p>Note that if revision information is stored internally in a non-printable (e.g. binary) format, then the agent must convert such information to a printable format, in an implementation-specific manner.</p> <p>If no specific hardware revision string is associated with the physical component, or if this information is unknown to the agent, then this object will contain a zero-length string.</p>	entPhysicalHardwareRev (1.3.6.1.2.1.47.1.1.1.1.8)	character string	character string
Physical Firmware Revision (fw-rev)	<p>The vendor-specific firmware revision string for the physical entity.</p> <p>Note that if revision information is stored internally in a non-printable (e.g. binary) format, then the agent must convert such information to a printable format, in an implementation-specific manner.</p> <p>If no specific firmware revision string is associated with the physical component, or if this information is unknown to the agent, then this object will contain a zero-length string.</p>	entPhysicalFirmwareRev (1.3.6.1.2.1.47.1.1.1.1.9)	character string	character string

Attribute (CLI Attribute Name)	Description	SNMP Object ID	SNMP Syntax	CLI Syntax
Physical Software Revision (sw-rev)	<p>The vendor-specific software revision string for the physical entity.</p> <p>Note that if revision information is stored internally in a non-printable (e.g. binary) format, then the agent must convert such information to a printable format, in an implementation-specific manner.</p> <p>If no specific software revision string is associated with the physical component, or if this information is unknown to the agent, then this object will contain a zero-length string.</p>	entPhysicalSoftwareRev (1.3.6.1.2.1.47.1.1.1.1.10)	character string	character string
Physical Serial Number (serial)	<p>The vendor-specific serial number string for the physical entity. The preferred value is the serial number string actually printed on the component itself (if present).</p> <p>Not every physical component will have a serial number, or even need one. Physical entities for which the associated value of the entPhysicalIsFRU object is equal to 'false(2)' (e.g. the repeater ports within a repeater module), do not need their own unique serial number. An agent does not have to provide write access for such entities, and may return a zero-length string.</p>	entPhysicalSerialNum (1.3.6.1.2.1.47.1.1.1.1.11)	character string (up to 32 chars)	character string (up to 32 chars)

Attribute (CLI Attribute Name)	Description	SNMP Object ID	SNMP Syntax	CLI Syntax
Physical Manufacturer Name (mfg-name)	<p>The name of the manufacturer of this physical component. The preferred value is the manufacturer name string actually printed on the component itself (if present).</p> <p>If the manufacturer name string associated with the physical component is unknown to the agent, then this object will contain a zero-length string.</p>	entPhysicalMfgName (1.3.6.1.2.1.47.1.1.1.1.12)	character string	character string
Physical Model Name (model-name)	<p>The vendor-specific model name identifier string associated with this physical component. The preferred value is the customer-visible part number, which may be printed on the component itself.</p> <p>If the model name string associated with the physical component is unknown to the agent, then this object will contain a zero-length string.</p>	entPhysicalModelName (1.3.6.1.2.1.47.1.1.1.1.13)	character string	character string
Field Replaceable Unit Indicator (fru)	<p>This object indicates whether or not this physical entity is considered a 'field replaceable unit' by the vendor. If this object contains the value 'true(1)' then this entPhysicalEntry identifies a field replaceable unit. For all entPhysicalEntries that represent components permanently contained within a field replaceable unit, the value 'false(2)' should be returned for this object.</p>	entPhysicalIsFRU (1.3.6.1.2.1.47.1.1.1.1.16)	{true (1), false(2)}	{replaceable not-replaceable}

Attribute (CLI Attribute Name)	Description	SNMP Object ID	SNMP Syntax	CLI Syntax
Last Change Time (last-change)	The value of sysUpTime at the time the configuration of the entity has changed.	1.3.6.1.2.1.47.1.4.1 (entLastChangeTime)	TimeTicks	ddd:hh:mm:ss, wherein ddd – decimal integer representing days (it may include arbitrary number of digits), hh – two-digit decimal integer representing hours of day [0..23], mm – two-digit decimal integer representing minutes of hour [0..59], ss – two-digit decimal integer representing seconds of minute [0..59].

Physical Inventory Entities

Figure 12-2 shows all physical inventory entities and their relationship.

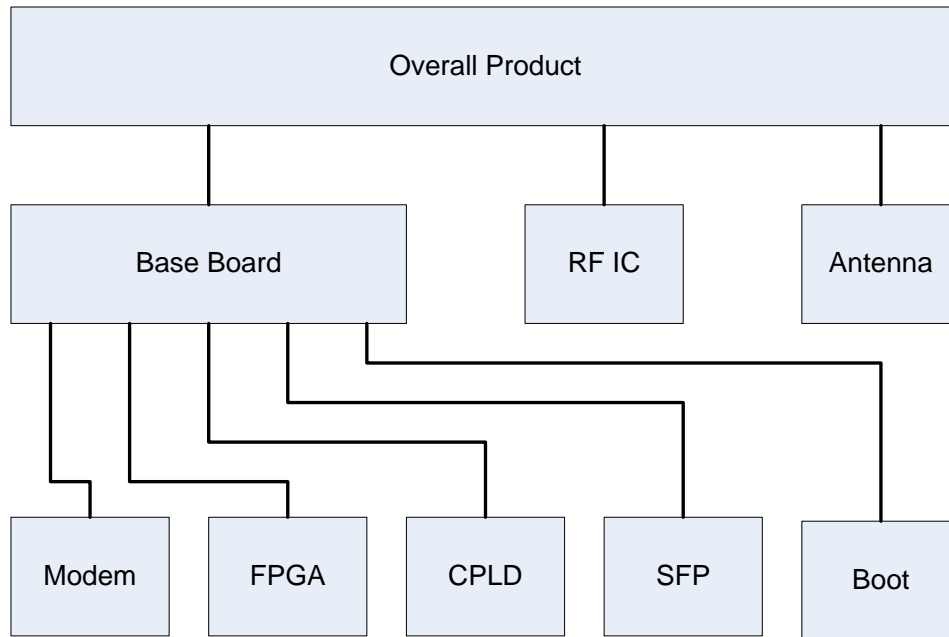


Figure 12-2: Physical Inventory Hierarchy Scheme

Overall Product

Table 12-10: Overall Product

Attribute	Value
Inventory Index	1
Descriptor	"Netronics NetBeam 1Gx"
Contained In	0
Class	chassis
Parent Relative Position	-1
Name	"NB-1G1"
Hardware Revision	empty
Firmware Revision	empty
Software Revision	empty
Serial Number	<to be read in runtime>
Manufacturer Name	"Netronics"

Attribute	Value
Model Name	"NB-1G1"
Field Replaceable Unit Indicator	replaceable

Antenna

Table 12-11: Antenna

Attribute	Value
Inventory Index	2
Descriptor	"Netronics Antenna"
Contained In	1
Class	other
Parent Relative Position	0
Name	"Antenna"
Hardware Revision	empty
Firmware Revision	empty
Software Revision	empty
Serial Number	empty
Manufacturer Name	"Netronics"
Model Name	empty
Field Replaceable Unit Indicator	not-replaceable

RF IC

Table 12-12: RF IC

Attribute	Value
Inventory Index	3
Descriptor	"Netronics NB-1G1 RF IC"
Contained In	1
Class	module

Attribute	Value
Parent Relative Position	1
Name	"RF IC"
Hardware Revision	<to be read in runtime>
Firmware Revision	empty
Software Revision	empty
Serial Number	<to be read in runtime>
Manufacturer Name	"Netronics"
Model Name	empty
Field Replaceable Unit Indicator	not-replaceable

Base Band Board

Table 12-13: Base Band Board

Attribute	Value
Inventory Index	4
Descriptor	"Netronics NB-1G1 Base Band Board"
Contained In	1
Class	container
Parent Relative Position	2
Name	"Base Band Board"
Hardware Revision	<to be read in runtime>
Firmware Revision	empty
Software Revision	empty
Serial Number	<to be read in runtime>
Manufacturer Name	"Netronics"
Model Name	empty
Field Replaceable Unit Indicator	not-replaceable

Modem*Table 12-14: Modem*

Attribute	Value
Inventory Index	5
Descriptor	"Netronics NB-1G1 Modem"
Contained In	4
Class	module
Parent Relative Position	0
Name	"Modem"
Hardware Revision	<to be read in runtime>
Firmware Revision	empty
Software Revision	empty
Serial Number	empty
Manufacturer Name	"Netronics"
Model Name	empty
Field Replaceable Unit Indicator	not-replaceable

FPGA*Table 12-15: FPGA*

Attribute	Value
Inventory Index	6
Descriptor	"Netronics NB-1G1 FPGA"
Contained In	4
Class	module
Parent Relative Position	1
Name	"FPGA"
Hardware Revision	empty
Firmware Revision	<to be read in runtime>
Software Revision	empty

Attribute	Value
Serial Number	empty
Manufacturer Name	empty
Model Name	empty
Field Replaceable Unit Indicator	not-replaceable

CPLD*Table12-16: CPLD*

Attribute	Value
Inventory Index	7
Descriptor	"Netronics NB-1G1 CPLD"
Contained In	4
Class	module
Parent Relative Position	2
Name	"CPLD"
Hardware Revision	empty
Firmware Revision	<to be read in runtime>
Software Revision	empty
Serial Number	empty
Manufacturer Name	"Netronics"
Model Name	empty
Field Replaceable Unit Indicator	not-replaceable

SFP*Table 12-17: SFP*

Attribute	Value
Inventory Index	7
Descriptor	"Netronics NB-1G1 SFP"

Attribute	Value
Contained In	4
Class	module
Parent Relative Position	3
Name	"SFP"
Hardware Revision	<to be read in runtime>
Firmware Revision	empty
Software Revision	empty
Serial Number	empty
Manufacturer Name	<to be read in runtime>
Model Name	empty
Field Replaceable Unit Indicator	replaceable

Boot

Table 12-18: Boot

Attribute	Value
Inventory Index	8
Descriptor	"Netronics NB-1G1 Boot"
Contained In	4
Class	module
Parent Relative Position	5
Name	"Boot"
Hardware Revision	empty
Firmware Revision	empty
Software Revision	<to be read in runtime>
Serial Number	empty
Manufacturer Name	"Netronics"
Model Name	empty
Field Replaceable Unit Indicator	not-replaceable

Radio Object Attributes

RF Object Attributes

This section lists configurable RF attributes (Table 12-19) and read-only RF attributes (Table 12-21) separately.

Table 12-19: Configurable RF Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Default
Number of Channels (num-of-channels)	The maximum allowed bandwidth, expressed in MHz.	rfNumOfChannels (1.3.6.1.4.1.31926.2.1.1.2)	1..2	2
Operational Frequency (frequency)	The frequency at which the RF operates, expressed in MHz.	rfOperationalFrequency (1.3.6.1.4.1.31926.2.1.1.4)	50000..80000	74000
Role (role)	The current role of the RF device.	rfRole (1.3.6.1.4.1.31926.2.1.1.5)	master, slave	master
Mode Selector (mode)	The current RF device operating mode. When static mode is specified, only certain sub-parameter combinations produce a valid result. When an invalid combination is specified on the command line, the CLI responds with: "the modulation does not exist in the modulation table."	rfModeSelector (1.3.6.1.4.1.31926.2.1.1.6)	adaptive, static, alignment When static mode is specified, additional sub-parameters are used to define additional relevant operating characteristics, as shown in Table 12-20.	adaptive
CINR Low (cinr-low)	The lowest acceptable value for CINR, expressed in decibels (dB).	rfCinrLow (1.3.6.1.4.1.31926.2.1.1.13)	-128..127	0
CINR Interval (cinr-interval)	The interval used to determine the value for CINR, expressed in milliseconds.	rfCinrInterval (1.3.6.1.4.1.31926.2.1.1.15)	0..2000	0

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Default
RSSI Interval (rssi-interval)	The interval used to determine the value for RSSI, expressed in milliseconds.	rfRssiInterval (1.3.6.1.4.1.31926.2.1.1.16)	0..2000	0
RX Link ID (rx-link-id)	The RF receive link ID.	rfRxLinkId (1.3.6.1.4.1.31926.2.1.1.22)	Varies	0
TX Link ID (tx-link-id)	The RF transmit link ID.	rfTxLinkId (1.3.6.1.4.1.31926.2.1.1.23)	Varies	0
Transmit Asymmetry (tx-asymmetry)	Percentage of the TX part in the airframe.		integer. CLI syntax is {10tx-90rx 25tx-75rx 50tx-50rx 75tx-25rx 90tx-10rx}.	50tx-50rx
Lowest Modulation	Dropping below the Lowest Mode causes RF link failure, wherein: mod = Modulation type. {QPSK, QAM16, QAM64} scnum = The number of subchannels [1..4] rep = Repetition {1, 2, 4} fec = FEC {0.5, 0.67, 0.8} frame = The frame number to be used for the execution of the new modulation (only in static mode) The mode must be present in the Modulation Table.			

Table 12-20: Static Mode Sub-Parameters

Argument	Description	Values	SNMP Reference
modu	modulation	QPSK, QAM16, QAM64	rfModulationType (1.3.6.1.4.1.31926.2.1.1.7)
num-subch	Number of subchannels	1..4	rfNumOfSubchannels (1.3.6.1.4.1.31926.2.1.1.8)
repeat	Repetitions	1, 2, 4	rfNumOfRepetitions (1.3.6.1.4.1.31926.2.1.1.9)
fec	FEC rate	0.5, 0.67, 0.8	rfFecRate (1.3.6.1.4.1.31926.2.1.1.10)

Table 12-21: Read-Only RF Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Default
Channel Width (channel-width)	The channel width, expressed in MHz.	rfChannelWidth (1.3.6.1.4.1.31926.2.1.1.3)	250	N/A
RX State (rx-state)	The current state of the RF receive link.	rfRxState (1.3.6.1.4.1.31926.2.1.1.25)	1= Sync 2= Search countdown 3= Found countdown 4= Normal	N/A
TX State (tx-state)	The current state of the RF transmit link.	rfTxState (1.3.6.1.4.1.31926.2.1.1.24)	1= Sync 2= Search countdown 3= Found countdown 4= Normal	N/A
Operational State (operational)	The current operating state of the RF device.	rfOperationalState (1.3.6.1.4.1.31926.2.1.1.17)	up, down	N/A
Average CINR	Average carrier to interference noise ratio [-6..30]. This object is only accessible via SNMP.	rfAverageCinr (1.3.6.1.4.1.31926.2.1.1.18)	integer	
Average RSSI	Average received signal strength indication, measured in DB [-100..-60]. This object is only accessible via SNMP.	rfAverageRssi (1.3.6.1.4.1.31926.2.1.1.19)	integer	
RF Temperature (rf-temperature)	The current temperature of the RF device.	rfTemperature (1.3.6.1.4.1.31926.2.1.1.26)	Varies	N/A

Radio Statistics

Table 12-22: Radio Statistic Descriptions

Attribute (CLI Attribute Name)	Description	SNMP Object ID
Incoming Octets (in-	The total number of octets received	rflnOctets (1.3.6.1.4.1.31926.2.2.1.1)

Attribute (CLI Attribute Name)	Description	SNMP Object ID
octets)	from the RF link.	
Incoming Idle Octets (in-idle-octets)	The total number of octets received from the RF link while idle.	rfInIdleOctets (1.3.6.1.4.1.31926.2.2.1.2)
Incoming Good Octets (in-good-octets)	The number of good octets received from the RF link.	rfInGoodOctets (1.3.6.1.4.1.31926.2.2.1.3)
Incoming Erroneous Octets (in-errored-octets)	The number of received erred octets from the RF link.	rfInErroredOctets (1.3.6.1.4.1.31926.2.2.1.4)
Outgoing Octets (out-octets)	The total number of octets transmitted to the RF link.	rfOutOctets (1.3.6.1.4.1.31926.2.2.1.5)
Outgoing Idle Octets (out-idle-octets)	The total number of octets transmitted to the RF link while idle.	rfOutIdleOctets (1.3.6.1.4.1.31926.2.2.1.6)
Incoming Packets (in-pkts)	The total number of packets received from the RF link.	rfInPkts (1.3.6.1.4.1.31926.2.2.1.7)
Incoming Good Packets (in-good-pkts)	The total number of good packets received from the RF link.	rfInGoodPkts (1.3.6.1.4.1.31926.2.2.1.8)
Incoming Erroneous Packets (in-errored-pkts)	The total number of erred packets received from the RF link.	rfInErroredPkts (1.3.6.1.4.1.31926.2.2.1.9)
Incoming Lost Packets (in-lost-pkts)	The total number of lost packets received from the RF link.	rfInLostPkts (1.3.6.1.4.1.31926.2.2.1.10)
Outgoing Packets (out-pkts)	The total number of packets transmitted to the RF link.	rfOutPkts (1.3.6.1.4.1.31926.2.2.1.11)

Table 12-23: Statistics History for the RF Object

usrHistoryObjectIndex	usrHistoryObjectVariable
1	rfInOctets (1.3.6.1.4.1.31926.2.2.1.1)
2	rfInIdleOctets (1.3.6.1.4.1.31926.2.2.1.2)
3	rfInGoodOctets (1.3.6.1.4.1.31926.2.2.1.3)
4	rfInErroredOctets (1.3.6.1.4.1.31926.2.2.1.4)
5	rfOutOctets (1.3.6.1.4.1.31926.2.2.1.5)
6	rfOutIdleOctets (1.3.6.1.4.1.31926.2.2.1.6)
7	rfInPkts (1.3.6.1.4.1.31926.2.2.1.7)
8	rfInGoodPkts (1.3.6.1.4.1.31926.2.2.1.8)

9	rfInErroredPkts (1.3.6.1.4.1.31926.2.2.1.9)
10	rfInLostPkts (1.3.6.1.4.1.31926.2.2.1.10)
11	rfOutPkts (1.3.6.1.4.1.31926.2.2.1.11)

Encryption Object Attributes

Table 12-24: Encryption Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access	Default
Encryption	Encryption mode. This attribute is only visible to an admin user.		{disabled static-key}	disabled	Encryption
Static Key	This is the only key (that is to say the current key and next key are always the same and equal to this configured key).		string of 32 hexadecimal digits	92E3C2802 0570998E7 4B 41C06A58 BB40	Static Key

Connectivity Fault Management (CFM) Object Attributes

Maintenance Domain (MD) Object Attributes

Table 12-25: Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access	Default
MD Index	Value to be used as the index of the MA table entries for this MD when the management entity wants to create a new entry in that table. An MD Index entry cannot be deleted if it is used as the key in MA, MEP, Received CCM Presentation, Peer MEP, or LTR DB.	dot1agCfmMdIndex (1.3.111.2.802.1.1.8.1.5.2.1.1)	Integer	N/A	
Name (name)	Each MD has a unique name. This facilitates easy identification of administrative responsibility for each Maintenance Domain.	dot1agCfmMdName (1.3.111.2.802.1.1.8.1.5.2.1.1)	{dns-like mac-and-unit string} “<name according to format>”	RC	Empty
Format (format)	Represents a type (and the resulting format) of the MD Name. Can be up to 256 characters.	dot1agCfmMdFormat (1.3.111.2.802.1.1.8.1.5.2.1.2)	{dns-like mac-and-unit string} “<name according to format>”	RC	String
Level (level)	Represents the Maintenance Domain Level.	dot1agCfmMdMlevel (1.3.111.2.802.1.1.8.1.5.2.1.4)	0..7	RC	0
MHF Creation (mhf-creation)	Enumerated value indicating whether the management entity can create MHFs (MIP Half Function) for this MD.	dot1agCfmMdMhfCreation (1.3.111.2.802.1.1.8.1.5.2.1.5)	{none default explicit}	RC	None
MHF ID Permission (mhf-permission)	Enumerated value indicating what, if anything, is to be included in the Sender ID TLV (21.5.3) transmitted by MPs configured in this MD.	dot1agCfmMdMhfIdPermission (1.3.111.2.802.1.1.8.1.5.2.1.6)	{none chassis mgmg chassis-mgmg}	RC	None

Maintenance Association (MA) Object Attributes

Table 12-26: MA Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access	Default
MD Index	Value to be used as the index of the MA table MD Domain when the management entity wants to create a new entry in that table. Entering the MD Index for an MA enables use of the common command structure.	dot1agCfmMdIndex (1.3.111.2.802.1.1.8.1.5.2.1.1)	Integer	N/A	
MA Index	Index of the MA table (dot1agCfmMdMaNextIndex), which needs to be inspected to find an available index for row-creation. An MA Index entry cannot be deleted if it is used as the key in MA, MEP, Received CCM Presentation, Peer MEP Create, or LTR DB.	dot1agCfmMaIndex (1.3.111.2.802.1.1.8.1.6.1.1.1)		N/A	
MA Format (format)	A value that represents a type (and the resulting format) of the MD Name.	dot1agCfmMaNetFormat(1.3.111.2.802.1.1.8.1.6.1.1.2)	{vid string vpnid}	RW	vid
MA Name (name)	The short MA name. The type/format of this object is determined by the value of the dot1agCfmMaNetNameType object. This name must be unique within an MD.	dot1agCfmMaNetName (1.3.111.2.802.1.1.8.1.6.1.1.3)	{vid string vpnid} “<name according to format>”	RC	1
Interval (interval)	The interval to be used between CCM transmissions by all MEPs in the MA.	1.3.111.2.802.1.1.8.1.6.1.1.4 (dot1agCfmMaNetCcmInterval)	{3.3ms 10ms 100ms 1s 10s 1min 10min}	RC	1s

Component MA Object Attributes

Table 12-27: Component MA Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access	Default
Component	The bridge component within the system to which the information in this dot1agCfmMaCompEntry applies. The component must be defined in the Bridge component table (Table 12-38).	ieee8021CfmMaComponentId (1.3.111.2.802.1.1.8.1.6.4.1.1)	component <comp-id-list>	N/A	
MD Index	Value to be used as the index of the MA table entries for the MD when the management entity wants to create a new entry in that table. Entering the MD Index for a Component MA enables use of the common command structure.	dot1agCfmMdIndex (1.3.111.2.802.1.1.8.1.5.2.1.1)	Integer	N/A	
MA Index	Index of the MA table (dot1agCfmMdMaNextIndex), which needs to be inspected to find an available index for row-creation. An MA Index entry cannot be deleted if it is used as the key in MA, MEP, Received CCM Presentation, Peer MEP Create, or LTR DB.	dot1agCfmMaIndex (1.3.111.2.802.1.1.8.1.6.1.1.1)		N/A	

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access	Default
Service Selector (vlan)	Service Selector identifier to which the MP is attached, or 0, if none. The type of the Service Selector is defined by the value of ieee8021CfmMaCompPrimaryS electorType. In the current implementation the type is always VLAN ID. Thus the Service Selector is the Primary VLAN ID with which the Maintenance Association is associated, or 0 if the MA is not attached to any VID. The VLAN must be defined in the VLAN Table (<i>Table 12-44</i>).	ieee8021CfmMaCompPrimarySelectorOrNone (1.3.111.2.802.1.1.8.1.6.4.1.3)	{none 1..4094}	RC	None
MHF Creation (mhf-creation)	Enumerated value indicating whether the management entity can create MHFs (MIP Half Function) for this MA.	ieee8021CfmMaCompMhfCreation (1.3.111.2.802.1.1.8.1.6.4.1.4)	{mhf-creation none default explicit defer}	RC	defer
MHF ID Permission (mhf-permission)	Enumerated value indicating what, if anything, is to be included in the Sender ID TLV (21.5.3) transmitted by MPs configured in this MA.	ieee8021CfmMaCompIdPermission (1.3.111.2.802.1.1.8.1.6.4.1.5)	{mhf-permission none chassis mgmg chassis-mgmg}	RC	None

Maintenance End Point (MEP) Object Attributes

This section includes separate tables for configurable MEP object attributes (*Table 12-28*) and read-only MEP object attributes (*Table 12-29*).

Table 12-28: Configurable MEP Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access	Default
MD Index	Value to be used as the index of the MA table entries for the MD when the management entity wants to create a new entry in that table. Entering the MD Index for a MEP enables use of the common command structure.	dot1agCfmMdIndex (1.3.111.2.802.1.1.8.1.5.2.1.1)	Integer	N/A	
MA Index	Index of the MA table (dot1agCfmMdMaNextIndex), which needs to be inspected to find an available index for row-creation. An MA Index entry cannot be deleted if it is used as the key in MA, MEP, Received CCM Presentation, Peer MEP Create, or LTR DB.	dot1agCfmMaIndex (1.3.111.2.802.1.1.8.1.6.1.1.1)		N/A	
MEPID	An integer that is unique for all the MEPs in the same MA that identifies a specific MA End Point. Adding an entry with a specific MEPID creates associated entries in the Peer MEP DB. Similarly, deleting a specific MEPID entry causes deletion of association entries in the Peer MEP DB.	1.3.111.2.802.1.1.8.1.7.1.1.1 (dot1agCfmMep Identifier)	integer	RC	1
Interface (interface)	The index of the interface either of a Bridge Port, or an aggregated IEEE 802.1 link within a Bridge Port, to which the MEP is attached. The component associated with the MEP interface must exist in the Component MA Table. In addition, only one MEP can be defined for the same combination of Interface, Direction and	1.3.111.2.802.1.1.8.1.7.1.1.2 (dot1agCfmMepIf Index)	{eth0 eth1 eth2 host}	RC	eth1

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access	Default
	Primary VLAN.				
Direction (dir)	The direction in which the MEP is facing on the Bridge Port. Only one MEP can be defined for the same combination of Interface, Direction and Primary VLAN.	1.3.111.2.802.1.1.8.1.7 .1.1.3 (dot1agCfmMep Direction)	{up down}	RC	down
Primary VLAN (vlan)	An integer indicating the Primary VID of the MEP. A value of 0 indicates that either the Primary VID is that of the MEP's MA, or that the MEP's MA is not associated with any VID. The associated VLAN must be defined in the VLAN Table (<i>Table 12-44</i>). In addition, only one MEP can be defined for the same combination of Interface, Direction and Primary VLAN.	1.3.111.2.802.1.1.8.1.7 .1.1.4 (dot1agCfmMep PrimaryVid)	0..4094	RC	0
Administrative State (admin-state)	The administrative state of the MEP. True (active) indicates that the MEP is to function normally; False (inactive) indicates that the MEP is to cease functioning.	1.3.111.2.802.1.1.8.1.7 .1.1.5 (dot1agCfmMep Active)	{active inactive}	RC	Inactive
CCI (cci)	If set to True, the MEP will generate CCM messages.	1.3.111.2.802.1.1.8.1.7 .1.1.7 (dot1agCfmMepCciEnabled)	{enabled disabled}	RC	disabled
Message Priority (msg-prio)	The priority value for CCMs and LTMs transmitted by the MEP. The default value is the highest priority value allowed passing through the Bridge Port for any of the MEP VIDs. The Management Entity can obtain the default value for this variable from the priority regeneration table by extracting the highest priority value in this table on this MEP's Bridge Port (1 is lowest, followed by 2, then 0, then 3-7).	1.3.111.2.802.1.1.8.1.7 .1.1.8 (dot1agCfmMep CcmLtmPriority)	0..7	RC	0

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access	Default
Lowest Primary Defect (low-defect)	An integer specifying the lowest priority defect that is allowed to generate a fault alarm.	1.3.111.2.802.1.1.8.1.7 .1.1.10 (dot1agCfmMep LowPrDef)	{all-def mac-rem- err-xcon rem-err- xcon err- xcon xcon no- xcon}	RC	mac- rem-err- xcon
Alarm Time (alarm-time)	The time that a defect must be present before a fault alarm is issued.	1.3.111.2.802.1.1.8.1.7 .1.1.11 (dot1agCfmMep FngAlarmTime)	250..000	RC	250
Reset Time (reset-time)	The time that a defect must be absent before resetting a fault alarm.	1.3.111.2.802.1.1.8.1.7 .1.1.12 (dot1agCfmMep FngResetTime)	250..1000	RC	1000
LBM Destination MAC Address (lbm-dst-mac)	A unicast destination MAC address specifying the target MAC address field to be transmitted. This address will be used if the value for the column dot1agCfmMepTransmitLbmDestIsMepId is False.	1.3.111.2.802.1.1.8.1.7 .1.1.27 (dot1agCfmMepTrans mitLbmDestMacAdres s)	Mac address in the form NN-NN- NN-NN- NN-NN, where N is a hexadeci mal number (for example 00-AF-DD- 1E-2D-A3)	RC	00-00- 00-00- 00-00
LBM Destination MEPID (lbm-dst-mepid)	The MA End Point Identifier of another MEP in the same MA to which the LBM is to be sent. This address will be used if the value of the column dot1agCfmMepTransmitLbmDestIsMepId is True.	1.3.111.2.802.1.1.8.1.7 .1.1.28 (dot1agCfmMepTrans mitLbmDestMepId)	Integer	RC	0
LBM Destination Type (lbm-dst-type)	The destination type indicator for purposes of Loopback transmission, either the unicast destination MAC address of the target MEP or the MEPID of the	1.3.111.2.802.1.1.8.1.7 .1.1.29 (dot1agCfmMepTrans mitLbmDestIs MepId)	{mac mepid}	RC	mac

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access	Default
	target MEP.				
Number of LBMs to Transmit (lbm-tx-num)	The number of Loopback messages to be transmitted.	1.3.111.2.802.1.1.8.1.7 .1.1.30 (dot1agCfmMepTransmitLbmMessages)	1..1024	RC	1
LBM Data TLV (lbm-tx-data)	An arbitrary amount of data to be included in the Data TLV, if the Data TLV is selected to be sent.	1.3.111.2.802.1.1.8.1.7 .1.1.31 (dot1agCfmMepTransmitLbmDataTlv)	String of hexadecimal digits. Two digits constitute an octet therefore the length must be even.	RC	Empty String
LBM Transmit VLAN Priority (lbm-tx-prio)	Priority. 3-bit value to be used in the VLAN tag, if present in the transmitted frame.	1.3.111.2.802.1.1.8.1.7 .1.1.32 (dot1agCfmMepTransmitLbmVlanPriority)	0..7	RC	0
LBM Transmit VLAN Drop Eligibility (lbm-tx-drop)	Drop Enable bit value to be used in the VLAN tag, if present in the transmitted frame. For more information about VLAN Drop Enable, see IEEE 802.1ad.	1.3.111.2.802.1.1.8.1.7 .1.1.33 (dot1agCfmMepTransmitLbmVlanDropEnable)	{enable disable}	RC	Enable
LTM Destination MAC Address (ltm-dst-mac)	A unicast destination MAC address specifying the target MAC Address Field to be transmitted. This address is used if the value of the column dot1agCfmMepTransmitLtmTargetsMepld is False.	1.3.111.2.802.1.1.8.1.7 .1.1.38 (dot1agCfmMepTransmitLtmTargetMacAddress)	MAC address in the form NN-NN-NN-NN-NN-NN, where N is a hexadecimal number (for example 00-AF-DD-1E-2D-A3)	RC	00-00-00-00-00-00
LTM Destination MEPID	The MA End Point Identifier of another MEP in the same MA to which the LTM is to be sent. This	1.3.111.2.802.1.1.8.1.7 .1.1.39 (dot1agCfmMepTrans	0..8191	RC	0

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access	Default
(itm-dst-mepid)	address is used if the value of the column dot1agCfmMepTransmitLtmTargetIsMepid is True.	mitLtmTargetIsMepid)			
LTM Destination Type (itm-dst-type)	The destination type indicator for purposes of LTM transmission, either the unicast destination MAC address of the target MEP or the MEPID of the target MEP.	1.3.111.2.802.1.1.8.1.7 .1.1.40 dot1agCfmMepTransmitLtmTargetIsMepid	{mac mepid}	RC	mac
LTM Transmit TTL (itm-tx-ttl)	The TTL field indicates the number of hops remaining to the LTM. Decrement by one by each Linktrace Responder that handles the LTM. The value returned in the LTR is one less than that received in the LTM. If the LTM TTL is 0 or 1, the LTM is not forwarded to the next hop, and if 0, no LTR is generated.	1.3.111.2.802.1.1.8.1.7 .1.1.41 (dot1agCfmMepTransmitLtmTtl)	0..250	RC	64

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access	Default
Transmit LBM Status (lbn-tx-status)	<p>A Boolean flag set to True by the Bridge Port to indicate that another LBM may be transmitted. Reset to False by the MEP Loopback Initiator State Machine.</p> <p>Setting the status to True (tx-pending) initiates LBM sending.</p> <p>The number of LBM sent is defined by the Number of LBM to Transmit. After transmitting the specified number of LBM the value automatically changes to False (tx-idle). Note that if the Number of LBM to Transmit is zero the status immediately turns to False (tx-idle).</p>	1.3.111.2.802.1.1.8.1.7 .1.1.26 (dot1agCfmMep TransmitLbm Status)	{tx-pending, tx-idle}	RC	tx-idle
Transmit LTM Status (ltm-tx-status)	<p>A Boolean flag set to True by the Bridge Port to indicate that another LTM may be transmitted. Reset to False by the MEP Linktrace Initiator State Machine.</p> <p>Setting the status to True (tx-pending) initiates LTM sending. Only one message is sent, after which the value automatically changes to False (tx-idle). Note that if the Number of LTM to Transmit is zero, the status immediately turns to False (tx-idle).</p>	1.3.111.2.802.1.1.8.1.7 .1.1.36 (dot1agCfmMep TransmitLtmStatus)	{tx-pending, tx-idle}	RC	tx-idle

Table 12-29: Read-Only MEP Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax
Fault Notification Generator State (fng-state)	The current state of the MEP Fault Notification Generator state machine. See 802.1ag clauses 12.14.7.1.3:f and 20.35.	1.3.111.2.802.1.1.8.1.7.1.1.6 (dot1agCfmMepFngState)	{reset defect report-defect defect-reported defect-clearing}
MEP MAC Address (mac)	MAC address of the MEP.	1.3.111.2.802.1.1.8.1.7.1.1.9 (dot1agCfmMepMacAddress)	MAC address in the form NN-NN-NN-NN-NN-NN, where N is a hexadecimal number (for example 00-AF-DD-1E-2D-A3)
Highest Priority Defect (high-defect)	The highest priority defect that has been present since the MEPs Fault notification Generator State Machine was last in the reset state.	1.3.111.2.802.1.1.8.1.7.1.1.13 (dot1agCfmMepHighestPriorityDefect)	{none rdi-ccm mac-status remote-ccm error-ccm xcon-ccm}
MEP Defects (defects)	A vector of Boolean error conditions from IEEE 802.1ag Table 20-1, any of which may be true. A MEP can detect and report a number of defects, and multiple defects can be present at the same time.	1.3.111.2.802.1.1.8.1.7.1.1.14 (dot1agCfmMepDefects)	Any combination of: {rdi-ccm, mac-status, remote-ccm, error-ccm, xcon-ccm}
CCM Sequence Errors (ccm-seq-errors)	The total number of out-of-sequence CCMs that have been received from all remote MEPs.	1.3.111.2.802.1.1.8.1.7.1.1.17 (dot1agCfmMepCcmSequenceErrors)	Integer
CCM Transmit Counter (ccm-tx)	Total number of Continuity Check messages transmitted.	1.3.111.2.802.1.1.8.1.7.1.1.18 (dot1agCfmMepCciSentCcms)	Integer
LBM Transmit Result (lbm-tx-result)	Indicates the result of the operation.	1.3.111.2.802.1.1.8.1.7.1.1.34 (dot1agCfmMepTransmitLbmResultOK)	{ok not-ok}

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax
LBM Transmit Sequence Number (lbr-tx-sn)	The Loopback Transaction Identifier (dot1agCfmMepNextLbmTransId) of the first LBM sent. The value returned is undefined if dot1agCfmMepTransmitLbmResult OK is False.	1.3.111.2.802.1.1.8.1.7.1.1.35 (dot1agCfmMepTransmitLbmSeqNumber)	Integer
LBM Next Sequence Number (lbr-next-sn)	Next sequence number/transaction identifier to be sent in a Loopback message. This sequence number can be zero when it wraps around.	1.3.111.2.802.1.1.8.1.7.1.1.19 (dot1agCfmMepNextLbmTransId)	Integer
Incoming In Order LBR Counter (lbr-in-order)	Total number of valid, in-order Loopback Replies received.	1.3.111.2.802.1.1.8.1.7.1.1.20 (dot1agCfmMepLbrIn)	Integer
Incoming Out of Order LBR Counter (lbr-out-of-order)	The total number of valid, out-of-order Loopback Replies received.	1.3.111.2.802.1.1.8.1.7.1.1.21 (dot1agCfmMepLbrInOutOfOrder)	Integer
Transmit LBR Counter (lbr-tx)	Total number of Loopback Replies transmitted.	1.3.111.2.802.1.1.8.1.7.1.1.25 (dot1agCfmMepLbrOut)	Integer
LTM Next Sequence Number (ltm-next-sn)	Next transaction identifier/sequence number to be sent in a Linktrace message. This sequence number can be zero when it wraps around.	1.3.111.2.802.1.1.8.1.7.1.1.23 (dot1agCfmMepLtmNextSeqNumber)	Integer
Unexpected Incoming LTR (ltr-unexpected)	The total number of unexpected LTRs received.	1.3.111.2.802.1.1.8.1.7.1.1.24 (dot1agCfmMepUnexpltrIn)	Integer
LTM Transmit Result (ltm-tx-result)	Indicates the result of the operation.	1.3.111.2.802.1.1.8.1.7.1.1.42 (dot1agCfmMepTransmitLtmResult)	{ok not-ok}
LTM Transmit Sequence Number (ltm-tx-sn)	The LTM Transaction Identifier (dot1agCfmMepLtmNextSeqNumber) of the LTM sent. The value returned is undefined if dot1agCfmMepTransmitLtmResult is False.	1.3.111.2.802.1.1.8.1.7.1.1.43 (dot1agCfmMepTransmitLtmSeqNumber)	Integer

CCM Message Object Attributes

Table 12-30: CCM Message Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access	Default
MD Index	Value to be used as the index of the MA table entries for the MD when the management entity wants to create a new entry in that table. An entry cannot be created if a corresponding MD Index does not exist.	dot1agCfmMdIndex (1.3.111.2.802.1.1.8.1.5.2.1.1)	Integer	N/A	
MA Index	Index of the MA table (dot1agCfmMdMaNextIndex), which needs to be inspected to find an available index for row-creation. An entry cannot be created if a corresponding MA Index does not exist.	dot1agCfmMaIndex (1.3.111.2.802.1.1.8.1.6.1.1.1)		N/A	
MEPID	An integer that is unique for all the MEPs in the same MA that identifies a specific MA End Point. An entry cannot be created if a corresponding MEPID does not exist.	1.3.111.2.802.1.1.8.1.7.1.1.1 (dot1agCfmMepIdentifier)	integer	RC	1
Last Error Condition CCM (last-error-ccm)	The last-received CCM that triggered an DefErrorCCM fault.	1.3.111.2.802.1.1.8.1.7.1.1.15 (dot1agCfmMepErrorCcmLastFailure)		RO	
Last Xcon Condition CCM (last-xcon-ccm)	The last-received CCM that triggered an DefErrorCCM fault.	1.3.111.2.802.1.1.8.1.7.1.1.16 (dot1agCfmMepXconCcmLastFailure)		RO	

Peer MEP Object Attributes

Table 12-31: Peer MEP Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access
MD Index	Value to be used as the index of the MA table entries for the MD when the management entity wants to create a new entry in that table. An entry cannot be created if a corresponding MD Index does not exist.	dot1agCfmMdIndex (1.3.111.2.802.1.1.8.1.5.2.1.1)	Integer	N/A
MA Index	Index of the MA table (dot1agCfmMdMaNextIndex), which needs to be inspected to find an available index for row-creation. An entry cannot be created if a corresponding MA Index does not exist.	dot1agCfmMaIndex (1.3.111.2.802.1.1.8.1.6.1.1.1)		N/A
Peer MEPID	Integer identifying a specific Peer MA End Point.	dot1agCfmMaMepListIdentifier (1.3.111.2.802.1.1.8.1.6.3.1.1)	1..8191	N/A

Peer MEP Database Attributes

Table 12-32: Peer MEP Database Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access
MD Index	Value to be used as the index of the MA table entries for the MD when the management entity wants to create a new entry in that table. An entry cannot be created if a corresponding MD Index does not exist.	dot1agCfmMdIndex (1.3.111.2.802.1.1.8.1.5.2.1.1)	Integer	N/A
MA Index	Index of the MA table (dot1agCfmMdMaNextIndex), which needs to be inspected to find an available index for row-creation. An entry cannot be created if a corresponding MA Index does not exist.	dot1agCfmMaIndex (1.3.111.2.802.1.1.8.1.6.1.1.1)		N/A
MEPID	An integer that is unique for all the MEPs in the same MA that identifies a specific MA End Point. An entry cannot be created if a corresponding MEPID does not exist.	1.3.111.2.802.1.1.8.1.7.1.1.1 (dot1agCfmMepIdentifier)	integer	RC
Peer MEPID	Integer identifying a specific Peer Maintenance Association End Point.	1.3.111.2.802.1.1.8.1.7.3.1.1 (dot1agCfmMepDbRMepIdentifier)	1..8191	N/A

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access
Peer MEP State (state)	The operational state of the remote MEP IFF State machines. This state machine monitors the reception of valid CCMs from a remote MEP with a specific MEPID. It uses a timer that expires in 3.5 times the length of time indicated by the dot1agCfmMaNetCcmInterval object.	1.3.111.2.802.1.1.8.1.7.3.1.2 (dot1agCfmMepDbRMepState)	{idle start failed ok}	RO
Peer MEP Failed OK Time (failed-ok-time)	The time (SysUpTime) at which the peer MEP state machine last entered either the Failed or OK state.	1.3.111.2.802.1.1.8.1.7.3.1.3 (dot1agCfmMepDbRMepFailedOkTime)	ddd:hh:mm:ss, wherein ddd – decimal integer representing days (it may include arbitrary number of digits), hh – two-digit decimal integer representing hours of day [0..23], mm – two-digit decimal integer representing minutes of hour [0..59], ss – two-digit decimal integer representing seconds of minute [0..59].	RO

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access
Peer MEP MAC Address (mac)	The MAC address of the remote MEP.	1.3.111.2.802.1.1.8.1.7.3.1.4 (dot1agCfmMepDbMacAddress)	MAC address in the form NN-NN-NN-NN-NN-NN, where N is a hexadecimal number (for example 00-AF-DD-1E-2D-A3)	RO
Remote Defect Indication (rdi)	State of the RDI bit in the last received CCM. On corresponds to True.	1.3.111.2.802.1.1.8.1.7.3.1.5 (dot1agCfmMepDbRdi)	{on off}	RO
Peer Port Status (port-status)	An enumerated value of the Port status TLV received in the last CCM from the remote MEP or the default value psNoPortStateTLV indicating either no CCM has been received, or that no port status TLV was received in the last CCM.	1.3.111.2.802.1.1.8.1.7.3.1.6 (dot1agCfmMepDbPortStatusTlv)	{none blocked up}	RO
Peer Interface Status (if-status)	An enumerated value of the Interface status TLV received in the last CCM from the remote MEP or the default value isNoInterfaceStatus TLV indicating either no CCM has been received, or that no interface status TLV was received in the last CCM.	1.3.111.2.802.1.1.8.1.7.3.1.7 (dot1agCfmMepDbInterfaceStatusTlv)	{none up down testing unknown dormant not-present lower-layer-down}	RO
Peer Chassis ID Subtype (chassis-id-subtype)	This object specifies the format of the Chassis ID received in the last CCM.	1.3.111.2.802.1.1.8.1.7.3.1.8 (dot1agCfmMepDbChassisIdSubtype)	{chassis-comp if-alias port-comp mac net-addr if-name}	RO
Peer Chassis ID (chassis-id)	The Chassis ID. The format of this object is determined by the value of the dot1agCfmLtrChassisIdSubtype object.	1.3.111.2.802.1.1.8.1.7.3.1.9 (dot1agCfmMepDbChassisId)	Hexadecimal string	RO
Management Address Domain	The TDomain that identifies the type and format of the	1.3.111.2.802.1.1.8.1.7.3.1.10 (dot1agCfmMepDbMan	{snmp-udp,	RO

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access
(mng-addr-domain)	related dot1agCfmMepDbManAddress object, used to access the SNMP agent of the system transmitting the CCM. Received in the CCM Sender ID TLV from that system.	AddressDomain)	snmp-ieee802}	
Management Address (mng-addr)	The TAddress that can be used to access the SNMP agent of the system transmitting the CCM, received in the CCM Sender ID TLV from that system. If the related object dot1agCfmMepDbManAddressDomain contains the value 'zeroDotZero', this object dot1agCfmMepDbManAddress must have a zero-length OCTET STRING as a value.	1.3.111.2.802.1.1.8.1.7.3.1.11 (dot1agCfmMepDbManAddress)	IP Address – dotted notation. MAC Address - NN-NN-NN-NN-NN-NN, where N is a hexadecimal number (for example 00-AF-DD-1E-2D-A3), the rest – hexadecimal string	RO

LTR Object Attributes

Table 12-33: LTR Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access
MD Index	Value to be used as the index of the MA table entries for the MD when the management entity wants to create a new entry in that table. An entry cannot be created if a corresponding MD Index does not exist.	dot1agCfmMdIndex (1.3.111.2.802.1.1.8.1.5.2.1.1)	Integer	N/A
MA Index	Index of the MA table (dot1agCfmMdMaNextIndex), which needs to be inspected to find an available index for row-creation. An entry cannot be	dot1agCfmMaIndex (1.3.111.2.802.1.1.8.1.6.1.1.1)		N/A

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access
	created if a corresponding MA Index does not exist.			
MEPID	An integer that is unique for all the MEPs in the same MA that identifies a specific MA End Point. An entry cannot be created if a corresponding MEPID does not exist.	1.3.111.2.802.1.1.8.1.7.1.1.1 (dot1agCfmMepIdentifier)	integer	RC
LTR SN	Transaction identifier/sequence number returned by a previous transmit linktrace message command, indicating which LTM's response is going to be returned.	1.3.111.2.802.1.1.8.1.7.2.1.1 (dot1agCfmLtrSeq Number)	Integer	N/A
LTR Received TTL (rx-ttl)	TTL field value for a returned LTR	1.3.111.2.802.1.1.8.1.7.2.1.3 (dot1agCfmLtrTtl)	0..250	RO
LTR Forwarded Indicator (ltr-forward)	Indicates if an LTM was forwarded by the responding MP, as returned in the 'FwdYes' flag of the flags field.	1.3.111.2.802.1.1.8.1.7.2.1.4 (dot1agCfmLtrForwarded)	{forwarded not-forwarded}	RO
LTR Relay Indicator (relay-action)	Possible values the Relay action field can take.	1.3.111.2.802.1.1.8.1.7.2.1.8 (dot1agCfmLtrRelay)	{hit fdb mpdb}	RO
LTR Chassis ID Subtype (chassis-id-subtype)	This object specifies the format of the Chassis ID returned in the Sender ID TLV of the LTR, if any.	1.3.111.2.802.1.1.8.1.7.2.1.9 (dot1agCfmLtrChassisId Subtype)	{chassis-comp if-alias port-comp mac net-addr if-name}	RO
LTR Chassis ID (chassis-id)	The Chassis ID returned in the Sender ID TLV of the LTR, if any. The format of this object is determined by the value of the dot1agCfmLtrChassisIdSubtype object.	1.3.111.2.802.1.1.8.1.7.2.1.10 (dot1agCfmLtrChassisId)	Format in accordance with LTR Chassis ID Subtype. A hexadecimal string is used if no format is known.	RO
LTR Management Address Domain (mng-addr-	The TDomain that identifies the type and format of the related dot1agCfmMepDbManAddress object, used to access the SNMP	1.3.111.2.802.1.1.8.1.7.2.1.11 (dot1agCfmLtrMan AddressDomain)	{snmp-udp, snmp-ieee802}	RO

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access
domain)	agent of the system transmitting the LTR.			
LTR Management Address (mng-addr)	The TAddress that can be used to access the SNMP agent of the system transmitting the LTR, received in the LTR Sender ID TLV from that system.	1.3.111.2.802.1.1.8.1.7.2.1.12 (dot1agCfmLtrManAddress)	IP Address – dotted notation. MAC Address - NN-NN-NN-NN-NN-NN, where N is a hexadecimal number (for example 00-AF-DD-1E-2D-A3), the rest – hexadecimal string	RO
LTR Ingress Action (ingr-action)	The value returned in the Ingress Action Field of the LTM. The value ingNoTlv(0) indicates that no Reply Ingress TLV was returned in the LTM.	1.3.111.2.802.1.1.8.1.7.2.1.13 (dot1agCfmLtrIngress)	{none ok down blocked vid}	RO
LTR Ingress MAC Address (ingr-mac)	MAC address returned in the ingress MAC address field. If the dot1agCfmLtrIngress object contains the value ingNoTlv(0), then the contents of this object are meaningless.	1.3.111.2.802.1.1.8.1.7.2.1.14 (dot1agCfmLtrIngressMac)	MAC Address - NN-NN-NN-NN-NN-NN, where N is a hexadecimal number (for example 00-AF-DD-1E-2D-A3), the rest – hexadecimal string	RO
LTR Ingress Port ID Subtype (ingr-port-id-subtype)	Format of the Ingress Port ID. If the dot1agCfmLtrIngress object contains the value ingNoTlv(0), then the contents of this object are meaningless.	1.3.111.2.802.1.1.8.1.7.2.1.15 (dot1agCfmLtrIngressPortIdSubtype)	{if-alias port-comp mac net-addr if-name agent-circuit-id local}	RO
LTR Ingress Port ID	Ingress Port ID. The format of this	1.3.111.2.802.1.1.8.1.7.2.1.	Format in	RO

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access
(ingr-port-id)	object is determined by the value of the dot1agCfmLtrIngressPortIdSubtype object. If the dot1agCfmLtrIngress object contains the value ingNoTlv(0), then the contents of this object are meaningless.	16 (dot1agCfmLtrIngressPortId)	accordance with LTR Chassis ID Subtype. A hexadecimal string is used if no format is known.	
LTR Egress Action (egr-action)	The value returned in the Egress Action Field of the LTM. The value egrNoTlv(0) indicates that no Reply Egress TLV was returned in the LTM.	1.3.111.2.802.1.1.8.1.7.2.1.17 (dot1agCfmLtrEgress)	{none ok down blocked vid}	RO
LTR Egress MAC Address (egr-mac)	MAC address returned in the ingress MAC address field. If the dot1agCfmLtrIngress object contains the value ergNoTlv(0), then the contents of this object are meaningless.	1.3.111.2.802.1.1.8.1.7.2.1.18 (dot1agCfmLtrEgressMac)	MAC Address - NN-NN-NN-NN-NN-NN, where N is a hexadecimal number (for example 00-AF-DD-1E-2D-A3), the rest – hexadecimal string	RO
LTR Egress Port ID Subtype (egr-port-id-subtype)	Format of the Egress Port ID. If the dot1agCfmLtrEgress object contains the value ergNoTlv(0), then the contents of this object are meaningless.	1.3.111.2.802.1.1.8.1.7.2.1.19 (dot1agCfmLtrEgressPortIdSubtype)	{if-alias port-comp mac net-addr if-name agent-circuit-id local}	RO
LTR Ingress Port ID (egr-port-id)	Egress Port ID. The format of this object is determined by the value of the dot1agCfmLtrEgressPortIdSubtype object. If the dot1agCfmLtrEgress object contains the value ergNoTlv(0), then the contents of this object are meaningless.	1.3.111.2.802.1.1.8.1.7.2.1.20 (dot1agCfmLtrEgressPortId)	Format in accordance with LTR Chassis ID Subtype. A hexadecimal string is used if no format is known.	RO
LTR Terminal MEP	A boolean value stating whether	1.3.111.2.802.1.1.8.1.7.2.1.	{on off}	RO

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access
(trm-mep)	the forwarded LTM reached a MEP enclosing its MA, as returned in the Terminal MEP flag of the Flags field.	5 (dot1agCfmLtrTerminalMep)		
LTR Last Egress Identifier (last-egr-id)	An octet field holding the Last Egress Identifier returned in the LTR Egress Identifier TLV of the LTR. The Last Egress Identifier identifies the MEP Linktrace Initiator that originated, or the Linktrace Responder that forwarded, the LTM to which this LTR is the response. This is the same value as the Egress Identifier TLV of that LTM.	1.3.111.2.802.1.1.8.1.7.2.1.6 (dot1agCfmLtrLastEgressIdentifier)	Eight pairs hexadecimal digits, each pair separated by dashes: NN-NN-NN-NN-NN-NN-NN, for example: 00-00-00-AF-DD-1E-2D-A3	RO
LTR Next Egress Identifier (next-egr-id)	An octet field holding the Next Egress Identifier returned in the LTR Egress Identifier TLV of the LTR. The Next Egress Identifier identifies the Linktrace Responder that transmitted this LTR, and can forward the LTM to the next hop. This is the same value as the Egress Identifier TLV of the forwarded LTM, if any. If the FwdYes bit of the Flags field is false, the contents of this field are undefined, i.e. any value can be transmitted, and the field is ignored by the receiver.	1.3.111.2.802.1.1.8.1.7.2.1.7 (dot1agCfmLtrNextEgressIdentifier)	Eight pairs hexadecimal digits, each pair separated by dashes: NN-NN-NN-NN-NN-NN-NN, for example: 00-00-00-AF-DD-1E-2D-A3	RO

Network Object Attributes

Ethernet Interface Attributes

This section lists configurable Ethernet Interface attributes (*Table 12-34*) and read-only Ethernet Interface attributes (*Table 12-35*) separately.

Table 12-34: Configurable Ethernet Interface Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Default
Administrative Status (admin)	The desired operational state of the interface, expressed as an integer. There are no restrictions for adding an interface in the Down state to VLAN egress and untagged lists, or to FDP.	ifAdminStatus (1.3.6.1.2.1.2.2.1.7)	1 = Up (operational) 2 = Down (not operational) When the set command is used together with the admin attribute, the device will report the administrative status of the device immediately after command execution. For example: Interface eth7 admin set down	1 (Up)
State Trap (trap)	An integer that indicates whether linkUp/linkDown traps should be generated for this interface.	ifLinkDownTrap Enable (1.3.6.1.2.1.31.1.1.1.14)	1 = Enabled 2 = Disabled	1 = Enabled
Alias (alias)	A text string containing an 'alias' name for the interface, as assigned by a network manager. This value provides a non-volatile 'handle' for the interface. The value of this attribute must be unique with respect to other interface aliases.	ifAlias (1.3.6.1.2.1.31.1.1.1.18)	Up to 256 characters. When the set command is used together with the alias attribute, only one interface can be addressed per invocation.	0 length string

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Default
Ethernet Type (eth-type)	<p>This object identifier represents the operational type of MAU that the administrator has assigned.</p> <p>If auto-negotiation is not enabled or is not implemented for this MAU, the value of this attribute is used to determine the operational type of the MAU. In such a case, a set command is used to force the MAU into the specified operating mode.</p> <p>If auto-negotiation is implemented and enabled for this MAU, the operational type of the MAU is determined by auto-negotiation, and the value of this attribute denotes the type to which the MAU automatically revert if/when auto-negotiation is later disabled.</p>	<p>ifMauDefaultType (1.3.6.1.2.1.26.2.1.1.11)</p> <p>Part of ifMauTable (1.3.6.1.2.1.26.2.1)</p>	For possible values, refer to <i>Table 12-36</i> .	1000fd

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Default
Auto Negotiation Admin Status (auto-neg)	<p>An integer representing the administrative state of auto-negotiation signaling for the interface.</p> <p>Setting this attribute to enabled causes the auto-negotiation signaling ability of the interface to be operational.</p> <p>Setting this attribute to disabled causes the auto-negotiation signaling ability of the interface to be non-operational, and no auto-negotiation signaling will be performed. In such a case, the MAU type is forced to the value that has been assigned in the eth-type attribute.</p>	<p>ifMauAutoNegAdmin Status (1.3.6.1.2.1.26.5.1.1.1)</p> <p>Part of ifMauAutoNegTable (1.3.6.1.2.1.26.5.1)</p>	<p>1 = Enabled 2 = Disabled</p>	Enabled
Loopback Mode (loopback-mode)	Loopback mode operation.	N/A	{disabled external internal}	Disabled
Loopback Timeout (loopback-timeout)	Loopback timeout, expressed in seconds.	N/A	Integer	Disabled

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Default
Alarm Propagation Mode (alarm-propagation)	Alarm propagation mode is used to define system behavior in case of a link failure	N/A	<p>The possible alarm propagation values are:</p> <p>Disabled = No propagation is performed.</p> <p>Backward = The Ethernet link is set to down if the radio link is down or if a “Peer Eth Down” notification has been received at the radio interface.</p> <p>Forward = A “Peer Eth Down” notification is sent to the other end of the radio link if the Ethernet link is down.</p> <p>Both Directions = Both Backward and Forward alarm propagation is performed.</p>	Disabled

Table 12-35: Read-Only Ethernet Interface Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Default
Description (description)	A text string describing the interface. This value generally includes the manufacturer’s name, the product name and the interface hardware and software versions.	ifDescr (1.3.6.1.2.1.2.1.2)	Variable text	{“Netronics NB-1G1 Host”; “ Netronics NB-1G1 Eth 0”; “ Netronics NB-1G1 Eth 1”; “ Netronics NB-1G1 Eth 2”}

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Default
MTU Size (mtu)	<p>The size of the largest packet which can be sent/received on the interface, specified in octets.</p> <p>For interfaces that are used for transmitting network datagrams, this is the size of the largest network datagram that can be sent on the interface.</p>	ifMtu (1.3.6.1.2.1.2.2.1.4)	9216	9216
MAC Address (mac-addr)	The address of the interface at its protocol sub-layer.	ifPhysAddress (1.3.6.1.2.1.2.2.1.6)	host0 = <mac_base_address> (read from hardware) rf0 = <mac_base_address> + 1 eth1 = <mac_base_address> + 2 eth2 = <mac_base_address> + 3	NN-NN-NN-NN-NN-NN where NN is a hexadecimal number (for example 00-AF-DD-1E-2D-A3)

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Default
Operational Status (operational)	<p>The current operational state of the interface, expressed as an integer.</p> <p>When this attribute is in the Down state, but the Administrative Status attribute (admin) is in the Up state, then a fault condition is presumed to exist on the interface.</p> <p>If the Administrative Status attribute (admin) is in the Down state, then the operational attribute should also be in the Down state.</p> <p>If the Administrative Status attribute (admin) changes to the Up state, then the operational attribute should also change to the Up state if the interface is ready to transmit and receive network traffic. It should remain in the Down state if and only if there is a fault condition that prevents the interface from going to the Up state.</p>	ifOperStatus (1.3.6.1.2.1.2.2.1.8)	1 = Up (Ready to pass packets) 2 = Down (Not available for host0)	N/A

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Default
Last Change Time (lastChange)	The value of sysUpTime at the time the interface entered its current operational state. If the current operational state was entered prior to the last reinitialization of the local network management subsystem, then the value of this attribute is 0.	ifLastChange (1.3.6.1.2.1.2.2.1.9)	ddd:hh:mm:ss, where: ddd =decimal integer representing days (it can be an arbitrary number of digits) hh =two-digit decimal integer representing the hours of a day [0..23] mm =two-digit decimal integer representing minutes of an hour [0..59] ss =two-digit decimal integer representing seconds of a minute [0..59]	N/A
Name (name)	The name of the interface.	ifName (1.3.6.1.2.1.31.1.1.1)	host, eth0, eth1, eth2	None
Connector (connector)	An integer that indicates whether the interface sub-layer has a physical connector.	ifConnectorPresent (1.3.6.1.2.1.31.1.1.17)	1 =True (Connector is present) 2=False True (Connector is absent)	N/A

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Default
Actual Ethernet Type (eth-act-type)	This object identifier represents the operational type of the MAU, as determined by either: The result of the auto-negotiation process, or If auto-negotiation is not enabled or is not implemented for this MAU, then the value that has been assigned in the eth-type attribute is used.	ifMauType (1.3.6.1.2.1.26.2.1.1.3) Part of ifMauTable (1.3.6.1.2.1.26.2.1)	For possible values, refer to <i>Table 12-36</i> .	1000fd

Table 12-36: Ethernet Type Values

Value	Description
10hd	dot3MauType10BaseTHD (1.3.6.1.2.1.26.4.10)
10fd	dot3MauType10BaseTFD (1.3.6.1.2.1.26.4.11)
100hd	dot3MauType100BaseTXHD (1.3.6.1.2.1.26.4.15)
100fd	dot3MauType100BaseTXFD (1.3.6.1.2.1.26.4.16)
1000hd	dot3MauType1000BaseTHD (1.3.6.1.2.1.26.4.29)
1000fd	dot3MauType1000BaseTFD (1.3.6.1.2.1.26.4.30)
1000sxhd	dot3MauType1000BaseXHD (1.3.6.1.2.1.26.4.21)
1000sxfd	dot3MauType1000BaseXFD (1.3.6.1.2.1.26.4.22)
1000lxhd	dot3MauType1000BaseXHD (1.3.6.1.2.1.26.4.21)
1000lxfd	dot3MauType1000BaseXFD (1.3.6.1.2.1.26.4.22)

Ethernet Statistic Descriptions

Table 12-37: Ethernet Statistics

Attribute (CLI Attribute Name)	Description	SNMP Object ID
Incoming Octets (in-octets)	The total number of octets received on the interface, including framing characters.	ifInOctets 1.3.6.1.2.1.2.2.1.10
Incoming Unicast Packets (in-ucast-pkts)	The number of unicast packets received on the interface.	ifInUcastPkts 1.3.6.1.2.1.2.2.1.11
Discarded Incoming Packets (in-discards)	The number of packets which were chosen to be discarded due to RX FIFO full.	ifInDiscards 1.3.6.1.2.1.2.2.1.13
Erroneous Incoming Packets (in-errors)	The number of received erred packets.	ifInErrors 1.3.6.1.2.1.2.2.1.14
Outgoing Octets (out-octets)	The total number of octets transmitted out of the interface, including framing characters.	ifOutOctets 1.3.6.1.2.1.2.2.1.16
Outgoing Unicast Packets (out-ucast-pkts)	The number of unicast packets transmitted out of the interface.	ifOutUcastPkts 1.3.6.1.2.1.2.2.1.17
Discarded Outgoing Packets (out-discards)	The number of outbound packets which were chosen to be discarded due to excessive collision or excessive deferral.	ifOutDisacrd 1.3.6.1.2.1.2.2.1.19
Erroneous Outgoing Packets (out-errors)	The number of outbound packets that could not be transmitted because of errors.	ifOutErrors 1.3.6.1.2.1.2.2.1.20
Incoming Multicast Packets (in-mcast-pkts)	The number of multicast packets received on the interface.	ifInMulticastPkts 1.3.6.1.2.1.31.1.1.1.2
Incoming Broadcast Packets (in-bcast-pkts)	The number of broadcast packets received on the interface.	ifInBroadcastPkts 1.3.6.1.2.1.31.1.1.1.3
Outgoing Multicast Packets (out-mcast-pkts)	The number of multicast packets transmitted out of the interface.	ifOutMulticastPkts 1.3.6.1.2.1.31.1.1.1.4
Outgoing Broadcast Packets (out-bcast-pkts)	The number of broadcast packets transmitted out of the interface.	ifOutBroadcastPkts 1.3.6.1.2.1.31.1.1.1.5

Bridge Object Attributes

Table 12-38: Bridge Object Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
Component ID	Used to distinguish between the multiple virtual bridge instances within a PBB. The component id = s1 cannot be supplied as an argument when using the <code>clear</code> command.	ieee8021BridgeBaseComponentId (1.3.111.2.802.1.1.2.1.1.1.1.1)		None ¹	
Bridge Address (addr)	The MAC address to be used by this bridge when it must be referred to in a unique fashion. It is the address of the Host interface (interface 1). The MAC base address is the same as the address of the Host interface 1.	ieee8021BridgeBaseBridgeAddress (1.3.111.2.802.1.1.2.1.1.1.1.2)	Octet string	RO	NN-NN-NN-NN-NN-NN where : NN is a hexadecimal number (for example 00-AF-DD-1E-2D-A3).
Component Number of Ports (num-ports)	The number of ports controlled by this bridging entity.	ieee8021BridgeBaseNumPorts (1.3.111.2.802.1.1.2.1.1.1.1.3)	Integer (32 bit)	RO	Always 2 for C-components Always 4 for S-components

¹ This attribute is used as the index key to ieee8021BridgeBaseTable (1.3.111.2.802.1.1.2.1.1).

Bridging Port Object Attributes

Table 12-39: Bridging Port Object Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
Component ID	The component identifier is used to distinguish between the multiple virtual bridge instances within a PB. Component identifiers must be defined in the Bridge Component table (Table 12-38).	ieee8021BridgeBasePort ComponentId (1.3.111.2.802.1.1.2.1.1.4.1.1)	<comp-id-list>	N/A	N/A
Bridge Base Port	The number of the port for which this entry contains bridge management information. In the CLI port name is used instead of number	ieee8021BridgeBasePort (1.3.111.2.802.1.1.2.1.1.4.1.2)	host, eth0, eth1, eth2, s1, c2, c3, c4	N/A	N/A
Bridge Port Interface Index (interface)	The interface that corresponds to this port.	ieee8021BridgeBasePortIf Index (1.3.111.2.802.1.1.2.1.1.4.1.3)	host, eth0, eth1, eth2 In the current version, when a port is bound to an internal interface (s1, c1, c2, c3, c4) then the value for this attribute is 0.	RO	N/A

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
Bridge Port PVID (pvid)	The port-level VLAN ID that is assigned to untagged frames or Priority-Tagged frames received on the port. Each PVID must correspond to a valid VLAN on the corresponding component. In practice, this means that the VLAN must already be configured in the VLAN Table for the component before its VID can be assigned as the PVID for a port.	ieee8021QBridgePvid (1.3.111.2.802.1.1.4.1.4.5.1.1)	1..4094	RW	1
Bridge Port Default Priority (Prio)	An integer indicating the default ingress User Priority for this port. This attribute is relevant for protocols that do not support native User Priority, such as Ethernet.	ieee8021BridgePortDefaultUserPriority (1.3.111.2.802.1.1.2.1.3.1.1.1)	0..7	RW	0
Bridge Port Acceptable Frame Types (admit)	The frame types that are accepted on the port and assigned to a VID. VID assignment is based on the PVID and VID Set for the port. When this is admitTagged(3), the device will discard untagged frames or Priority-Tagged frames received on this port. When admitAll(1), untagged frames or Priority-Tagged frames received on this port will be accepted. This attribute does not affect VLAN-independent	ieee8021QbridgePortAcceptableFrameTypes (1.3.111.2.802.1.1.4.1.4.5.1.2)	All = Admit all untagged and priority-tagged frames. Untagged = Admit untagged frames only. Tagged = Admit tagged frames only.	RW	All

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
	<p>Bridge Protocol Data Unit (BPDU) frames, such as MVRP or Spanning Tree Protocol (STP). However, it does affect VLAN-dependent BPDU frames, such as MMRP.</p> <p>If ingress filtering is enabled on the same port, then accepting untagged frames only is not compatible, since the combination effectively leads to discarding all frames on the port.</p>				
Bridge Port Ingress Filtering (filter)	<p>The ingress filtering state of the port.</p> <p>When Enabled, the device discards incoming frames for VLANs that do not include the port in its Member Set. When disabled, the device accepts all incoming frames to the port.</p> <p>If untagged frames are admitted on the port, then ingress filtering is not compatible, since the combination effectively leads to discarding all frames on the port.</p>	ieee8021QbridgePortIngressFiltering (1.3.111.2.802.1.1.2.1.4.5.3)	Enabled Disabled	RW	Disabled

Outgoing Queue Object Attributes*Table 12-40: Outgoing Queue Attributes*

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access
Interface Name	Interface name		{eth0 eth1 eth2 rf all}	N/A
Queue ID	Queue ID		Range from 1 to 8	N/A
Tx Frame Counter	The counter of the per-Q transmitted frames.		tx 0..264	RO
Drop Frame Counter	The counter of the per-Q dropped frames.		drop 0..264	RO

Incoming Queue Object Attributes*Table 12-41: Incoming Queue Attributes*

Attribute (CLI Attribute Name)	Description	Syntax	Access
Interface Name	Interface name	rf (currently only one, but may be extended in the future)	N/A
Queue ID	Queue ID	Range from 1 to 4	N/A
Good Frame Counter	The counter of the per-Q received good frames.	good 0..264	RO
Erroneous Frame Counter	The counter of the per-Q received erroneous frames.	error 0..264	RO
Lost Frame Counter	The counter of the per-Q lost rx frames.	lost 0..264	RO

IP Object Attributes

Table 12-42: IP Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	SNMP Syntax	Value	Access	Default
IP Index	The index to the IP address table.	N/A	N/A	1..4	N/A	
IP Address (ip-addr)	The IP address to which this entry's addressing information pertains. The address type of this object is specified in ipAddressAddrType. All IP addresses in the table must be different.	1.3.6.1.2.1.4.34.1.2 (ipAddressAddr)	InetAddress	ip address in the form X.X.X.X where X is a decimal number from 0 to 255 (for example 10.0.15.74).	RC	0.0.0.0
IP Address Mask (mask)	The subnet to which the IP address belongs.	N/A – not part of the MIB		ip mask in the form X.X.X.X where X is a decimal number from 0 to 255 (for example 255.255.255.0)	RC	255.255.255.0
IP Default Router Address	The IP address of the default router represented by this row.	1.3.6.1.2.1.4.37.1.2 (ipDefaultRouterAddress)	InetAddress	ip address in the form X.X.X.X where X is a decimal number from 0 to 255 (for example 10.0.15.74)	NA	0.0.0.0
VLAN (vlan)	VLAN assigned to the IP. Two different IP addresses cannot be assigned the same VLAN (therefore all VLANs in the table must be different).	N/A		0..4094	RC	

VLAN Common Table Attributes

Table 12-43: VLAN Common Attributes

Attribute (CLI Attribute Name)	Description	CLI Object ID	Access	Default
Component ID	Used to distinguish between the multiple virtual bridge instances within a PB. Component identifiers must be defined in the Bridge Component table (<i>Table 12-38</i>).	ieee8021QBridgeComponentId 1.3.111.2.802.1.1.4.1.1.1.1.1		s1
VLAN Version Number (version)	The version number of IEEE 802.1Q that this device supports.	ieee8021QbridgeVlanVersion Number (1.3.111.2.802.1.1.4.1.1.1.1.2)	RO	version1
Maximum VLAN ID (max vid)	The maximum IEEE 802.1Q VLAN-ID that this device supports. Possible values are 1..4094.	ieee8021QBridgeMaxVlanId (1.3.111.2.802.1.1.4.1.1.1.1.3)	RO	n/a
Maximum Number of VLANs (max-num)	The maximum number of IEEE 802.1Q VLANs that this device supports. Possible values are 1..4094.	ieee8021QBridgeMaxSupportedVlans (1.3.111.2.802.1.1.4.1.1.1.1.4)	RO	n/a
Current Number of VLANs (curr-num)	The number of IEEE 802.1Q VLANs currently active on the network. This attribute is updated each time a VLAN is added or deleted from the network. Possible values are 1..4094.	ieee8021QBridgeNumVlans (1.3.111.2.802.1.1.4.1.1.1.1.5)	RO	n/a

VLAN Table Attributes

Table 12-44: VLAN Table Attributes

Attribute (CLI Attribute Name)	Description	CLI Object ID	Access	Default
Component Identifier	Used to distinguish between multiple virtual bridge instances within a PB. Component identifiers must be defined in the Bridge Component table (<i>Table 12-38</i>).	ieee8021QbridgeVlanStaticComponentId (1.3.111.2.802.1.1.4.1.4.3.1.1)	N/A	s1
VLAN ID	The VLAN-ID referring to this VLAN.	ieee8021QbridgeVlanStaticVlanIndex (1.3.111.2.802.1.1.4.1.4.3.1.2)	N/A	1
Egress Ports Set (egress)	The set of ports that are permanently assigned by management to the egress list for this VLAN. Only those ports that belong to the corresponding component can be included in the set.	ieee8021QbridgeVlanStaticEgressPorts (1.3.111.2.802.1.1.4.1.4.3.1.4)	RC	Empty
Untagged Ports Set (Untagged)	The set of ports that should transmit egress packets for this VLAN as untagged. This set is allowed only for S-VLANs. This set must be subset of the Egress Ports Set attribute.	ieee8021QbridgeVlanStaticUntaggedPorts (1.3.111.2.802.1.1.4.1.4.3.1.4)	RC	Empty
FDB ID (fdb-id)	The ID of the filtering database used for this VLAN. Possible values are 1..64.	ieee8021QBridgeVlanFdbId (1.3.111.2.802.1.1.4.1.4.2.1.4)	RC	1
Per-VLAN Incoming Packets (in-pkts)	The number of valid frames received by this port from its segment that were classified as belonging to this VLAN. Note: A frame received on this port is counted by this object only if it is for a protocol being processed by the local forwarding process for this VLAN. This object includes received bridge management frames that are classified as belonging to this VLAN (e.g. MMRP, but not MVRP or STP).	ieee8021QbridgeTpVlanPortInFrames (1.3.111.2.802.1.1.4.1.4.6.1.1)	RO	n/a

Attribute (CLI Attribute Name)	Description	CLI Object ID	Access	Default
Per-VLAN Outgoing Packets (out-pkts)	The number of valid frames transmitted by this port to its segment from the local forwarding process for this VLAN. This object includes bridge management frames originated by this device that are classified as belonging to this VLAN (e.g. MMRP, but not MVRP or STP). Possible values are 0..264.	ieee8021QbridgeTpVlanPort Out Frames (1.3.111.2.802.1.1.4.1.4.6.1.2)	RO	n/a
Per-VLAN Dropped Packets (drop-pkts)	The number of valid frames received by this port from its segment that were classified as belonging to this VLAN and that were discarded due to VLAN-related reasons. This object refers specifically to the IEEE 802.1Q counters for Discard Inbound and Discard on Ingress Filtering. Possible values are 0..264.	ieee8021QbridgeTpVlanPortIn Discards (1.3.111.2.802.1.1.4.1.4.6.1.3)	RO	n/a

C-LAN Registration Table Attributes

Table 12-45: C-LAN Registration Table Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
Bridge Port	The bridge port for the C-VLAN Registration entry. The bridge port specified in the command must match the Component ID in the VLAN Table (Table 12-44). For example, if the Component ID is c4 then the port must be external port 4).	ieee8021BridgeBasePort (1.3.111.2.802.1.1.2.1.1.4.1.2)	<ext-bridge-port-list>	N/A	N/A

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
C-VID	The C-VID of this C-VLAN Registration entry. The VID must be defined in the VLAN Table (<i>Table 12-44</i>). The bridge component port specified in the command must match the Component ID in the VLAN Table. For example, if the Component ID is c4 then the port must be external4.	ieee8021PbCvid RegistrationCvid (1.3.111.2.802.1.1.5.1.2.1.1)	1..4094	N/A	N/A
S-VID (svlan)	The S-VID of this C-VLAN Registration entry. This value will be added to the C-tagged frames of the C-VID. The VID must be defined in the VLAN Table (<i>Table 12-44</i>) for an S-component.	ieee8021PbCvid RegistrationSVid (1.3.111.2.802.1.1.5.1.2.1.2)	1..4094	RC	N/A
Untagged CEP (untag-cep)	A flag indicating whether this C-VID should be carried untagged at the CEP.	ieee8021PbCvid RegistrationUntaggedCep (1.3.111.2.802.1.1.5.1.2.1.4)	Yes = The C-VID will be untagged No = The C-VID will be tagged	RC	No
Untagged PEP (untag-pep)	A flag indicating if this C-VID should be carried untagged at the PEP.	ieee8021PbCvid RegistrationUntaggedPep (1.3.111.2.802.1.1.5.1.2.1.3)	Yes = The C-VID will be untagged No = The C-VID will be tagged	RC	No

PEP Virtual Port Table Attributes

Table 12-46: PEP Virtual Port Table Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
Bridge Port (bridge-port)	The bridge port for the PEP Virtual Port entry. The Bridge Port specified in the command must be an internal port (PEP) that belongs to the corresponding C-component.	ieee8021BridgeBasePort (1.3.111.2.802.1.1.4.1.2)	s1	N/A	N/A
PEP S-VID (s-vid)	The 12-bit S-VID that is associated with the PEP.	ieee8021PbEdgePortSVid (1.3.111.2.802.1.1.5.1.3.1.1)	1..4094	N/A	N/A
PEP C-PVID (cpvid)	The 12-bit C-VID that will be used for untagged frames received at the PEP. The VID must be defined in the VLAN Table for the port's C-component (<i>Table 12-44</i>).	ieee8021PbEdgePortPVID (1.3.111.2.802.1.1.5.1.3.1.2)	1..4094	RC	N/A
PEP Default User Priority (prio)	An integer range from 0-7 to be used for untagged frames received at the Provider Edge Port.	ieee8021PbEdgePortDefaultUserPriority (1.3.111.2.802.1.1.5.1.3.1.3)	0..7	RC	None
PEP Acceptable Frame Types (admit)	The frame types that will be accepted upon receipt at the PEP.	ieee8021PbEdgePortAcceptableFrameTypes (1.3.111.2.802.1.1.5.1.3.1.4)	All = Admit all untagged and priority-tagged frames. Untagged = Admit untagged frames only. Tagged = Admit tagged frames only.	RC	All
PEP Ingress Filtering	The ingress filtering state of	ieee8021PbEdge	Enabled,	RC	Disabled

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
(filter)	the PEP. When enabled, the device discards incoming frames for VLANs that do not include the port in its Member Set. When disabled, the device accepts all incoming frames to the port.	Port EnableIngressFiltering (1.3.111.2.802.1.1.5.1.3.1.5)	Disabled		

S-VID Translation Table Attributes

Table 12-47: S-VID Translation Table Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
Bridge Port	The bridge port for the VID Translation Table entry.	ieee8021BridgeBasePort (1.3.111.2.802.1.1.2.1.1.4.1.2)	host, eth0, eth1, eth2	N/A	N/A
Local S-VID (local-svid)	The internal S-VID on received (transmitted) at the ISS of a CNP or PNP. The VID must be defined in the VLAN Table (<i>Table 12-44</i>) and the Bridge Port specified in the command must belong to the S-component. Because VID translation is bidirectional, two entries cannot use the same Local S-VID for the same port. <i>Figure 12-3</i> shows the bidirectional relationships for Local S-VID.	ieee8021PbVid TranslationLocalVid (1.3.111.2.802.1.1.5.1.1.1.1)	1..4094	N/A	N/A

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
Relay S-VID (relay-svid)	<p>The translated S-VID delivered (received) over the EISS from a CNP or PNP.</p> <p>The VID must be defined in the VLAN Table (<i>Table 12-44</i>) and the Bridge Port specified in the command must belong to the S-component.</p> <p>Because VID translation is bidirectional, two entries cannot use the same Relay S-VID for the same port. <i>Figure 12-3</i> shows the bidirectional relationships for Relay S-VID.</p>	ieee8021PbVid TranslationRelayVid (1.3.111.2.802.1.1.5.1.1.1.2)	1..4094	RC	N/A

XLAT Entry: Port=PN, Local S-VID = X, Relay S-VID = Y

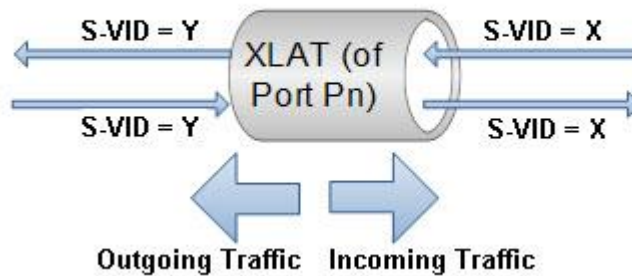


Figure 12-3: Bidirectional Definitions of S-VID Translation

SNMP ifTable Attributes

Table 12-48: SNMP ifTable Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	SNMP Access	Value
Description	A text string containing information about the interface. This string should include the name of the manufacturer, the product name, and the version of the interface hardware/software.	ifDescr (1.3.6.1.2.1.2.2.1.2)	RO	ASCII representation of the VLAN ID
Type	The type of interface. Additional values for ifType are assigned by the Internet Assigned Numbers Authority (IANA), through updating the syntax of the IANA ifType textual convention.	ifType (1.3.6.1.2.1.2.2.1.3)	RO	l2vlan (135)
MTU Size	The size of the largest packet which can be sent/received on the interface, specified in octets. For interfaces that are used for transmitting network datagrams, this is the size of the largest network datagram that can be sent on the interface.	ifMtu (1.3.6.1.2.1.2.2.1.4)	RO	9216
MAC Address	The interface's address at its protocol sub-layer.	ifPhysAddress (1.3.6.1.2.1.2.2.1.6)	RO	The MAC address of the corresponding Eth.
Administrative Status	The desired state of the interface.	ifAdminStatus (1.3.6.1.2.1.2.2.1.7)	RW (Only a single value is allowed)	Up (1)

Attribute (CLI Attribute Name)	Description	SNMP Object ID	SNMP Access	Value
Operational Status	<p>The current operational state of the interface.</p> <p>The Down state of ifOperStatus has two meanings, depending on the value of ifAdminStatus:</p> <p>If ifAdminStatus is not Down and ifOperStatus is Down then a fault condition is presumed to exist on the interface.</p> <p>If ifAdminStatus is Down, then ifOperStatus will normally also be Down i.e. there is not necessarily a fault condition on the interface.</p>	ifOperStatus (1.3.6.1.2.1.2.2.1.8)	RO	Up (1) = Ready to pass packets
Last Change Time (lastchange)	The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last reinitialization of the local network management subsystem, then this object contains a zero value.	ifLastChange (1.3.6.1.2.1.2.2.1.9)	RO	0
Name	The textual name of the interface.	ifName (1.3.6.1.2.1.31.1.1.1.1)	RO	ASCII representation of the VLAN ID
State Trap	Indicates whether linkUp/linkDown traps should be generated for this interface.	ifLinkDownTrap Enable (1.3.6.1.2.1.31.1.1.1.14)	RW (only a single value is allowed.)	Disabled (2)
High Speed Indication	An estimate of the interface's current bandwidth in units of 1,000,000 bits per second.	ifHighSpeed (1.3.6.1.2.1.31.1.1.1.15)	RO	1000

Attribute (CLI Attribute Name)	Description	SNMP Object ID	SNMP Access	Value
Promiscuous Mode	This object has a value of False (2) if this interface only accepts packets/frames that are addressed to this station. This object has a value of True (1) when the station accepts all packets/frames transmitted on the media.	ifPromiscuousMode (1.3.6.1.2.1.31.1.1.1.16)	RO	False (0)
Connector	This object has the value True (1) if the interface sub-layer has a physical connector. Otherwise, this object has the value False(2).	ifConnectorPresent (1.3.6.1.2.1.31.1.1.1.17)	RO	False (2)
Alias	This object is an alias name for the interface as specified by a network manager, and provides a non-volatile handle for the interface.	ifAlias (1.3.6.1.2.1.31.1.1.1.18)	RW	Zero-length string

Forwarding Data Base (FDB) Object Attributes

Table 12-49: FDB Object Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
Bridge Component ID	The component identifier is used to distinguish between the multiple virtual bridge instances within a PBB. In the current product version, the value of this object is equal to s1.	ieee8021QbridgeFdb ComponentId (1.3.111.2.802.1.1.2.1.2.1.1.1). It is an index to ieee8021QbridgeFdb Table (1.3.111.2.802.1.1.2.1.2.1)	s1 (forced)	N/A	s1
FDB ID (fdb-id)	The identity of this Forwarding Database. The system maintains 64 permanent instances of the FDB object.	ieee8021QbridgeFdb Id (1.3.111.2.802.1.1.2.1.2.1.1.2). It is an index to ieee8021QbridgeFdb Table (1.3.111.2.802.1.1.2.1.2.1)	1..64	N/A	1
Aging Time (aging)	The timeout period in seconds for aging out dynamically-learned forwarding information.	ieee8021QbridgeFdb AgingTime (1.3.111.2.802.1.1.2.1.2.1.1.5). It belongs to ieee8021QbridgeFdb Table (1.3.111.2.802.1.1.2.1.2.1)	10..1000000	RW	172800

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
Learned Entry Discards (full-table-counter)	<p>The total number of Forwarding Database entries that have been or would have been learned, but have been discarded due to a lack of storage space in the Forwarding Database.</p> <p>When this counter is increasing, it indicates that the FDB is regularly becoming full, a condition which generally has adverse performance effects on the sub network. When this counter has a large value but is not currently increasing, it indicates that entry discards have been occurring but are not persistent.</p> <p>View the value of this object using the show command together with the statistics qualifier.</p>	<p>ieee8021QbridgeFdb LearnedEntryDiscards (1.3.111.2.802.1.1.2.1.2.1.1.4)</p> <p>It belongs to ieee8021QbridgeFdb Table (1.3.111.2.802.1.1.2.1.2.1)</p>	Varies	RO	N/A
Dynamic Count (num-of-dynamic)	<p>The current number of dynamic entries in this Forwarding Database. The value of this object is incremented each time an entry is created or deleted</p> <p>View the value of this object using the show command together with the statistics qualifier.</p>	<p>ieee8021QbridgeFdb DynamicCount (1.3.111.2.802.1.1.2.1.2.1.1.3)</p> <p>It belongs to ieee8021QbridgeFdb Table (1.3.111.2.802.1.1.2.1.2.1)</p>	Varies	RO	N/A

FDB Address Table Attributes

Table 12-50: FDB Address Table Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
Bridge Component ID	The component identifier is used to distinguish between the multiple virtual bridge instances within a PBB. In the current product version, the value of this object is equal to s1.	ieee8021QbridgeFdbComponentId (1.3.111.2.802.1.1.2.1.2.1.1) It is an index to ieee8021QbridgeTpFdbTable (1.3.111.2.802.1.1.4.1.2.2) and also to ieee8021QbridgeFdbTable (1.3.111.2.802.1.1.2.1.2.1)	s1 (forced)	N/A	s1
FDB ID (fdb-id-list)	The identity of this Forwarding Database. The system maintains 64 permanent instances of the FDB Address Table object.	ieee8021QBridgeFdbId (1.3.111.2.802.1.1.2.1.2.1.2) It is an index to ieee8021QbridgeTpFdbTable (1.3.111.2.802.1.1.4.1.2.2) and also to ieee8021QbridgeFdbTable (1.3.111.2.802.1.1.2.1.2.1)	1..64	N/A	1

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
FDB MAC Address (addr)	The unicast MAC address for which the device has forwarding and/or filtering information.	ieee8021QbridgeTpFdb Address (1.3.111.2.802.1.1.4.1.2.2.1.1) It is an index to ieee8021QbridgeTpFdb Table (1.3.111.2.802.1.1.4.1.2.2)	NN-NN-NN- NN-NN-NN <i>where</i> NN is a hexadecimal number (for example 00- AF-DD-1E-2D- A3)	N/A	N/A
FDB Port (port)	The bridge port from which the MAC address has been learned.	ieee8021QbridgeTpFdb Port (1.3.111.2.802.1.1.4.1.2.2.1.2) It belongs to ieee8021QbridgeTpFdb Table (1.3.111.2.802.1.1.4.1.2.2)	host, eth0, eth1, eth2, c1, c2, c3, c4, s1	RC	N/A
Address Entry Status (status)	The status of this FDB Address Table entry.	ieee8021QbridgeTpFdb Status (1.3.111.2.802.1.1.4.1.2.2.1.3) It belongs to ieee8021QbridgeTpFdb Table (1.3.111.2.802.1.1.4.1.2.2)	Learned = The port was learned and is being used. Self = The port indicates which of the device's ports has this address. Mgmt = The entry has been assigned by management.	RO	N/A

ARP Table Attributes

Table 12-51: ARP Table Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
ARP Interface (interface)	The index value that uniquely identifies the interface for this entry. The interface identified here is identical to that of the MIB's ifIndex.	ipNetToPhysicalIfIndex (1.3.6.1.2.1.4.35.1.1)	1..4	N/A	1
ARP IP Address	The IP Address that corresponds to the media-dependent physical address.	ipNetToPhysicalNetAddress (1.3.6.1.2.1.4.35.1.3)	X.X.X.X, where: X is a decimal number from 0 to 255 (for example 10.0.15.74)	RC	None
ARP MAC Address (mac-addr)	The media-dependent physical address.	ipNetToPhysicalPhysAddress (1.3.6.1.2.1.4.35.1.4)	NN-NN-NN-NN-NN-NN, where: NN is a hexadecimal number (for example 00-AF-DD-1E-2D-A3)	RC	None