MINI-LINK TN ETSI

Operation Manual

MINI-LINK™

ERICSSON

MINI-LINK TN ETSI

Operating Instruction

ERICSSON

Contents

1	**Introduction**	**1**
1.1	Target Group	2
1.2	Revision Information	2
1.3	Related Documents	2
1.4	Conventions	3
1.5	Copyright for Third Party Software Products	4
1.6	Technical Support	5
2	**System Overview**	**7**
2.1	Indoor Part with AMM	8
2.2	Indoor Part with ATU	14
2.3	Outdoor Part	15
2.4	Management	16
3	**Getting Started**	**17**
3.1	System Requirements	17
3.2	Installing Software	18
3.3	Starting the LCT	22
3.4	Uninstalling Software	34
4	**Using the EEM**	**35**
4.1	User Interface Overview	35
4.2	Navigation Tree	36
4.3	Menus	36
4.4	Status Bar	41
4.5	Confirm Button	42
4.6	Using the Help	42
4.7	Naming Principles	44
4.8	EEM Troubleshooting	47
5	**Initial Setup**	**49**
5.1	Radio Terminal Configuration	49
5.2	Automatic Configuration of NE Parameters	53
5.3	Manual Configuration of NE Parameters	54

6	**Configuration Management**	**59**
6.1	Typical Workflow	59
6.2	Administrative Status	60
6.3	Unit and Interface Configuration	61
6.4	Radio Terminal Configuration	62
6.5	Working with MSP Protection	68
6.6	Working with 1+1 E1 SNCP Protection	70
6.7	Configuring the Ethernet Bridge	79
6.8	Working with Traffic Routing of E1 Interfaces	79
6.9	Working with E1 Overview	83
6.10	DCN Configuration	85
6.11	Uploading a Configuration File to an FTP Server	90
6.12	Software Upgrade	91
6.13	Introduction to CLI	97
6.14	Generating Configuration Reports	111
7	**Fault Management**	**113**
7.1	Operational Status	113
7.2	Alarms and Events	115
7.3	Viewing the DCN Status	126
7.4	Loops	126
7.5	Error Log Handling	129
8	**Performance Management**	**131**
8.1	Specifying the PM Start Time	131
8.2	Viewing Performance Data	131
8.3	Running a BERT on an E1 Interface	132
9	**Security Management**	**135**
9.1	User Names	135
9.2	Changing Passwords	136
9.3	Replacing Lost Passwords	136
10	**Hardware Maintenance**	**139**
10.1	Adding Plug-in Units	140
10.2	Replacing an LTU 16x2, LTU 12x2, LTU 155 or SMU2 (co-siting)	140
10.3	Replacing an MMU2 or SMU2 (protection)	142
10.4	Replacing an MMU2 B/C	143

10.5	Replacing a PFU	145
10.6	Replacing an NPU 8x2	147
10.7	Replacing an NPU1 B	149
10.8	Replacing an NPU2	151
10.9	Replacing an ATU (B)	152
10.10	Changing the Traffic Capacity of a Radio Terminal with MMU2	153
10.11	Changing the Traffic Capacity of a Radio Terminal with MMU2 B/C	154
10.12	Changing an 1+0 Radio Terminal to a 1+1 Radio Terminal with MMU2	154
10.13	Changing an 1+0 Radio Terminal to a 1+1 Radio Terminal with MMU2 B/C	155
10.14	Changing the Traffic Capacity of an SMU2 (co-siting)	156
11	**User Interface Reference**	**157**
11.1	Radio Terminal Configuration	158
11.2	Automatic Configuration	159
11.3	Manual Configuration	160
11.4	Software Upgrade – Installation Wizard	161
11.5	E1 DCN Configuration	162
11.6	Finish Installation	163
11.7	Installation Finished	164
11.8	Change Password	165
11.9	Emergency Fallback	166
11.10	Perform Emergency Fallback	167
11.11	Factory Setting	168
11.12	Delete Configuration File	169
11.13	Configuration File Deleted	170
11.14	Restore NPU Configuration	171
11.15	Basic NE Configuration	172
11.16	Ethernet/LAN/Servers Configuration	174
11.17	Bridge Configuration	176
11.18	PPP Configuration	177
11.19	Static Routing Configuration	179
11.20	Modify Static Route	180
11.21	OSPF Area Configuration	181
11.22	Modify OSPF Area	183

11.23	PFU1 Configuration	184
11.24	PFU2 Configuration	185
11.25	PFU3 Configuration	186
11.26	FAU Configuration	187
11.27	NPU1 B Configuration	188
11.28	NPU 8x2 Configuration	189
11.29	NPU2/ATU NPU Configuration	190
11.30	Ethernet Bridge Configuration	191
11.31	LTU 12x2 Configuration	192
11.32	LTU 16x2 Configuration	193
11.33	LTU 155 Configuration	194
11.34	MMU2 Configuration	196
11.35	SMU2 Configuration	198
11.36	MMU2 B/C Configuration	201
11.37	RAU IF Configuration	203
11.38	RAU Configuration	204
11.39	RF Configuration	207
11.40	Reset Configuration	208
11.41	Restore Configuration	209
11.42	SWITCH Configuration	210
11.43	SWITCH Protection	211
11.44	MS/RS Configuration	213
11.45	MSP Configuration	215
11.46	VC-4 Configuration	216
11.47	VC-12 Configuration	218
11.48	All VC-12 Configuration	220
11.49	E3 Configuration	222
11.50	E2 Configuration	223
11.51	E1 Configuration	224
11.52	All E1 Configuration	225
11.53	E1 Overview	226
11.54	User Input Configuration	228
11.55	User Output Configuration	229
11.56	Traffic Routing Select Interfaces	230
11.57	Traffic Routing Matrix View	232
11.58	Traffic Routing List View	234

11.59	Create Traffic Routing	236
11.60	Create Multiple Traffic Routings	237
11.61	Modify Traffic Routing	238
11.62	1+1 E1 SNCP Select Interfaces	239
11.63	1+1 E1 SNCP Matrix View	241
11.64	1+1 E1 SNCP List View	243
11.65	Create 1+1 E1 SNCP	245
11.66	Create Multiple 1+1 E1 SNCP	247
11.67	Modify 1+1 E1 SNCP	248
11.68	Create MSP Protection	250
11.69	Creating Protection	251
11.70	Modify MSP Protection	252
11.71	Deleting Protection	254
11.72	Inventory	255
11.73	Edit Asset ID	256
11.74	Report	257
11.75	View Report	258
11.76	Upgrade of Baseline	260
11.77	Upgrade of Modules	262
11.78	Settings	263
11.79	Start Upgrade	265
11.80	View Units	266
11.81	Preferences	267
11.82	Upgrade Progress – Baseline	269
11.83	Upgrade Progress – Modules	271
11.84	Scheduled Activation	272
11.85	Activation in Progress	273
11.86	Confirm New Software Configuration	274
11.87	Load Configuration	275
11.88	Load Configuration Progress	277
11.89	Restart	278
11.90	Help Setup	279
11.91	NE Alarms and Status	280
11.92	Ethernet Bridge Alarms and Status	282
11.93	Bridge Alarm and Status	285
11.94	Ethernet/LAN Status	287

11.95	USB Status	289
11.96	PPP Status	290
11.97	PPP and ML-PPP Counters	291
11.98	TCP Status	293
11.99	UDP Status	295
11.100	ARP Status	296
11.101	IP/ICMP Status	297
11.102	Static Routing Status	299
11.103	OSPF General Status	300
11.104	OSPF Area Status	302
11.105	OSPF Interface Status	304
11.106	OSPF Neighbor Status	307
11.107	OSPF Host Status	309
11.108	PFU Alarms and Status	310
11.109	FAU Alarms and Status	311
11.110	NPU1 B Alarms and Status	312
11.111	NPU 8x2 Alarms and Status	314
11.112	NPU2/ATU NPU Alarms and Status	316
11.113	LTU 16x2 Alarms and Status	317
11.114	LTU 12x2 Alarms and Status	319
11.115	LTU 155 Alarms and Status	320
11.116	Radio Terminal Alarms and Status	322
11.117	MMU2 Alarms and Status	326
11.118	RAU Alarms and Status for MMU2	328
11.119	RF Alarms and Status for MMU2	330
11.120	RAU IF Alarms and Status for MMU2	331
11.121	SWITCH Alarms and Status for MMU2	333
11.122	SMU2 Alarms and Status	334
11.123	Unsupported Unit Alarms and Status	336
11.124	E1 Alarms and Status	337
11.125	E2 Alarms and Status	338
11.126	E3 Alarms and Status	339
11.127	MS/RS Alarms and Status	340
11.128	MSP Alarms and Status	342
11.129	VC-4 Alarms and Status	344
11.130	VC-12 Alarms and Status	346

11.131	User Input Alarms and Status	347
11.132	User Output Alarms and Status	348
11.133	Alarm List	349
11.134	Event Log	351
11.135	Load Error Log	353
11.136	Activities	354
11.137	NE Loops	356
11.138	Loops	357
11.139	MS/RS Performance	359
11.140	MS/RS Performance 15 Minute Intervals	361
11.141	MSP Performance	363
11.142	MSP Performance 15 minute Intervals	365
11.143	VC-4 Performance	367
11.144	VC-4 Performance 15 minute Intervals	369
11.145	VC-12 Performance	371
11.146	VC-12 Performance 15 minute Intervals	373
11.147	E1 Performance	375
11.148	E1 Performance 15 Minute Intervals	376
11.149	RF Power	377
11.150	Bit Error Ratio Test (BERT)	378
11.151	Security	380
11.152	Select Option	381
Glossary		**383**
Index		**389**

1 Introduction

A MINI-LINK TN Network Element (NE) has an embedded Web server hosting an Embedded Element Manager (EEM) application. Local management is performed using a Local Craft Terminal (LCT), that is a locally connected PC, accessing the EEM from a Web browser. The EEM can also be accessed remotely over the DCN or launched from MINI-LINK Manager.

This operating instruction mainly describes how to use an LCT to set up, configure and maintain MINI-LINK TN equipment. However, the information is valid for other ways of accessing the EEM, unless otherwise stated.

MINI-LINK Service Manager (MSM) is conveniently launched from the EEM for management of Radio Terminals with MMU2.

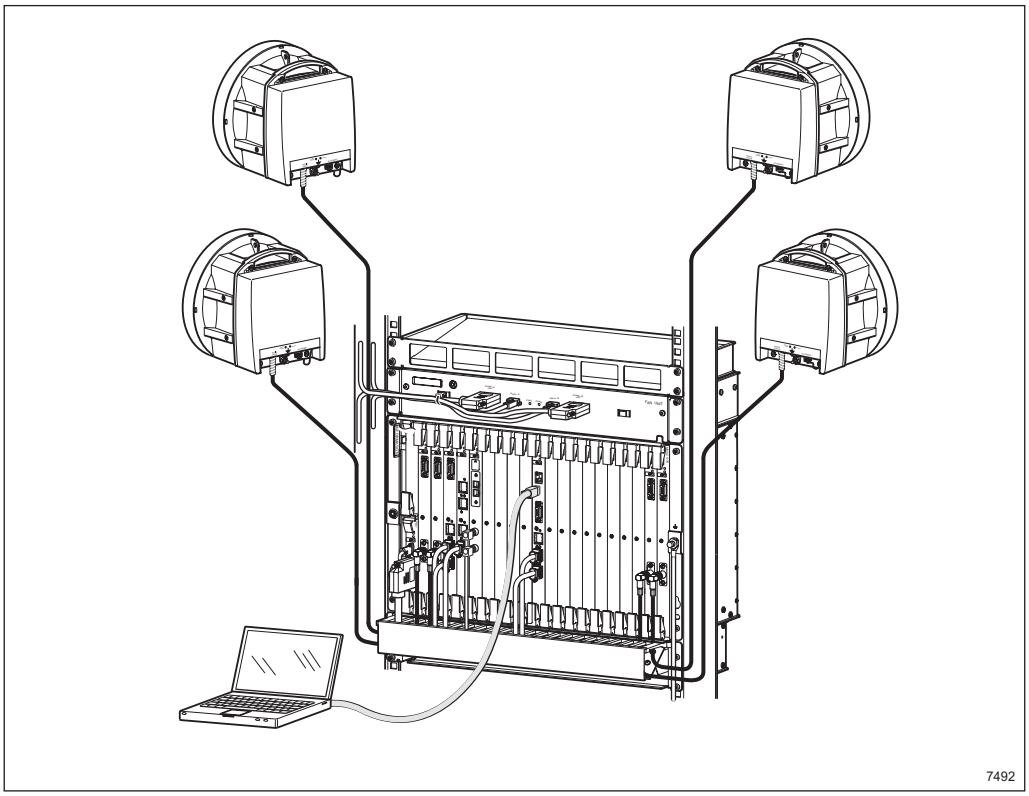


Figure 1 Local management using the LCT

1.1 Target Group

This operating instruction is written for field technicians and supervisors who work with installation, configuration and maintenance of MINI-LINK TN equipment on site.

It is assumed that the user:

- Has basic understanding of MINI-LINK network design, operation and terminology.
- Is familiar with his or her own MINI-LINK network configuration.
- Has basic understanding of networking technologies.
- Is familiar with window-based computer systems and interfaces.
- Has the proper education, training and competence required to perform the tasks in this document correctly.

1.2 Revision Information

This release of the operating instruction applies to MINI-LINK TN 2.2.

The information is updated due to the following:

- Support for MMU2 B/C
- Improvements and minor changes of the EEM GUI.

1.3 Related Documents

Table 1 on page 2 contains documents related to installation and operation of MINI-LINK TN equipment. References are made in *Italics* using the document name only.

Table 1 Related documents

MSM 6.4 User Guide	EN/LZT 712 0193
MSM 6.4 Installation Guide	EN/LZT 712 0069
MINI-LINK TN ETSI Indoor Installation Manual	EN/LZT 712 0122
MINI-LINK TN, MINI-LINK HC, MINI-LINK E Outdoor Installation Manual	EN/LZT 712 0015
ATU Installation Instruction	EN/LZT 712 0224
MINI-LINK TN, MINI-LINK HC, MINI-LINK E ETSI Product Catalog	EN/LZT 712 0191
MINI-LINK TN ETSI Technical Description	EN/LZT 712 0211
MINI-LINK DCN Guideline	1/15443-FGB 101 004/1

1.4 Conventions

This section states the typographic and safety conventions used in this operating instruction.

1.4.1 Typographic Conventions

The following typographic conventions are used:

- Elements in the user interface – such as window names, dialog box titles and options and menu commands – are formatted like this: **AaBbCc123**
- Resource identifiers – such as file paths, database names and Uniform Resource Locators (URLs) – are formatted like this: `AaBbCc123`
- Keywords, functions and anything else that the system provides are formatted like this: `AaBbCc123`.
- Variables and other placeholders that the system provides are formatted like this: *<AaBbCc123>*.
- Keywords, functions and anything else that have to be entered exactly as shown are formatted like this: **`AaBbCc123`**.
- Variables and other placeholders you have to provide are formatted like this: ***<AaBbCc123>***.

1.4.2 Safety Conventions

At some places the user must be careful to do as described to avoid disturbing ongoing traffic, initiate ESD or cause a loss of data. To highlight such sensitive parts the following safety conventions are used.

Caution

Caution!

Caution means that disturbances may occur if the warning is neglected. This type of disturbance may cause damage to tangible property or cause traffic interruptions when doing software work.

Notes

Note: Notes are used to call to the attention of the reader key points that might otherwise be overlooked.

Electrostatic Discharge

Figure 2 ESD symbol

The Electrostatic Discharge (ESD) symbol indicates when external ESD protection must be used to avoid possible damage to the equipment.

1.5 Copyright for Third Party Software Products

- BullletProof FTP Server. © 1998-2003 Gene6 SARL. Used under license by Digital Candle, Inc.
- Envoy (SNMP). © Wind River Systems.
- MontaVista Linux. © MontaVista Software, Inc.
- ZebOS for Linux. © IP Infusion Inc.
- Adobe and Acrobat Reader are registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.
- USBLAN software. © Belcarra Technologies Corp.
- USB driver. © Arabella Software Ltd.

1.6 Technical Support

If you have a technical question or have encountered a problem working with MINI-LINK TN equipment, please contact your local Ericsson representative. When contacting your local Ericsson representative, please provide the following information for the fastest possible service:

- Product serial number.
- Your name, company name and phone number.
- Product name and version number.
- Type and version of operating system, including service packs.
- Type and version of Web browser.
- Complete description of the problem, including steps to reproduce it.
- Exact wording of any messages displayed when you encountered the problem.
- Steps taken to resolve the problem.
- All previous correspondence with Ericsson.

2 System Overview

MINI-LINK TN provides a platform for flexible, scalable and cost-effective wireless transmission. The system offers integrated traffic routing, PDH and SDH multiplexing, Ethernet transport as well as protection mechanisms on link and network level. The software configurable traffic routing minimizes the use of cables, improves network quality and facilitates control from a remote location.

The modular system enables new interface units to be added while in operation. This hot insertion of new plug-in units and automatic software upgrade ensure that traffic is operational during replacement and functional upgrade.

Configurations range from small end sites with one single Radio Terminal to large hub sites where all the traffic from a number of southbound links is aggregated into one link, microwave or optical, in the northbound direction.

A Network Element (NE) comprises two parts:

- Indoor part of two types:
  - Access Module Magazine (AMM) with plug-in units, see Section 2.1 on page 8.
  - Access Termination Unit (ATU), see Section 2.2 on page 14.
- Outdoor part, see Section 2.3 on page 15.

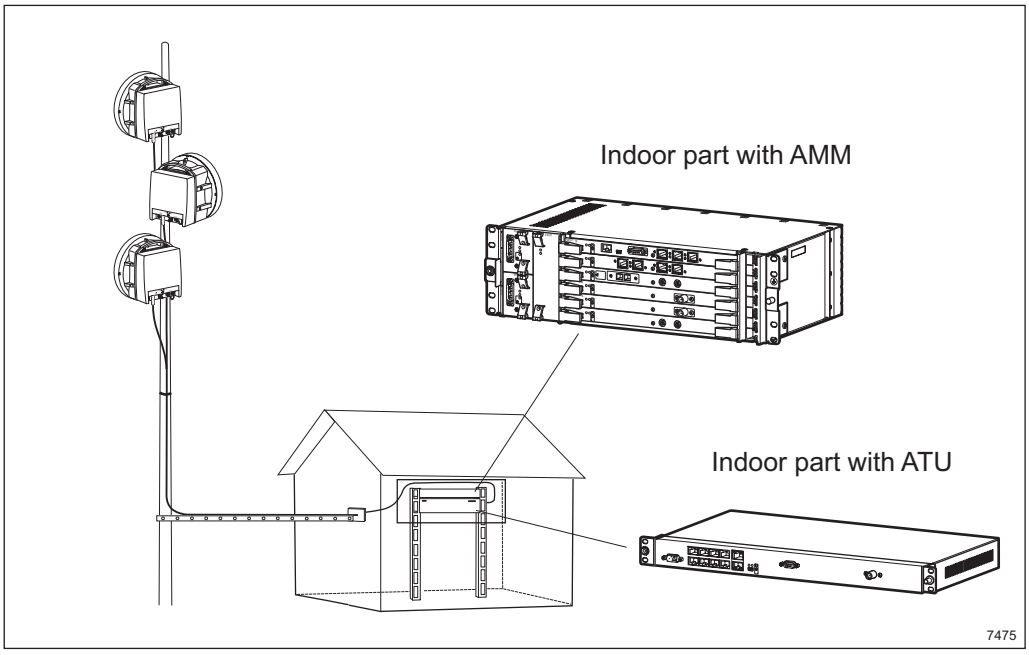


Figure 3 Indoor and outdoor parts

2.1 Indoor Part with AMM

The summary below introduces the standard types of indoor units, available in different versions further described in this section.

Access Module Magazine (AMM)	Houses the plug-in units and provides backplane interconnection of traffic, power and control signals.
Node Processor Unit (NPU)	Handles the system's control functions. It also provides traffic and management interfaces.
Line Termination Unit (LTU)	A plug-in unit that provides PDH or SDH traffic interfaces.
Modem Unit (MMU)	The indoor part of a Radio Terminal. This plug-in unit determines the traffic capacity of the Radio Terminal.
Switch Multiplexer Unit (SMU)	Provides protection for the Radio Terminals. Alternatively it can be configured to interface MINI-LINK E equipment on the same site.
Power Filter Unit (PFU)	Filters the external power and distributes the internal power to the plug-in units via the backplane.
Fan Unit (FAU)	Provides cooling for the indoor part.

The interconnection between the outdoor part (Radio Units and antennas) and the indoor part is one coaxial cable per MMU carrying full duplex traffic, DC supply voltage, as well as operation and maintenance data.

2.1.1 AMM

The AMM houses the plug-in units and provides backplane interconnection of traffic, power and control signals. One plug-in unit occupies one slot in the AMM. The AMM fits into standard 19" or metric racks and cabinets. It is available in three sizes described below.

2.1.1.1 AMM 2p

The AMM 2p is suitable for end site and repeater site applications. It has two full-height slots and two half-height slots and it houses one NPU2, one or two MMUs, and the optional LTU 12x2 and FAU4.

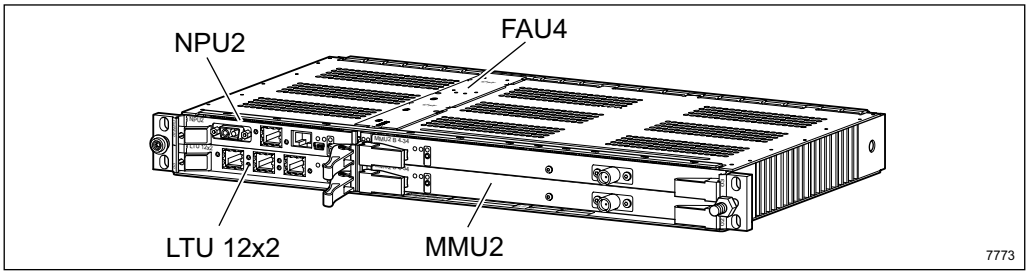


Figure 4 AMM 2p

2.1.1.2 AMM 6p

The AMM 6p is suitable for medium-sized hub sites. It has six full-height slots and two half-height slots and it houses one NPU1 B or NPU 8x2, one PFU2 and one FAU2. The remaining slots are equipped with MMUs, SMUs and LTUs.

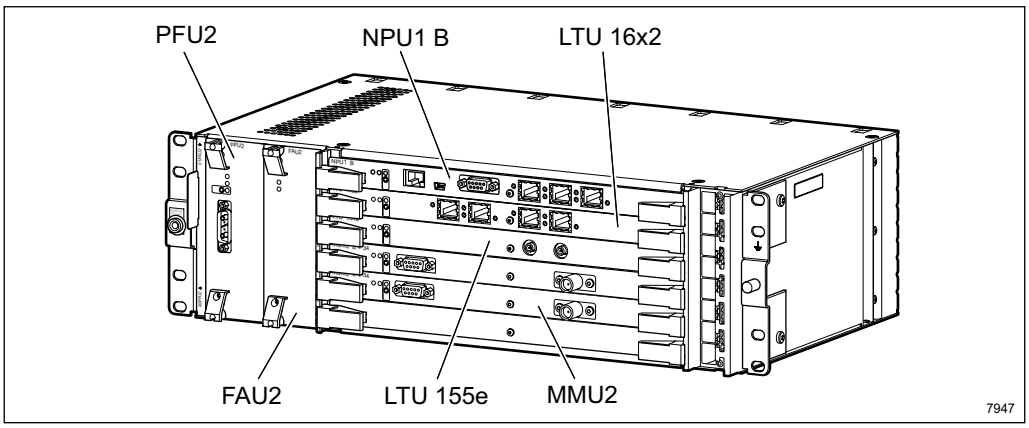


Figure 5 AMM 6p

2.1.1.3 AMM 6p B

The AMM 6p B is the successor of AMM 6p, providing power redundancy. It has six full-height slots and two half-height slots and it houses one NPU1 B or NPU 8x2, one or two PFU3 (in one half-height slot) and one FAU2. The remaining slots are equipped with MMUs, SMUs and LTUs.

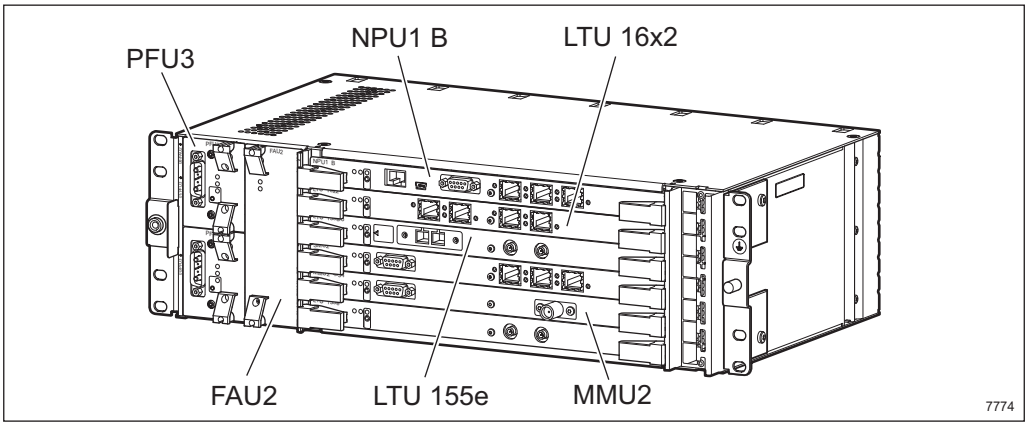


Figure 6 AMM 6p B

2.1.1.4 AMM 20p

The AMM 20p is suitable for large-sized hub sites, for example at the intersection between the optical network and the microwave network. It has 20 full-height slots and two half-height slots and it houses one NPU1 B or NPU 8x2, and one or two PFU1. The remaining slots are equipped with MMUs, SMUs and LTUs.

A cable shelf is fitted directly underneath the AMM to enable neat handling of cables connected to the fronts of the plug-in units. An FAU1 is fitted on top of the AMM unless forced air-cooling is provided. An air guide plate is fitted right above the FAU1.

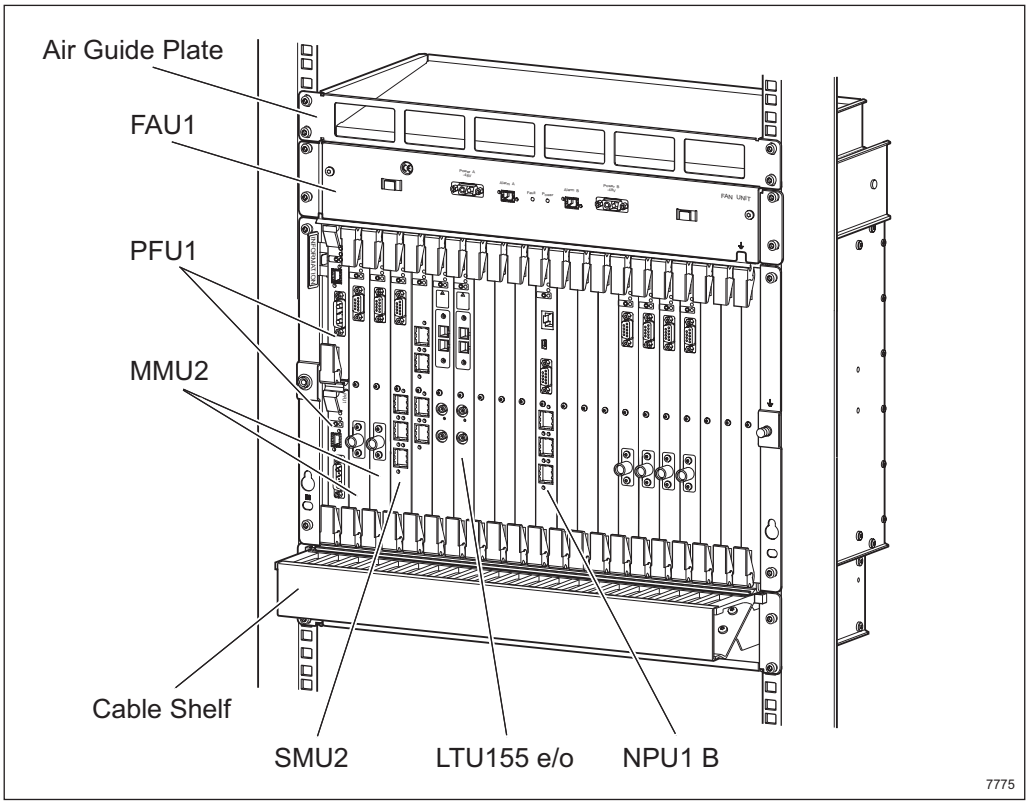


Figure 7 AMM 20p

2.1.2 NPU

The NPU holds the system's control functions. One NPU is always required in the AMM. The NPU also provides E1, DCN and management interfaces.

2.1.2.1 NPU2

The unit fits in an AMM 2p. The external power supply is connected directly to the NPU2. It provides 4xE1 for traffic connection, USB interface for LCT connection and a 10/100BASE-T Ethernet interface. The Ethernet interface can be configured to detect the type of cable used and is intended for the optional features Ethernet Site LAN or Ethernet Traffic.

2.1.2.2 NPU 8x2

The unit fits in an AMM 6p (B) and AMM 20p. It provides 8xE1 for traffic connection, 10BASE-T Ethernet interface for LCT connection, three User Input and three User Output ports.

2.1.2.3 NPU1 B

NPU1 B is the successor of NPU 8x2. It provides 8xE1 for traffic connection, USB interface for LCT connection, three User Input, three User Output ports and a 10/100BASE-T Ethernet interface. The Ethernet interface can be configured to detect the type of cable used and is intended for the optional feature Ethernet Site LAN.

2.1.3 LTU

The LTUs are used to connect traffic from external PDH or SDH equipment.

2.1.3.1 LTU 12x2

The unit fits in an AMM 2p. For sites where the four E1 interfaces on the NPU2 are insufficient, the LTU 12x2 provides 12 additional E1 interfaces.

2.1.3.2 LTU 16x2

The unit fits in an AMM 6p (B) and AMM 20p. For sites where the eight E1 interfaces on the NPU are insufficient, the LTU 16x2 provides 16 additional E1 interfaces.

2.1.3.3 LTU 155e

The unit fits in an AMM 6p (B) and AMM 20p. It provides one electrical STM-1 interface.

2.1.3.4 LTU 155e/o

The unit fits in an AMM 6p (B) and AMM 20p. It provides one optical or one electrical STM-1 interface.

2.1.4 MMU2

The MMU2 is the indoor part of a Radio Terminal determining the traffic capacity (4 to 34 Mbit/s). It is denoted MMU2 4-34 or similar, where in this case 4-34 implies a software configurable traffic capacity of 4 to 34 Mbit/s.

A protected (1+1) Radio Terminal requires two MMU2 units and one SMU2.

Local management is mainly done using MSM, which is launched from the LCT.

2.1.5 SMU2

The SMU2 provides either 1+1 radio protection or co-siting features for MINI-LINK E equipment, depending on how the unit is configured. It has one O&M connector, one DIG SC connector (2x64 kbit/s) for IP DCN connection,

and also one E1 and one E2/E3 connector for co-siting with MINI-LINK E equipment.

2.1.6 PFU

The PFU is connected to the external power supply, which is filtered and distributed to the plug-in units via the backplane.

2.1.6.1 PFU1

The unit fits in AMM 20p. Two PFU1 units connected to separate power supply sources provide power redundancy.

2.1.6.2 PFU2

The unit fits in AMM 6p.

2.1.6.3 PFU3

The unit fits in AMM 6p B. Two PFU3 units connected to separate power supply sources provide power redundancy.

2.1.7 FAU

The FAU provides cooling for the AMM and plug-in units.

2.1.7.1 FAU1

The unit is fitted directly above the AMM 20p.

2.1.7.2 FAU2

The unit is fitted in the AMM 6p (B).

2.1.7.3 FAU4

The unit is fitted in the AMM 2p.

2.2 Indoor Part with ATU

The Access Termination Unit (ATU) implements the indoor part of an NE dedicated as an edge node for microwave transmission in mobile networks. It can also be used in Ethernet bridge applications.

The ATU comprises one self-contained unit for installation in 19” or metric racks and cabinets. It can also be mounted on a wall.

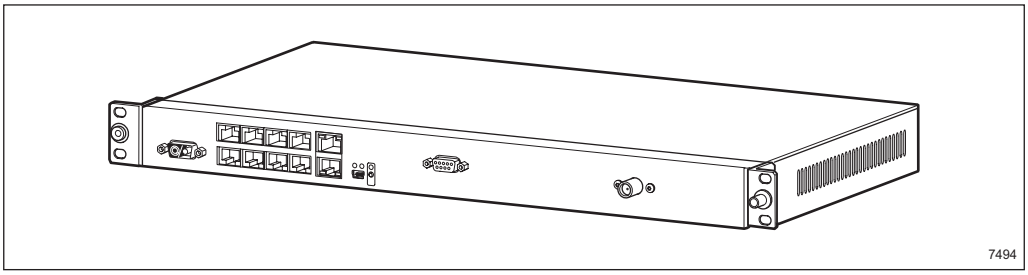


Figure 8 Example of an ATU

The ATU provides unprotected (1+0) microwave transmission within the 7 to 38 GHz frequency bands using C-QPSK modulation, when connected to an RAU with antenna. The interconnection between the ATU and the outdoor part is one coaxial cable carrying full duplex traffic, DC supply voltage, as well as management data.

The available traffic capacity from 2x2 to 17x2 Mbit/s can be shared between PDH traffic with a maximum of 8xE1 and Ethernet traffic over a maximum of 16xE1.

This document covers two ATU variants:

ATU This unit has eight E1 interfaces enabled by default while the 10/100BASE-T interface for traffic can be enabled as an optional feature.

ATU B This unit has one 10/100BASE-T Ethernet interface for traffic enabled by default while eight E1 interfaces can be enabled as an optional feature.

The designation ATU (B) is used when referring to ATU and ATU B at the same time.

There is also a third variant, ATU C, which has 4 E1 interfaces. This unit is managed locally only from MSM and is not further described in this document. For more information on MSM, see *MSM User Guide*.

ATU (B) has one 10BASE-T interface for site LAN, one USB interface for LCT connection, one power supply connector, one radio cable connector and one connector used for the Local Upgrade application.

ATU (B) is presented in the EEM as one physical unit with two internal logical units:

ATU NPU Implements the system control and DCN functions, Ethernet and E1 traffic interfaces, as well as power handling.

ATU MMU2 Implements the indoor part of an unprotected (1+0) Radio Terminal.

The logical units are managed in the same way as similar plug-in units, NPU and MMU2, unless otherwise stated.

2.3 Outdoor Part

The outdoor part is supplied for various frequency bands. It consists of an antenna, a Radio Unit (RAU) and associated installation hardware. For protected (1+1) systems, two RAUs and one or two antennas are used. When using one antenna, the two RAUs are connected to the antenna using a power splitter. The RAU and the antenna are easily installed on a wide range of support structures. The RAU is fitted directly to the antenna as standard, integrated installation. The RAU and the antenna can also be fitted separately and connected by a flexible waveguide. In all cases, the antenna is easily aligned and the RAU can be disconnected and replaced without affecting the antenna alignment.

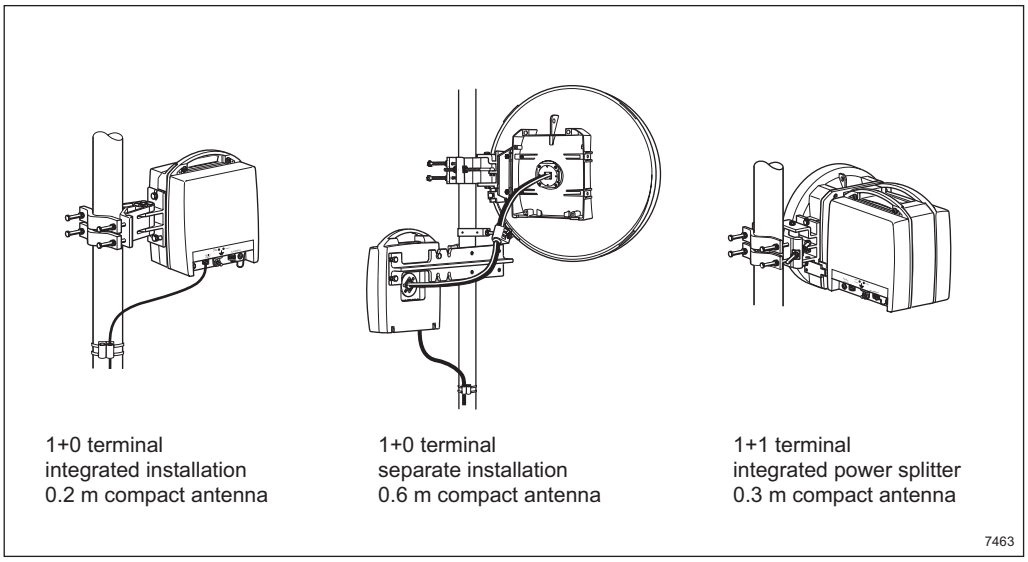


Figure 9 RAUs and antennas in different installation alternatives

The antennas range from 0.2 m up to 3.7 in diameter Antennas up to 1.8 m in diameter can be fitted integrated with the RAU and all antennas can be installed separately, if required.

2.4 Management

Below follows a summary of the tools used to manage a MINI-LINK TN network.

EEM

The element management function is implemented as an Embedded Element Manager (EEM) application, accessed using a standard web browser. For local management a Local Craft Terminal (LCT) is used, that is the EEM is accessed locally by connecting a PC to the NPU or ATU (B), with a crossed Ethernet cable (NPU 8x2) or a USB cable (NPU2/NPU1 B and ATU (B)). The EEM can also be accessed over the site LAN or remotely over the DCN.

Local management of Radio Terminals based on MMU2 is mainly done with MSM, which is launched from the EEM. Terminals based on MMU2 B or MMU2 C are handled by the EEM itself.

CLI

A Command Line Interface (CLI) is provided for advanced IP router configuration and troubleshooting. It is similar to Cisco's industry standard router configuration and is accessed from a Command Prompt window using telnet.

MINI-LINK Manager

Remote management is typically done using MINI-LINK Manager, the network management tool for all MINI-LINK products. The EEM is launched from MINI-LINK Manager for access of a single NE.

Each NE provides an SNMP agent enabling easy integration with any other SNMP based management system.

MINI-LINK Connexion

This application provides a way to provision end-to-end E1 connections in a MINI-LINK TN network.

3 Getting Started

This section covers the following:

- *System Requirements*, see Section 3.1 on page 17.
- *Installing Software*, see Section 3.2 on page 18.
- *Starting the LCT*, see Section 3.3 on page 22.
- *Uninstalling Software*, see Section 3.4 on page 34.

3.1 System Requirements

Make sure that your PC fulfils the following requirements:

- Pentium III 750 MHz processor
- One of the following operating systems:
  - Microsoft Windows 2000 Service Pack 2
  - Microsoft Windows XP Professional
- 256 MB RAM
- 100 MB of free disk space
- 1024×768 monitor resolution
- CD-ROM drive
- Keyboard and mouse (or other pointing device)
- One serial port
- A network card with a 10BASE-T port
- A USB 1.1 compatible port
- Microsoft Internet Explorer 6.0

3.2 Installing Software

The following LCT related software can be installed on the PC:

- BulletProof FTP Server (2.15 or later), for downloading and uploading load modules and configuration files, see Section 3.2.1 on page 18.
- MSM (6.4 or later), to manage Radio Terminals with MMU2 or ATU (B), see Section 3.2.2 on page 21.

  Note: MSM is not needed for Radio terminals with MMU2 B/C.
- USB driver, for LCT connection to an NPU2/NPU1 B or ATU (B), see Section 3.2.3 on page 21.
- Load modules, for software upgrade, see Section 3.2.4 on page 22.

3.2.1 Installing and Configuring BulletProof FTP Server

BulletProof FTP server (2.15 or later) is used for uploading and downloading load modules and configuration files. A user account for MINI-LINK TN on the FTP server and a correct directory structure must be created.

3.2.1.1 Installing BulletProof FTP Server

To install BulletProof FTP Server with default settings:

1. Start the BulletProof FTP Server installation program from the MINI-LINK Service Software CD (LZY 214 2358/1).
2. In the **Licence Agreement** dialog box, click **Next** to accept the licence agreement.
3. In the **Installation Options** dialog box, click **Next** to accept the installation type **Standard**.
4. In the **Installation directory** dialog box, click **Next** to accept the default location of the FTP server files.
5. In the **Completed** dialog box, click **Close** to exit the installation program.

3.2.1.2 Directory Structure of the FTP Server

When using the FTP server certain directories must be present as shown in Figure 10 on page 19.

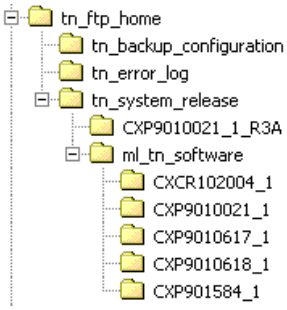


Figure 10 The FTP server directory structure

Note: A correct directory structure is a prerequisite for software upgrade and load of files.

The root directory (`tn_ftp_home`) and the directories directly below (`tn_backup_configuration`, `tn_error_log` and `tn_system_release`) are created by the FTP Server installation program on the MINI-LINK Service Software CD.

`tn_backup_configuration` is used to store configuration files uploaded from an NE as backup and configuration files to be downloaded to an NE. A configuration file is named *<hostname>*`.cfg` where *<hostname>* is typically the name or IP address of an NE.

`tn_error_log` is used to store error log files loaded from the NE, for example *<hostname>*`_active.elog`.

Note: Since `tn_backup_configuration` and `tn_error_log` are likely to hold files belonging to several NEs it is important to use file names that can be easily identified. To avoid overwriting existing files the extension `.old` should be added, for example *<hostname>*`.cfg.old`, before loading a new file to the FTP server.

`tn_system_release` is used for load modules and the directories below is created when installing a load module, see Section 3.2.4 on page 22.

MINI-LINK TN 2.1 introduces a new software upgrade concept which puts new requirements on the directory structure. In MINI-LINK TN 2.0 all load modules are contained in one Software System Release (SSR) file. The content is described in an System Release Description File (SRDF).

In MINI-LINK TN 2.1, each load module resides in a separate directory. The load modules included in a Software Baseline (SBL) is described in a Software Baseline Description File (SBDF).

To facilitate software upgrade and NPU repair in a network with both “post-2.1” and “pre-2.1” products, the software must be stored in both the old (2.0) and new (2.1 and later) file structure.

Example 1 on page 20 and Example 2 on page 20 show lists of available files under `tn_system_release`.

```
.\tn_system_release\CXP9010021_1_R3A\
      srdf.tn                          (SRDF 2.0)
      CXP901584_1_R3A                  (NPU 8x2)
      CXP9010618_1_R1A                 (NPU1 B)
      CXP9010617_1_R3A                 (NPU2)
      CXCR102004_1_R3A                 (LTU 155)
```

Example 1 Old (2.0) directory structure

```
.\tn_system_release\ml_tn_software\
      CXP9010021_1\CXP9010021_1_R3A   (SBDF 2.1 and later)
      CXP901584_1\CXP901584_1_R3A     (NPU 8x2)
      CXP9010618_1\CXP9010618_1_R1A   (NPU1 B)
      CXP9010617_1\CXP9010617_1_R3A   (NPU2)
      CXCR102004_1\CXCR102004_1_R3A   (LTU 155)
```

Example 2 New (2.1 and later) directory structure

3.2.1.3 Configuring BulletProof FTP Server

To configure the FTP Server:

Creating a User

1. On the **Start** menu, point to **Programs→BulletProof FTP Server** and then click **BPFTP Server**.
2. On the **Setup** menu, click **User Accounts**.
3. The **Setup User Accounts** dialog box appears.

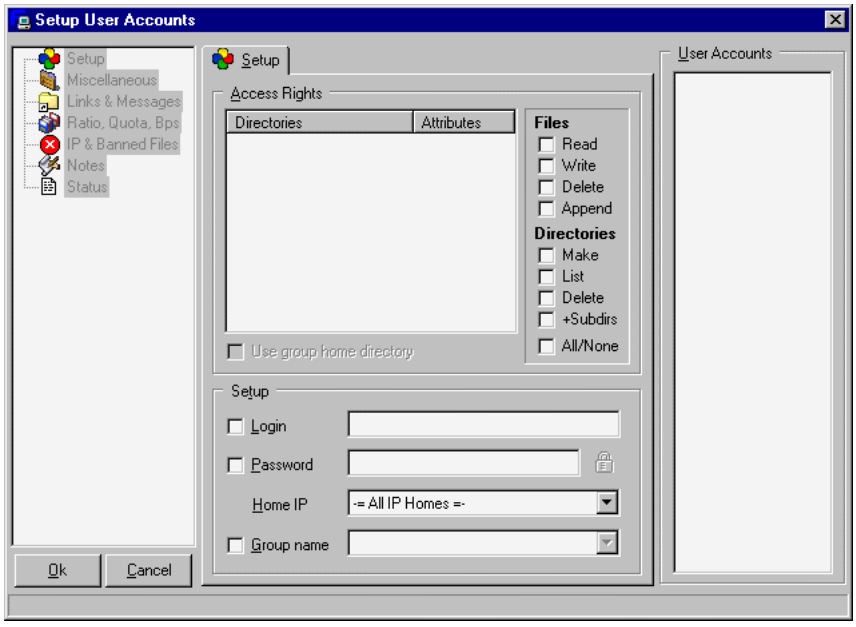


Figure 11 The Setup User Accounts window

4. Right-click in the **User Accounts** list and then click **Add** on the shortcut menu.

5. In the **Enter Account Name** dialog box, type **`anonymous`** and click **OK**. This is the default user name.

6. In the **Setup User Accounts** dialog box, type **`anonymous`** in the **Password** box. This is the default password.

Specifying the FTP Server Root Directory

7. Right-click in the **Directories** list and then click **Add** on the shortcut menu.

8. In the **Select Directory** dialog box, browse to the `<drive:>\tn_ftp_home` directory and click **Select**. The NE uses this directory and its sub-directories for uploading and downloading configuration files and load modules.

9. In the **Directories** list, select the `<drive:>\tn_ftp_home` directory.

10. Under **Files**, select the **Read**, **Write** and **Append** check boxes.

11. Under **Directories**, select the **Make**, **List** and **+Subdirs** check boxes.

12. Click **OK**. The FTP server is now configured to be used by the NE.

Configuring the FTP Server to be Activated on Startup

13. On the **Setup** menu, point to **Main** and then click **General**.

14. In the **FTP Server Setup** dialog box, select the **Activate Ftp server on startup** check box and then click **OK**.

Starting the FTP Server

15. On the **Server** menu, click **Go On-line** to start the FTP server.

3.2.2 Installing MINI-LINK Service Manager (MSM)

MSM (6.4 or later) is required to manage Radio Terminals with MMU2 or ATU (B). Install MSM according to the *MSM Installation Guide*.

Note: MSM is not needed for Radio terminals with MMU2 B/C.

3.2.3 Installing USB Driver

A USB driver must be installed on the PC to be able to connect to the NPU2/NPU1 B or ATU (B). The MINI-LINK Service Software CD (LZY 214 2358/1) provides an installation program for Belcarra Windows USBLAN Software, hereafter referred to as USBLAN.

To install USBLAN:

Note: Make sure the USB cable is disconnected from the PC.

1. Locate and click the link on the CD that starts the installation program.
2. In the **Ericsson Installer ... License Agreement"** dialog box, click **I Agree** to accept the license agreement.
3. In the **Ericsson Installer ... Installation Folder** dialog box, click **Install** to accept the default location (`C:\Program Files\Ericsson\USBLAN\`).
4. The first time the USB cable is connected between the PC and the NPU or ATU (B), the **Found New Hardware** dialog box will appear. Complete the procedure on the screen in order to start USBLAN automatically each time the cable is connected.

More information on installation of USBLAN is found in the `readme.txt` file available on the CD. After installation, the file will be located in `C:\Program Files\Ericsson\USBLAN\`.

3.2.4 Installing Load Modules

This section describes how to install new load modules for software upgrade. The load module file is named *<product number>_<R-state>*`.tar.z` and must be unpacked according to the instruction below.

To install a load module on the PC:

1. Extract the file to the *<drive:>*`\tn_ftp_home` directory.

   Note: Make sure the internal directory structure is preserved as described in Figure 10 on page 19. For example when using WinZip, the **Use folder names** check box must be selected in the **Extract** dialog box.

3.3 Starting the LCT

This section describes how to connect the PC to the equipment and access the EEM. It also contains supplementary information regarding PC and browser settings.

- Section 3.3.1 on page 22 describes how to start the LCT when working with an NPU2/NPU1 B.
- Section 3.3.2 on page 26 describes how to start the LCT when working with an NPU 8x2.
- Section 3.3.3 on page 30 describes how to start the LCT when working with an ATU (B).

3.3.1 Starting the LCT for NPU2/NPU1 B

This section describes how to start the LCT when working with an NPU2 or NPU1 B.

Locally, the NE is accessed using a USB connection and a default IP address (`10.0.0.1`). The PC (and the FTP server on the PC) obtains a dynamic IP address (`10.0.0.2`) from a DHCP server in the NE. This means that the PC should be configured to use dynamic IP addressing.

Remotely, the NE is accessed using the IP address to be used during normal operation. It is typically found in the site documentation or on the information plate of the NE. The PC uses a static or dynamic IP address, depending on whether a DHCP server is used or not, and must be configured accordingly. It is recommended to use a DHCP server if available.

The NE has two modes of operation as described below.

3.3.1.1 Normal Mode

This mode is used for normal operation, allowing complete configuration possibilities. The BR (yellow) LED is OFF when the NE is in Normal mode.

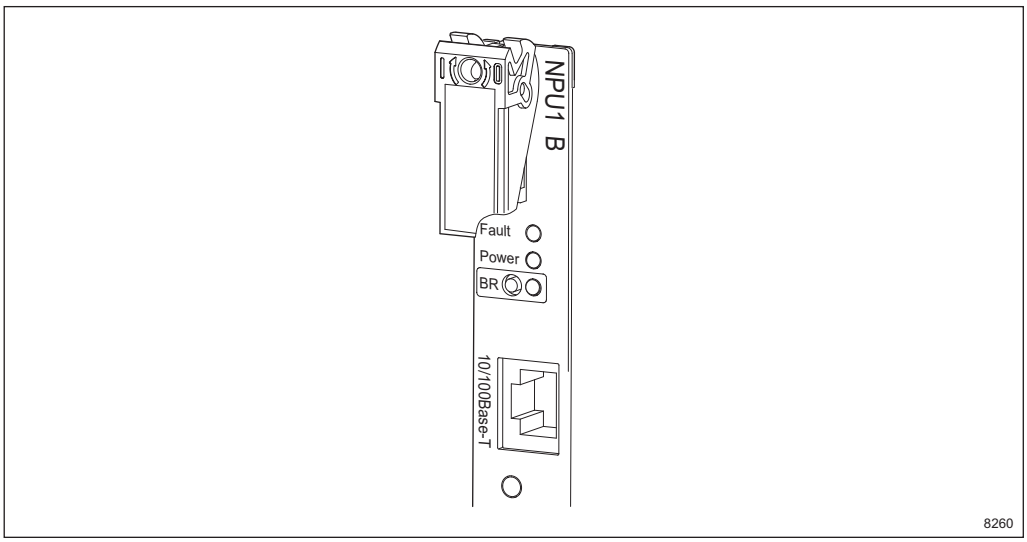


Figure 12 LEDs and BR button on the NPU1 B. For a full description of the LEDs, see the MINI-LINK TN ETSI Indoor Installation Manual.

3.3.1.2 NPU Installation Mode

This mode is used for replacement of the NPU. The LCT will give the possibility to download a new configuration file in order to restore the configuration.

Default user names and passwords are used for the NE and the FTP server, see Section 9.1 on page 135 and Section 3.2.1.3 on page 20.

The NPU Installation mode is entered by inserting the NPU in an active NE (only NPU1 B) and immediately pressing the BR button during NPU power up (Fault (red), Power (green) and BR (yellow) LEDs on the NPU are ON). The BR (yellow) LED will start flashing, indicating that the NE is in NPU Installation mode. The NPU Installation mode is normally left as a result of the completed

replacement procedure. However, the mode can always be left by pressing the BR button.

The procedures of replacing the NPU is described in Section 10.7 on page 149 and Section 10.8 on page 151.

3.3.1.3 Starting the LCT

To start the LCT:

1. Do one of the following:

To connect:	Then:
Locally	• Make sure that the USB driver is installed on the PC, see Section 3.2.3 on page 21. • Connect the USB cable between your PC and the USB connector on the NPU. • Configure the PC to use a dynamic IP address obtained from the DHCP server in the NE (it is also possible to configure the PC to use the static IP address `10.0.0.2`). For more information on IP addressing, see Section 3.3.4 on page 32. • Start a Web browser and make sure your browser is configured not to use a proxy server. For more information, see Section 3.3.5 on page 33. • In your Web browser, enter the URL **`http://10.0.0.1`**.
Remotely	In your Web browser, enter the URL to be used during normal operation. The IP address is typically found in the site documentation or on the information plate of the NE.

2. In the **Enter Network Password** dialog box, type the user name and password, and click **OK**. For more information see Section 9.1 on page 135.

3. A non-configured NE lacks a configuration a file and an installation wizard will be provided for the initial setup, see Figure 13 on page 24. The initial setup is described in Section 5 on page 49.

   A configured NE will display a page like the one in Figure 14 on page 25. From here you can perform all operations, for example configuration, see Section 6 on page 59.

   Should the NE be in NPU Installation mode, the LCT will give the possibility to download a new configuration file in order to restore the configuration, see Figure 15 on page 25. The procedures of replacing the NPU is described in Section 10.7 on page 149 and Section 10.8 on page 151.

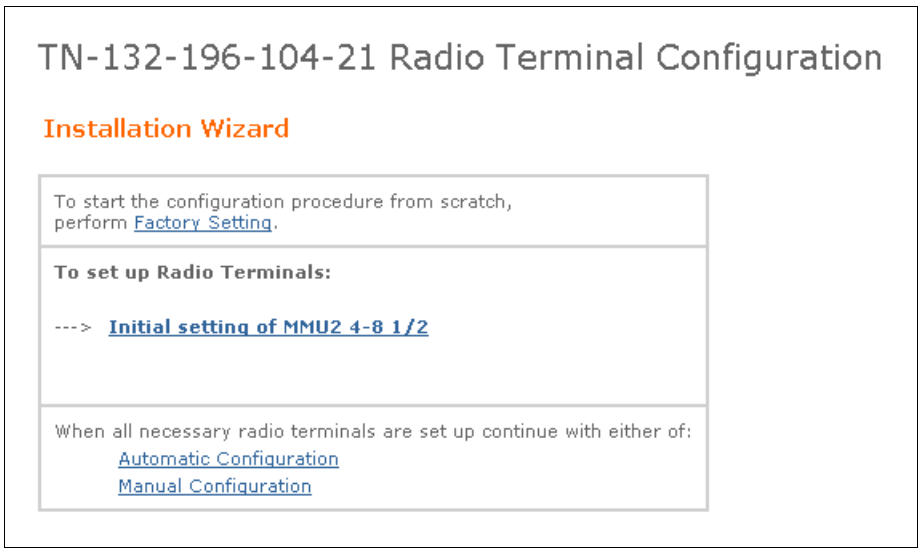


Figure 13 The Radio Terminal Configuration page

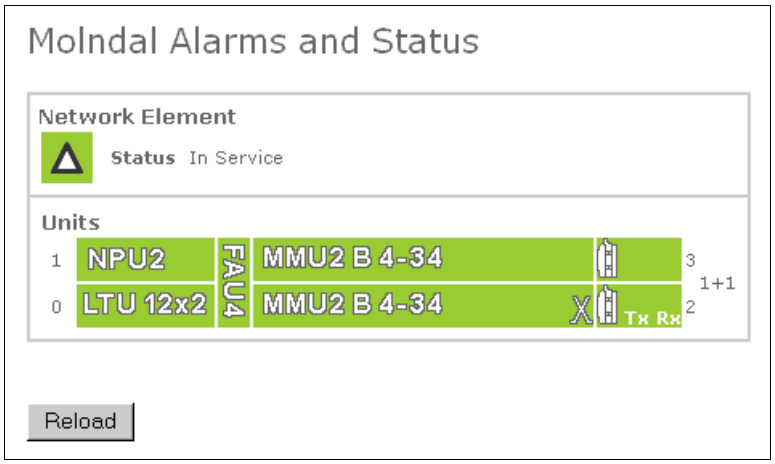


Figure 14 The Alarms and Status page for an AMM 2p

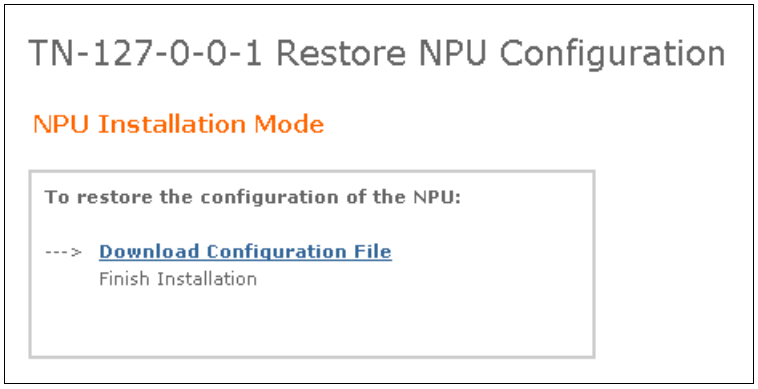


Figure 15 The Restore NPU Configuration page

3.3.2 Starting the LCT for NPU 8x2

This section describes how to start the LCT when working with an NPU 8x2. The NE is accessed using an Ethernet connection.

3.3.2.1 Operation Modes

The NE can operate in different modes providing different functions when working with the LCT. Below follows a short description of the different modes.

Node Installation Mode

This mode is used for initial setup of an NE, allowing a limited set of parameters to be set. It is also used for some specific maintenance procedures. The NE is accessed using a default IP address (`10.0.0.1`) and the PC (and the FTP server on the PC) obtains a dynamic IP address (`10.0.0.2`) from a DHCP server in the NE. This means that the PC should be configured to use dynamic IP addressing. However, using the static IP address `10.0.0.2` on the PC will also work.

Default user name and password are used for the NE and the FTP server, see Section 9.1 on page 135 and Section 3.2.1.3 on page 20.

The Node Installation mode is entered by pressing the BR button on the NPU 8x2 during NE power up, that is when the Fault (red), Power (green) and BR (yellow) LEDs on the NPU 8x2 are ON. The BR (yellow) LED will then start flashing, indicating that the NE is in Node Installation mode.

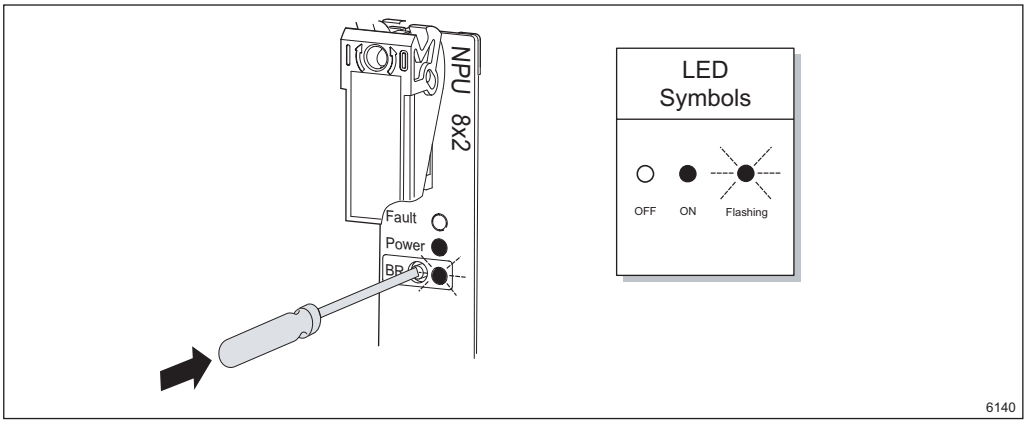


Figure 16 Entering Node Installation mode

When the initial setup is completed, the NE leaves Node Installation mode and goes into Normal mode. However, the Node Installation mode can always be left by pressing the BR button. An automatic save of the running configuration is always performed, when leaving the Node Installation mode.

The initial setup is described in Section 5 on page 49.

NPU Installation Mode

This mode is used for replacement of the NPU. The LCT will give the possibility to download a new configuration file in order to restore the configuration.

The NE is accessed using a default IP address (`10.0.0.1`) and the PC (and the FTP server on the PC) obtains a dynamic IP address (`10.0.0.2`) from a DHCP server in the NE. This means that the PC should be configured to use dynamic IP addressing. However, using the static IP address `10.0.0.2` on the PC will also work.

Default user names and passwords are used for the NE and the FTP server, see Section 9.1 on page 135 and Section 3.2.1.3 on page 20.

The NPU Installation mode is entered by inserting the NPU in an active NE and immediately pressing the BR button during NPU power up (Fault (red), Power (green) and BR (yellow) LEDs on the NPU are ON). The BR (yellow) LED will start flashing, indicating that the NE is in NPU Installation mode. The mode is also entered if the NPU 8x2 lacks a startup configuration file.

The NPU Installation mode is normally left as a result of the completed replacement procedure. However, the mode can always be left by pressing the BR button.

The procedure of replacing the NPU 8x2 is described in Section 10.6 on page 147.

Normal Mode

This mode is used for normal operation, allowing complete configuration possibilities. The NE is accessed using the IP address to be used during normal operation. It is typically found in the site documentation or on the information plate of the NE. The PC uses a static or dynamic IP address, depending on whether a DHCP server is used or not, and must be configured accordingly. It is recommended to use a DHCP server if available.

The BR (yellow) LED is OFF when the NE is in Normal mode.

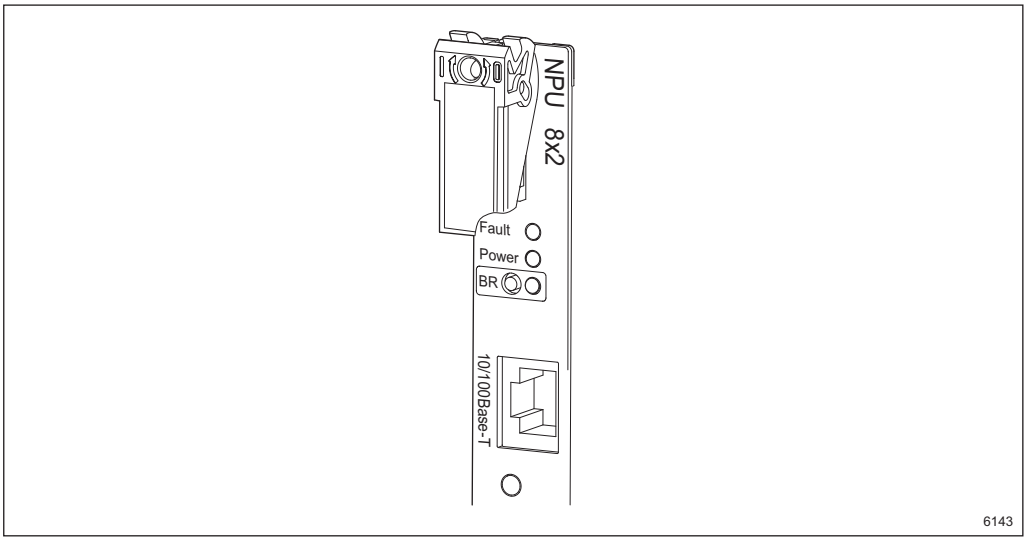


Figure 17 LEDs and BR button on the NPU 8x2. For a full description of the LEDs, see the MINI-LINK TN ETSI Indoor Installation Manual.

To start the LCT while the NE is in:

- Node/NPU Installation mode, see Section 3.3.2.2 on page 28.
- Normal mode, see Section 3.3.2.3 on page 29.

3.3.2.2 Starting the LCT in Node/NPU Installation Mode

1. Connect the Ethernet cable (twisted pair) between your PC and the 10/100BASE-T connector on the NPU 8x2.
2. Configure the PC to use a dynamic IP address obtained from the DHCP server in the NE. For more information on IP addressing, see Section 3.3.4 on page 32.

   Note: It is also possible to configure the PC to use the static IP address `10.0.0.2`.
3. Start a Web browser and make sure your browser is configured not to use a proxy server. For more information, see Section 3.3.5 on page 33.
4. In your Web browser, enter the URL **`http://10.0.0.1`**.

5. In the **Enter Network Password** dialog box, type the user name and password, and click **OK**. For more information see Section 9.1 on page 135.

   Figure 18 on page 29 shows an example of what will be displayed in your browser when in Node Installation mode. The initial setup is described in Section 5 on page 49.

   Should the NE be in NPU Installation mode, the LCT will give the possibility to download a new configuration file in order to restore the configuration, see Figure 19 on page 29. The procedure of replacing the NPU 8x2 is described in Section 10.6 on page 147.

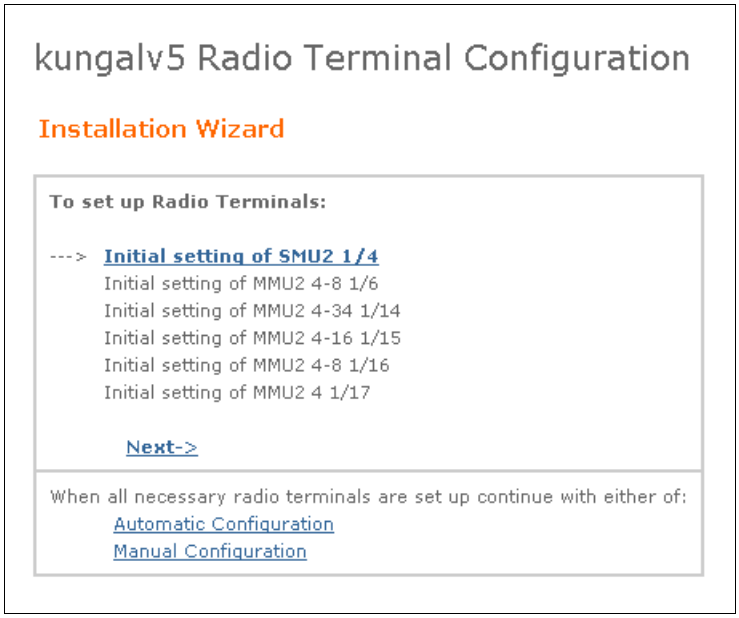


Figure 18 The Radio Terminal Configuration page

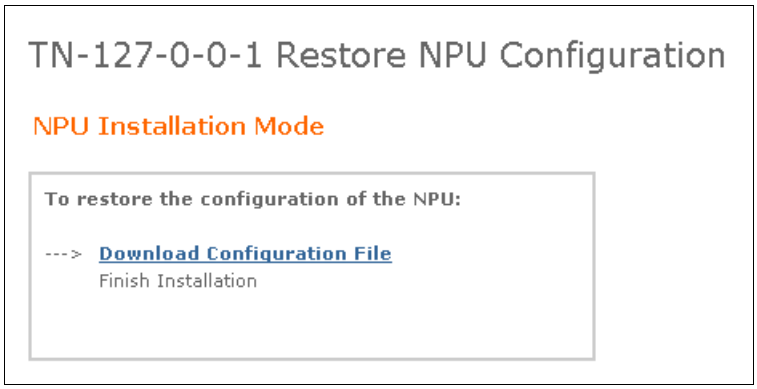


Figure 19 The Restore NPU Configuration page

3.3.2.3 Starting the LCT in Normal Mode

1. Connect the Ethernet (twisted pair) cable between your PC and the 10/100BASE-T connector on the NPU 8x2.

2. Make sure the PC is properly configured regarding the use of DHCP server. The configuration defines whether dynamic or static IP addressing should be used. It is recommended to use a DHCP server if available. For more information on IP addressing, see Section 3.3.4 on page 32.

3. Start a Web browser and make sure your browser is configured not to use a proxy server. For more information, see Section 3.3.5 on page 33.

4. Find out the IP address of the NE, typically from the site documentation or on the information plate of the NE and enter the URL **`http://`***`<IP address>`*.

5. In the **Enter Network Password** dialog box, type the user name and password, and click **OK**. For more information see Section 9.1 on page 135.

   Figure 20 on page 30 shows an example of what will be displayed in your browser: From here you can perform all operations, for example configuration, see Section 6 on page 59.

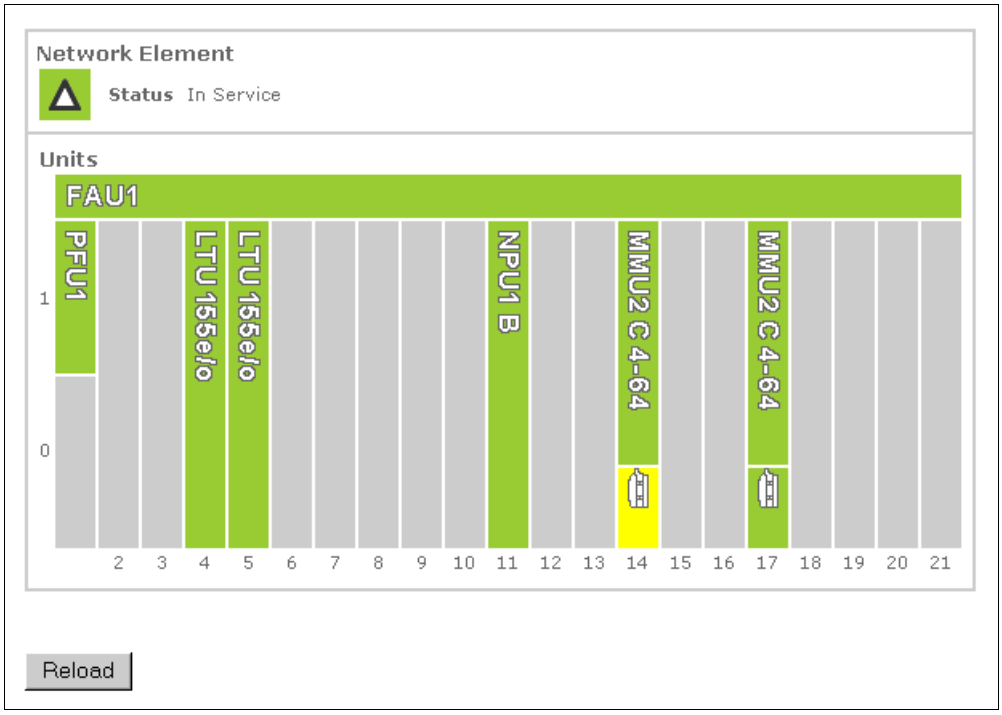


Figure 20 The NE Alarms and Status page for an AMM 20p

3.3.3 Starting the LCT for ATU (B)

This section describes how to start the LCT when working with an ATU (B). The NE is accessed locally using a USB connection and a default IP address (`10.0.0.1`). The PC (and the FTP server on the PC) obtains a dynamic IP address (`10.0.0.2`) from a DHCP server in the NE. This means that the PC should be configured to use dynamic IP addressing.

To start the LCT:

1. Make sure that the USB driver is installed on the PC, see Section 3.2.3 on page 21.

2. Connect the USB cable between your PC and the USB connector (O&M) on the ATU (B).

3. Configure the PC to use a dynamic IP address obtained from the DHCP server in the NE. For more information on IP addressing, see Section 3.3.4 on page 32.

   Note: It is also possible to configure the PC to use the static IP address `10.0.0.2`.

4. Start a Web browser and make sure your browser is configured not to use a proxy server. For more information, see Section 3.3.5 on page 33.

5. In your Web browser, enter the URL **`http://10.0.0.1`**.

6. In the **Enter Network Password** dialog box, type the user name and password, and click **OK**. For more information see Section 9.1 on page 135.

7. A non-configured NE lacks a configuration a file and an installation wizard will be provided for the initial setup, see Figure 21 on page 31. The initial setup is described in Section 5 on page 49.

   A configured NE will display a page like the one in Figure 22 on page 31. From here you can perform all operations, for example configuration, see Section 6 on page 59.

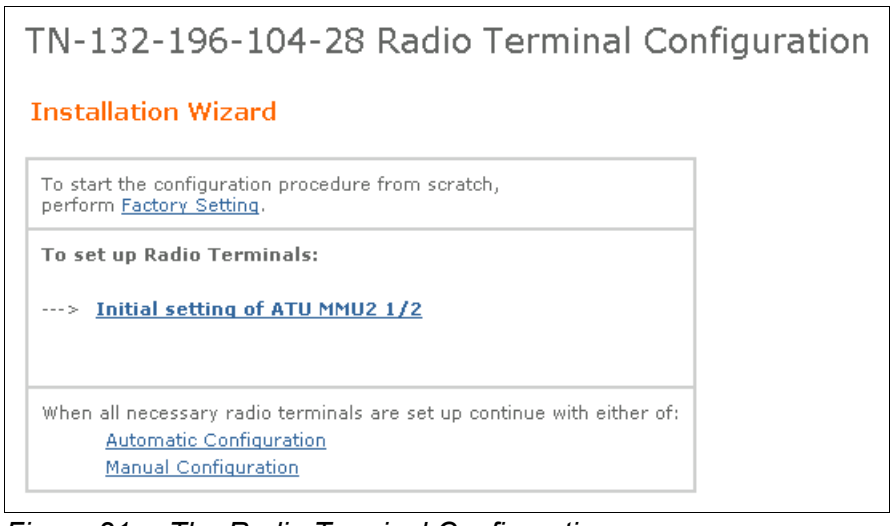


Figure 21 The Radio Terminal Configuration page

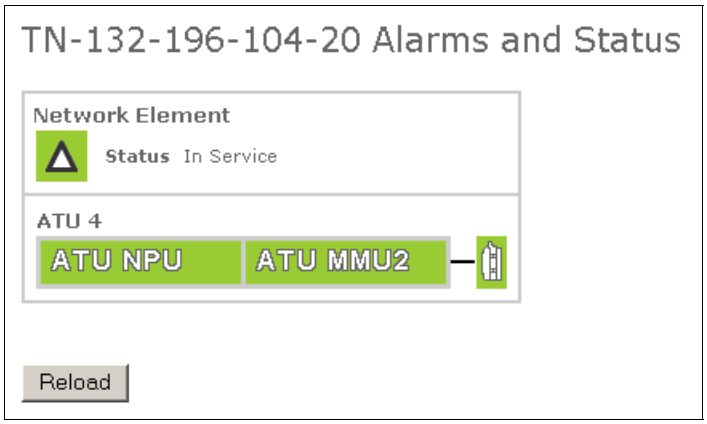


Figure 22 The Alarms and Status page for an ATU (B)

3.3.4 Configuring IP Addressing

Your PC can be configured to obtain a dynamic IP address from a DHCP server. Without the use of a DHCP server, only a static IP address can be used. Follow the instructions in the section that apply to your operating system.

3.3.4.1 Configuring IP Addressing in Windows 2000

To configure for static IP addressing:

1. On the **Start** menu, click **Control Panel**.
2. In **Control Panel**, double-click **Network and Dial-up Connections**.
3. In the **Network and Dial-up Connections** folder, right-click the connection to be used and click **Properties** on the shortcut menu.
4. In the **Connection Properties** dialog box, select **Internet Protocol (TCP/IP)** and click **Properties**.
5. In the **Internet (TCP/IP) Properties** dialog box, select **Use the following IP address**.
6. Type **IP Address** and **Subnet Mask**.
7. Click **OK**.

To configure for dynamic IP addressing:

1. On the **Start** menu, click **Control Panel**.
2. In **Control Panel**, double-click **Network and Dial-up Connections**.
3. In the **Network and Dial-up Connections** folder, right-click the connection to be used and click **Properties** on the shortcut menu.

4. In the **Connection Properties** dialog box, select **Internet Protocol (TCP/IP)** and click **Properties**.
5. In the **Internet (TCP/IP) Properties** dialog box, select **Obtain an IP address automatically**.
6. Click **OK**.

3.3.4.2 Configuring IP Addressing in Windows XP

To configure for static IP addressing:

1. On the **Start** menu, click **Control Panel**.
2. In **Control Panel**, double-click **Network Connections**.
3. In the **Network Connections** folder, right-click the connection to be used and click **Properties** on the shortcut menu.
4. In the **Connection Properties** dialog box, select **Use the following IP address**.
5. Type **IP Address** and **Subnet Mask**.
6. Click **OK**.

To configure for dynamic IP addressing:

1. On the **Start** menu, click **Control Panel**.
2. In **Control Panel**, double-click **Network Connections**.
3. In the **Network Connections** folder, right-click the connection to be used and click **Properties** on the shortcut menu.
4. In the **Connection Properties** dialog box, select **Obtain an IP address automatically**.
5. Click **OK**.

3.3.5 Configuring Internet Explorer Not to Use a Proxy Server

This section describes how to configure your browser not to use a proxy server.

To configure Internet Explorer:

1. On the **Tools** menu, click **Internet Options**.
2. In the **Internet Options** dialog box, click the **Connections** tab.
3. Click **LAN Settings**.
4. In the **Local Area Network (LAN) settings** dialog box, clear the **Use a proxy server** check box and click **OK**.

3.4 Uninstalling Software

The following should be uninstalled if you want to remove all LCT related software from the PC:

- BulletProof FTP server, see Section 3.4.1 on page 34.
- MINI-LINK Service Manager (MSM), see Section 3.4.2 on page 34.
- USB driver, see Section 3.4.3 on page 34.
- Load modules Section 3.4.4 on page 34.

3.4.1 Uninstalling BulletProof FTP Server

To uninstall the FTP server:

1. On the **Start** menu, point to **Programs→BulletProof FTP Server** and then click **Uninstall**.
2. Follow the instructions on the screen.

3.4.2 Uninstalling MINI-LINK Service Manager (MSM)

Uninstall MSM according to the *MSM Installation Guide*.

3.4.3 Uninstalling USB Driver

To uninstall the USB driver:

1. Connect the USB cable between your PC and the USB connector on the NPU or ATU (B).
2. Remove the USB hardware device using the **Control Panel**. This is described in detail in the file `C:\Program Files\Ericsson\USBLAN \readme.txt`.
3. Uninstall USBLAN, by double-clicking the file `C:\Program Files\Ericsson\USBLAN\uninstall.exe`.
4. Do a manual file search for `erblan*` and delete the files found.

3.4.4 Uninstalling Load Modules

To uninstall load modules.

1. Start **Windows Explorer** and locate the *<drive:>*`\tn_ftp_home\tn_system_release\ml_tn_software` folder.
2. Select a folder containing load modules or a specific load module, right-click and then click **Delete**.

4 Using the EEM

This section describes the basics of how to work with the EEM.

4.1 User Interface Overview

Figure 23 on page 35 shows the different parts of the EEM user interface. The main frame displays information on different pages, further described in Section 11 on page 157. The other parts are described in the following sections.

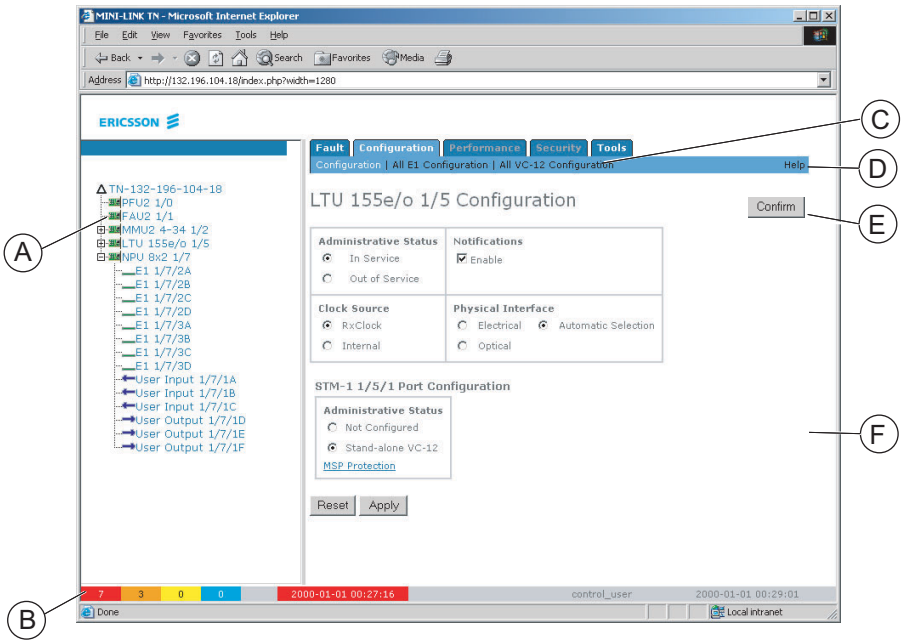


Figure 23 EEM user interface

A	Navigation Tree	**D**	Help
B	Status Bar	**E**	Confirm button
C	Menu	**F**	Page

4.2 Navigation Tree

The Navigation Tree is used to locate entities of different types, that is the NE, plug-in units, interfaces and ports. It is only available in Normal mode.

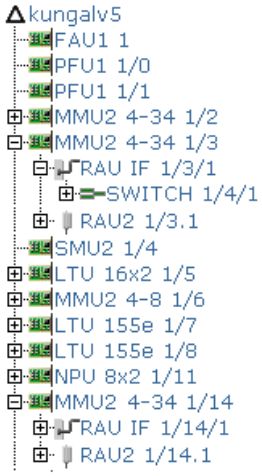


Figure 24 The Navigation Tree

Each entity is displayed with an icon and name. Entities that contain sub-entities, for example a plug-in unit that contains interfaces, are displayed with a plus-sign in front of its icon. When the plus-sign or the icon is clicked the entity is expanded and the sub-entities are displayed.

The NE is located at the top of the tree and the plug-in units are located below. A plug-in unit can contain interfaces and/or ports in different structures depending on the unit type and the current configuration of the unit. An interface can contain higher layer interfaces. In this case the interface icon has a plus-sign that displays the higher layer interfaces when selected.

4.3 Menus

The functionality of the EEM is represented by pages reached by clicking menu commands. The menus change dynamically depending on what type of entity (plug-in units, interfaces etc.) you have selected in the Navigation Tree. Different menus are provided depending on the NE's mode of operation. A dimmed menu indicates a non-available function for the selected entity.

4.3.1 Menus in the Installation Wizard

An installation wizard for the initial setup is provided in the following cases:

- A non-configured NPU2/NPU1 B NE or ATU (B). The wizard will also be available when the initial setup is finished.

- An NPU 8x2 NE in Node Installation mode.

The menu commands are described below.

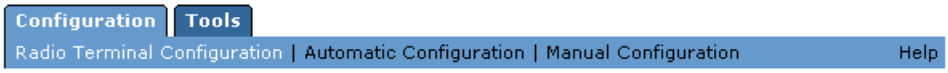


Figure 25 Menus in the installation wizard

- **Configuration** — Displays a menu with configuration commands.
  - **Radio Terminal Configuration** — Opens the **Radio Terminal Configuration** page, providing a guide for initial configuration of Radio Terminals, see Section 11.1 on page 158.
  - **Automatic Configuration** — Opens the **Automatic Configuration** page, providing a guide for initial configuration of the NE using a configuration file, see Section 11.2 on page 159. This always includes configuration of security, DCN and system parameters. Depending on the contents of the configuration file, it could also include the configuration of plug-in units and interfaces.
  - **Manual Configuration** — Opens the **Manual Configuration** page, providing a guide for configuration of the NE without using a configuration file, see Section 11.3 on page 160. This includes configuration of security, DCN and system parameters.
  - **Exit Wizard** — Exits the installation wizard.
- **Tools** — Displays a menu with miscellaneous commands.
  - **Change Password** — Opens the **Change Password** page, where you can change the passwords for the control_user and view_user, see Section 11.8 on page 165.
  - **Emergency Fallback** — Opens the **Emergency Fallback** page, where you can activate the previous NPU software release, see Section 11.9 on page 166.
  - **Factory Setting** — Opens the **Factory Setting** page, where you can delete an existing configuration file and revert the NE to factory setting, see Section 11.11 on page 168. Only available if there is an existing configuration file.
  - **Help Setup** — Opens the **Help Setup** page, where you can specify the location of the Help file, see Section 11.90 on page 279.
- **Help** — Displays information on the functions available on a specific page. Available on all menus.

4.3.2 Menus in NPU Installation Mode

The menu commands in NPU Installation mode are described below.

Figure 26 Menus in NPU Installation mode

- **Configuration** — Displays a menu with configuration commands.
  - **Restore NPU Configuration** — Opens the **Restore NPU Configuration** page, providing a guide to restore the NPU, see Section 11.14 on page 171.
- **Tools** — Displays a menu with miscellaneous commands.
  - **Help Setup** — Opens the **Help Setup** page, where you can specify the location of the Help file, see Section 11.90 on page 279.
- **Help** — Displays information on the functions available on a specific page. Available on all menus.

4.3.3 Menus in Normal Mode

The menu commands in Normal mode are described below. The available commands on a menu depend on the selected entity.

Figure 27 Menus in Normal mode

- **Fault** — Displays a menu with fault commands.
  - **Alarms and Status** — Opens an **Alarms and Status** page for an entity, where you can view alarm and status information. See for example Section 11.115 on page 320.
  - **Alarm List** — Opens the **Alarm List** page, where you can view all active alarms for the NE, a unit or interface, see Section 11.133 on page 349.
  - **Event Log** — Opens the **Event Log** page for the NE, where you can access alarm and event information in the Event Log, see Section 11.134 on page 351.
  - **Error Log** — Opens the **Load Error Log** page, where you can load an Error Log from the NE to the FTP server, see Section 11.135 on page 353. It is also possible to delete the Error Log.
  - **DCN** — Opens the **Ethernet/LAN Status** page for the NE, where you can view the status of the Ethernet interface, see Section 11.94 on page 287. From this page you can also reach other pages displaying

DCN related status parameters, see Section 11.96 on page 290 to Section 11.107 on page 309.

- **Ethernet Bridge** — Opens the **Ethernet Bridge Status** page, where you can view the status of the Ethernet Bridge implemented in the NPU2 and ATU (B), see Section 11.92 on page 282.

- **Activities** — Opens the **Activities** page, where you can view the status of software upgrade, loops and BERTs in the NE, see Section 11.136 on page 354.

- **Configuration** — Displays a menu with configuration commands.

  - **Configuration** — Opens a **Configuration** page, where you can configure an entity. See for example Section 11.33 on page 194.

  - **Traffic Routing** — Opens the **Traffic Routing Select Interfaces** page for the NE, where you set up traffic routing for E1 interfaces, see Section 11.56 on page 230.

  - **1+1 E1 SNCP** — Opens the **1+1 E1 SNCP Select Interfaces** page for the NE, where you can create SNCP protections for E1 interfaces, see Section 11.62 on page 239.

  - **Basic NE** — Opens the **Basic NE Configuration** page, where you can specify general NE parameters, see Section 11.15 on page 172.

  - **DCN** — Opens the **Ethernet/LAN/Servers Configuration** page for the NE, where you can specify parameters for Ethernet communication and DCN servers, see Section 11.16 on page 174. Other pages for DCN configuration are accessible from this page.

  - **Load Configuration** — Opens the **Load Configuration** page for the NE, where you can upload and download configuration files, see Section 11.87 on page 275.

  - **Ethernet Bridge** — Opens the **Ethernet Bridge Configuration** page, where you can set the number of E1s to be used for transmission of Ethernet traffic, see Section 11.30 on page 191.

  - **Installation Wizard** — Opens the installation wizard for an NPU2/NPU1 B or ATU (B) NE, see Section 4.3.1 on page 36.

  - **All E1 Configuration** — Opens the **All E1 Configuration** page for a plug-in unit with E1 interfaces, see Section 11.52 on page 225. The page is used to configure all E1 interfaces on the plug-in unit simultaneously.

  - **All VC-12 Configuration** — Opens the **All VC-12 Configuration** page, where you can configure all VC-12 interfaces on the LTU 155 simultaneously, see Section 11.48 on page 220.

  - **Protection** — Opens the **SWITCH Protection** page, where you can configure the protection of a Radio Terminal, see Section 11.43 on page 211.

  - **Reset** — Opens the **Reset Configuration** page, where you can reset the configuration of a Radio Terminal with MMU2 B/C to default values, see Section 11.40 on page 208.

  - **Restore** — Opens the **Restore Configuration** page, where you can restore configuration of a Radio Terminal with MMU2 B/C, see Section 11.41 on page 209.

- **Performance** — Displays a menu with performance commands.

  - **Performance** — Opens a **Performance** page, where you can view performance data for an interface. See for example Section 11.145 on page 371.

  - **Power** — Opens the Power page, where you can view input and output power performance data for the RF interface on the RAU, see Section 11.149 on page 377.

- **Security** — Displays a menu with security commands.

  - **Security** — Opens the **Security** page for the NE, where you set security parameters, see Section 11.151 on page 380.

- **Tools** — Displays a menu with miscellaneous commands.

  - **Report** — Opens the **Report** page for the NE, where you can generate a configuration and inventory report, see Section 11.74 on page 257.

  - **Loops** — Opens the **Loops** page where loops can be set on interfaces for fault localization. This page can be opened on unit or interface level, see Section 11.138 on page 357. It also possible to select **Loops** on NE level, opening a page with links to unit and interface level, see Section 11.137 on page 356.

  - **Inventory** — Opens the **Inventory** page for the NE, where hardware and software inventory data is displayed, see Section 11.72 on page 255.

  - **Restart** — Opens the **Restart** page, where you can restart the NE or a plug-in unit, see Section 11.89 on page 278.

  - **Test** — Opens the **Test** page, where you can start a BERT on an E1 interface for performance evaluation, see Section 11.150 on page 378. The page can be opened for an NE, E1 interface or a plug-in unit that contains an E1 interface.

  - **Software Upgrade** — Opens a wizard, where you can upgrade the NE with a new baseline or specific load modules, see Section 11.76 on page 260 and Section 11.77 on page 262.

  - **Help Setup** — Opens the **Help Setup** page, where you can specify the location of the Help file, see Section 11.90 on page 279.

- **Help** — Displays information on the functions available on a specific page. Available on all menus.

4.4 Status Bar

The Status Bar gives a summary of all alarms and is found at the bottom of all pages. It also displays additional information as described in Table 2 on page 41. The Status Bar is automatically updated every tenth second.

Note: If the Status Bar is not displayed properly, the page must me refreshed.

Figure 28 The Status Bar

Table 2 Status Bar information

Item	Description
Red field 8	Displays the number of alarms with severity *Critical*. Clicking the field opens the **Alarm List** page displaying all alarms with this severity, see Section 11.133 on page 349.
Orange field 1	Displays the number of alarms with severity *Major*. Clicking the field opens the **Alarm List** page displaying all alarms with this severity, see Section 11.133 on page 349.
Yellow field 0	Displays the number of alarms with severity *Minor*. Clicking the field opens the **Alarm List** page displaying all alarms with this severity, see Section 11.133 on page 349.
Blue field 4	Displays the number of alarms with severity *Warning*. Clicking the field opens the **Alarm List** page displaying all alarms with this severity, see Section 11.133 on page 349.
Activities Activities	Opens the **Activities** page, where you can view the status of loops, BERTs and software upgrade in the NE, see Section 11.136 on page 354.
Date and time 2001-11-13 10:11:02	The date and time of the last notification. The background color depends on the severity of the last notification.
Confirm Confirm 14:16	Indicates the time left before the NE reverts to the last saved configuration. Clicking the field will allow you to confirm the configuration of some specific DCN related parameters. A pop-up dialog is displayed when there are 3, 2 and 1 minutes left. Only available if you are logged on as control_user. For more information, see Section 4.5 on page 42.

Item	Description
User name control_user	Displays the user name currently logged on.
Clock 2003-01-17 11:25:33	The date and time kept by the NE timer.

4.5 Confirm Button

Configuration of parameters that could lead to loss of a DCN channel, for example change of IP address, need to be confirmed. The confirmation is made automatically if an NE generated ping command to the EEM PC is successful. Otherwise, the confirmation must be done manually. This is done using the **Confirm** button 

, displayed in the upper right-hand corner on a page. The button is only displayed in Normal mode.

The **Status Bar** indicates the remaining time and warnings will be issued when time is running out.

Caution!

If you do not confirm your configurations within 15 minutes, the NE will make a warm restart, restoring the saved configurations, and your unconfirmed changes will be lost.

Note: The contact with the Web server in the NE will be lost during the restart.

4.6 Using the Help

The Help provides on-screen information about the user interface as well as working instructions. Information on a specific page is accessed by clicking **Help** on a menu.

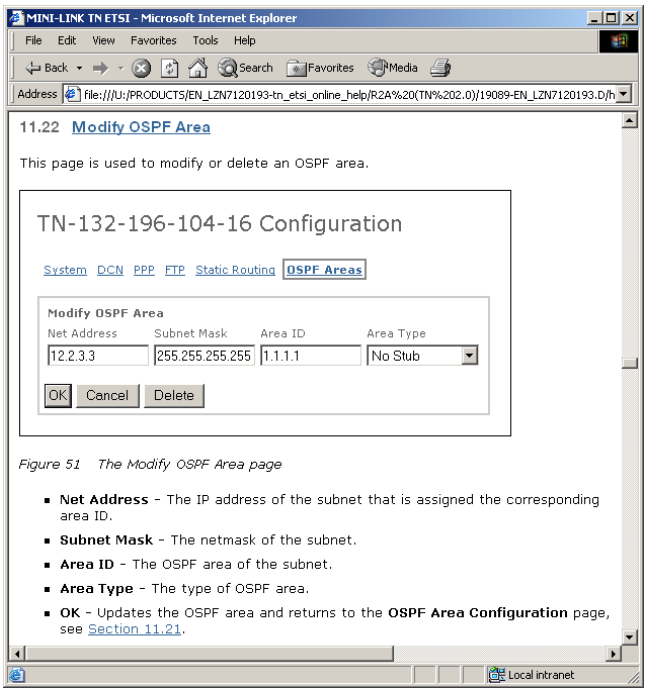


Figure 29 Help window

The Help file can be located on a PC or on a Web server. It is available on the MINI-LINK Service Software CD (LZY 214 2358/1) or on the internal Ericsson web. The help file is named `19089-EN_LZN7120177.<version>.zip` or similar and should be unpacked preserving the internal directory structure.

To install the Help on the local drive:

1. Extract the file to `C:\`.

   Note: Make sure the internal directory structure is preserved. When using WinZip, the **Use folder names** check box must be selected in the **Extract** dialog box.

2. The help file will be unpacked with the following path: `C:\MINI-LINK\Documentation\TN_help\ETSI_<revision>\help.html`

When installing the Help file on a web server, `C:` is replaced by *<URL>*.

To be able to access the Help, the location of the file must be pointed out. The location is saved as a cookie in your browser, one for each NE, but it is sometimes necessary to do a new setup, for example if a new version is available.

To set up the Help:

1. On the **Tools** menu, click **Help Setup**.

2. On the **Help Setup** page, do one of the following:
   - To access the Help from the PC, click **Insert default local path** and add `ETSI_<revision>/help.html`.
   - To access the Help from a Web server, select **Insert default server path** and add `ETSI_<revision>/help.html`.

3. Click **Apply**.

   Note: If the Help cannot be accessed, make sure that cookies are enabled in your browser and that you have typed the correct path or URL.

   Note: A security feature in Internet Explorer 6 SP1 sometimes denies the browser to access the Help file on your PC. Should this occur do the following in your browser: Click **Tools->Internet Options->Security** and add `http://<IP address of the NE>` as a “Trusted Site”.

4.7 Naming Principles

This section describes the principles used to denote the NE, plug-in units, ports and interfaces.

4.7.1 Naming of the NE

The NE name is specified in the **Name** box on the **System Configuration** page, see Section 11.15 on page 172. The name is used for example to denote the root in the Navigation Tree.

4.7.2 Naming of Physical Entities

Physical entities in the AMM are named as: *Name + Magazine/Position/Port*.

For example an NPU 8x2 in position 11 in an AMM 20p gives the following names:

- *NPU 8x2 1/11* for the plug-in unit.
- *User Input 1/11/1A* for User Input port A on connector 1 on the plug-in unit.
- *E1 1/11/2A* for E1 port A on connector 2 on the plug-in unit.

An RAU is denoted in accordance with the MMU it is connected to. For example an *RAU 1/6.1* is connected to an *MMU2 4-34 1/6*.

4.7.3 Naming of Interfaces

Interfaces are named as: *Name* + *Magazine/Position/Port* + *Hierarchy Number*, where:

- *Magazine/Position/Port* denotes the port to which the interface is connected.

- *Hierarchy Number*, comprising up to three digits, is used when applicable according to the following principles:

  - It is not used when there is one-to-one mapping between the interface and the port:

    - *E1 1/11/2A* denotes the E1 interface on the port with the same name.

    - MS/RS, MSP and VC-4 are denoted identical to the STM-1 port on the LTU 155. For example *MS/RS 1/4/1* on an *LTU 155 1/4*.

    - *RAU IF 1/6/1* denotes the radio interface on the *MMU2 4-34 1/6*.

  - It is used to denote contained interfaces as in the following examples:

    - The radio interface *RAU IF 1/6/1* contains an *E3 1/6/1 1* and an *E1 1/6/1 2*.

    - *E3 1/6/1 1* contains four E2 interfaces denoted *E2 1/6/1 1.1*, *E2 1/6/1 1.2* etc.

    - *E2 1/6/1 1.1* contains four E1 interfaces denoted *E1 1/6/1 1.1.1*, *E1 1/6/1 1.1.2* etc.

  - VC-12 are denoted using standard SDH KLM numbering. For example *VC-4 1/2/1* contains *VC-12 1/2/1 a.b.c* where $1 \leq a \leq 3$, $1 \leq b \leq 7$ and $1 \leq c \leq 3$.

  - An *s* at the end of the hierarchy number indicates an E1 over a VC-12. For example *E1 1/8/1 1.2.3s* over *VC-12 1/8/1 1.2.3*.

The following principles also apply:

- For a protected (1+1) Radio Terminal with SMU2, the interfaces below the two radio interfaces are denoted in accordance with the identity of the SMU2. For example:

  - A terminal comprises *MMU2 4-34 1/6*, *MMU2 4-34 1/7* and *SMU2 1/8*. The radio interfaces are denoted *RAU IF 1/6/1* and *RAU IF 1/7/1*. The active *RAU IF 1/6/1* holds the *SWITCH 1/8/1* interface. A contained E3 interface is denoted *E3 1/8/1 1* below both radio interfaces.

- *RF* indicates the RAU's interface with an antenna. For example *RF 1/6.1/1* in an *RAU 1/6.1* connected to an *MMU2 4-34 1/6*.

- The name of the protected E1 interface in a 1+1 E1 SNCP protection ends with an asterisk (*). Furthermore, the protected E1 interface inherits the name of the first of the two unprotected E1s. For example:
  - The unprotected *E1 1/3/4A* and *E1 1/3/3C* interfaces are used to create the protected *E1 1/3/4A** interface.
- MSP protection follows the same principle as 1+1 E1 SNCP protection. For example:
  - The *MS/RS 1/4/1* and *MS/RS 1/5/1* interfaces are used to create the protected *MSP 1/4/1** interface. The asterisk is propagated to all contained interface names.
- A PPP interface over an E1 gets the same name as the E1.
- The two PPP interfaces in a Radio Terminal are named for example *1/4/1 SC1* and *1/4/1 SC2*.
- The PPP interfaces over STM-1 are named for example *1/5/1 MS:D4-6*, *1/5/1 MS:D7-9*, *1/5/1 MS:D10-12* or *1/5/1 RS:D1-3*.
- An ML-PPP interface is named *<near end IP address> - <far end IP address>*.
- The HDLC interface is named according to the near end MAC address, for example *00:80:37:89:89:89 - IM*.
- The IM interface gets the name according to its server E1, for example *IM 1/2/1 1.1*.

4.8 EEM Troubleshooting

This section contains descriptions of potential EEM related problems that could occur and instructions how to solve them.

4.8.1 Graphical Layout Problems in the Browser

After a software upgrade, there is a possibility that the browser experiences some graphical layout problems, for example wrong background color for the menu, wrong tree icons or plug-in unit pictures. This behavior is caused by the caching mechanism of the browser, often Internet Explorer 5.5 and 6. To solve this problem you have to clear the cache file of the browser.

To clear the cache file in Internet Explorer:

1. On the **Tools** menu, click **Internet Options**.
2. In the **Internet Options** dialog box, click **Delete Files**.
3. In the **Delete Files** dialog box, select the **Delete all offline content** check box and click **OK**.

4.8.2 MSM Launch Failure

MSM 6.4 or later must be installed on the PC in order to completely manage a Radio Terminal with MMU2. During the installation an association is created making it possible to launch MSM from the EEM.

Should the launch of MSM fail displaying an error message similar to `Error opening file C:\DOCUMENTS AND SETTINGS\ADMINISTRATOR\LOCAL SETTINGS\TEMPORARY INTERNET FILES\CONTENT.IE5\O5QNCPYN\TEST[1].mxm`, you have to delete the temporary Internet files on your PC.

Should the launch of MSM otherwise fail, reinstall MSM according to the instructions in *MSM Installation Guide*.

5 Initial Setup

This section describes the initial setup performed during the installation of a new NE. The initial setup is done following an installation wizard presented in the following cases:

- A non-configured NPU2/NPU1 B NE or ATU (B) when connected with an USB cable. You can exit the wizard at any time by clicking **Exit Wizard** on the **Configuration** menu. The wizard will also be available when the initial setup is finished.
- An NPU 8x2 NE in Node Installation mode.

The initial setup includes two major steps:

- *Radio Terminal Configuration*, see Section 5.1 on page 49.
- *Configuration of NE Parameters*, that is security, DCN, and system parameters. This can be done in two ways:
  - *Automatic Configuration* using a configuration file, see Section 5.2 on page 53.
  - *Manual Configuration* without using a configuration file, see Section 5.3 on page 54.

When the initial setup is completed the configuration is continued in Normal mode, see Section 6 on page 59.

5.1 Radio Terminal Configuration

The Radio Terminal configuration in the installation wizard is a part of the hardware installation procedure in order to establish communication over a hop. As a minimum, the Radio Terminals used for DCN communication must be configured at this stage. The DCN is a requirement for remote configuration of the NE after the installation. For more information on DCN configuration, see Section 6.10 on page 85.

The Radio Terminal configuration is started indoors with a station radio cable connecting the MMU and the RAU. For further instructions, see *MINI-LINK TN ETSI Indoor Installation Manual* or *ATU Installation Instruction*.

The procedure for configuration of the Radio Terminal depends on the MMU type:

- *Configuring a Radio Terminal with MMU2 or ATU (B)*, see Section 5.1.1 on page 50.
- *Configuring a Radio Terminal with MMU2 B/C*, see Section 5.1.2 on page 51.

5.1.1 Configuring a Radio Terminal with MMU2 or ATU (B)

Note: For NPU2/NPU1 B NE and ATU (B), you can exit the wizard at any time by clicking **Exit Wizard** on the **Configuration** menu.

To configure a Radio Terminal with MMU2:

1. On the **Radio Terminal Configuration** page, click **Next** until **Initial setting of MMU2 ...** appears as a link for the unit you want to configure, and then click the link. For a protected (1+1) terminal any of the two MMU2s can be selected.
2. On the **MMU2 Configuration** page, under **Protection Mode**, select one of the following:
   - **Prepare for 1+0 configuration**, for a 1+0 terminal.
   - **Prepare for 1+1 configuration**, for a 1+1 terminal.

   Click **Apply**. The page is reloaded and displays information about administrative status and notifications for the unit.

   Note: The 1+1 configuration is only possible if the units are placed in adjacent AMM positions according to specifications in *MINI-LINK TN ETSI Indoor Installation Manual*.

   Note: This step is not applicable for ATU (B).
3. For each unit, select **In Service** and clear the **Enable** check box.
4. Click **Apply**.
5. Click **Perform AM Setup and Hop Setup**.
6. In MSM, perform an AM and Hop Setup. Follow the instructions in *MSM User Guide* or *MSM online Help*. Exit MSM when finished.
7. On the **MMU2 Configuration** page , select the **Enable** check box for all units in the Radio Terminal and click **Apply**.
8. Repeat the procedure if more terminals should be configured.

This procedure is followed by outdoor equipment installation, indoor and outdoor radio cabling, and antenna alignment. Follow the instructions in *MINI-LINK TN ETSI Indoor Installation Manual* or *ATU Installation Instruction*, and *MINI-LINK TN, MINI-LINK HC, MINI-LINK E Outdoor Installation Manual*.

The initial setup is finished by the configuration of NE parameters, that is security, DCN and system parameters. This can be done in two ways:

- *Automatic Configuration using a configuration file*, see Section 5.2 on page 53.
- *Manual Configuration without using a configuration file*, see Section 5.3 on page 54.

5.1.2 Configuring a Radio Terminal with MMU2 B/C

Note: To configure a protected (1+1) terminal, you must first configure two temporary unprotected (1+0) Radio Terminals, one for each MMU that will be part of the final protected terminal.

You can then go **Back** in the wizard and create a protected terminal by changing the protection mode of the MMU in the lower position to **1+1**. Optionally, you can exit the wizard and then create the protected terminal as described in Section 6.4.2 on page 64.

To be able to configure a protected terminal, the following conditions apply:

- The MMUs must be placed in adjacent AMM positions according to specifications in *MINI-LINK TN ETSI Indoor Installation Manual*.
- Both of the temporary terminals must be configured to use the same traffic capacity, modulation method, and identity.
- For 1+1 Hot configurations, both RAUs must have *the same* frequency.
- For 1+1 Work configurations, both RAUs must have *different* frequencies.

Note: For NPU2/NPU1 B NE and ATU (B), you can exit the wizard at any time by clicking **Exit Wizard** on the **Configuration** menu.

To configure a Radio Terminal with MMU2 B/C:

1. On the **Radio Terminal Configuration** page, click **Next** until **Initial setting of MMU2 B/C [...]** appears as a link for the unit you want to configure, and then click the link.
2. Click **Perform MMU2 B/C [...]** to open the **MMU2 B/C Configuration** page.
3. Under **ID**, type the identity of this Radio Terminal in the **Near End** box.
4. If this terminal should send notifications, select the **Notifications** check box.
5. If an alarm should be generated when the received traffic originates from the wrong far-end, type the expected far-end identity in the **Far End** box, and select the **Radio ID Check** check box.
6. Under **Traffic Capacity**, select the wanted traffic capacity.

7. Under **Protection Mode**, select the wanted protection mode.

   Note: If you are creating a temporary unprotected terminal, select **1+0**.

8. Click **Apply** to set the protection mode.
9. Under **BER Alarm Threshold**, select the threshold for generating BER alarms.
10. Under **Modulation**, select the wanted modulation method.
11. Under **MMU2 B/C <ID>**, select all check boxes.
12. Click **Apply**, then click **Next**.
13. Click **Perform RAU [...]** to open the **RAU Configuration** page.
14. Under **Near End Radio Terminal <ID>**, select all check boxes.
15. Under **RAU <ID>**, type the transmit frequency in the **Tx Frequency** box.
16. Select the **Transmitter On** check box.
17. In the **Tx Attenuator** box, type the value of the fixed attenuator (if used).
18. In the **Output Power Mode** list, select how the output power is to be controlled.

    Note: The **ATPC** option is only available when all units in the radio link support ATPC. Click **Show ATPC Capabilities** to see which units support ATPC.

19. Do one of the following:

If	Then
RTPC is selected	type the **Output Power** value.
ATPC is selected	type the **Max Output Power** and **Target Input Power (far-end)** values.

20. In the **RF Input Alarm Threshold** box, type the threshold for generating RF Input Threshold alarms.
21. Click **Apply**, then click **Next**.
22. If you have configured a protected terminal, click **Perform Protection Configuration** to open the **SWITCH Protection** page.
23. Configure the protection as described in Section 11.43 on page 211.
24. Click **Apply**, then click **Next**.
25. Click **Next**.

26. Repeat this procedure if more terminals should be configured.

    Note: When you have configured the two temporary unprotected terminals, you can go **Back** in the wizard and create a protected terminal by changing the protection mode of the MMU in the lower position to **1+1**.

This procedure is followed by outdoor equipment installation, indoor and outdoor radio cabling, and antenna alignment. Follow the instructions in *MINI-LINK TN ETSI Indoor Installation Manual* or *ATU Installation Instruction*, and *MINI-LINK TN, MINI-LINK HC, MINI-LINK E Outdoor Installation Manual*.

The initial setup is finished by the configuration of NE parameters, that is security, DCN and system parameters. This can be done in two ways:

- *Automatic Configuration using a configuration file*, see Section 5.2 on page 53.
- *Manual Configuration without using a configuration file*, see Section 5.3 on page 54.

5.2 Automatic Configuration of NE Parameters

This section describes the configuration of NE parameters, using a configuration file. This always includes configuration of security, DCN and system parameters. The configuration file could also include the configuration of plug-in units and interfaces.

The configuration files are located in the `<drive:>\tn_ftp_home\tn_backup_configuration` folder on the FTP server. A configuration file is named `<hostname>.cfg` where `<hostname>` is typically the name or IP address of an NE. The file extension `.cfg.old` is used when a configuration file is uploaded using a file name that already exists.

Note: For NPU2/NPU1 B NE and ATU (B), you can exit the wizard at any time by clicking **Exit Wizard** on the **Configuration** menu.

To configure the NE parameters automatically:

1. On the **Configuration** menu, click **Automatic Configuration**.
2. On the **Automatic Configuration** page, click **Download Configuration File**.
3. On the **Load Configuration** page, type the **File Name** and then click **Apply**.

4. On the **Load Configuration Progress** page, click **Update Progress** until the download is finished. If the configuration file requires new software to be loaded, this will be done automatically. This requires that the software is present in the *<drive:>*\tn_ftp_home\tn_system_release\ml_tn_software folder.

   A progress bar displays the progress of the software upgrade. When the download and software upgrade is finished, the NE will make a warm restart. After the restart you can continue with the configuration of the plug-in units and their interfaces, see Section 6 on page 59.

5. For an NPU 8x2 the following also applies:

   After the restart it will run in Normal mode. The IP address of the NE is changed during the automatic configuration. To start the LCT in Normal mode you have to enter the URL **http://***<IP address>* where IP address is typically found in the site documentation or on the information plate of the NE. See also Section 3.3.2.3 on page 29.

5.3 Manual Configuration of NE Parameters

This section describes the configuration of the NE parameters, without using a configuration file. This includes configuration of security, DCN and system parameters.

Note: Make sure the Radio Terminals which will carry DCN are up and that the antennas are aligned before starting this procedure, see Section 5.1 on page 49.

Note: The procedure below may contain steps not applicable to your configuration.

Note: For NPU2/NPU1 B NE and ATU (B), you can exit the wizard at any time by clicking **Exit Wizard** on the **Configuration** menu.

To configure the NE parameters manually:

1. On the **Configuration** menu, click **Manual Configuration**.

Performing a Local Software Upgrade

2. On the **Manual Configuration** page, click **Perform Software Upgrade**. If a software upgrade is not required click **Next** and continue to Step 8 on page 55.

3. On the **Software Upgrade – Installation Wizard** page, under **Desired Baseline**, enter the **Product Number** and **Release** of the new baseline.

4. Click **Start Upgrade**. The **Upgrade Progress – Baseline** page monitors the download of the new software. The page is refreshed every fifth second. When all load modules have been correctly received, the baseline gets status `Upgrade Finished` and the **Activate** button appears.

5. Click **Activate**. When the activation is done, the **Confirm New System Configuration** page is displayed.

   Note: You can check if the restart is finished by refreshing the page in your browser. While the Web server is down you will get an error message.

6. Click **Confirm**. The new baseline is now the active software in the NE.

   Note: If you do not confirm the new software configuration within 15 minutes of the restart, a new restart will occur and the NE will revert to the previous software configuration.

7. Click **Next**.

Setting Passwords

8. On the **Manual Configuration** page, click **Configure Basic Security**.

9. On the **Security** page, under **Set control_user** and **Set view_user,** type **Password** and **Confirm Password** and then click **Apply**.

10. Click **Next**.

Configuring Basic NE Parameters

11. On the **Manual Configuration** page, click **Configure Basic NE**.

12. On the **Basic NE Configuration** page, under **Basic NE Data**, type the **NE Name**.

13. Specify **NE Location** and **NE Contact** information, such as the telephone number of the person responsible.

14. Type the **NE IP Address**, **Subnet Mask** and **Default Gateway** of the NE.

15. Under **FAU/PFU Settings**, select **In Service** for the units to be used.

    Note: This step is not applicable for ATU (B).

16. Under **General Settings**, in the **Date/Time** boxes, type the current date (yyyy-mm-dd) and time (hh:mm:ss).

17. Type **Alarm Filter Time** or use the default value of 2.5 seconds.

18. In the **PM Start Time** box, type the time of day that 24 hour performance interval starts or use the default value 00:00. This time can be set in the range 00:00 - 23:45 in steps of 15 minutes.

19. In the **Automatic Backup** list, select where automatic backups of the configuration should be sent.
20. Click **Apply**.
21. Click **Next**.

Configuring DCN Parameters

22. On the **Manual Configuration** page, click **Configure DCN**.
23. On the **Ethernet/LAN/Servers Configuration** page do one of the following:
    - For NPU2/NPU1 B and ATU (B), go to Step 24 on page 56.
    - For NPU 8x2, go to Step 27 on page 56
24. Specify **Administrative Status** of the **Ethernet/LAN** interface.
25. Select the **Enable Notifications** check box if notifications should be sent for the Ethernet/LAN interface.
26. Select the **Speed** of the **Ethernet/LAN** interface and **MDI-MDIX**.
27. Under **SNMP Manager (Trap Receiver)**, select the **Enable Notifications** check box if SNMP traps should be sent to SNMP Managers.
28. In the **SNMP Manager** box, type the IP address of each SNMP Manager to be used. An SNMP Manager is for example MINI-LINK Manager.
29. In the **Port** box, for each SNMP Manager, type the port number that the SNMP Manager uses for SNMP communication.
30. Select SNMP **Version** for each SNMP Manager.
31. Under **Network Services**, type the **Domain** name
32. Type the IP address of each **DNS Server** to be used.
33. Type the IP address or host name of the **NTP Server**.
34. Type the **DHCP Address** or host name of the DHCP server the NE is a relay for.
35. Under FTP, specify the IP address of the **Remote FTP Server**, **User Name** and **Password**.
36. Repeat the previous step for the **Local FTP Server**.
37. Click **Apply**.
38. On the **Ethernet/Lan/Servers Configuration** page, click **PPP**.
39. On the **PPP Configuration** page, for each interface, specify the **Administrative Status** and **Notifications**.

40. For each numbered interface, type the **IP Address**. The box should be left empty for an un-numbered interface.

Caution!

It is recommended to set all interfaces destined to the same NE as either numbered or un-numbered. Mixing both types may cause DCN instability.

41. Click **Apply**.

Creating Static Routes

42. On the **PPP Configuration** page, click **Static Routing**.
43. On the **Static Routing Configuration** page, type **Destination**, **Route Mask** and **Gateway**.
44. Click **Create**. The static route is displayed under **Current Static Routes**.
45. Repeat the two previous steps for each static route to be created. To modify or delete a static routes, see Section 6.10.6 on page 89.

Creating OSPF Areas

46. On the **Static Routing Configuration** page, click **OSPF Areas**.
47. On the **OSPF Areas Configuration** page, type **Net Address**, **Subnet Mask**, **Area ID** and select **Area Type**.
48. Click **Create**. The OSPF area is displayed under **Current OSPF Areas**.
49. Repeat the two previous steps for each OSPF area to be created. To modify or delete OSPF areas, see Section 6.10.4 on page 88.
50. Click **Next**.

Configuring E1 for DCN (NPU 8x2/NPU1 B only)

51. On the **Manual Configuration** page, click **Configure E1 DCN**.
52. On the **E1 DCN Configuration** page, select the E1 interface to be used for DCN and then click **Apply**.

    Note: All interfaces are not available at this stage. When the initial setup is completed, the **E1 Configuration** page can be used to select an E1 for DCN, see Section 11.51 on page 224.

53. Click **Next**.

Finishing the Installation

54. On the **Manual Configuration** page, click **Finish Installation**.

55. On the **Finish Installation** page, click **OK**. This will exit the installation wizard and you can continue with the configuration of the plug-in units and their interfaces, see Section 6 on page 59.

56. For NPU 8x2 the following also applies:

    The NE will make a warm restart. After the restart it will run in Normal mode. The IP address of the NE is changed during the manual configuration. To start the LCT in Normal mode you have to enter the URL **`http://`***`<IP address>`* where IP address is the one set in Step 14 on page 55. See also Section 3.3.2.3 on page 29.

6 Configuration Management

This section contains information and instructions related to configuration tasks performed after the initial setup has been completed. It includes the configuration of plug-in units, Radio Terminals, interfaces, traffic routing, protection and DCN.

The following is covered:

- *Typical Workflow*, see Section 6.1 on page 59.
- *Administrative Status*, see Section 6.2 on page 60.
- *Unit Configuration*, see Section 6.3 on page 61.
- *Radio Terminal Configuration*, see Section 6.4 on page 62
- *Working with MSP Protection*, see Section 6.5 on page 68.
- *Working with 1+1 E1 SNCP Protection*, see Section 6.6 on page 70.
- *Configuring the Ethernet Bridge*, see Section 6.7 on page 79.
- *Working with Traffic Routing of E1 Interfaces*, see Section 6.8 on page 79.
- *Working with E1 Overview*, see Section 6.9 on page 83.
- *DCN Configuration*, see Section 6.10 on page 85.
- *Uploading a Configuration File to an FTP Server*, see Section 6.11 on page 90.
- *Software Upgrade*, see Section 6.12 on page 91.
- *CLI Introduction*, see Section 6.13 on page 97.

6.1 Typical Workflow

When the initial setup is completed, the following steps represent a typical workflow:

1. Configure plug-in units and their interfaces, see Section 6.3 on page 61.
2. Finalize the configuration of the Radio Terminals, see Section 6.4 on page 62.
3. Create MSP protection, see Section 6.5.1 on page 68.
4. Create 1+1 E1 SNCP protection, see Section 6.6.1 on page 70.

5. Configure the Ethernet Bridge (NPU2 and ATU (B) only), see Section 6.7 on page 79.

6. Create traffic routing of E1 interfaces, see Section 6.8.1 on page 79.

7. Upload a configuration file as backup to an FTP server, see Section 6.11 on page 90.

6.2 Administrative Status

The desired status of a plug-in unit or interface is set as **Administrative Status** on the applicable **Configuration** page.

The signification of the administrative status of a plug-in unit is described in Table 3 on page 60.

Table 3 Administrative status of a plug-in unit

Administrative status	Description
In Service	Sets the unit in operating mode.
Out of Service	Sets the unit in non-operating mode. All notifications from the unit and its interfaces are disabled. No active alarms are displayed.

The signification of the administrative status of an interface is described in Table 4 on page 60.

Table 4 Administrative status of an interface

Administrative status	Description
Up	Sets the interface in operating mode.
Down	Sends an AIS instead of traffic on the interface (in both directions). Notifications from this interface and higher layer interfaces are suppressed.

When a new unconfigured plug-in unit is inserted the administrative status of the unit is In Service and its interfaces are Up by default. The notifications from the unit and its interfaces will be enabled. However, to prevent too many alarms from not traffic routed E1s, notifications are default disabled on these interfaces.

6.3 Unit and Interface Configuration

Note: This section describes how to configure units and interfaces not included in a Radio Terminal. The configuration of Radio Terminals is described in Section 6.4 on page 62.

To configure a unit or interface:

1. In the **Navigation Tree**, navigate to and select the entity to configure.
2. On the **Configuration** menu, click **Configuration**.
3. Configure the entity.

   Click **Help** for information on the configuration options. See also Table 5 on page 61 to find the applicable configuration page description.
4. Click **Apply** on the configuration page to apply the changes.

Table 5 References to configuration pages

Unit and related entities	See
PFU1	Section 11.15 on page 172 Section 11.23 on page 184
PFU2	Section 11.24 on page 185
PFU3	Section 11.15 on page 172 Section 11.25 on page 186
FAU	Section 11.15 on page 172 Section 11.26 on page 187
NPU1 B NPU 8x2 NPU2 • Ethernet Interface (NPU2/NPU1 B) • Single E1 Interface • All E1 Interfaces • User Input (NPU 8x2/NPU1 B) • User Output (NPU 8x2/NPU1 B)	Section 11.27 on page 188 Section 11.28 on page 189 Section 11.29 on page 190 • Section 11.16 on page 174 • Section 11.51 on page 224 • Section 11.52 on page 225 • Section 11.54 on page 228 • Section 11.55 on page 229
LTU 12x2 LTU 16x2 • Single E1 Interface • All E1 Interfaces	Section 11.31 on page 192 Section 11.32 on page 193 • Section 11.51 on page 224 • Section 11.52 on page 225
LTU 155 • MS/RS Interface • MSP Interface(1) • VC-4 Interface • Single VC-12 Interface • All VC-12 Interfaces • Single E1 Interface • All E1 Interfaces	Section 11.33 on page 194 • Section 11.44 on page 213 • Section 11.45 on page 215 • Section 11.46 on page 216 • Section 11.47 on page 218 • Section 11.48 on page 220 • Section 11.51 on page 224 • Section 11.52 on page 225

Unit and related entities	See
SMU2 (co-siting) (2) • DIG SC (2x64 kbit/s) • E3 • E2 • Single E1 Interface • All E1 Interfaces	Section 11.35 on page 198 • Section 11.18 on page 177 • Section 11.49 on page 222 • Section 11.50 on page 223 • Section 11.51 on page 224 • Section 11.52 on page 225
MMU2 B/C • RAU unit • RF Interface • RAU Interface • SWITCH Interface • Single E1 Interface • All E1 Interfaces	Section 11.36 on page 201 • Section 11.38 on page 204 • Section 11.39 on page 207 • Section 11.37 on page 203 • Section 11.42 on page 210 • Section 11.51 on page 224 • Section 11.52 on page 225
ATU (B) • LAN Interface • Bridge Interface • Single E1 Interface • All E1 Interfaces	Section 11.29 on page 190 • Section 11.16 on page 174 • Section 11.17 on page 176 • Section 11.51 on page 224 • Section 11.52 on page 225

(1) Configured after both units and their interfaces are configured. See also Section 6.5.1 on page 68 on how to create MSP protection.
(2) An SMU2 used for protection is configured according to Section 6.4.4 on page 66.

6.4 Radio Terminal Configuration

This section describes how to configure a Radio Terminal. It could be a completion of a configuration made during the initial setup or a completely new installation. The procedure is started indoors with a station radio cable connecting the MMU and the RAU. For further instructions, see *MINI-LINK TN ETSI Indoor Installation Manual*.

The following procedures are covered:

- *Configuring an Unprotected (1+0) Radio Terminal with MMU2 B/C*, see Section 6.4.1 on page 63.
- *Configuring a Protected (1+1) Radio Terminal with MMU2 B/C*, see Section 6.4.2 on page 64.
- *Configuring an Unprotected (1+0) Radio Terminal with MMU2 or ATU (B)*, see Section 6.4.3 on page 66.
- *Configuring a Protected (1+1) Radio Terminal with MMU2*, see Section 6.4.4 on page 66.

6.4.1 Configuring an Unprotected (1+0) Radio Terminal with MMU2 B/C

To configure an unprotected (1+0) Radio Terminal when the indoor part comprises one MMU2 B or MMU2 C:

1. In the **Navigation Tree**, click an MMU2 B or MMU2 C.
2. Click the **Configuration** menu to open the **MMU2 B/C Configuration** page.
3. Under **ID**, type the identity of this Radio Terminal in the **Near End** box.
4. If this terminal should send notifications, select the **Notifications** check box.
5. If an alarm should be generated when the received traffic originates from the wrong far-end, type the expected far-end identity in the **Far End** box, and select the **Radio ID Check** check box.
6. Under **Traffic Capacity**, select the wanted traffic capacity.
7. Under **Protection Mode**, select **1+0**.
8. Select **BER Alarm Threshold**.
9. Under **Modulation**, select the wanted modulation method.
10. Under **MMU2 B/C <ID>**, select all check boxes.
11. Click **Apply**.
12. Under **MMU2 B/C <ID>**, click the **RAU <ID>** link to open the **RAU Configuration** page.
13. Under **Near End Radio Terminal <ID>**, select all check boxes.
14. Under **RAU <ID>**, type the transmit frequency in the **Tx Frequency** box.
15. Select the **Transmitter On** check box.
16. In the **Tx Attenuator** box, type the value of the fixed attenuator (if used).
17. In the **Output Power Mode** list, select how the output power is to be controlled.

    Note: The **ATPC** option is only available when all units in the radio link support ATPC. Click **Show ATPC Capabilities** to see which units support ATPC.

18. Do one of the following:

If	Then
RTPC is selected	Type the **Output Power** value.
ATPC is selected	Type the **Max Output Power** and **Target Input Power (far-end)** values.

19. In the **RF Input Alarm Threshold** box, type the threshold for generating RF Input Threshold alarms.

20. Click **Apply**.

21. Carry out the outdoor equipment installation, indoor and outdoor radio cabling, and antenna alignment. Follow the instructions in *MINI-LINK TN ETSI Indoor Installation Manual* and *MINI-LINK TN, MINI-LINK E, MINI-LINK HC Outdoor Installation Manual*.

22. Configure the applicable interfaces.
    - RAU IF, see Section 11.37 on page 203
    - RF, see Section 11.39 on page 207
    - E3 Interface, see Section 11.49 on page 222
    - E2 Interface, see Section 11.50 on page 223.
    - Single E1 Interface, see Section 11.51 on page 224
    - All E1 Interfaces, see Section 11.52 on page 225

6.4.2 Configuring a Protected (1+1) Radio Terminal with MMU2 B/C

Note: The 1+1 configuration is only possible if the units are placed in adjacent AMM positions according to specifications in *MINI-LINK TN ETSI Indoor Installation Manual*.

To configure a protected (1+1) terminal when the indoor part comprises two MMU2 B or MMU2 C units:

1. Configure two temporary unprotected (1+0) Radio Terminals, one for each MMU that will be part of the final protected terminal, as described in Section 6.4.1 on page 63.

   Note: Do not turn on the transmitters when creating the temporary terminals.

   Note: To be able to configure a protected terminal, the following conditions apply:

   - Both of the temporary terminals must be configured to use the same traffic capacity, modulation method, and identity.
   - For 1+1 Hot configurations, both RAUs must have *the same* frequency.
   - For 1+1 Work configurations, both RAUs must have *different* frequencies.

2. In the **Navigation Tree**, click the MMU in the lower position.

3. Click the **Configuration** menu to open the **MMU2 B/C Configuration** page.

4. Under **Protection Mode**, select **1+1 Hot** or **1+1 Work**.

5. Click **Apply** to set the protection mode.

6. Click the **Configure Protection** link to open the **SWITCH Protection** page.

7. Configure the protection as described in Section 11.43 on page 211, then go back to the **MMU2 B/C Configuration** page.

Note: Step 8 on page 65 to Step 10 on page 65 is repeated for both RAUs.

8. Under **MMU2 B/C <ID>**, click the **RAU <ID>** link to open the **RAU Configuration** page.

9. Select the **Transmitter On** check box, then click **Apply**.

10. Under **Near End radio Terminal <ID>**, click the **MMU2 B/C <ID>** link to return to the **MMU2 B/C Configuration** page. Repeat from Step 8 on page 65 to Step 10 on page 65 for the other RAU.

11. Under **MMU2 B/C <ID>**, select all check boxes, then click **Apply**.

12. Configure the applicable interfaces.

    - RAU IF, see Section 11.37 on page 203
    - RF, see Section 11.39 on page 207
    - E3 Interface, see Section 11.49 on page 222
    - E2 Interface, see Section 11.50 on page 223.
    - Single E1 Interface, see Section 11.51 on page 224
    - All E1 Interfaces, see Section 11.52 on page 225

6.4.3 Configuring an Unprotected (1+0) Radio Terminal with MMU2 or ATU (B)

To configure an unprotected (1+0) Radio Terminal when the indoor part comprises one MMU2 or ATU (B):

1. In the **Navigation Tree**, click an MMU2.
2. Click the **Configuration** menu.
3. On the **MMU2 Configuration** page, select **In Service**, clear the **Enable** check box and select **Prepare for 1+0 configuration**.
4. Click **Apply**.
5. Click **Perform AM Setup and Hop Setup**.
6. In MSM, perform an AM and Hop Setup. Follow the instructions in *MSM User Guide* or *MSM online Help*. Exit MSM when finished.
7. Carry out the outdoor equipment installation, indoor and outdoor radio cabling, and antenna alignment. Follow the instructions in *MINI-LINK TN ETSI Indoor Installation Manual* and *MINI-LINK TN, MINI-LINK HC, MINI-LINK E Outdoor Installation Manual*.
8. Configure the applicable interfaces.
   - E3 Interface, see Section 11.49 on page 222
   - E2 Interface, see Section 11.50 on page 223
   - Single E1 Interface, see Section 11.51 on page 224
   - All E1 Interfaces, see Section 11.52 on page 225
9. On the **MMU2 Configuration** page, select the **Enable** check box and click **Apply**.

6.4.4 Configuring a Protected (1+1) Radio Terminal with MMU2

Note: The 1+1 configuration is only possible if the units are placed in adjacent AMM positions according to specifications in *MINI-LINK TN ETSI Indoor Installation Manual*.

To configure a protected (1+1) Radio Terminal when the indoor part comprises two MMU2 units and one SMU2:

1. In the **Navigation Tree**, click one of the MMU2s.
2. Click the **Configuration** menu.
3. On the **MMU2 Configuration** page, select **Prepare for 1+1 configuration** and click **Apply**.
4. For all three units, select **In Service**, clear the **Enable** check box and click **Apply**.

5. Click **Perform AM Setup and Hop Setup**.

6. In MSM, perform an AM and Hop Setup. Follow the instructions in *MSM User Guide* or *MSM online Help*. Exit MSM when finished.

7. Carry out the outdoor equipment installation, indoor and outdoor radio cabling, and antenna alignment. Follow the instructions in *MINI-LINK TN ETSI Indoor Installation Manual* and *MINI-LINK TN, MINI-LINK HC, MINI-LINK E Outdoor Installation Manual*.

8. Configure the applicable interfaces.

   - E3 Interface, see Section 11.49 on page 222
   - E2 Interface, see Section 11.50 on page 223
   - Single E1 Interface, see Section 11.51 on page 224
   - All E1 Interfaces, see Section 11.52 on page 225

9. On the **MMU2 Configuration** page, select the **Enable** check box for all three units and click **Apply**.

6.5 Working with MSP Protection

This section describes how to create, modify and delete MSP protection.

6.5.1 Creating MSP Protection

This procedure describes how to create MSP protection including two adjacent LTU 155s. Each unit's STM-1 port will have the status `MSP 1+1 VC-12`.

Note: The two LTU 155s must be placed in adjacent AMM positions according to specifications in *MINI-LINK TN ETSI Indoor Installation Manual*.

Note: Creating MSP protection will remove the existing traffic routings on the LTU 155.

To create MSP protection:

1. Make sure that both units and their interfaces are configured, see Section 6.3 on page 61.
2. In the **Navigation Tree**, click one of the two LTU 155s.
3. Click the **Configuration** menu.
4. On the **LTU 155 Configuration** page, under **Port Configuration**, click **MSP Protection**.
5. On the **Create MSP Protection** page, click **OK**.
6. The selected LTU 155 along with its adjacent unit will be configured to operate together as a protected pair, in an MSP protection. During the process it is indicated how many units (0,1 or 2) that have been configured so far. The page is refreshed every fifth second to give up-to-date information about the progress.
7. When the MSP protection has been created the **Modify MSP Protection** page is displayed.

To verify or change the configuration of the MSP protection do the following:

8. In the **Navigation Tree**, click the MSP interface found below one of the LTU 155s.
9. On the **Configuration** menu, click **Configuration**. The **MSP Configuration page** is displayed, where the configuration can be changed.

6.5.2 Modifying MSP Protection

This procedure describes how to change active line and switch mode for an existing MSP protection, including two adjacent LTU 155 units.

To modify MSP protection:

1. In the **Navigation Tree**, click one of the two LTU 155s.
2. Click the **Configuration** menu.
3. On the **LTU 155 Configuration** page, under **Port Configuration**, click **MSP Protection**.
4. On the **Modify MSP Protection** page, change **Active Line** and/or **Switch Mode**.
5. Click **Apply**.

6.5.3 Deleting MSP Protection

This procedure describes how to delete an existing MSP protection, including two adjacent LTU 155s. Deleting MSP protection will set the status of each unit's STM-1port to `Not Configured`, that is the port does not provide traffic until it is configured using the **LTU 155 Configuration** page, see Section 11.33 on page 194.

To delete MSP protection:

1. In the **Navigation Tree**, click one of the two LTU 155s.
2. Click the **Configuration** menu.
3. On the **LTU 155 Configuration** page, under **Port Configuration**, click **MSP Protection**.
4. On the **Modify MSP Protection** page, change the status for both units to **Not Configured**.
5. Click **OK**.
6. The selected LTU 155 along with its adjacent unit will be set to operate alone. During the process the **Deleting MSP Protection** page indicates how many units (0,1 or 2) that have been configured so far. The page is refreshed every fifth second to give up-to-date information about the progress.

   Note: If you leave the **Deleting Protection** page during the process and then enter it later, you have to re-specify the status of the second unit's STM-1 port.

7. When the MSP protection has been deleted the **LTU 155 Configuration** page is displayed.

6.6 Working with 1+1 E1 SNCP Protection

This section describes how to create, modify and delete 1+1 E1 SNCP protection using the EEM.

Note: If MINI-LINK Connexion is used to provision end-to-end E1 connections, then only use the EEM to *view* current connections. Creating, modifying, and deleting E1 connections shall in this case be done with MINI-LINK Connexion.

Note: 1+1 SNCP protection is not applicable for ATU (B).

6.6.1 Creating 1+1 E1 SNCP Protection

Protection of E1 interfaces can be created in two ways:

- *Using the Matrix View*, see Section 6.6.1.1 on page 70. One interface pair can be protected at a time.
- *Using the List View*, see Section 6.6.1.2 on page 72. One or multiple interface pairs can be protected simultaneously.

6.6.1.1 Creating 1+1 E1 SNCP Protection Using the Matrix View

1. In the **Navigation Tree**, click the NE.
2. On the **Configuration** menu, click **1+1 E1 SNCP**.
3. On the **1+1 E1 SNCP Select Interfaces** page, under **Interface Type**, select **E1** and then click **Select**.

   Note: This version of EEM supports only selection of E1.
4. Under **Select units for interface views**, select the two units, one from each list, that contain the interfaces to be protected.
5. Click **Matrix View**.

6. On the **1+1 E1 SNCP Matrix View** page, click the blank button  in the intersection point between the two interfaces to be protected. This creates a protection with default settings indicated by a P button  in the intersection point.

   You can use an interface interval link 1.1.1-1.6.2 to locate interfaces currently not present on an axis. The interfaces on an MMU2 in a protected (1+1) Radio Terminal are denoted in accordance with the SMU2.

   Note: If there is no blank button in the intersection point, the two interfaces cannot be used. To find out why, click the interface names to display the **E1 Overview** page. The possible reasons can be summarized as follows:

   - One or both of the interfaces are already part of a 1+1 E1 SNCP protection.
   - Both interfaces are already routed.
   - The interface is used for DCN.

To modify the protection, route the protected interface or modify a traffic routing of the protected interface (optional):

7. Click the P button  .

8. On the **Modify 1+1 E1 SNCP** page, do one of the following:

To	Do this
Modify the protection	• Specify the protection parameters. Clicking **Configure <Protected E1 Interface Name>** opens the **E1 Configuration** page where you can specify the parameters for the protected interface. Use the **Back** button to navigate back. • Click **OK**. The **1+1 E1 SNCP Matrix View** page is displayed.
Route the protected interface	• Under **Traffic Routing**, click **Create**. • On the **Traffic Routing List View** page, select the interface to be routed to (**Interface 2**) and then click **Create**. • On the **Create Traffic Routing** page, type the **Name** of the traffic routing and then click **OK**. The **Modify 1+1 E1 SNCP** page is displayed.
Modify a traffic routing of the protected interface. This case will occur if one of the interfaces in the protection was routed. The protected interface will then inherit the traffic routing.	• Under **Traffic Routing**, click **Modify**. • On the **Modify Traffic Routing** page, type the **Name** of the traffic routing and click **OK**. The **Modify 1+1 E1 SNCP** page is displayed.

6.6.1.2 Creating 1+1 E1 SNCP Protection Using the List View

1. In the **Navigation Tree**, click the NE.

2. On the **Configuration** menu, click **1+1 E1 SNCP**.

3. On the **1+1 E1 SNCP Select Interfaces** page, under **Interface Type**, select **E1** and then click **Select**.

   Note: This version of EEM supports only selection of E1.

4. Under **Select units for interface views**, select the units, one unit or All Units from each list, that contain the interfaces to be protected.

5. Click **List View**.

6. On the **1+1 E1 SNCP List View** page, select one or multiple interface pairs to be protected. When selecting multiple items, the topmost selected interfaces in the two lists will form an interface pair and so on. Use CTRL or SHIFT to select multiple items.

   Note: The interfaces on an MMU2 in a protected (1+1) Radio Terminal are denoted in accordance with the SMU2.

7. Click **Create** and do one of the following:

To	Do this
Create a single 1+1 E1 SNCP protection	• On the **Create 1+1 E1 SNCP** page, under **Interfaces**, select the **Active** interface. • Under **Settings**, specify **Hold-Off Time** and **Switch Mode**. • Click **OK**.
Create multiple 1+1 E1 SNCP protections	On the **Create Multiple 1+1 E1 SNCP** page, click **OK**. This will create the protections with default settings which can be changed later by modifying an existing protection.

8. The **1+1 E1 SNCP List View** page is displayed. Click **Show Current Protections** to display the **Current Protections** list.

To modify a protection, route the protected interface or modify a traffic routing of the protected interface (optional):

9. Locate the protection and click **Modify**.

10. On the **Modify 1+1 E1 SNCP** page, do one of the following:

To	Do this
Modify the protection	• Specify the protection parameters. Clicking **Configure <Protected E1 Interface Name>** opens the **E1 Configuration** page where you can specify the parameters for the protected interface. Use the **Back** button to navigate back. • Click **OK**. The **1+1 E1 SNCP List View** page is displayed.
Route the protected interface	• Under **Traffic Routing**, click **Create**. • On the **Traffic Routing List View** page, select the interface to be routed to (**Interface 2**) and then click **Create**. • On the **Create Traffic Routing** page, type the **Name** of the traffic routing and then click **OK**. The **Modify 1+1 E1 SNCP** page is displayed.
Modify a traffic routing of the protected interface. This case will occur if one of the interfaces in the protection was routed. The protected interface will then inherit the traffic routing.	• Under **Traffic Routing**, click **Modify**. • On the **Modify Traffic Routing** page, type the **Name** of the traffic routing and click **OK**. The **Modify 1+1 E1 SNCP** page is displayed.

6.6.2 Modifying or Deleting 1+1 E1 SNCP Protection

Existing protection of E1 interfaces can be modified, that is change the protection parameters or route the protected interface, or deleted in two ways:

- *Using the Matrix View*, see Section 6.6.2.1 on page 75. One protection can be handled at a time.

- *Using the List View*, see Section 6.6.2.2 on page 77. One protection can be modified and multiple protections can be deleted simultaneously.

6.6.2.1 Modifying or Deleting 1+1 E1 SNCP Protection Using the Matrix View

1. In the **Navigation Tree**, click the NE.

2. On the **Configuration** menu, click **1+1 E1 SNCP**.

3. On the **1+1 E1 SNCP Select Interfaces** page, under **Interface Type**, select **E1** and then click **Select**.

   Note: This version of EEM supports only selection of E1.

4. Under **Select units for interface views**, select the two units, one from each list, that contain the interfaces in the protection.

5. Click **Matrix View**.

6. On the **1+1 E1 SNCP Matrix View** page, click the P button  in the intersection point between the two interfaces in the protection.

   Note: You can use an interface interval link 1.1.1-1.6.2 to locate interfaces currently not present on an axis.

   Note: The interfaces on an MMU2 in a protected (1+1) Radio Terminal are denoted in accordance with the SMU2.

7. On the **Modify 1+1 E1 SNCP** page do one of the following:

To	Do this
Modify the protection	• Specify the protection parameters. Clicking **Configure <Protected E1 Interface Name>** opens the **E1 Configuration** page where you can specify the parameters for the protected interface. Use the **Back** button to navigate back. • Click **OK**. The **1+1 E1 SNCP Matrix View** page is displayed reflecting your changes.
Delete the protection	• Click **Delete**. • Click **OK** in the confirmation dialog box. The **1+1 E1 SNCP Matrix View** page is displayed reflecting your changes.
Route the protected interface	• Under **Traffic Routing**, click **Create**. • On the **Traffic Routing List View** page, select the interface to be routed to (**Interface 2**) and then click **Create**. • On the **Create Traffic Routing** page, type the **Name** of the traffic routing and then click **OK**. The **Modify 1+1 E1 SNCP** page is displayed.
Modify a traffic routing of the protected interface.	• Under **Traffic Routing**, click **Modify**. • On the **Modify Traffic Routing** page, type the **Name** of the traffic routing and click **OK**. The **Modify 1+1 E1 SNCP** page is displayed.

6.6.2.2 Modifying or Deleting 1+1 E1 SNCP Protection Using the List View

1. In the **Navigation Tree**, click the NE.
2. On the **Configuration** menu, click **1+1 E1 SNCP**.
3. On the **1+1 E1 SNCP Select Interfaces** page, under **Interface Type**, select **E1** and then click **Select**.

   Note: This version of EEM supports only selection of E1.
4. Under **Select units for interface views**, select the two units, one unit or All Units from each list, that contain the interfaces in the protection.
5. Click **List View**.
6. On the **1+1 E1 SNCP List View** page, click **Show Current Protections** to display the **Current Protections** list.

7. Under **Current Protections**, do one of the following:

To	Do this
Modify a protection	• Locate the protection and click **Modify**. • On the **Modify 1+1 E1 SNCP** page, specify the protection parameters. Clicking **Configure <Protected E1 Interface Name>** opens the **E1 Configuration** page where you can specify the parameters for the protected interface. Use the **Back** button to navigate back. • Click **OK**. The **1+1 E1 SNCP List View** page is displayed reflecting your changes.
Delete one or multiple protections	• Select the check boxes for the protections to be deleted and click **Delete**. • Click **OK** in the confirmation dialog box. The **1+1 E1 SNCP List View** page is displayed reflecting your changes. **Note:** You can also delete a single protection from the **Modify 1+1 E1 SNCP** page.
Route the protected interface	• Under **Traffic Routing**, click **Create**. • On the **Traffic Routing List View** page, select the interface to be routed to (**Interface 2**) and then click **Create**. • On the **Create Traffic Routing** page, type the **Name** of the traffic routing and then click **OK**. The **Modify 1+1 E1 SNCP** page is displayed.
Modify a traffic routing of the protected interface.	• Under **Traffic Routing**, click **Modify**. • On the **Modify Traffic Routing** page, type the **Name** of the traffic routing and click **OK**. The **Modify 1+1 E1 SNCP** page is displayed.

Note: The interfaces on an MMU2 in a protected (1+1) Radio Terminal are denoted in accordance with the SMU2.

6.7 Configuring the Ethernet Bridge

This section describes how to configure the Ethernet Bridge, implemented in the NPU2 and ATU (B). A maximum of 16 E1s can be used for transmission of Ethernet traffic.

To configure the Ethernet Bridge:

1. In the **Navigation Tree**, click the NE.
2. On the **Configuration** menu, click **Ethernet Bridge**.
3. On the **Ethernet Bridge Configuration** page, under **Units**, select the unit that contain the E1s to be bridged and click **Select**.
4. Under **Interfaces**, select the E1s that should be bridged and click **Add**. Use CTRL or SHIFT to select multiple items.
5. If the E1s to be bridged belong to more than one unit, repeat the two previous steps.
6. If E1s should be removed do the following:

   Under **Bridged Interfaces**, select the E1s to be removed and click **Remove**.
7. Select the **Enable** check box if alarm notifications should be sent for the bridge's HDLC encapsulation interface.
8. Click **Apply**.

6.8 Working with Traffic Routing of E1 Interfaces

This section describes how to create, modify and delete traffic routing of E1 interfaces.

Note: If MINI-LINK Connexion is used to provision end-to-end E1 connections, then only use the EEM to *view* current connections. Creating, modifying, and deleting E1 connections shall in this case be done with MINI-LINK Connexion.

6.8.1 Creating Traffic Routing of E1 Interfaces

Traffic routing of E1 interfaces can be done in two ways:

- *Using the Matrix View*, see Section 6.8.1.1 on page 80. One interface pair can be routed at a time.
- *Using the List View*, see Section 6.8.1.2 on page 80. One or multiple interface pairs can be routed simultaneously.

6.8.1.1 Creating Traffic Routing of E1 Interfaces Using the Matrix View

1. In the **Navigation Tree**, click the NE.
2. On the **Configuration** menu, click **Traffic Routing**.
3. On the **Traffic Routing Select Interfaces** page, under **Interface Type**, select **E1** and then click **Select**.
4. Under **Select units for interface views**, select the two units, one from each list, that contain the interfaces to be routed.
5. Click **Matrix View**.
6. On the **Traffic Routing Matrix View** page, click the blank button  in the intersection point between the two interfaces to be routed. This creates a nameless traffic routing indicated by an X button  in the intersection point.

   Note: You can use an interface interval link 1.1.1-1.6.2 to locate interfaces currently not present on an axis.

   Note: If there is no blank button in the intersection point the two interfaces cannot be used. To find out why, click the interface names to display the **E1 Overview** page. The possible reasons can be summarized as follows:

   - One or both of the interfaces are already routed or part of a 1+1 E1 SNCP protection where the protected interface is already routed.
   - The two interfaces are part of the same 1+1 E1 SNCP protection.

   Note: The interfaces on an MMU2 in a protected (1+1) Radio Terminal are denoted in accordance with the SMU2.

To name the traffic routing (optional):

7. Click the X button  to modify the traffic routing.
8. On the **Modify Traffic Routing** page, type the **Name** and then click **OK**. The **Traffic Routing Matrix View** page will be opened.

6.8.1.2 Creating Traffic Routing of E1 Interfaces Using the List View

1. In the **Navigation Tree**, click the NE.
2. On the **Configuration** menu, click **Traffic Routing**.
3. On the **Traffic Routing Select Interfaces** page, under **Interface Type**, select **E1** and then click **Select**.

4. Under **Select units for interface views**, select the two units, one unit or All Units from each list, that contain the interfaces to be routed.

5. Click **List View**.

6. On the **Traffic Routing List View** page, select one or multiple interface pairs to be routed. When selecting multiple items, the topmost selected interfaces in the two lists will form one interface pair and so on. Use CTRL or SHIFT to select multiple items.

   Note: The interfaces on an MMU2 in a protected (1+1) Radio Terminal are denoted in accordance with the SMU2.

7. Click **Create** and do one of the following:
   - On the **Create Traffic Routing** page, type the **Name** of the single traffic routing and then click **OK**.
   - On the **Create Multiple Traffic Routing** page, type the common **Name** of the multiple traffic routings and then click **OK**. An individual name can be set later by modifying an existing traffic routing.

8. The **Traffic Routing List View** page is displayed. Click **Show Current Routings** to display the **Current Traffic Routings** list.

6.8.2 Modifying or Deleting Traffic Routing of E1 Interfaces

Existing traffic routing of E1 interfaces can be modified or deleted in two ways:

- *Using the Matrix View*, see Section 6.8.2.1 on page 81. One traffic routing can be handled at a time.

- *Using the List View*, see Section 6.8.2.2 on page 82. One traffic routing can be modified and multiple traffic routings can be deleted simultaneously.

6.8.2.1 Modifying or Deleting Traffic Routing of E1 Interfaces Using the Matrix View

1. In the **Navigation Tree**, click the NE.

2. On the **Configuration** menu, click **Traffic Routing**.

3. On the **Traffic Routing Select Interfaces** page, under **Interface Type**, select **E1** and then click **Select**.

4. Under **Select units for interface views**, select the two units, one from each list, that contain the interfaces in the traffic routing.

5. Click **Matrix View**.

6. On the **Traffic Routing Matrix View** page, click the X button  in the intersection point between the two interfaces in the traffic routing.

   Note: You can use an interface interval link 1.1.1-1.6.2 to locate interfaces currently not present on an axis.

   Note: The interfaces on an MMU2 in a protected (1+1) Radio Terminal are denoted in accordance with the SMU2.

7. On the **Modify Traffic Routing** page, do one of the following:
   - Modify the **Name** of the traffic routing and click **OK**.
   - Click **Delete** and then click **OK** in the confirmation dialog box.

8. The **Traffic Routing Matrix View** page is displayed reflecting your changes.

6.8.2.2 Modifying or Deleting Traffic Routing of E1 Interfaces Using the List View

1. In the **Navigation Tree**, click the NE.

2. On the **Configuration** menu, click **Traffic Routing**.

3. On the **Traffic Routing Select Interfaces** page, under **Interface Type**, select **E1** and then click **Select**.

4. Under **Select units for interface views**, select the two units, one unit or All Units from each list, that contain the interfaces in that are routed.

5. Click **List View**.

6. On the **Traffic Routing List View** page, click **Show Current Routings** to display the **Current Traffic Routings** list.

7. Under **Current Traffic Routings** do one of the following:

To	Do this
Modify a traffic routing	• Locate the traffic routing and click **Modify**. • On the **Modify Traffic Routing** page, modify the **Name** of the traffic routing and click **OK**.
Delete one or multiple traffic routings	• Select the check boxes for the traffic routings to be deleted and click **Delete**. • Click **OK** in the confirmation dialog box. **Note:** You can also delete a single traffic routing from the **Modify Traffic Routing** page.

Note: The interfaces on an MMU2 in a protected (1+1) Radio Terminal are denoted in accordance with the SMU2.

8. The **Traffic Routing List View** page is displayed reflecting your changes.

6.9 Working with E1 Overview

The **E1 Overview** page is opened in a separate window and provides a convenient way to view and change the configuration of an E1 interface, as well as handle its 1+1 E1 SNCP protection and traffic routing. Furthermore, it is possible to handle the E1 as part of the Ethernet Bridge, implemented in the NPU2 and ATU (B).

This section covers the following procedures:

- *Configuring an E1, Creating 1+1 E1 SNCP Protection and Traffic Routing*, see Section 6.9.1 on page 83.
- *Adding an E1 to the Ethernet Bridge*, see Section 6.9.2 on page 85.

6.9.1 Configuring an E1, Creating 1+1 E1 SNCP Protection and Traffic Routing

This procedure describes how to use the main features of the **E1 Overview** page, excluding the Ethernet Bridge handling. The different parts of the procedure can also be used standalone, when applicable.

Opening the E1 Overview page and Configuring an E1

1. In the **Navigation Tree**, click an E1 that is neither protected nor routed.
2. On the **Configuration** menu, click **Configuration.**

3. On the **E1 Configuration** page, view the parameters at hand. If required, make changes and click **Apply**.

4. Click **E1 Overview** to open the **E1 Overview** page in a separate window. The upper part of the page displays the configuration of the E1 for which the page is opened. The lower part is a graphical view used to display and change protection and traffic routing related to this E1.

   Note: The upper part of the page will have links to the **E1 Configuration** page for all E1s related to the one for which the page is opened. Use these links to change the configuration, if required.

Creating a 1+1 E1 SNCP Protection

Note: 1+1 SNCP protection is not applicable for ATU (B).

5. On the **E1 Overview** page, click **Create 1+1 E1 SNCP**. The **1+1 E1 SNCP List View** page is opened in the main EEM browser window. The E1 for which the **E1 Overview** page is opened is preselected in the **Interface 1** list. The **Interface 2** list contains all available E1s that can be used to create a protection.

6. On the **1+1 E1 SNCP List View** page, under **Interface 2**, select an E1 and click **Create**.

7. On the **Create 1+1 E1 SNCP** page, define **Hold-Off Time** and **Switch Mode**. Click **Apply**.

8. On the **E1 Overview** page, click **Reload**. The page is now updated with an SNCP symbol for the new protection. The configuration of the two unprotected and the protected E1s are also displayed in the upper part of the page.

Creating a Traffic Routing

9. On the **E1 Overview** page, click **Create Traffic Routing**.

10. The **Traffic Routing List View** page is opened in the main EEM browser window. The protected E1 is preselected in the **Interface 1** list. The **Interface 2** list contains all available E1s that can be used to create a traffic routing.

11. On the **Traffic Routing List View** page, under **Interface 2**, select an E1 and click **Create**.

12. On the **Create Traffic Routing** page, specify a **Name** of the traffic routing and click **Apply**.

13. On the **E1 Overview** page, click **Reload**. The page is now updated with a Traffic Routing symbol. The configuration of the E1 selected under **Interface 2** is also displayed in the upper part of the page.

Creating a 1+1 E1 SNCP Protection

Note: 1+1 SNCP protection is not applicable for ATU (B).

14. If the E1 selected under **Interface 2** in Step 11 on page 84 should be protected as well, repeat Step 5 on page 84 to Step 8 on page 84 above. This protection will be displayed with an SNCP symbol to the right. The configuration of the E1s in this protection is also displayed in the upper part of the page.

6.9.2 Adding an E1 to the Ethernet Bridge

The **E1 overview** page displays if an E1 is used for the Ethernet Bridge, implemented in the NPU2 and ATU (B). If not, the E1 can be added. See also how to configure the Ethernet Bridge in Section 6.7 on page 79.

To add an E1 to the Ethernet Bridge:

1. In the **Navigation Tree**, click an E1 that is not used for the Ethernet Bridge.
2. On the **Configuration** menu, click **Configuration**.
3. On the **E1 Configuration** page, view the parameters at hand. If required, make changes and click **Apply**.
4. Click **E1 Overview** to open the **E1 Overview** page in a separate window.
5. On the **E1 Overview** page, click **Add E1 to Ethernet Bridge**.
6. The **Ethernet Bridge Configuration** page is opened in the main EEM browser window. The selected E1 and the unit containing it are preselected.
7. On the **Ethernet Bridge Configuration** page, click **Add**. The E1 is added to the **Bridged Interfaces** list.
8. On the **E1 Overview** page, click **Reload**. The Ethernet Bridge symbol is now displayed.

6.10 DCN Configuration

This section covers general information and procedures related to the Data Communication Network (DCN), providing IP based transport of operation and maintenance data between management systems and MINI-LINK TN equipment.

The DCN parameters are normally set during the initial setup but can also be changed later following procedures in this section.

6.10.1 Overview

Each NE holds an internal IP router using numbered and un-numbered interfaces. PPP interfaces configured for an Area Border Router (ABR) use numbered interfaces. All other interfaces are un-numbered, that is inheriting the IP address of the router.

Basic DCN parameters, such as IP address and default gateway, are set during the initial setup, see Section 5.3 on page 54. These parameters can always be changed from the **Ethernet/LAN/Servers Configuration** page, see Section 11.16 on page 174.

The preferred IP routing strategy for MINI-LINK TN is the Open Shortest Path First (OSPF) protocol, which makes use of automatically updated routing tables in order to determine the most efficient transmission of data. The OSPF areas can be created during the initial setup or at a later occasion, see Section 6.10.3 on page 88. The Command Line Interface (CLI) is used for advanced OSPF configuration and troubleshooting, see Section 6.13.3 on page 107.

MINI-LINK TN supports static routing from the EEM. Static routing can be configured during the initial setup or at a later occasion, see Section 6.10.5 on page 89. The CLI also provides configuration of static routing, see Section 6.13.4 on page 110.

The available DCN channels are briefly described below.

E1

One E1 interface per an NPU 8x2/NPU1 B NE can be used for transport of DCN traffic. The interface can be selected during the initial setup, see Section 5.3 on page 54. It is also possible to select the interface from the **E1 Configuration** page, see Section 11.51 on page 224.

Radio Terminal

An unprotected (1+0) protected or protected (1+1) Radio Terminal provides two 64 kbit/s PPP interfaces by default.

STM-1

The STM-1 interface (stand-alone or MSP) on the LTU 155 provides PPP interfaces in the RSOH and MSOH bytes of the SDH frame. The default bandwidth is DCC_R=192 kbit/s and DCC_M=192 kbit/s. The bandwidth can be changed, see Section 6.10.2.1 on page 87.

Ethernet/LAN

The Ethernet interface on the NPU is the recommended way to connect to an external DCN. The NPU 8x2 provides 10 Mbit/s. For NPU2/NPU1 B it is possible to configure the interface to 10 or 100 Mbit/s on the **Ethernet/Servers Configuration** page, see Section 11.16 on page 174.

For ATU (B), the LAN interface is used to connect to an external DCN. It is possible to configure this 10 Mbit/s

interface on the **LAN/Servers Configuration** page, see Section 11.16 on page 174.

DIG SC The SMU2 in co-siting mode provides 2x64 kbit/s channels for DCN connection, typically to co-sited MINI-LINK E equipment, see Section 6.10.2.2 on page 88.

For more specific information on DCN for MINI-LINK, see *MINI-LINK DCN Guideline*.

6.10.2 Configuring the PPP Interfaces

This section describes how to configure the PPP interfaces. They can specifically be used to change the default bandwidth of the STM-1 PPP interfaces and to set the number of DIG SC (2x64 kbit/s) for SMU2 in co-siting mode.

To configure the PPP interfaces:

1. In the **Navigation Tree**, click the NE.
2. On the **Configuration** menu, click **DCN** and then click **PPP**.
3. On the **PPP Configuration** page, for each interface, specify the **Administrative Status** and **Notifications**.
4. For a numbered interface, type the **IP Address**. The box should be left empty for an un-numbered interface.

Caution!

It is recommended to set all interfaces destined to the same NE as either numbered or un-numbered. Mixing both types may cause DCN instability.

5. Click **Apply**.

6.10.2.1 Changing the Bandwidth of the STM-1 PPP Interfaces

The STM-1 interface (stand-alone or MSP) on the LTU 155 provides PPP interfaces in the RSOH and MSOH bytes of the SDH frame. Table 6 on page 88 and Table 7 on page 88 show the possible and default bandwidth of the interfaces.

For increased bandwidth it is recommended to change the administrative status of the interfaces in accordance with the tables.

Table 6 Bandwidth of the STM-1 RSOH PPP interfaces

Bandwidth [kbit/s]	**DCC_R (D1–3) status**
0	Down
192	**Up (Default)**

Table 7 Bandwidth of the STM-1 MSOH PPP interfaces

Bandwidth [kbit/s]	**DCC_M (D4–6) status**	**DCC_M (D7–9) status**	**DCC_M (D10–12) status**
0	Down	Down	Down
192	**Up (Default)**	Down	Down
384	Up	Up	Down
576	Up	Up	Up

6.10.2.2 Setting the Number of DIG SC (2x64 kbit/s) for SMU2 in Co-siting Mode

The SMU2 in co-siting mode provides 2x64 kbit/s channels for DCN connection, typically to co-sited MINI-LINK E equipment. If a channel should be used, the administrative status of the interface must be set to Up.

6.10.3 Creating OSPF Areas

The Open Shortest Path First (OSPF) protocol makes use of automatically updated routing tables in order to determine the most efficient transmission of data. OSPF networks are divided in sections, so called OSPF areas. The EEM can be used to create OSPF areas as described below. If there is only one ABR within an area, it is recommended to define the area as a stub area in order to improve the performance of the routing.

To create an OSPF area:

1. In the **Navigation Tree**, click the NE.
2. On the **Configuration** menu, click **DCN** and then click **OSPF Areas**.
3. On the **OSPF Areas Configuration** page, type **Net Address**, **Subnet Mask**, **Area ID** and select **Area Type**.
4. Click **Create**. The OSPF area is displayed under **Current OSPF Areas**.

6.10.4 Modifying or Deleting OSPF Areas

To modify or delete an existing OSPF area:

1. In the **Navigation Tree**, click the NE.
2. On the **Configuration** menu, click **DCN** and then click **OSPF Areas**.

3. On the **OSPF Areas Configuration** page, under **Current OSPF Areas**, do one of the following:

To	Do this
Modify an OSPF area	• Locate the OSPF area and click **Modify**. • On the **Modify OSPF Area** page, specify the new parameters and click **OK**.
Delete one or multiple OSPF areas	• Select the check boxes for the OSPF areas to be deleted and click **Delete**. • Click **OK** in the confirmation dialog box. **Note:** You can also delete a single OSPF area from the **Modify OSPF Area** page.

4. The **OSPF Areas Configuration** page is displayed reflecting your changes.

6.10.5 Creating Static Routes

Static routing means that a fixed routing scheme is used where the address of the router that a message will be sent to, has to be entered manually. A maximum of 100 static routes is possible.

To create a static route:

1. In the **Navigation Tree**, click the NE.
2. On the **Configuration** menu, click **DCN** and then click **Static Routing**.
3. On the **Static Routing Configuration** page, type **Destination**, **Route Mask** and **Gateway**.
4. Click **Create**. The static route is displayed under **Current Static Routes**.

See also Section 6.13.4 on page 110 on how to use the CLI to create static routes.

6.10.6 Modifying or Deleting Static Routes

To modify or delete an existing static route:

1. In the **Navigation Tree**, click the NE.
2. On the **Configuration** menu, click **DCN** and then click **Static Routing**.

3. On the **Static Routing Configuration** page, under **Current Static Routes**, do one of the following:

To	Do this
Modify a route	• Locate the route and click **Modify**. • On the **Modify Static Route** page, specify the new parameters and click **OK**.
Delete one or multiple routes	• Select the check boxes for the route to be deleted and click **Delete**. • Click **OK** in the confirmation dialog box. **Note:** You can also delete a single route area from the **Modify Static Route** page.

4. The **Static Routing Configuration** page is displayed reflecting your changes.

6.11 Uploading a Configuration File to an FTP Server

This procedure describes how to upload a configuration file to an FTP Server for backup purposes.

Note: It is recommended to carry out this procedure when the installation and configuration of a new NE is completed.

To upload a configuration file:

1. In the **Navigation Tree**, click the NE.

2. On the **Configuration** menu, click **Load Configuration**.

3. On the **Load Configuration** page, under **Configuration File**, select **Upload to FTP server**.

4. Specify **File Name**. The configuration will be stored in the `<drive:>\tn_ftp_home\tn_backup_configuration` folder.

5. Under **FTP**, do one of the following:
   - If the configuration file should be stored on a remote FTP server, select **Remote server @ <IP address>**.
   - If the configuration file should be stored on the PC, select **Local server**. Specify **User Name** and **Password**.

6. Click **Apply**.

6.12 Software Upgrade

Whenever the system configuration is changed, for example by adding or replacing plug-in units, it could be necessary to upgrade the system software. The process can be performed locally with the PC connected directly to the NE or from remote utilizing a DCN connection.

Note: Software Upgrade cannot be performed when the NE is in fault mode.

The following tasks are covered:

- *Performing an Upgrade of Baseline*, see Section 6.12.1 on page 91.
- *Performing an Upgrade of Modules*, see Section 6.12.2 on page 93.
- *Performing Emergency Fallback for NPU2/NPU1 B and ATU NPU*, see Section 6.12.3 on page 95.
- *Performing Emergency Fallback for NPU 8x2*, see Section 6.12.4 on page 96.

6.12.1 Performing an Upgrade of Baseline

This procedure describes how to perform a software upgrade, where all load modules comply with a baseline defined in a Software Baseline Description File (SBDF).

Note: The SBDF and the load modules must be stored in specific folders under: `<drive:>\tn_ftp_home\tn_system_release\ml_tn_software`, see Section 3.2.1.2 on page 18.

Note: MMU2 and SMU2 (protection) are upgraded using MSM, Local Upgrade or MINI-LINK Manager.

Note: Modules should be updated step-wise, not skipping any major versions.

This means that, when you want to upgrade from R1<*letter*> to R3<*letter*>, you should first upgrade to R2<*letter*> and then to R3<*letter*>, where <*letter*> indicates any minor version.

Since a new baseline can contain load modules of versions that do not belong to the next major version, you need to upgrade those modules individually to versions that can be upgraded to the new baseline. See Section 6.12.2 on page 93 for instructions.

To perform an upgrade of baseline:

1. In the **Navigation Tree**, click the NE.
2. On the **Tools** menu, click **Software Upgrade**.

3. On the **Upgrade of Baseline** page, under **Desired Baseline**, specify the **Product Number** and **Release** state of the new baseline.

4. Click **Apply** and then click **Next**.

5. On the **Settings** page, under **FTP server**, do one of the following:
   - If the new software configuration resides on a remote FTP server, select **Remote server**.
   - If the new software configuration resides on the PC, select **Local server**. Click **PC** to enter the IP address, specify **User Name** and **Password**.

6. Under **Activation**, do one of the following:
   - If you want the NE to run on the new software configuration immediately after the software upgrade is finished, select **Immediate**.
   - If you want the NE to run on the new software configuration from a certain point of time in the future, select **Scheduled** and specify **Date** (yyyy-mm-dd) and **Time** (hh:mm).

7. Under **Confirmation**, do one of the following:
   - If you want to manually confirm the new software configuration, select **Manual**. This is not feasible together with a scheduled activation.
   - If you want the NE to automatically confirm the new software configuration, select **Automatic**.

8. Verify the **Preferences** used for the software upgrade. The following is recommended:
   - Automatic Upgrade – ON
   - Automatic Downgrade – ON
   - Accept Failures – OFF

   If Automatic Upgrade or Downgrade is OFF, the preferences can be changed after the SBDF has been loaded. This will then initiate an automatic software upgrade/downgrade.

9. On the **Settings** page, click **Next**.

10. On the **Start Upgrade** page, verify the requested actions and click **Start Upgrade**.

    The **Upgrade Progress – Baseline** page monitors the download of the new software configuration. The page is refreshed every fifth second. When all load modules have been correctly received, the status `Upgrade Finished` is displayed for the software baseline.

11. Depending on the selected activation method the following apply:

If	Then
Activation>Immediate was selected	• Click **Activate**. The **Activation** page is displayed. • If manual confirmation was selected, the **Confirm New Software Configuration** page will be displayed. Click **Confirm**. The new software configuration is now the active software in the NE. **Note:** If you do not confirm within 15 minutes the NE will revert to the old software configuration. Clicking **Fallback** will give the same result.
Activation->Scheduled was selected	The **Scheduled Activation** page is displayed. The new software configuration will be automatically confirmed at the specified time.

6.12.2 Performing an Upgrade of Modules

This procedure describes how to perform a software upgrade of specific load modules.

Note: The load modules must be stored in specific folders under: `<drive:>\tn_ftp_home\tn_system_release\ml_tn_software`, see Section 3.2.1.2 on page 18.

Note: MMU2 and SMU2 (protection) are upgraded using MSM, Local Upgrade or MINI-LINK Manager.

Note: Performing an upgrade of modules will disable version control.

Note: Modules should be updated step-wise, not skipping any major versions.

This means that, when you want to upgrade from R1<*letter*> to R3<*letter*>, you should first upgrade to R2<*letter*> and then to R3<*letter*>, where <*letter*> indicates any minor version.

To perform an upgrade of modules:

1. In the **Navigation Tree**, click the NE.
2. On the **Tools** menu, click **Software Upgrade**.
3. On the **Upgrade of Baseline** page, click **Upgrade of Modules**.
4. On the **Upgrade of Modules** page, enter the **New Release** and select the **Upgrade** check box for each module to be included in the upgrade.

5. Click **Apply** and then click **Next**.

6. On the **Settings** page, under **FTP server**, do one of the following:
   - If the new software configuration resides on a remote FTP server, select **Remote server**.
   - If the new software configuration resides on the PC, select **Local server**. Click **PC** to enter the IP address, specify **User Name** and **Password**.

7. Under **Activation**, select **Immediate**.

8. Under **Confirmation**, do one of the following:
   - If you want to manually confirm the new software configuration, select **Manual**.
   - If you want the NE to automatically confirm the new software configuration, select **Automatic**.

   Note: Selecting **Manual** requires an action whenever the confirmation takes place.

9. On the **Settings** page, click **Next**.

10. On the **Start Upgrade** page, verify the requested actions and click **Start Upgrade**.

    The **Upgrade Progress – Modules** page monitors the download of the new software configuration. The page is refreshed every fifth second. When all load modules have been correctly received, the status `Upgrade Finished` is displayed for the all modules and the **Activate** button appears.

11. Click **Activate**. The **Activation** page is displayed.

12. If manual confirmation was selected, click **Confirm** on the **Upgrade Progress – Modules** page. The new software configuration is now the active software in the NE.

    Note: If you do not confirm within 15 minutes the NE will revert to the old software configuration. Clicking **Fallback** will give the same result.

13. When the software upgrade is finished, you can use the **View Units** page to verify the load module version in each unit, see Section 11.80 on page 266.

    Should a failure occur, the **Event Log** page provides information about the software upgrade, see Section 11.134 on page 351.

6.12.3 Performing Emergency Fallback for NPU2/NPU1 B and ATU NPU

This procedure describes how to revert to a previous software release for an NPU2/NPU1 B and ATU NPU.

Caution!

Use this function restrictively and only in the unlikely event that you have performed a software upgrade to a software version, from which you cannot perform a full software upgrade back to a correct version.

To perform an emergency fallback:

1. Connect the USB cable to the USB connector on the NPU or ATU (B).
2. Start a Web browser and enter the URL `http://10.0.0.1`.
3. In the **Enter Network Password** dialog box, type the user name and password, and click **OK**. For more information see Section 9.1 on page 135.
4. On the **Configuration** menu, click **Installation Wizard**.
5. On the **Tools** menu, click **Emergency Fallback**.
6. On the **Emergency Fallback** page, click **Perform Emergency Fallback**.
7. On the **Perform Emergency Fallback** page, click **OK**.
8. Click **OK**, in the confirmation dialog box.
9. On the **Emergency Fallback** page, click **Finish Installation**.
10. On the **Finish Installation** page, click **OK**.
11. The NE will make a warm restart. After the restart the NE is in NPU Installation mode where a configuration file can be downloaded that will cause an upgrade to a consistent system.

    Note: NPU Installation mode is not applicable for ATU (B). Instead, the system starts with the Installation Wizard.

6.12.4 Performing an Emergency Fallback for NPU 8x2

This procedure describes how to revert to a previous software release for an NPU 8x2.

Caution!

Use this function restrictively and only in the unlikely event that you have performed a software upgrade to a software version, from which you cannot perform a full software upgrade back to a correct version.

Note: The NE is accessed in Node Installation mode. Configure the PC to use a dynamic IP address obtained from the DHCP server in the NE or alternatively use the static IP address `10.0.0.2`. For more information on IP addressing, see Section 3.3.4 on page 32.

To perform an emergency fallback:

1. Switch off and switch on the power supply.

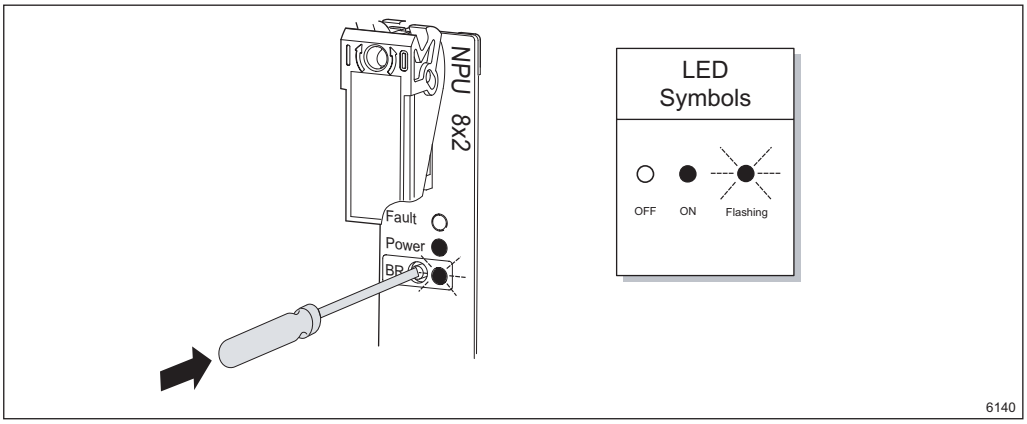


Figure 30 Entering Node Installation mode

2. While the Fault (red), Power (green) and BR (yellow) LEDs on the NPU 8x2 are ON (NE power up), press the BR button gently and release it. The BR (yellow) LED will start flashing, indicating that the NE is in Node Installation mode.
3. Connect the Ethernet cable (twisted pair) to the 10/100BASE-T port.
4. Start a Web browser and enter the URL **`http://10.0.0.1`**.
5. In the **Enter Network Password** dialog box, type the user name and password, and click **OK**. For more information see Section 9.1 on page 135.
6. On the **Tools** menu, click **Emergency Fallback**.

7. On the **Emergency Fallback** page, click **Perform Emergency Fallback**.
8. On the **Perform Emergency Fallback** page, click **OK**.
9. Click **OK**, in the confirmation dialog box.
10. On the **Emergency Fallback** page, click **Finish Installation**.
11. On the **Finish Installation** page, click **Apply**.
12. The **Installation Finished** page is displayed and the NE will make a warm restart.

6.13 Introduction to CLI

This section gives an introduction to the Command Line Interface (CLI), a text based configuration tool similar to industry standards used for router configuration. It is intended for specific configuration and troubleshooting of IP routing parameters and accessed from a Command Prompt window using telnet.

The following is covered:

- *CLI Overview*, see Section 6.13.1 on page 97.
- *Summary of Important Commands*, see Section 6.13.2 on page 103. This includes standard commands, such as **`ping`** and **`traceroute`**, used for general IP DCN troubleshooting.
- *OSPF Configuration and Troubleshooting*, see Section 6.13.3 on page 107.
  - *Defining an OSPF Area as a Stub Area*, see Section 6.13.3.1 on page 107.
- *Configuration of Static Routing*, used when the preferred OSPF routing strategy can not be used, see Section 6.13.4 on page 110.

6.13.1 Overview

This section describes how to use the CLI and the modes of operation.

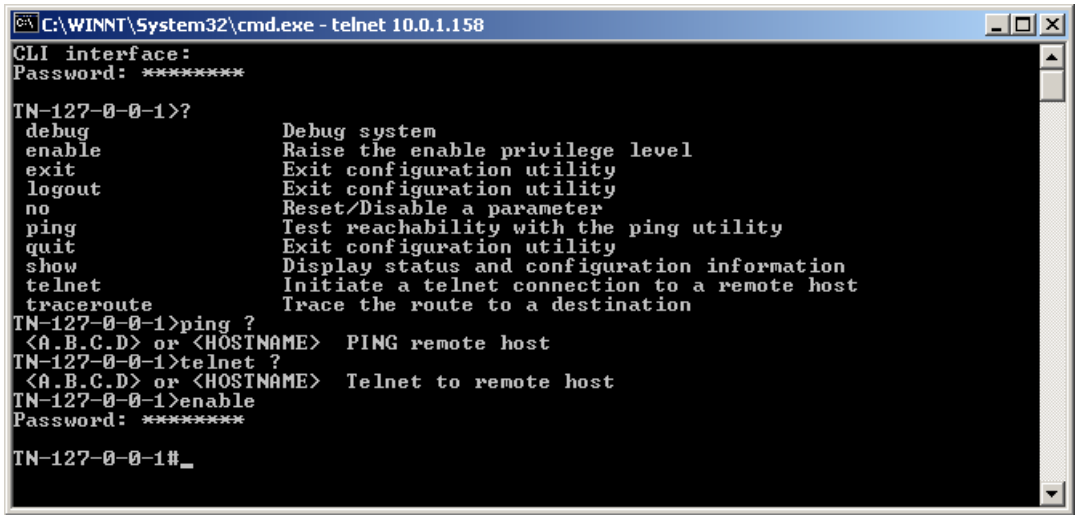


Figure 31 CLI in a Command Prompt window

6.13.1.1 Confirmation of Configuration

Configuration of parameters that could lead to loss of a DCN channel, for example change of IP address, need to be confirmed. The confirmation is made automatically if an EEM user is logged on as control_user and an NE generated **`ping`** command to the EEM PC is successful. Otherwise, confirmation of these parameters must be done manually.

Confirmation from the CLI is done using the **`write`** command, see Table 10 on page 104. It is also possible to use the **Confirm** button. The Status Bar indicates the remaining time and warnings will be issued when time is running out. It is also possible to use the **`show confirm timer`** command to display the remaining time, see Table 10 on page 104.

Caution!

If you do not confirm your configurations within 15 minutes, the NE will make a warm restart, restoring the saved configurations, and your unconfirmed changes will be lost.

6.13.1.2 Help Facility

The CLI contains a text based help facility accessed by typing in the full or partial command string then typing “?”. The CLI displays the command keywords or parameters plus a short description. Typing only “?” displays all commands that can be entered.

For example, at the CLI command prompt, type “ping?” (the CLI does not display the question mark). The CLI displays the following keyword list with short descriptions for each keyword:

```
<HOST> Hostname to ping

<A.B:C:D> IP Address to ping
```

The CLI can complete the spelling of command or parameter keywords, using the TAB key. The following example shows how this function can be used.

1. Type the beginning of a command. The CLI displays the complete command (if not ambiguous).

   `TN-10-0-1-1>`**`sh`**. Press the TAB key.

   ```
   TN-10-0-1-1>show
   ```

2. The CLI shows if the command or parameter partial spelling is ambiguous and displays the choices that match the abbreviation.

   `TN-10-0-1-1>`**`show i`**. Press the TAB key.

   ```
   interface

   ip
   ```

3. Type a character that excludes one of the choices.

   `TN-10-0-1-1>show i`**`n`**. Press the TAB key.

   ```
   TN-10-0-1-1>show interface
   ```

4. Type “?” to display the parameters for the specific command.

   ```
   [IFNAME] Interface name

   TN-10-0-1-1>show interface
   ```

6.13.1.3 Command Modes

The CLI commands are sorted into classes: Exec commands and Configuration commands. Configuration commands are further categorized into the following modes: Global Configuration, Interface Configuration and Router Configuration. Figure 32 on page 100 illustrates the command modes.

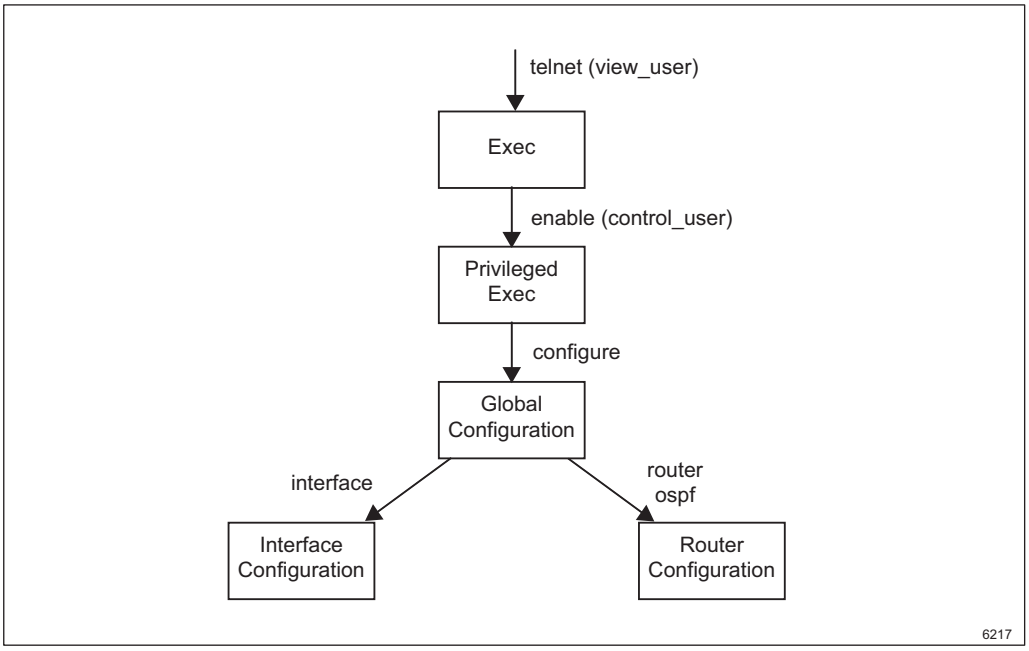


Figure 32 Command modes

Below follows a description of the command modes. The IP address `10.0.1.1` is used as an example.

6.13.1.3.1 Exec Mode

Access method Start a telnet session.

`C:\>`**`telnet 10.0.1.1`**

`Password:`***`<view_user password>`***

Prompt `TN-10-0-1-1>`

Exit method **`exit, quit, logout`** terminates the session.

Description Change terminal settings and perform basic tests. Display non-configurable information.

6.13.1.3.2 Privileged Exec Mode

Access method Enter **`enable`** in Exec mode.

`Password:`***`<control_user password>`***

Prompt `TN-10-0-1-1#`

Exit method **`disable`** exits to Exec mode. **`exit`**, **`quit`** or **`logout`** terminates the session.

Description Verify information and save configurations.

6.13.1.3.3 Global Configuration Mode

Access method Enter **`configure`** in Privileged Exec mode.

Prompt `TN-10-0-1-1(config)#`

Exit method **`exit`**, **`end`** or **`CTRL+Z`** exits to Privileged Exec mode.

Description A gateway to other modes. Configuration of general IP parameters.

6.13.1.3.4 Interface Configuration Mode

Access method Enter one of the following commands in Global Configuration mode:

`interface ethernet`

`interface ospf` ***`<if>`***

`interface serial`<***`if`***>

Prompts `TN-10-0-1-1-(interface-ethernet)#`

`TN-10-0-1-1-ospf(config-if)#`

`TN-10-0-1-1-(interface-serial)#`

Exit method **`exit`** or **`quit`** exits to Global Configuration mode.

`end` or **`CTRL+Z`** exits to Privileged Exec mode.

Description Configuration of Ethernet, PPP interfaces and OSPF parameters related to specific interfaces.

6.13.1.3.5 Router Configuration Mode

Access method Enter **`router ospf`** in Global Configuration mode.

Prompt `TN-10-0-1-1-ospf(config-router)#`

Exit method **`exit`** or **`quit`** exits to Global Configuration mode.

`end` or **`CTRL+Z`** exits to Privileged Exec mode.

Description Configuration of the OSPF routing protocol.

6.13.1.4 Command Editing Keys and Functions

Table 8 on page 102 describes the editing features of the CLI.

Note: The telnet client must be configured for VT100 emulation for the arrow keys to work.

Table 8 Command editing keys and functions

Keys	Description
TAB	Completes a partial command name entry. When you enter a unique set of characters and press the TAB key, the system completes the command name. If you enter a set of characters that could indicate more than one command, the system beeps to indicate an error and provides a list of commands that begin with that string.
?	Entering a stand-alone question mark (?) provides a list of all available commands. Entering a question mark (?) immediately after a partial command (no space), provides a list of commands that begin with that string.
BACKSPACE	Erases the character to the left of the cursor.
ENTER	Performs the function of processing a command. At the ”>” prompt on a terminal screen, pressing the ENTER key scrolls down one line.
LEFT ARROW	Moves the cursor one character to the left. When you enter a command that extends beyond a single line, you can press the LEFT ARROW key repeatedly to scroll back toward the system prompt and verify the beginning of the command entry.
RIGHT ARROW	Moves the cursor one character to the right.
UP ARROW or CTRL+P	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
DOWN ARROW or CTRL+N	Returns to more recent commands in the history buffer after recalling commands with UP ARROW or CTRL+P. Repeat the key sequence to recall successively more recent commands.
CTRL+A	Moves the cursor to the beginning of the line.
CTRL+B	Moves the cursor back one character.
CTRL+C	Starts on a new command line.
CTRL+D	Deletes the character at the cursor.
CTRL+E	Moves the cursor to the end of the command line.
CTRL+F	Moves the cursor forward one character.
CTRL+H	Deletes the character in front of the cursor.
CTRL+K	Deletes all characters from the cursor to the end of the command line.
CTRL+L	Redisplays the system prompt and command line.
CTRL+U	Deletes all characters from the command line.
CTRL+W	Deletes the word to the left of the cursor.
CTRL+Z	Exits to Privileged Exec mode.

6.13.2 Summary of Important Commands

This section gives a summary of the most important commands in the different modes. Use the help utility to get all available options for each command.

Table 9 Commands in Exec mode

Command	Parameter	Description
debug	**ospf**	Enables debugging of OSPF information. The following additional parameters are supported: **route** — OSPF route information **packet** — OSPF route information **nfsm** — Neighbor state machine **lsa** — Link state advertisement **ifsm** — Interface state machine **event** — OSPF event information
enable	—	Enters Privileged Exec mode, see Table 10 on page 104. Protected by a control_user password.
exit	—	Terminates the current telnet session.
logout	—	Terminates the current telnet session.
ping	—	Used for testing a bi-directional IP connection.
quit	—	Terminates the current telnet session.
show	—	Displays information as described below.
	interface	Displays the configuration and status of the interfaces (PPP and Ethernet)
	networks	Lists all DCN networks with interface type, NE identification, interface name, bandwidth and status.
	history	Displays CLI command history per command mode. The list is cleared after each telnet session. Use the UP ARROW/DOWN ARROW keys in order to access the command history buffer. Note: the telnet client must be configured for VT100 emulation for the arrow keys to work.
	ip	The following additional parameters are supported: **route** — IP routing table **protocols** — Protocol process parameters and statistics **ospf** — OSPF information. **forwarding** — IP forwarding status **traffic** — IP statistics
	confirm timer	Displays the remaining time until a configuration confirm must be done.
telnet	—	To establish a telnet session onto a host.
traceroute	—	Used to test IP connections with other NEs, listing routers visited on the way.

Table 10 Commands in Privileged Exec mode

Command	Parameter	Description
configure	—	Enters global configuration mode, see Table 11 on page 105.
debug	**ospf**	Enables debugging of OSPF information. The following additional parameters are supported: **route** — OSPF route information **packet** — OSPF route information **nfsm** — Neighbor state machine **lsa** — Link state advertisement **ifsm** — Interface state machine **event** — OSPF event information
disable	—	Returns to Exec mode, see Table 9 on page 103.
enable	—	No effect since already in Privileged Exec mode.
exit	—	Terminates the current telnet session.
logout	—	Terminates the current telnet session.
no	—	Negates a configuration
ping	—	Used for testing a bi-directional IP connection.
quit	—	Terminates the current telnet session.
show	—	Displays information as described below.
	interface	Displays the configuration and status of the interfaces (PPP and Ethernet).
	networks	Lists all DCN networks with interface type, NE identification, interface name, bandwidth and status.
	history	Displays CLI command history per command mode. The list is cleared after each telnet session. Use the UP ARROW/DOWN ARROW keys in order to access the command history buffer. Note: the telnet client must be configured for VT100 emulation for the arrow keys to work.
show	**ip**	The following additional parameters are supported: **route** — IP routing table **protocols** — Protocol process parameters and statistics **ospf** — OSPF information. **forwarding** — IP forwarding status **traffic** — IP statistics
	confirm timer	Displays the remaining time until a configuration confirm must be done.
telnet	—	To establish a telnet session onto another NE or get access to a local host shell.
terminal	**ospf**	Enables OSPF debug printouts to the telnet console.
	no	Negates a command or set its default.

Command	Parameter	Description
traceroute	—	Used to test IP connections with other NEs, listing routers visited on the way.
write	—	Sends operator confirm for configuration of parameters that could cause loss of a DCN channel. **Caution!** If you do not save your configurations within 15 minutes, the NE will make a warm restart, restoring the saved configurations, and your unconfirmed changes will be lost. For more information, see Section 6.13.1.1 on page 98.

Table 11 Commands in Global Configuration mode

Command	Parameter	Description
debug	**ospf**	Enables debugging of OSPF information. The following additional parameters are supported: **route** — OSPF route information **packet** — OSPF route information **nfsm** — Neighbor state machine **lsa** — Link state advertisement **ifsm** — Interface state machine **event** — OSPF event information
end	—	Exits to Privileged Exec mode.
exit	—	Exits to Privileged Exec mode.
ip	—	IP configuration as described below.
	route	Sets up static IP routes, including the default gateway route.
	forwarding	Turns on IP forwarding (default).
	name-server	Configures one, two or three Domain Name Servers (DNS). This is normally done from the EEM.
	domainname	Configures the name of the domain the NE belongs to. This is used for name resolution. This is normally done from the EEM.
	dhcp relayaddress	Configures the IP address of the DHCP server the NE is a relay for. This is normally done from the EEM.
no	—	Negates a configuration as described below.
	router	Disables a routing protocol.
	interface	Selects an interface to delete.
	ip	Removes IP configuration.
ntp	**server**	Defines the address of the NTP server. This is normally done from the EEM.
router	**ospf**	Used to configure OSPF, see Table 13 on page 106. For a summary of the most common OSPF related commands, see Section 6.13.3.2 on page 108.

Table 12 Commands in Interface Configuration mode

Command in Global Configuration mode	Command	Description
`interface ethernet`	`ip address`	Configures the IP address of the ethernet interface. This is normally done from the EEM.
`interface ospf <if>`	—	Configures OSPF parameters for the selected interface as described below. For a summary of the most common commands, see Section 6.13.3.2 on page 108 .
	`description`	Interface specific description.
	`end`	Exits to Privileged Exec mode, see Table 10 on page 104.
	`exit`	Exits to Global Configuration mode, see Table 11 on page 105.
	`ip`	Configuration of IP parameters.
	`list`	Prints the command list.
	`no`	Negates a command or sets its default value.
	`ospf`	OSPF interface commands.
	`quit`	Exits to Global Configuration mode, see Table 11 on page 105.
	`write`	Displays the OSPF running-config file.
`interface serial <if>`	—	Specifies a particular serial interface as described below.
	`trapenable`	Enables traps for the interface.
	`shutdown`	Sets the administrative status to Down.
	`exit`	Exits to Global Configuration mode, see Table 11 on page 105.

Table 13 Commands in Router Configuration mode

Command	Description
`area`	Sets OSPF area parameters.
`auto-cost`	Calculates OSPF interface cost according to bandwidth.
`compatible`	OSPF compatibility list.
`default-information`	Controls distribution of default information.
`default-metric`	Sets metric of redistributed routes.
`distance`	Defines an administrative distance.
`distribute-list`	Filters networks in routing updates.
`end`	Exits to Privileged Exec mode, see Table 10 on page 104.
`exit`	Exits to Global Configuration mode, see Table 11 on page 105.
`help`	Description of the interactive help system.
`list`	Prints the command list.

Command	Description
neighbor	Specifies neighbor router.
network	Enables routing on an IP network.
no	Negate a command or set its defaults
opaque-lsa-capable	Enables Opaque-LSA capability
ospf	OSPF specific commands.
overflow	Controls overflow.
passive-interface	Suppresses routing updates on an interface.
quit	Exits to Global Configuration mode, see Table 11 on page 105.
redistribute	Redistributes information from another routing protocol.
refresh	Adjusts refresh parameters.
router-id	Sets the router ID for the OSPF process.
summary-address	Creates aggregate addresses.
timers	Adjusts routing timers.
write	Displays the OSPF running-config file.

6.13.3 OSPF Configuration and Troubleshooting

This section introduces how to use the CLI for OSPF configuration and troubleshooting.

6.13.3.1 Defining an OSPF Area as a Stub Area

If there is only one Area Border Router (ABR) within an area, it is recommended to define the area as a stub area, in all routers within the area, in order to reduce the size of the routing table. Using stub areas improves the performance of the OSPF routing by reducing the size of the link state database and the memory requirements of routers inside the areas.

Creating a stub area can also be done from the EEM, see Section 6.10.3 on page 88.

The following example shows how to define an area (area ID=1.1.1.1) as a stub area.

1. Log in in Exec mode.

```
C:\>telnet 10.0.1.1

Password:*****
```

2. Enter Privileged Exec mode.

   ```
   TN-10-0-1-1>enable

   Password:******
   ```

3. Enter Global Configuration mode.

   ```
   TN-10-0-1-1#configure
   ```

4. Enter Router Configuration mode for OSPF.

   ```
   TN-10-0-1-1(config)#router ospf
   ```

5. Define the area as a stub area.

   ```
   TN-10-0-1-1-ospf(config-router)#area 1.1.1.1 stub
   ```

   Note: For an ABR it is possible to add the **no-summary** parameter in order to stop the ABR from sending summary link advertisements into the stub area. This will reduce the routing table even more.

6. Exit Router Configuration mode.

   ```
   TN-10-0-1-1-ospf(config-router)#exit
   ```

7. Exit Global Configuration mode.

   ```
   TN-10-0-1-1(config)#exit
   ```

8. Save the configuration.

   ```
   TN-10-0-1-1#write
   ```

6.13.3.2 OSPF Configuration Commands

This section introduces the most common commands for OSPF configuration. Use the help utility to get all available parameter options for each command.

Table 14 OSPF configuration commands

Command	Mode	Description
interface ospf <if> Example: **interface ospf ppp0**	Global Configuration	Enters Interface Configuration mode.
router ospf	Global Configuration	Enters Router Configuration mode for OSPF.
area stub Example: **area 1.1.1.1 stub**	Router Configuration	Defines an area as a stub area. All routers (including the) in a stub area must be configured accordingly. See also Section 6.13.3.1 on page 107.

Command	Mode	Description
network Example: **network 10.0.0.0/8 area 1.1.1.1**	Router Configuration	Enables OSPF routing with a specified area ID on interfaces with IP addresses that match the specified network address.
redistribute Example: **redistribute connected**	Router Configuration	To redistribute routes from other routing protocols, static routes and kernel routes into an OSPF routing table
router-id Example: **router-id 2.3.4.5**	Router Configuration	To specify a router ID for the OSPF process.
cost Example: **ip ospf cost 10**	Interface Configuration	Sets the interface cost.
dead-interval Example: **ip ospf dead-interval 60**	Interface Configuration	Sets the dead-interval (default 40).
hello-interval Example: **ip ospf hello-interval 20**	Interface Configuration	Sets the hello-interval (default 10).
priority Example: **ip ospf priority 3**	Interface Configuration	Sets the router priority to determine the Designated Router (DR) for the network (default 1)

6.13.3.3 OSPF Show Commands

Table 15 on page 109 lists the most common commands showing OSPF configuration. Use the help utility to get all available parameter options for each command.

All commands are entered in Privileged Exec mode.

Table 15 OSPF show commands

Command	Description
show ip ospf database	Displays a database summary for OSPF information.
show ip ospf database network	Displays information about the network LSAs.
show ip ospf database router	Displays information about the router LSAs.
show ip ospf database summary	Displays information about the summary LSAs.
show ip ospf interface	Displays interface information for OSPF.
show ip ospf neighbor	Displays information on OSPF neighbors.
show ip ospf route	Displays the OSPF routing table.
show ip route	Displays the complete routing table including OSPF (O) entries.

6.13.4 Configuring Static Routing

Using static routing means that a fixed routing scheme is entered manually from the CLI. Static routing can also be done from the EEM, see Section 6.10.5 on page 89. A maximum of 100 static routes is possible.

The following command is used from the CLI:

ip route ***<destination> <gateway>***

The example below sets up a static route from an NE (IP address=`10.0.1.1`) to IP address `10.0.3.0`, subnet mask 24, through the gateway `10.0.2.1`.

1. Log in in Exec mode.

   ```
   C:\>telnet 10.0.1.1

   Password:******
   ```

2. Enter Privileged Exec mode.

   ```
   TN-10-0-1-1>enable

   Password:******
   ```

3. Enter Global Configuration mode.

   ```
   TN-10-0-1-1#configure
   ```

4. Set up the static route.

   ```
   TN-10-0-1-1(config)#ip route 10.0.3.0/24 10.0.2.1
   ```

5. Exit Global Configuration mode.

   ```
   TN-10-0-1-1(config)#exit
   ```

6. Save the configuration.

   ```
   TN-10-0-1-1#write
   ```

Although a default route is not required in OSPF networks it is recommended to configure a default gateway since it reduces the risk of loosing DCN contact with the NE. The example below defines a default gateway with IP address `10.0.2.1`.

1. Log in in Exec mode.

   ```
   C:\>telnet 10.0.1.1

   Password:******
   ```

2. Enter Privileged Exec mode.

   ```
   TN-10-0-1-1>enable

   Password:******
   ```

3. Enter Global Configuration mode.

   ```
   TN-10-0-1-1#configure
   ```

4. Define the default gateway.

   ```
   TN-10-0-1-1(config)#ip route 0.0.0.0/0 10.0.2.1
   ```

5. Exit Global Configuration mode.

   ```
   TN-10-0-1-1(config)#exit
   ```

6. Save the configuration.

   ```
   TN-10-0-1-1#write
   ```

6.14 Generating Configuration Reports

Reports on the NEs hardware and software inventory, and the configuration settings can be generated, viewed, and saved.

To generate a report:

1. In the **Navigation Tree**, click the NE (the root).
2. On the **Tools** menu, click **Report** to open the **Report** page.
3. Select the items to include on the report. You can click **Clear All** and **Select All** to toggle all check boxes on and off.
4. Click **View Report** to see the report in the LCT, or click **Save Report** to save the report as an HTML file on your computer. See Section 11.75 on page 258 for information on what the report contains.

7 Fault Management

This section contains information and instructions for typical fault, status and test handling tasks.

The following areas are covered:

- *Operational Status*, see Section 7.1 on page 113.
- *Alarms and Events*, see Section 7.2 on page 115.
- *Viewing the DCN Status*, see Section 7.3 on page 126.
- *Loops*, see Section 7.4 on page 126.
- *Error Log Handling*, see Section 7.5 on page 129.

7.1 Operational Status

This section describes the principles of the operational status of equipment and interfaces when working with the EEM.

7.1.1 Operational Status of Equipment

The operational status is a high-level status indication of a plug-unit or the NE. It is displayed as **Status** on an **Alarms and Status** page, see for example Section 11.114 on page 319. An equipment failure initiates an update of the operational status. A more detailed equipment status is indicated by alarms, for example high temperature, see Section 7.2.5 on page 118.

The signification of the operational status of a unit is listed in Table 16 on page 114.

Table 16 Operational status of equipment

Operational status	NE	Unit
In Service	The NE is operating properly.	The unit is operating properly.
Reduced Service	The traffic functionality in the backplane is available but the management functionality or a redundant function is reduced or unavailable. A further reduction will have impact on traffic.	The traffic functionality is available but the management functionality is reduced or unavailable.
Out of Service	The NE is not operating.	The unit is not operating, that is a traffic disturbing failure has occurred. A plug-in unit is in a cold reset state where all traffic, control and management logics are reset.

The relation between the operational status and alarm severity is listed in Table 17 on page 114.

Table 17 Relation between operational status and alarm severity

Operational status	Alarm severity
In Service	Clear/Warning
Reduced Service	Minor/Major
Out of Service	Critical

7.1.2 Operational Status of Interfaces

The possible operational status of an interface is listed in Table 18 on page 114.

Table 18 Operational status of an interface

Operational status	Description
Up	Payload is passing on the interface and one or several of the active lower layers have operational status Up.
Down	A defect is detected on the interface or administrative status is set to Down.
Unknown	The unit is in cold reset, warm reset or repair state.
Testing	The interface is in test mode, for example a loop is active or a BERT is running.
Lower Layer Down	The interface is Down due to lower layer interfaces. Payload is passing on the interface but not all active lower layers have operational status Up.

7.2 Alarms and Events

7.2.1 Alarm Notifications

The sending of alarm notifications can be disabled on the following levels:

- NE, preventing alarms from leaving the NE. This will send an event notification to the EEM (or MINI-LINK Manager) informing that no notifications will be sent. If the alarm notifications are enabled later on a new notification will be sent informing about the change. New alarms on NE level will always be added to the **Alarm List**.
- Plug-in unit, also suppressing notifications from all the interfaces on the unit. Disabling alarm notifications on a plug-in unit means that for all its existing alarms a clear alarm is sent removing the alarms from the **Alarm List**.
- Interface, also suppressing notifications from higher layer interfaces. Disabling alarm notifications on an interface means that for all its existing alarms a clear alarm is sent removing the alarms from the **Alarm List**.

Enabling of alarm notifications on any level means that new alarms are added to the **Alarm List**.

Alarm notifications on all levels are enabled by default. However, to prevent too many alarms from not traffic routed E1s, notifications are default disabled on these interfaces.

7.2.2 Viewing Alarms

The alarms and status information of the NE, a plug-in unit or an interface is displayed on a specific **Alarms and Status** page, see for example Section 11.91 on page 280.

To access an **Alarms and Status** page:

1. In the **Navigation Tree**, click the entity for which you want to view the alarms and status.
2. On the **Fault** menu, click **Alarms and Status**.

The alarms and status for DCN and Ethernet Bridge are accessed on the **Fault** menu by selecting the **NE** in the **Navigation Tree**.

The alarms and status of Radio Terminals with MMU2 B/C are displayed on the **Radio Terminal Alarms and Status** page, see Section 11.116 on page 322.

An **Alarm List** page displaying all active alarms is available on NE, unit and interface level, see Section 11.133 on page 349. The **Alarm List** is cleared after a restart (cold or warm) of the NPU or NE.

To display the **Alarm List**:

1. In the **Navigation Tree**, click the entity for which you want to display the **Alarm List**.

2. On the **Fault** menu, click **Alarm List**.

7.2.3 Viewing Logged Alarms and Events

The NE keeps a log of the 400 latest alarms and events, which can be accessed from the **Event Log** page, see Section 11.134 on page 351. The **Event Log** is cleared after a restart of the NPU or NE.

To display the **Event Log**:

1. In the **Navigation Tree**, click the **NE**.

2. On the **Fault** menu, click **Event Log**.

7.2.4 Severity

Table 19 on page 117 explains the signification of the alarm and event severities.

Table 19 Explanations of alarm and event severities

Color	Severity	Description
Green Cleared	Cleared	Indicates the clearing of one or more previously reported alarms.
Bluish-green Indeterminate	Indeterminate	Indicates that the severity level cannot be determined. This severity is not used on NE level.
Blue Warning	Warning	Indicates the detection of a potential or impending service affecting fault, before any significant effects are known. An action should be taken to further diagnose (if necessary) and correct the problem in order to prevent it from becoming more serious service affecting. Can also be used for events.
Yellow Minor	Minor	Indicates the existence of a non-service affecting fault condition and that a corrective action should be taken in order to prevent a more serious (for example, service affecting) fault. Such a severity can be reported, for example when the detected alarm condition is not currently degrading the capacity of the managed object. This severity is used for example in case of high temperature on a unit.
Orange Major	Major	Indicates that a service affecting condition has developed and an urgent corrective action is required. Such a severity can be reported, for example when there is a severe degradation in the capability of a unit or interface and its full capability must be restored, like in case of SES or high temperature on a unit.
Red Critical	Critical	Indicates that a service affecting condition has occurred and an immediate corrective action is required. Such a severity can be reported, for example when a unit or interface is totally Out of Service and its capability must be restored, like in case of a LOS.

7.2.5 Lists of Alarms and Events

This section gives a summary of:

- Alarms, see Table 20 on page 118.
- Events, see Table 21 on page 125.

Table 20 List of alarms

Entity	Specific Problem	Description	Severity
NE	Power Failure	A malfunction in the redundant PFU.	Major
	Node Installation	The NE is in Node Installation mode. Enter the URL `http://10.0.0.1` to reach the installation wizard.	Minor
	NPU Installation	The NE is in NPU Installation mode. Enter the URL `http://10.0.0.1` to reach the installation wizard.	Major
	Traffic System Failure	A malfunction related to traffic. At least one bus in the backplane fails.	Major: One bus fails. Critical: Two or three TDM busses fail.
	Control System Failure	A malfunction related to management. The NPU or the control bus fails. Load the Error Log. A software upgrade is probably required.	Major
	Node Fault Mode	The self-repair mechanism has failed and the NE is in a fault mode(1). A replacement of the NPU is probably required.	Critical
	OSPF LSA Database Overload	The OSPF routing database is full due to too many routers in the network.	Minor
Plug-in Unit	Unit Removed	The unit is removed.	Critical
	High Temperature	The unit has reached an abnormal temperature.	Minor
	Excessive Temperature	The unit has reached an excessive temperature.	Critical
	Wrong Software	A wrong load module release is running on the unit.	Critical

Entity	Specific Problem	Description	Severity
Plug-in Unit	Hardware Error	A malfunction related to hardware.	Minor: Control system failure. Critical: Traffic or power system failure.
	Unsupported Unit Type	Unit type not supported by SW.	Critical
	Wrong Position	The unit is in the wrong position in the AMM.	Critical
FAU	Hardware Error	A malfunction related to hardware.	Critical
MMU2 B/C(2)	RCC Unavailable	Communication is lost on the Radio Communication Channel, between the MMU and the RAU.	Major
	ICC Unavailable	Communication is lost on the Internal Communication Channel, between two MMUs	Major
	HCC Unavailable	Communication is lost on the Hop Communication Channel, between the near-end MMU and the far-end MMU.	Major
	ATPC Capability (Far-end)	The terminal on the far end is configured for ATPC but at least one of the indoor units does not support ATPC.	Major
RAU IF (on MMU2 B/C)	Dmod Clock	The internal data rate of the MMU does not correspond to the received data rate. This fault will cause bit slip in the composite bit stream.	Critical: Active transmitter. Major: Standby transmitter.
	LOS	Input traffic failure in the transmitting direction.	Critical: Active transmitter. Major: Standby transmitter.
	Rx IF Input	Failure on the receiver IF signal from the RAU to the MMU.	Major
	Tx IF Input	Failure on the received IF signal from the MMU to the RAU.	Critical: Active transmitter. Major: Standby transmitter.
	Radio Frame	The receiver failed to synchronize the frame of the received composite bit stream due to signal failure.	Critical: Active transmitter. Major: Standby transmitter.

Entity	Specific Problem	Description	Severity
RAU IF (on MMU2 B/C)	BER	The Bit Error Rate for the received signal has exceeded the BER alarm threshold.	Critical: Active transmitter. Major: Standby transmitter.
	Radio ID	The received traffic comes from a terminal with an ID not matching the far-end ID.	Critical: Active transmitter. Major: Standby transmitter.
	Mod Index	The modulation index of the MMU, controlled by the far end MMU, is out of the allowed range. Only valid for C-QPSK modulation.	Major
	AIS Received	AIS detected on the received traffic signal. Only available for a far-end terminal with MMU2 or a far-end MINI-LINK E terminal.	Critical: Active transmitter. Major: Standby transmitter.
	Unknown??	The status of the interface is unknown, for example due to loss of communication.	Major
	Rx Loop(3)	Indicates that an Rx Loop is set.	Warning
	IF Loop(3)	Indicates that an IF Loop is set.	Warning
SWITCH (MMU2 B/C)	Unable To Protect	The protection failed.	Major: A Tx or a common Tx/Rx alarm on one path. Also for an Rx alarm on one path and the duration is longer than 200 s. Critical:f alarms on both paths.
	Hitless Phase	Failure of synchronizing the received traffic in the two MMUs with a duration longer than 200 s.	Major
	Tx Switch Over	A TDM Tx switch or an active RAU transmitter switch. Only 1+1 Hot Standby.	Major
	Remote Tx Switch Over	An active RAU transmitter switch ordered from the far-end. Only 1+1 Hot Standby.	Major

Entity	Specific Problem	Description	Severity
RAU (connected to MMU2 B/C)	ATPC Capability	The terminal is configured for ATPC, but the RAU does not support ATPC. This alarm is activated only if ATPC is turned on (any direction).	Major
	Unit Removed	The RAU is disconnected from the MMU.	Critical
	Hardware Error	A malfunction related to hardware.	Minor: Control system failure. Critical: Traffic or power system failure.
	Incompatible Units	The wrong type of RAU is used.	Critical
	Unknown??	The status of the unit is unknown, for example due to loss of communication.	Major
RF (on RAU connected to MMU2 B/C)	Tx Frequency	The transmitter frequency synthesizer loop is unlocked.	Minor: Control system failure. Critical: Traffic or power system failure.
	Rx Frequency	The receiver frequency synthesizer loop is unlocked.	Minor: Control system failure. Critical: Traffic or power system failure.
	RF Output Level	A major degradation of the transmitter output power is detected.	Major
	Rx AFC	The frequency of the received signal is outside the range of the Automatic Frequency Control in the RAU receiver.	Major
	RF Input Level	The received RF input signal level has dropped below the threshold for the receiver.	Minor: Control system failure. Critical: Traffic or power system failure.
	RF Input Threshold	The RF input level has dropped below the specified threshold value in dBm for the input power.	Warning
	RF Loop[(3)]	Indicates that an RF Loop is set.	Warning
	Tx Off[(3)]	Indicates that the transmitter is off.	Warning

Entity	Specific Problem	Description	Severity
E1	LOS	Loss Of Signal is detected on the incoming traffic.	Critical
	AIS	An Alarm Indication Signal is detected on the incoming traffic.	Minor
	Unavailable State	Unavailable State is activated after 10 consecutive SES. 10 consecutive non-SES will cease the alarm.	Critical
1+1 E1 SNCP	Unable To Protect	The protection has failed.	Minor: The redundant interface fails. Critical: Both interfaces fail or the traffic is locked to a failing interface.
E2/E3	LOS	Loss Of Signal is detected on the incoming traffic.	Critical
	AIS	An Alarm Indication Signal is detected on the incoming traffic.	Minor: MMU2 B/C Critical: MMU2/SMU2
	Equipment OoS	Equipment Out of Service.	Critical
	LOF(4)	Loss Of Frame alignment.	Critical
	RAI(4)	Remote Alarm Indication	Critical
STM-1 port	Clock Loss of Reference	Loss of clock reference.	Minor
MS/RS	LOS	Loss Of Signal.	Critical
	LOF	Loss Of Frame Alignment.	Critical
	TIM	Trace Identifier Mismatch	Critical
	AIS	Alarm Indication Signal	Minor
	RDI	Remote Defect Indication	Minor
	DEG	Degraded Signal	Critical
	Unavailable State	Unavailable State is activated after 10 consecutive SES. 10 consecutive non-SES will cease the alarm.	Critical

Entity	Specific Problem	Description	Severity
MSP	Unable To Protect	The protection has failed.	Minor: The redundant interface fails. Critical: Both interfaces fail or the traffic is locked to a failing interface.
	Mode Mismatch	MSP mode mismatch. Far End configured as MSP 1:n	Minor
	Unavailable State	Unavailable State is activated after 10 consecutive SES. 10 consecutive non-SES will cease the alarm.	Critical
VC-4	LOP	Loss Of Pointer	Critical
	AIS	Alarm Indication Signal	Minor
	RDI	Remote Defect Indication	Minor
	Unequipped	The interface has no content since the unit is not configured	Critical
	PLM	Payload Mismatch	Critical
	TIM	Trace Identifier Mismatch	Critical
	DEG	Degraded Signal	Major
	LOM/TULOM	Loss Of Multiframe/Tributary Unit Loss Of Multiframe	Critical
	Unavailable State	Unavailable State is activated after 10 consecutive SES. 10 consecutive non-SES will cease the alarm.	Critical
VC-12	LOP	Loss Of Pointer	Critical
	AIS	Alarm Indication Signal	Minor
	RDI	Remote Defect Indication	Minor
	Unequipped	The interface has no content since the unit is not configured	Critical
	PLM	Payload Mismatch	Critical
	TIM	Trace Identifier Mismatch	Critical
	DEG	Degraded Signal	Major
	Unavailable State	Unavailable State is activated after 10 consecutive SES. 10 consecutive non-SES will cease the alarm.	Critical
User Input	User Defined	The Specific Problem and Severity is defined on the User Input Configuration page.	User Defined
PPP	PPP Down	Failure in the DCN communication.	Minor

Entity	Specific Problem	Description	Severity
OSPF	OSPF LSA database overload	The OSPF routing database is full.	Major
HDLC	Down/No Traffic	No throughput on the interface. All IM interfaces are Down.	Critical
	Degraded Service	One or several (but not all) IM interfaces are Down, leading to decreased speed on the bridge connection.	Major
Ethernet	Down	The interface is down.	Minor: Site LAN Critical: Ethernet Bridge
Bridge	Down	The interface is down.	Critical

(1) Software Upgrade cannot be performed when the NE is in fault mode.
*(2) Radio Terminal specific alarms. See also general alarms under **Plug-in Unit**.*
(3) No notification is sent.
(4) MMU2 B/C only.

Note: In addition to the alarms listed above, the **Alarm List** will also display a few alarms related to Radio Terminal units and interfaces. These alarms are, for terminals with MMU2, presented, described and handled in MSM.

Table 21 List of events

Entity	Specific Problem	Description	Severity
NE	Cold Restart	A restart of the control and management system as well as the traffic system. This type of restart will disturb all traffic.	Warning
	Warm Restart	A restart of the control and management system. Traffic is not disturbed by this type of restart.	Warning
	Notification Enable	Sent to all subscribers indicating that notifications are enabled.	Warning
	Notification Disable	Sent to all subscribers indicating that notifications are disabled.	Warning
	FTP Connection Error	An error in the communication with the FTP server has occurred.	Minor
	Load Module Error	Load module is corrupt or program error during software upgrade.	Minor
	Software Upgrade Started	A software upgrade procedure is started.	Warning
	Software Upgrade Finished	A software upgrade procedure is finished.	Warning
	Software Running	The new software is accepted and running.	Warning
	Management Software Fallback	NPU emergency fallback to the previous NPU software release.	Warning
	Software Upgrade Failed	Software upgrade failed.	Warning
	Software Upgrade Aborted	The software upgrade is aborted.	Warning
Plug-in Unit	Unit Inserted	A unit is inserted.	Warning
	Unit Removed	A unit is removed.	Warning
	Software not Conform to Baseline	Version control is enabled but upgrade/downgrade preferences do not allow DP software to be upgraded/downgraded to the revision corresponding to the SBL.	Warning
	Load Module not Part of Baseline	The load module that is required for the unit is not part of the SBL.	Warning
	Load Module Programming Failure	Software upgrade of this unit failed due to a programming failure (FLASH memory).	Warning
1+1 E1 SNCP	Protection Switch	A protection switch has occurred.	Warning

Entity	Specific Problem	Description	Severity
MSP	Protection Switch Reject	A requested protection switch has been rejected.	Warning
	Protection Switch Event	A protection switch has occurred.	Warning
SWITCH (MMU2 B/C)	Protection Switch	A protection switch has occurred.	Warning
MMU2 B/C and corresponding RAU	Spontaneous Restart	The processor in the RAU has restarted.	Warning
	Hot Swap Incomplete	A hot swap was made, but the configuration of the new unit is incomplete. This happens when the new unit does not support all configuration options of the old unit.	Warning

7.3 Viewing the DCN Status

There are several pages displaying the status of the DCN, in terms of parameters for interfaces and IP routing.

To view the DCN status:

1. In the **Navigation Tree**, click the NE.
2. On the **Fault** menu, click **DCN**.
3. The DCN parameters are grouped in different categories. Click a link to display a specific category.

7.4 Loops

Loops can be used to verify that the transmission system is working properly or they can be used to locate the faulty unit or interface in case of failure.

7.4.1 General

The following loops are supported:

Connection Loop Loops an E1 interface connected to the backplane back to its origin. The loop is done in the backplane. If the interface is traffic routed an AIS is transmitted to the other interface in the traffic routing.

Line Loop Loops an incoming line signal (MS/RS, E3, E2 and E1) back to its origin. The loop is done in the plug-in unit, close to the line interface. An AIS is sent to the backplane.

Local Loop Loops a line signal (MS/RS, E3, E2 and E1) received from the backplane back to its origin. The loop is done in the plug-in unit. An AIS is transmitted to the line interface.

Note: For loops in ATU (B), the ATU NPU and ATU MMU2 functions like plug-in units.

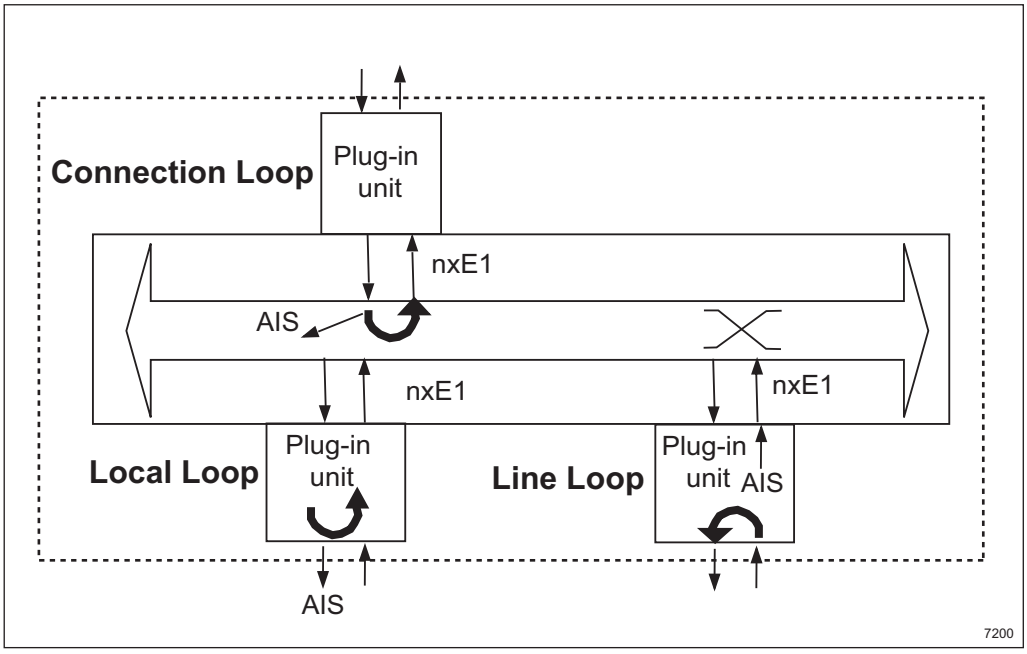


Figure 33 Loops

The following loops are supported for the Radio Terminal.

Note: Loops for Radio Terminals with MMU2 are mainly set using MSM

IF Loop In the MMU the traffic signal to be transmitted is, after being modulated, mixed with the frequency of a local oscillator and looped back for demodulation (on the receiving side).

RF Loop In the RAU a fraction of the RF signal transmitted is shifted in frequency and looped back to the receiving side.

Rx Loop This loop is similar to the Connection Loop but the loop is done in the plug-in unit close to the TDM bus, where a group of E1s in the traffic connection is looped back to its origin. The Rx Loop can be used to verify the communication over the radio path.

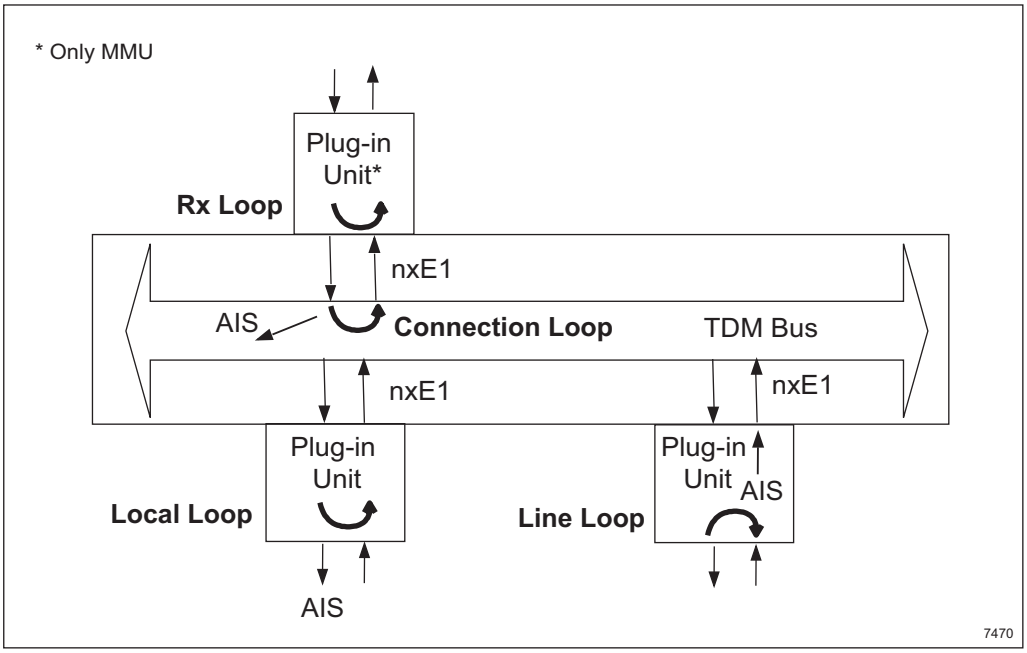


Figure 34 MMU2 B/C Rx Loop

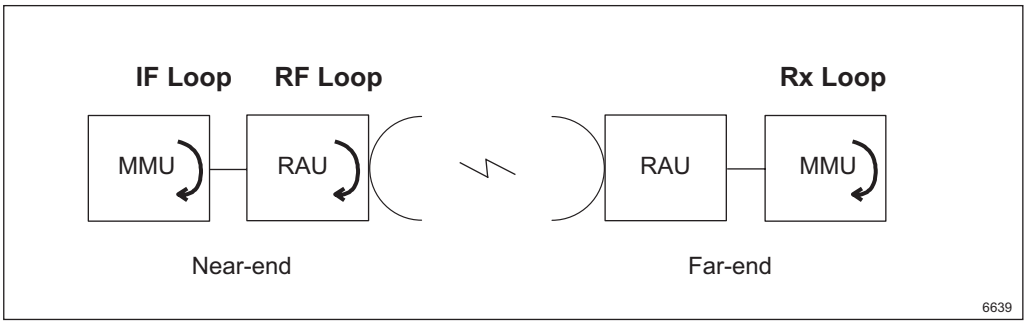


Figure 35 Radio Terminal loops

Section 7.4.2 on page 128 and Section 11.138 on page 357 give more information on how to set loops.

7.4.2 Setting a Loop on an Interface

This procedure describes how to set a loop on an interface in order to locate a fault.

Caution!

If the interface is used, the loop will disturb the traffic.

Note: An active loop will disable notifications from the interface.

To set a loop:

1. In the **Navigation Tree**, click the unit that contains the interface on which you want to set a loop.

   Note: A loop can also be set when the interface is selected in the Navigation Tree.

2. On the **Tools** menu, click **Loops**.

3. On the **Loops** page, in the **<IF type> Interface** list, select the interface on which you want to set a loop.

4. In the **Loop options** list, select loop type. See Table 22 on page 357 for a description of the loop types available for a specific interface.

5. Click **Add**. The loop is added to the **Active loops** list. The loop is removed by clicking **Remove** or **Remove All**.

Note: It is also possible to handle loops from the **Activities** page, see Section 11.136 on page 354.

7.5 Error Log Handling

The NE holds an Error Log containing information about internal hardware and software errors as well as restarts and equipment alarms. The Error Log comprises two files, `<hostname>_active.elog` and `<hostname>_passive.elog`.

Note: Evaluation of the Error Log requires deep knowledge about the system. Contact your Ericsson support for more information.

The following tasks are covered:

- *Uploading the Error Log to the FTP server*, see Section 7.5.1 on page 129.
- *Deleting the Error Log from the NE*, see Section 7.5.2 on page 130.

7.5.1 Uploading the Error Log to the FTP Server

Uploading the Error Log will load the `<hostname>_active.elog` and `<hostname>_passive.elog` files to the FTP server.

To upload the Error Log:

1. The Error Log will be uploaded to the `<drive:>\tn_ftp_home\tn_error_log` folder. To avoid overwriting an existing Error Log from the same NE, add the extension `.old` to the existing files, for example `<hostname>_active.elog.old`.

2. In the **Navigation Tree**, click the NE.
3. On the **Fault** menu, click **Load Error Log**.
4. Under **Error Log File**, select **Upload to FTP server**.
5. Under **FTP**, do one of the following:
   - If the Error Log should be stored on a remote FTP server, select **Remote server @ <IP address>**.
   - If the Error Log should be stored on the PC, select **Local server**. Specify **User Name** and **Password**.
6. Click **Apply**.

7.5.2 Deleting the Error Log from the NE

Deleting the Error Log will delete the `<hostname>_active.elog` file from the NE.

To delete the Error Log:

1. In the **Navigation Tree**, click the NE.
2. On the **Fault** menu, click **Load Error Log**.
3. Under **Error Log File**, select **Delete error log from Network Element**.
4. Click **Apply**.

8 Performance Management

This section contains instructions for typical performance management tasks.

The following tasks are covered:

- *Specifying the PM Start Time*, see Section 8.1 on page 131.
- *Viewing Performance Data*, see Section 8.2 on page 131.
- *Running a BERT on an E1 Interface*, see Section 8.3 on page 132.

8.1 Specifying the PM Start Time

This procedure describes how to specify the PM Start Time for 24 hours performance data error counting interval.

To specify the PM start time:

1. In the **Navigation Tree**, click the NE.
2. On the **Configuration** menu, click the **Basic NE** menu.
3. On the **Basic NE Configuration** page, under **General Settings**, type the **PM Start Time** (hh:mm where mm is 00, 15, 30 or 45).
4. Click **Apply**.

8.2 Viewing Performance Data

To be able to view performance data for interfaces, PM view must be enabled.

Note: Performance data (RF power) for the RF interface is always available, that is, you do not need to enable PM view.

To enable PM view:

1. In the **Navigation Tree**, click the interface for which you want to display performance data.
2. On the **Configuration** menu, click **Configuration**.
3. On the **Configuration** page for the interface, make sure **Enable PM View** is selected.
4. Click **Apply**.

Viewing Performance Data

To view performance data:

1. In the **Navigation Tree**, click the interface for which you want to display performance data.
2. Click the **Performance** menu.
3. The **Performance Data** page for the selected interface is displayed.

8.3 Running a BERT on an E1 Interface

This procedure describes how to run a Bit Error Ratio Test (BERT) on an E1 interface for performance measurement. The interface can be selected from the NE or any unit holding an E1 interface. A Pseudo Random Bit Sequence (PRBS) with test pattern $2^{15} – 1$ is sent on the selected interface.

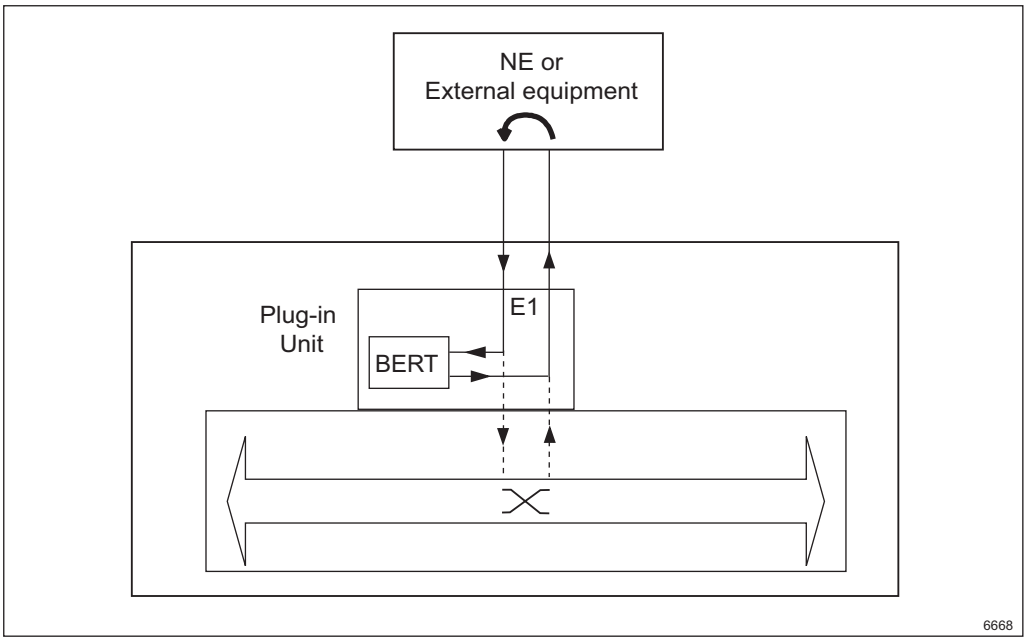


Figure 36 Bit Error Ratio Test (BERT)

Several BERTs can be executed concurrently with the following limitations:

- One BERT per plug-in unit
- One BERT on a protected 1+1 E1 SNCP interface per NE

Caution!

If the interface is used, the BERT will disturb the traffic.

To start a BERT:

1. In the **Navigation Tree**, click the unit that holds the E1 interface you want to test. Alternatively, click the NE name.
2. On the **Tools** menu, click **Test**.
3. On the **Test** page, under **Bit Error Ratio Test - BERT**, select the interface on which you want to run a BERT.
4. Click **Start Test**. The interface is added to the **Running Tests** list, indicating that the BERT is running on the interface.

To stop a BERT:

1. On the **Test** page, in the **Running Tests** list, locate the interface and then click **Stop Test**. The interface is removed from the **Running Tests** list and inserted in the **Previous Test Results** list, where the BER result and the elapsed time for the test is displayed.

Note: It is also possible to handle BERTs from the **Activities** page, see Section 11.136 on page 354.

9 Security Management

This section covers the following:

- *User Names*, see Section 9.1 on page 135.
- *Changing Passwords*, see Section 9.2 on page 136.
- *Replacing Lost Passwords*, see Section 9.3 on page 136.

9.1 User Names

Two user names are supported.

Figure 37 Logging in to the EEM

view_user

This user can only see the configuration. The default password is **`ericsson`**.

To prevent unauthorized access to the system it is recommended to change the password. This should be done during the initial setup, see Section 5.3 on page 54. However, the default password can always be used for local access of NPU2/NPU1 B.

control_user

This user can view and change the configuration. The default password is **`ericsson`**.

To prevent unauthorized access to the system it is recommended to change the password. This should be done during the initial setup, see Section 5.3 on page 54. However, the default password can always be used for local access of NPU2/NPU1 B and NPU 8x2 in Node/NPU Installation mode.

The control_user can change the passwords, see Section 9.2 on page 136.

9.2 Changing Passwords

This procedure describes how to change the control_user and view_user passwords when the NE is in Normal mode.

Note: Only the control_user is authorized to change the passwords.

To change the passwords:

1. In the **Navigation Tree**, click the NE.
2. On the **Security** menu, click **Security**
3. On the **Security** page there are two passwords to change:

To	Do this
Change the control_user password.	• Under **Set control_user**, in the **Password** box, type the new password. • Under **Set control_user**, in the **Confirm Password** box, repeat the new password.
Change the view_user password.	• Under **Set view_user**, in the **Password** box, type the new password. • Under **Set view_user**, in the **Confirm Password** box, repeat the new password.

4. Click **Apply**.

Note: You have to log in again if you have changed the control_user password.

9.3 Replacing Lost Passwords

Note: This section applies only to NPU 8x2. For an NPU2/NPU1 B, the control_user can always access the NE locally using the default password and change the passwords from the **Security** page, see Section 11.151 on page 380.

This procedure describes how to set new passwords in case the existing passwords have been lost.

Caution!

Use this function restrictively and only when you have lost the passwords to an already installed NE.

Note: The NE is accessed in Node Installation mode. Configure the PC to use a dynamic IP address obtained from the DHCP server in the NE or alternatively use the static IP address `10.0.0.2`. For more information on IP addressing, see Section 3.3.4 on page 32.

To set new passwords:

1. Switch off and switch on the power supply.

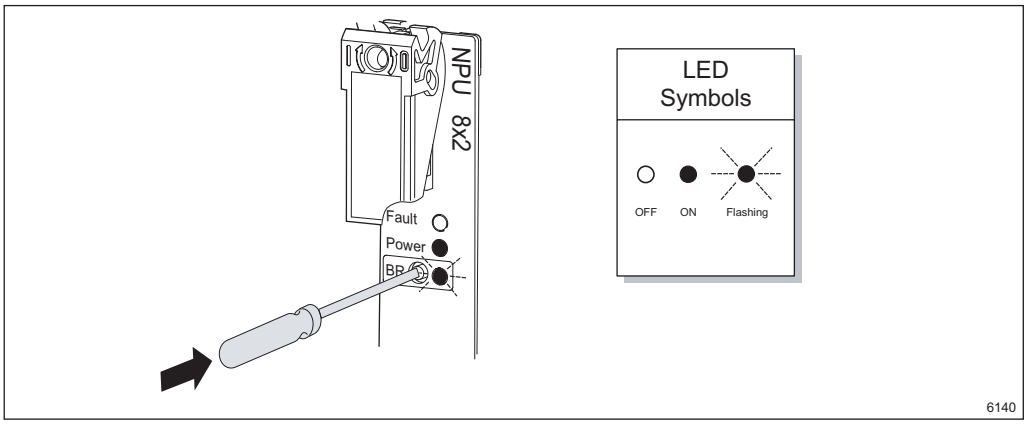


Figure 38 Entering Node Installation mode

2. While the Fault (red), Power (green) and BR (yellow) LEDs on the NPU 8x2 are ON (NE power up), press the BR button gently and release it. The BR (yellow) LED will start flashing, indicating that the NE is in Node Installation mode.

3. Connect the Ethernet cable (twisted pair) to the 10/100BASE-T port.

4. Start a Web browser and enter the URL **`http://10.0.0.1`**.

5. In the **Enter Network Password** dialog box, type the user name and password, and click **OK**. For more information see Section 9.1 on page 135.

6. On the **Tools** menu, click **Change Password**.

7. On the **Change Password** page, click **Configure Basic Security**.

8. On the **Security** page, there are two passwords to set:

To	Do this
Change the control_user password.	• Under **Set control_user**, in the **Password** box, type the new password. • Under **Set control_user**, in the **Confirm Password** box, repeat the new password.
Change the view_user password.	• Under **Set view_user**, in the **Password** box, type the new password. • Under **Set view_user**, in the **Confirm Password** box, repeat the new password.

9. Click **Apply** and then click **Next**.

10. On the **Change Password** page, click **Finish Installation**.

11. On the **Finish Installation** page, click **Apply**.

12. When the **Installation Finished** page is displayed the NE will make a warm restart and run in Normal mode.

13. Make sure the PC is properly configured regarding the use of DHCP server. The configuration defines if dynamic or static IP addressing is used. For information on how to configure the use of DHCP server, see Section 3.3.4 on page 32.

14. Find out the IP address of the NE, typically from the site documentation or the information plate of the NE. Start a Web browser and enter the URL **http://*<IP address>***.

Note: Installation mode can always be left by pressing the BR button on the front of the NPU 8x2.

10 Hardware Maintenance

This section describes hardware maintenance procedures.

Note: Follow the recommendations in *MINI-LINK TN ETSI Indoor Installation Manual* on troubleshooting and how to handle cables and plug-in units.

The following tasks are covered:

- *Adding Plug-in Units*, see Section 10.1 on page 140.
- *Replacing an LTU 16x2, LTU 12x2, LTU 155 or SMU2 (co-siting)*, see Section 10.2 on page 140.
- *Replacing an MMU2 or SMU2 (protection)*, see Section 10.3 on page 142.
- *Replacing an MMU2 B/C*, see Section 10.4 on page 143.
- *Replacing a PFU*, see Section 10.5 on page 145.
- *Replacing an NPU 8x2*, see Section 10.6 on page 147.
- *Replacing an NPU1 B*, see Section 10.7 on page 149.
- *Replacing an NPU2*, see Section 10.8 on page 151.
- *Replacing an ATU (B)*, see Section 10.9 on page 152.
- *Changing the Traffic Capacity of a Radio Terminal with MMU2*, see Section 10.10 on page 153.
- *Changing the Traffic Capacity of a Radio Terminal with MMU2 B/C*, see Section 10.11 on page 154.
- *Changing an Unprotected (1+0) Radio Terminal to a Protected (1+1) Radio Terminal with MMU2*, see Section 10.12 on page 154.
- *Changing an Unprotected (1+0) Radio Terminal to a Protected (1+1) Radio Terminal with MMU2 B/C*, see Section 10.13 on page 155.
- *Changing the Traffic Capacity of an SMU2 (co-siting)*, see Section 10.14 on page 156.

10.1 Adding Plug-in Units

Caution!

Electrostatic Discharge (ESD) may damage the equipment. Always use an approved antistatic bracelet to avoid damage to components fitted on printed circuit boards.

To add a new plug-in unit:

1. Remove the dummy unit.
2. Insert the new plug-in unit and fit the cables as described in *MINI-LINK TN ETSI Indoor Installation Manual*.
3. Configure the plug-in unit and its interfaces, see Section 6 on page 59.
4. On the applicable **Alarms and Status** page, make sure there are no active alarms.

10.2 Replacing an LTU 16x2, LTU 12x2, LTU 155 or SMU2 (co-siting)

This procedure describes how to replace an LTU 16x2, LTU 12x2, LTU 155 or SMU2 (co-siting).

Caution!

Electrostatic Discharge (ESD) may damage the equipment. Always use an approved antistatic bracelet to avoid damage to components fitted on printed circuit boards.

Note: When replacing an LTU 155 there is a check that the SW load module matches the current software release. If required, an automatic download of a new load module takes place. This requires a working connection to the FTP server and that the load module is present in the *<drive:>*\tn_ftp_home\tn_system_release folder.

Note: If an SMU2 has been used for protection it is recommended to do a preset to factory settings before using it for co-siting. For more information on how to do a preset, see *MSM User Guide* or *MSM online Help*.

To replace the plug-in unit:

1. Disconnect all cables from the plug-in unit.
2. Undo the two screws on the latches.

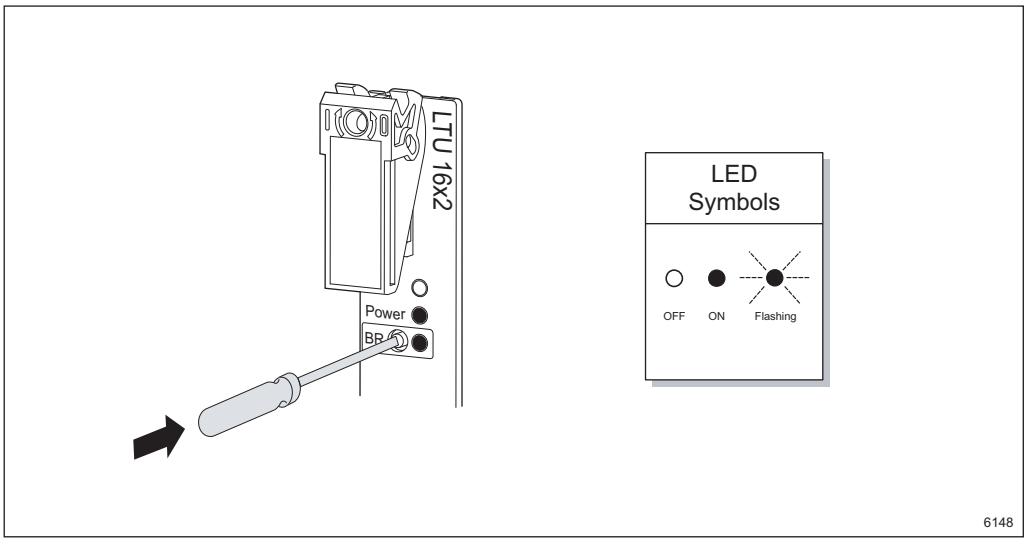


Figure 39 Pressing the BR button

3. Press the BR button gently and release it. This is a request to take the plug-in unit Out of Service and all traffic related alarms will be disabled.

   Note: The BR button should be pressed before the plug-in unit is removed, even if the Power (green) LED is OFF.

4. Wait until the BR (yellow) LED is ON and then remove the plug-in unit within 60 seconds. If the LED is not ON within 60 seconds, press and release the BR button again. Wait another 60 seconds and if the LED is still not ON, remove the unit anyway.
5. Insert the new plug-in unit within 15 minutes of removal. The plug-in unit will automatically be taken into service with the configuration used by the previous plug-in unit.

   Note: If the plug-in unit is not inserted within 15 minutes of removal, it has to be re-configured.

6. Tighten the two screws on the latches.
7. Connect all cables to the plug-in unit.
8. Start the LCT. For more information, see Section 3.3 on page 22.

9. In the **Navigation Tree**, click the plug-in unit type being replaced.

10. On the **Alarms and Status** page, make sure there are no active alarms.

10.3 Replacing an MMU2 or SMU2 (protection)

This procedure describes how to replace an MMU2, or an SMU2 used for protection in a (1+1) Radio Terminal.

Caution!

Electrostatic Discharge (ESD) may damage the equipment. Always use an approved antistatic bracelet to avoid damage to components fitted on printed circuit boards.

Note: To avoid transmission using the wrong frequency or output power it is recommended to insert an MMU2 with factory settings. If a preset to factory settings is required, use MSM with the unit inserted in an empty position in the AMM. MSM is launched from the **MMU2 Configuration** page, see Section 11.34 on page 196.

To replace the plug-in unit:

1. MMU2 only: Disconnect the station radio cable.

2. Undo the two screws on the latches.

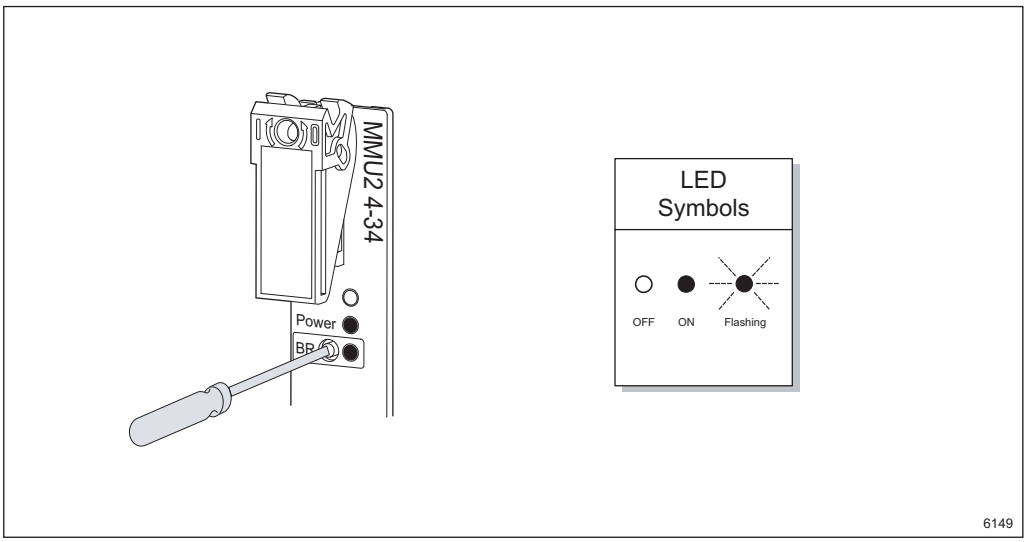


Figure 40 Pressing the BR button

3. Press the BR button gently and release it. This is a request to take the plug-in unit Out of Service and all traffic related alarms will be disabled.

   Note: The BR button should be pressed before the plug-in unit is removed, even if the Power (green) LED is OFF.

4. Wait until the BR (yellow) LED is ON and then remove the plug-in unit within 60 seconds. If the LED is not ON within 60 seconds, press and release the BR button again. Wait another 60 seconds and if the LED is still not ON, remove the unit anyway.

5. Insert the new plug-in unit within 15 minutes of removal. The plug-in unit will automatically be taken into service.

   Note: If the plug-in unit is not inserted within 15 minutes of removal, it has to be re-configured.

6. Tighten the two screws on the latches.

7. Connect the station radio cable.

8. Start the LCT. For more information, see Section 3.3 on page 22.

9. In the **Navigation Tree**, click the plug-in unit type being replaced.

10. On the **Configuration** menu, click **Configuration**.

11. On the **Configuration** page, click **Perform AM Setup and Hop Setup**.

12. In **MSM** perform a complete AM Setup and Hop Setup. Follow the instructions in *MSM User Guide* or *MSM online Help*.

13. In the **Navigation Tree**, click the plug-in unit being replaced.

14. On the **Alarms and Status** page, make sure there are no active alarms.

10.4 Replacing an MMU2 B/C

This procedure describes how to replace an MMU2 B or MMU2 C.

Caution!

Electrostatic Discharge (ESD) may damage the equipment. Always use an approved antistatic bracelet to avoid damage to components fitted on printed circuit boards.

Note: To avoid transmission using the wrong frequency or output power it is recommended to insert an MMU2 B/C with factory settings.

To replace the plug-in unit:

1. Disconnect the station radio cable.

2. Undo the two screws on the latches.

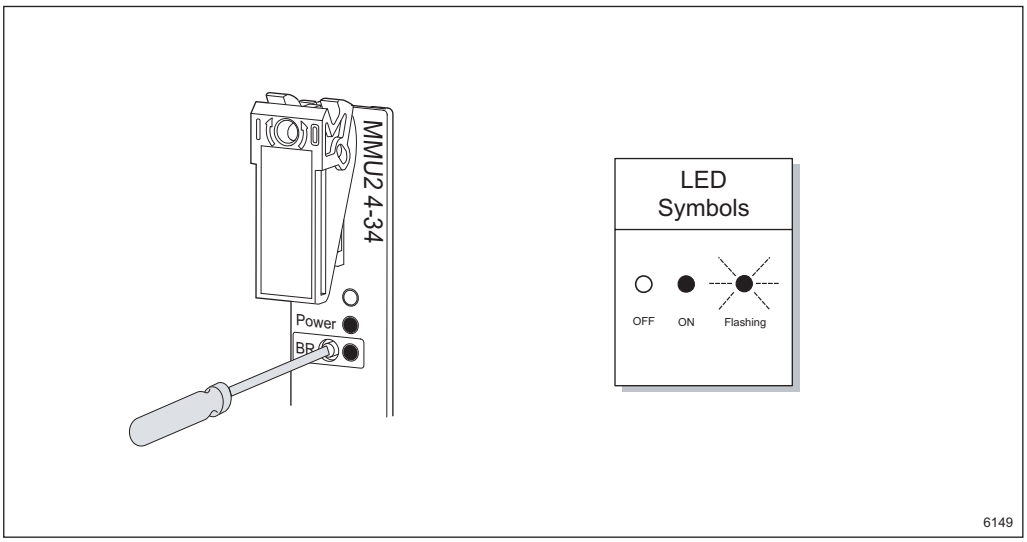


Figure 41 Pressing the BR button

3. Press the BR button gently and release it. This is a request to take the plug-in unit Out of Service and all traffic related alarms will be disabled.

   Note: The BR button should be pressed before the plug-in unit is removed, even if the Power (green) LED is OFF.

4. Wait until the BR (yellow) LED is ON and then remove the plug-in unit within 60 seconds. If the LED is not ON within 60 seconds, press and release the BR button again. Wait another 60 seconds and if the LED is still not ON, remove the unit anyway.

5. Insert the new plug-in unit within 15 minutes of removal. The plug-in unit will automatically be taken into service.

   Note: If the plug-in unit is not inserted within 15 minutes of removal, it has to be re-configured.

6. Tighten the two screws on the latches.

7. Connect the station radio cable.

8. Start the LCT. For more information, see Section 3.3 on page 22.

9. Do one of the following:

To:	See:
Configure an unprotected (1+0) Radio Terminal	Section 6.4.1 on page 63
Configure a protected (1+1) Radio Terminal	Section 6.4.2 on page 64

10. In the **Navigation Tree**, click the MMU being replaced.

11. On the **Alarms and Status** page, make sure there are no active alarms.

10.5 Replacing a PFU

This procedure describes how to replace a PFU1 (AMM 20p), PFU2 (AMM 6p) or PFU3 (AMM 6p B). PFU1 and PFU3 can be used in redundant power configurations.

Caution!

Electrostatic Discharge (ESD) may damage the equipment. Always use an approved antistatic bracelet to avoid damage to components fitted on printed circuit boards.

To replace the plug-in unit:

1. Undo the two screws on the latches.

2. Disconnect all cables from the plug-in unit.

Caution!

Make sure the external power is switched off when working with the DC cable.

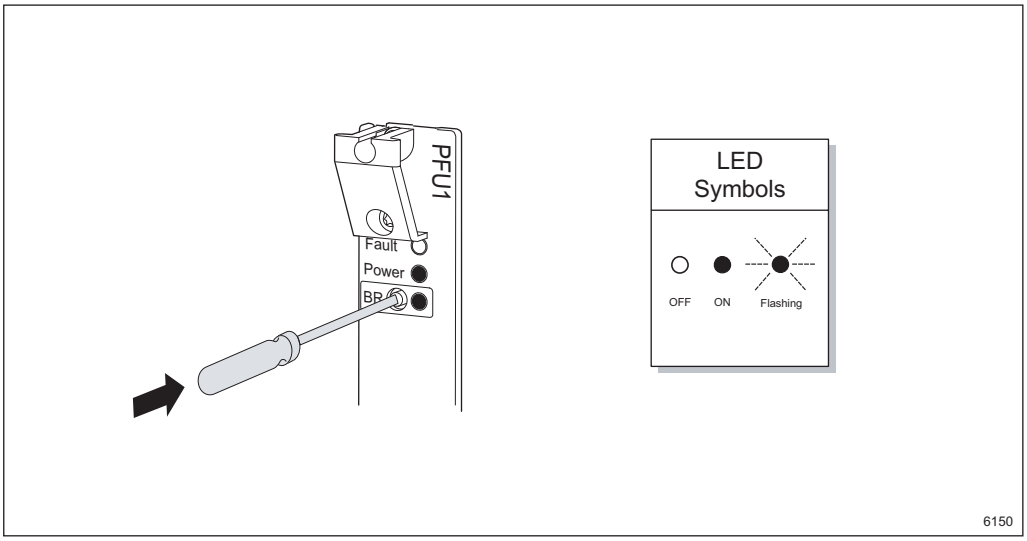


Figure 42 Pressing the BR button

3. Press the BR button gently and release it. This is a request to take the plug-in unit Out of Service and will suppress notifications from the PFU, including alarms from an FAU1 connected to a PFU1.

   Note: The BR button should be pressed before the plug-in unit is removed, even if the Power (green) LED is OFF.

4. Wait until the BR (yellow) LED is ON and then remove the plug-in unit within 60 seconds. If the LED is not ON within 60 seconds, press and release the BR button again. Wait another 60 seconds and if the LED is still not ON, remove the unit anyway.

   Note: A PFU failure could mean that the LEDs are not working.

5. Insert the new plug-in unit.

6. Tighten the two screws on the latches.

7. Connect all cables to the plug-in unit and switch on the external power supply.

   This will initiate a power up of the plug-in unit and for a non-redundant power configuration a power up of the NE.

8. Start the LCT. For more information, see Section 3.3 on page 22.

9. In the **Navigation Tree**, click the new PFU.

10. On the **PFU Alarms and Status** page, make sure there are no active alarms.

10.6 Replacing an NPU 8x2

The NPU 8x2, which holds the NE configuration data, can be replaced without disturbing all traffic not directly connected to the unit. The procedure is performed while the NE is running in NPU Installation mode, see also Section 3.3.2.1 on page 26.

Note: The NE is accessed in NPU Installation mode. Configure the PC to use a dynamic IP address obtained from the DHCP server in the NE or alternatively use the static IP address `10.0.0.2`. For more information on IP addressing, see Section 3.3.4 on page 32.

Caution!

Electrostatic Discharge (ESD) may damage the equipment. Always use an approved antistatic bracelet to avoid damage to components fitted on printed circuit boards.

To replace the NPU 8x2:

1. You need a backup configuration file on the FTP server on your PC. The configuration file must have the following path: `<drive:>\tn_ftp_home\tn_backup_configuration\<hostname.cfg>`. The file is typically fetched from the same directory on a remote FTP server.

   Note: If you do not have a configuration file you can, if possible, try to download the existing configuration file from the NE, see Section 11.87 on page 275.

   The final alternative is to make a complete setup of the NE, see Section 5 on page 49.

2. Disconnect all cables from the plug-in unit and undo the two screws on the latches.

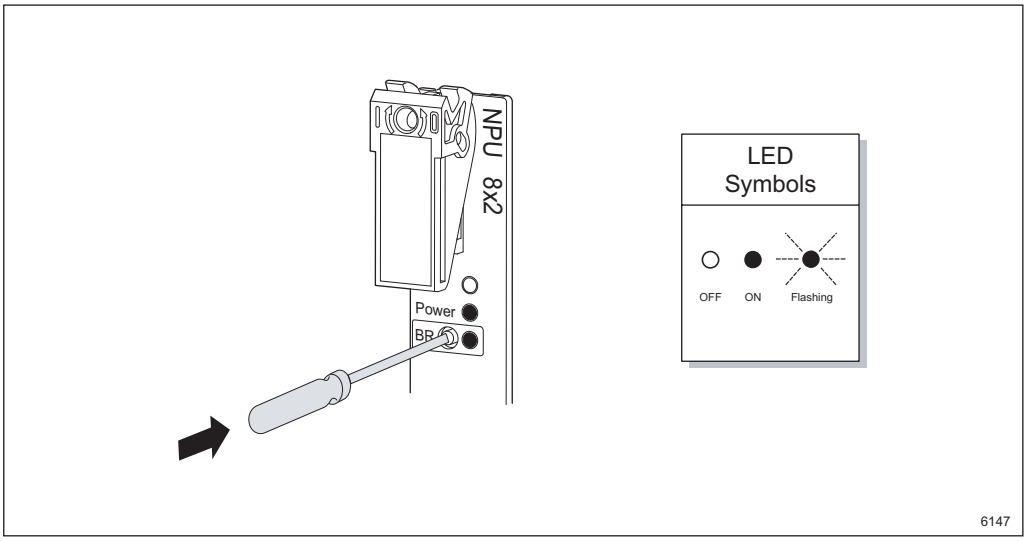


Figure 43 Pressing the BR button

3. Press the BR button gently and release it. This is a request to take the plug-in unit Out of Service and all traffic related alarms will be disabled.

   Note: The BR button should be pressed before the plug-in unit is removed, even if the Power (green) LED is OFF.

4. Wait until the BR (yellow) LED is ON and then remove the plug-in unit within 60 seconds. If the LED is not ON within 60 seconds, press and release the BR button again. Wait another 60 seconds and if the LED is still not ON, remove the unit anyway.

5. Insert the new NPU 8x2. Press and release the BR button while the Fault (red), Power (green) and BR (yellow) LEDs are ON (NPU power up). The BR (yellow) LED will start flashing, indicating that the NE is in NPU Installation mode.

6. Tighten the two screws on the latches.

7. Connect all cables, including the Ethernet cable (twisted pair) to the 10/100BASE-T port.

8. Start a Web browser and enter the URL `http://10.0.0.1`.

9. In the **Enter Network Password** dialog box, type the user name and password, and click **OK**. For more information see Section 9.1 on page 135.

10. On the **Restore NPU Configuration** page, click **Download Configuration File**.

11. On the **Load Configuration** page, type the name of the configuration file in the **File Name** box and then click **Apply**.

12. On the **Load Configuration Progress** page, click **Update Progress** until the download is finished. If the configuration file requires new software to be loaded, this will be done automatically. This requires that the software is present in the `<drive:>\tn_ftp_home\tn_system_release` folder.

    A progress bar displays the progress of the software upgrade. When the download and software upgrade is finished, the NE will make a warm restart. After the restart the NE will run in Normal mode with the correct configuration.

13. Enter the URL **`http://<IP address>`** where IP address is typically found in the site documentation or on the information plate of the NE. See also Section 3.3.2.3 on page 29.

14. In the **Navigation Tree**, click the NPU 8x2.

15. On the **NPU 8x2 Alarms and Status** page, make sure there are no active alarms.

10.7 Replacing an NPU1 B

The NPU1 B, which holds the NE configuration data, can be replaced without disturbing all traffic not directly connected to the unit.

Caution!

Electrostatic Discharge (ESD) may damage the equipment. Always use an approved antistatic bracelet to avoid damage to components fitted on printed circuit boards.

To replace the NPU1 B:

1. You need a backup configuration file on the FTP server on your PC. The configuration file must have the following path: `<drive:>\tn_ftp_home\tn_backup_configuration\<hostname.cfg>`. The file is typically fetched from the same directory on a remote FTP server.

   Note: If you do not have a configuration file you can, if possible, try to download the existing configuration file from the NE, see Section 11.87 on page 275.

   The final alternative is to make a complete setup of the NE, see Section 5 on page 49.

2. Disconnect all cables from the plug-in unit and undo the two screws on the latches.

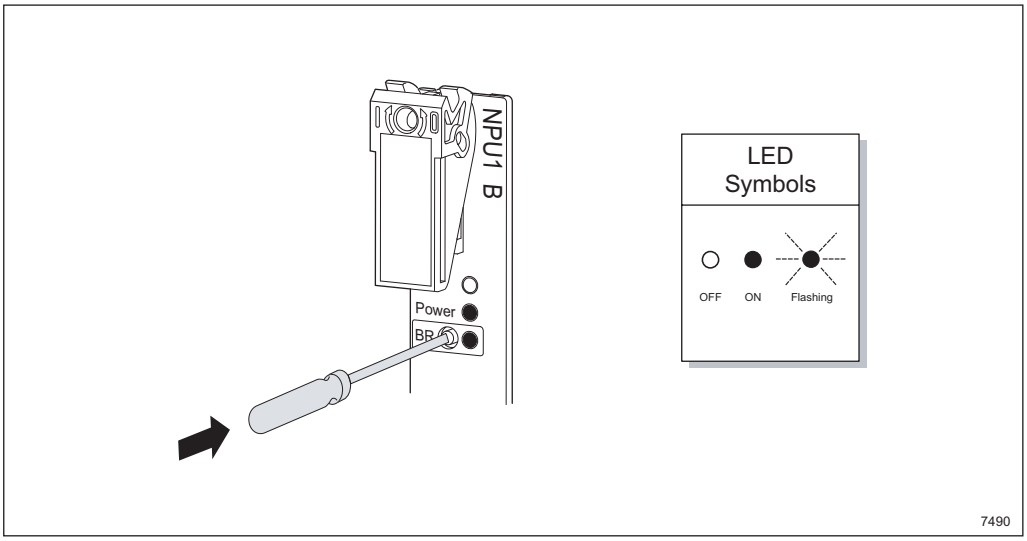


Figure 44 Pressing the BR button

3. Press the BR button gently and release it. This is a request to take the plug-in unit Out of Service and all traffic related alarms will be disabled.

   Note: The BR button should be pressed before the plug-in unit is removed, even if the Power (green) LED is OFF.

4. Wait until the BR (yellow) LED is ON and then remove the plug-in unit within 60 seconds. If the LED is not ON within 60 seconds, press and release the BR button again. Wait another 60 seconds and if the LED is still not ON, remove the unit anyway.

5. Insert the new NPU1 B. Press and release the BR button while the Fault (red), Power (green) and BR (yellow) LEDs are ON (NPU power up). The BR (yellow) LED will start flashing, indicating that the NE is in NPU Installation mode.

6. Tighten the two screws on the latches.

7. Connect all cables, including the USB cable.

8. Start a Web browser and enter the URL `http://10.0.0.1`.

9. In the **Enter Network Password** dialog box, type the user name and password, and click **OK**. For more information see Section 9.1 on page 135.

10. On the **Restore NPU Configuration** page, click **Download Configuration File**.

11. On the **Load Configuration** page, type the name of the configuration file in the **File Name** box and then click **Apply**.

12. On the **Load Configuration Progress** page, click **Update Progress** until the download is finished. If the configuration file requires new software to be loaded, this will be done automatically. This requires that the software is present in the `<drive:>\tn_ftp_home\tn_system_release` folder.

    A progress bar displays the progress of the software upgrade. When the download and software upgrade is finished, the NE will make a warm restart. After the restart the NE will run in Normal mode with the correct configuration.

13. In the **Navigation Tree**, click the NPU1 B.

14. On the **NPU1 B Alarms and Status** page, make sure there are no active alarms.

10.8 Replacing an NPU2

The NPU2 supplies the other units in the AMM with power so the NE will be down when replacing the NPU2. All cables and units should be handled according to instructions in the *MINI-LINK TN ETSI Installation Manual*.

Caution!

Make sure the external power is switched off when working with the DC cable.

To replace the NPU2:

1. You need a backup configuration file on the FTP server on your PC. The configuration file must have the following path: `<drive:>\tn_ftp_home\tn_backup_configuration\<hostname.cfg>`. The file is typically fetched from the same directory on a remote FTP server.

   Note: If you do not have a configuration file you can, if possible, try to download the existing configuration file from the NE, see Section 11.87 on page 275.

2. Switch off the external power.

3. Disconnect all cables from the NPU2 and undo the two screws on the latches.

4. Remove the old unit, insert the new one and tighten the two screws on the latches.

5. Connect all cables to the unit, including the USB cable between the unit and the PC.

6. Switch on the external power.

7. Press and release the BR button gently during power up. The BR (yellow) LED will start flashing, indicating that the NE is in NPU Installation mode.

8. Start a Web browser and enter the URL **`http://10.0.0.1`**.

9. In the **Enter Network Password** dialog box, type the user name and password, and click **OK**. For more information see Section 9.1 on page 135.

10. On the **Restore NPU Configuration** page, click **Download Configuration File**.

11. On the **Load Configuration** page, type the name of the configuration file in the **File Name** box and then click **Apply**.

12. On the **Load Configuration Progress** page, click **Update Progress** until the download is finished. If the configuration file requires new software to be loaded, this will be done automatically. This requires that the software is present in the *<drive:>*`\tn_ftp_home\tn_system_release` folder.

    A progress bar displays the progress of the software upgrade. When the download and software upgrade is finished, the NE will make a warm restart. After the restart the NE will run in Normal mode with the correct configuration.

13. In the **Navigation Tree**, click the NPU2.

14. On the **NPU2 Alarms and Status** page, make sure there are no active alarms.

10.9 Replacing an ATU (B)

All cables and units should be handled according to instructions in the *ATU Installation Instruction*.

Caution!

Make sure the external power is switched off when working with the DC cable.

To replace the ATU (B):

1. You need a backup configuration file on the FTP server on your PC. The configuration file must have the following path: *<drive:>*`\tn_ftp_home\tn_backup_configuration\`*<hostname.cfg>*. The file is typically fetched from the same directory on a remote FTP server.

   Note: If you do not have a configuration file you can, if possible, try to download the existing configuration file from the NE, see Section 11.87 on page 275.

2. Switch off the external power.

3. Disconnect all cables from the ATU (B) and undo the four screws that fits the unit to the rack.

4. Remove the old unit, insert the new one and tighten the four screws.

5. Connect all cables to the unit, including the USB cable between the unit and the PC.

6. Switch on the external power.

7. Start a Web browser and enter the URL **`http://10.0.0.1`**.

8. In the **Enter Network Password** dialog box, type the user name and password, and click **OK**. For more information see Section 9.1 on page 135.

9. On the **Configuration** menu, click **Load Configuration**.

10. On the **Load Configuration** page, type the name of the configuration file in the **File Name** box and then click **Apply**.

11. On the **Load Configuration Progress** page, click **Update Progress** until the download is finished. If the configuration file requires new software to be loaded, this will be done automatically. This requires that the software is present in the `<drive:>\tn_ftp_home\tn_system_release` folder.

    A progress bar displays the progress of the software upgrade. When the download and software upgrade is finished, the NE will make a warm restart. After the restart the NE will run in Normal mode with the correct configuration.

12. In the **Navigation Tree**, click the ATU NPU.

13. On the **ATU NPU Alarms and Status** page, make sure there are no active alarms.

14. Configure the ATU MMU2 as described in Section 6.4.3 on page 66.

10.10 Changing the Traffic Capacity of a Radio Terminal with MMU2

This procedure describes how to change the traffic capacity of an unprotected (1+0) or protected (1+1) Radio Terminal.

To change the traffic capacity:

1. Delete the existing traffic routings for E1s. Follow the instructions in Section 6.8.2 on page 81.

2. In the **Navigation Tree**, select an MMU2 in the terminal.

3. On the **MMU2 Configuration** page, click **Perform AM Setup and Hop Setup**. In MSM, perform AM Setup and Hop Setup to change the traffic capacity. Follow the instructions in *MSM User Guide* or *MSM online Help*.

4. Create new traffic routings for E1s. Follow the instructions in Section 6.8.1 on page 79.

5. On the **MMU2 Alarms and Status** page, make sure there are no active alarms.

10.11 Changing the Traffic Capacity of a Radio Terminal with MMU2 B/C

This procedure describes how to change the traffic capacity of an unprotected (1+0) or protected (1+1) Radio Terminal.

To change the traffic capacity:

1. In the **Navigation Tree**, select an MMU2 B/C in the terminal.

2. Click the **Configuration** menu to open the **MMU2 B/C Configuration** page.

3. Under **Traffic Capacity**, change the traffic capacity.

4. Click **Apply**.

5. On the **MMU2 Alarms and Status** page, make sure there are no active alarms.

10.12 Changing an 1+0 Radio Terminal to a 1+1 Radio Terminal with MMU2

This procedure describes how to change an unprotected (1+0) Radio Terminal to a protected (1+1) Radio Terminal.

1. Insert the new MMU2 and SMU2, see Section 10.1 on page 140.

   Note: The 1+1 configuration is only possible if the units are placed in adjacent AMM positions according to specifications in *MINI-LINK TN ETSI Indoor Installation Manual*.

2. Delete the existing traffic routings for E1s. Follow the instructions in Section 6.8.2 on page 81.

3. In the **Navigation Tree**, click the SMU2. On the **SMU2 Configuration** page, select **Protection** and click **Apply**.

4. In the **Navigation Tree**, click one of the MMU2s in the protected terminal.

5. On the **MMU2 Configuration** page, under **Protection Mode**, select **Prepare for 1+1 configuration**.

6. Click **Apply**.

7. Select **In Service** and clear the **Enable** check box, for all three units, and click **Apply**.

8. Click **Perform AM Setup and Hop Setup**. In MSM, perform AM Setup and Hop Setup. Follow the instructions in *MSM User Guide* or *MSM online Help*.

9. Carry out the outdoor equipment installation, indoor and outdoor radio cabling, and antenna alignment. Follow the instructions in *MINI-LINK TN ETSI Indoor Installation Manual* and *MINI-LINK TN, MINI-LINK HC, MINI-LINK E Outdoor Installation Manual*.

10. Configure the applicable interfaces:
    - E3 Interface, see Section 11.49 on page 222.
    - E2 Interface, see Section 11.50 on page 223.
    - Single E1 Interface, see Section 11.51 on page 224.
    - All E1 Interfaces, see Section 11.52 on page 225.

11. Create new traffic routings for E1s. Follow the instructions in Section 6.8.1 on page 79.

12. In the **Navigation Tree**, click one of the MMU2s in the protected terminal.

13. On the **MMU2 Configuration** page, select the **Enable** check box.

14. On one of the **MMU2 Alarms and Status** pages, make sure there are no active alarms.

10.13 Changing an 1+0 Radio Terminal to a 1+1 Radio Terminal with MMU2 B/C

This procedure describes how to change an unprotected (1+0) Radio Terminal to a protected (1+1) Radio Terminal.

Note: 1+1 configurations are only possible if the units are placed in adjacent AMM positions according to specifications in *MINI-LINK TN ETSI Indoor Installation Manual*.

1. Insert the new MMU2 B/C, see Section 10.1 on page 140..

2. Using the new MMU, configure a temporary unprotected (1+0) Radio Terminal, as described in Section 6.4.1 on page 63.

   Note: Do not turn on the transmitter when creating the temporary terminal.

   Note: To be able to configure a protected terminal, the following conditions apply:

   - The temporary terminal must be configured to use the same traffic capacity, modulation method, and identity as the existing terminal.
   - For 1+1 Hot configurations, both RAUs must have *the same* frequency.
   - For 1+1 Work configurations, both RAUs must have *different* frequencies.

3. When the temporary terminal is set up, configure a protected terminal as described in Section 6.4.2 on page 64.

4. In the **Navigation Tree**, click one of the MMUs in the protected terminal.

5. On the **Alarms and Status** page, make sure there are no active alarms.

10.14 Changing the Traffic Capacity of an SMU2 (co-siting)

The traffic capacity of an SMU2 in co-siting mode interfacing MINI-LINK E equipment is changed as described below.

To change the traffic capacity:

1. Delete the existing traffic routings for E1s. Follow the instructions in Section 6.8.2 on page 81 .

2. In the **Navigation Tree**, click the SMU2.

3. Click the **Configuration** menu.

4. On the **SMU2 Configuration** page, under **Traffic Capacity**, select the new traffic capacity and click **Apply**.

5. Create new traffic routings for E1s. Follow the instructions in Section 6.8.1 on page 79.

6. On the **SMU2 Alarms and Status**, make sure there are no active alarms.

11 User Interface Reference

This section gives information on all items available on the different pages displayed when working with the EEM. Each page is described in a separate section and the information is accessed from the EEM by clicking **Help**.

Note: Each figure in this section reflects a certain setting of the equipment. This means that some of the objects described in the text are not present in the figures.

11.1 Radio Terminal Configuration

This page provides a guided setup for configuration of Radio Terminals during the initial setup. At least the terminals used for DCN communication must be set up at this stage.

Figure 45 The Radio Terminal Configuration page

- **Factory Setting** — Opens the **Factory Setting** page, where you can revert the NE to factory settings, see Section 11.11 on page 168. Only available if there is an existing configuration file.
- **To set up Radio Terminals** — A list of Radio Terminal units (MMU2 and SMU2) that can be configured. Clicking a link opens the unit's configuration page. When the necessary Radio Terminals have been configured you continue with **Automatic Configuration**, see Section 5.2 on page 53, or **Manual Configuration**, see Section 5.3 on page 54.
- **Back** — Navigates one step backward in the installation wizard.

  Note: Configurations that you have performed are not reversed.

- **Next** — Navigates one step forward in the installation wizard.

See Also

- Initial setup of a Radio Terminal, see Section 5.1 on page 49.

11.2 Automatic Configuration

This page provides a guided setup to configure the NE using a configuration file. This includes configuration security, DCN and system parameters. Depending on the contents of the configuration file this could be a complete configuration excluding the parts configured with MSM.

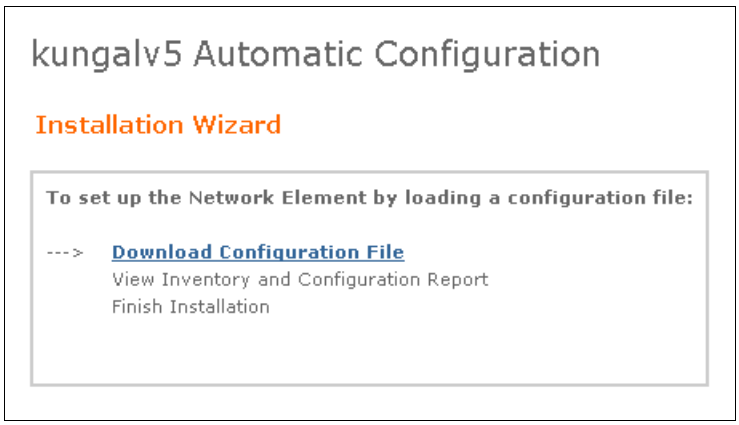


Figure 46 The Automatic Configuration page

- **Download Configuration File** — Opens the **Load Configuration** page, where you can download a configuration file from the default FTP server, see Section 11.87 on page 275. The default FTP server located on the PC with IP address `10.0.0.2`. After the download an automatic software upgrade is performed if necessary.
- **View Inventory and Configuration Report** — Opens the **View Report** page, where inventory and configuration information is displayed, see Section 11.75 on page 258.
- **Finish Installation** — Opens the **Finish Installation** page, see Section 11.6 on page 163.
- **Back** — Navigates one step backward in the installation wizard.

  Note: Configurations that you have performed are not reversed.

See Also

- Automatic configuration of NE parameters, see Section 5.2 on page 53.

11.3 Manual Configuration

This page provides a guided setup to configure the NE without using a configuration file.

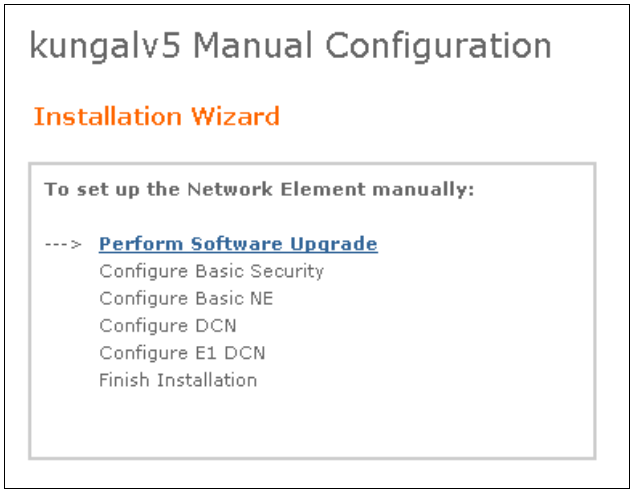


Figure 47 The Manual Configuration page

- **Perform Software Upgrade** — Opens the **Software Upgrade – Installation Wizard** page, where an upgrade to a new baseline can be performed, see Section 11.4 on page 161. The default FTP server is located on the PC with IP address `10.0.0.2`.
- **Configure Basic Security** — Opens the **Security** page, where passwords for the control_user and view_user are set, see Section 11.151 on page 380.
- **Configure Basic NE** — Opens the **Basic NE Configuration** page, where general NE parameters are set, see Section 11.15 on page 172.
- **Configure DCN** — Opens the **Ethernet/LAN/Servers page** page, where parameters for Ethernet communication and DCN servers are set, see Section 11.16 on page 174. Other pages for DCN configuration are also opened from this page.
- **Configure E1 DCN** — Opens the **E1 DCN Configuration** page, where an E1 interface can be selected to carry DCN traffic, see Section 11.5 on page 162.
- **Finish Installation** — Opens the **Finish Installation** page, see Section 11.6 on page 163.
- **Back** — Navigates one step backward in the installation wizard.

  Note: Configurations that you have performed are not reversed.

See Also

- Manual configuration of NE parameters, see Section 5.3 on page 54.

11.4 Software Upgrade – Installation Wizard

This page is used to perform an upgrade of baseline in the installation wizard. The baseline is described in a Software Baseline Description File (SBDF).

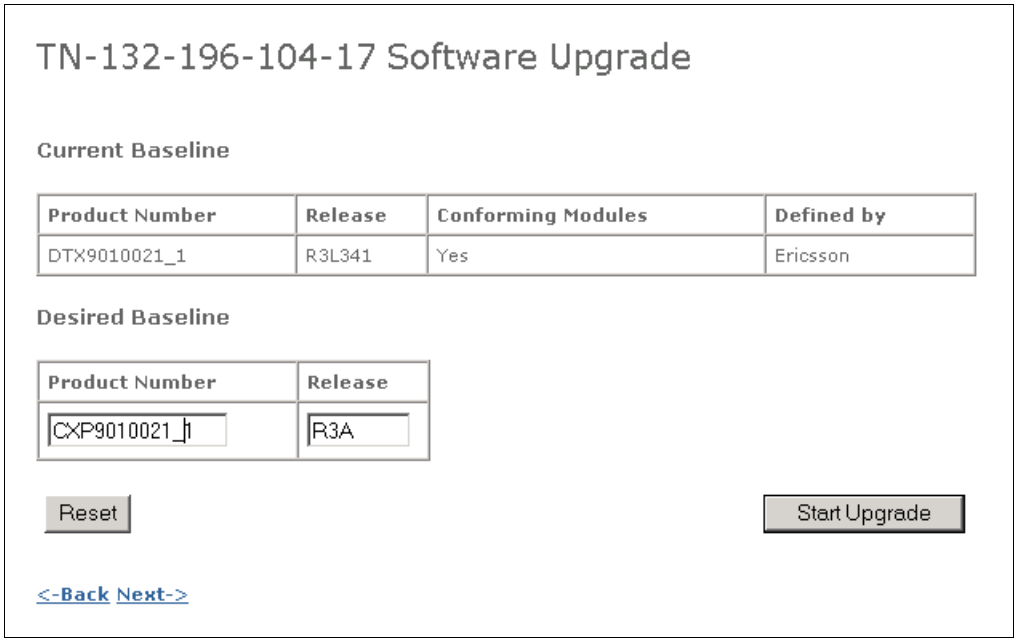


Figure 48 The Software Upgrade – Installation Wizard page

- **Current Baseline** — Information about the current baseline. If version control is disabled, N/A will be displayed.
  - **Product Number** — The product number of the current baseline.
  - **Release** — The release state (version) of the current baseline.
  - **Conforming Modules** — Displays if the current software configuration is compliant with the current baseline.
  - **Defined by** — Displays if the baseline is defined by Ericsson or not.
- **Desired Baseline** — Information about the desired baseline.

  Note: The SBDF and the load modules must be stored in specific folders under: `<drive:>\tn_ftp_home\tn_system_release\ml_tn_software`, see Section 3.2.1.2 on page 18.

  - **Product Number** — The product number of the desired baseline.
  - **Release** — The release state (version) of the desired baseline.
- **Reset** — Resets all settings to their initial values.
- **Start Upgrade** — Initiates the software upgrade.
- **Back** — Navigates one step backward in the installation wizard.
- **Next** — Navigates one step forward in the installation wizard.

11.5 E1 DCN Configuration

This page is used to select an E1 interface to carry DCN traffic, for an NPU 8x2/NPU1 B NE. When an E1 interface is selected the page displays the selected interface and enables a reselection.

Figure 49 The E1 DCN Configuration page, before and after an E1 is selected

- **Select an E1 to enable DCN** — For selection of the E1 interface to carry DCN traffic.
- **Apply** — Applies the selected E1 interface.
- **E1 with DCN enabled** — Displays the selected E1 interface.
- **Disable DCN** — Disables the DCN traffic on the selected E1 interface and enables a selection of a new E1 interface.
- **Back** — Navigates one step backward in the installation wizard.

  Note: Configurations that you have performed are not reversed.

- **Next** — Navigates one step forward in the installation wizard.

11.6 Finish Installation

This page is used to save the configuration in the installation wizard.

Figure 50 The Finish Installation page

- **OK** — Saves the configuration and exits the installation wizard.
- **Back** — Navigates one step backward in the installation wizard.

11.7 Installation Finished

This page is displayed when an NPU 8x2 NE is making a warm restart after leaving Node Installation mode. After the restart it will run in Normal mode. The IP address of the NE has been changed and you will have to use this address when you access the NE, see also Section 3.3.2.3 on page 29.

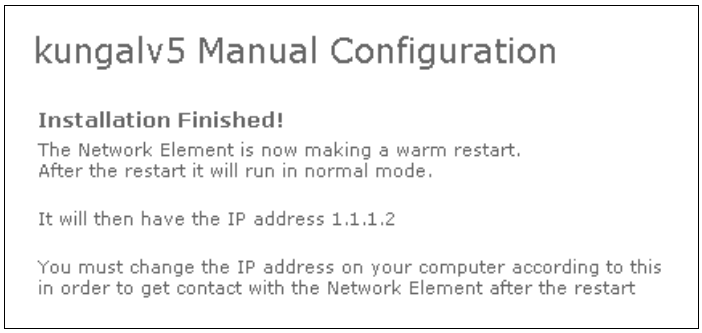


Figure 51 The Installation Finished page

11.8 Change Password

This page provides a guided setup to change the password for the control_user and view_user.

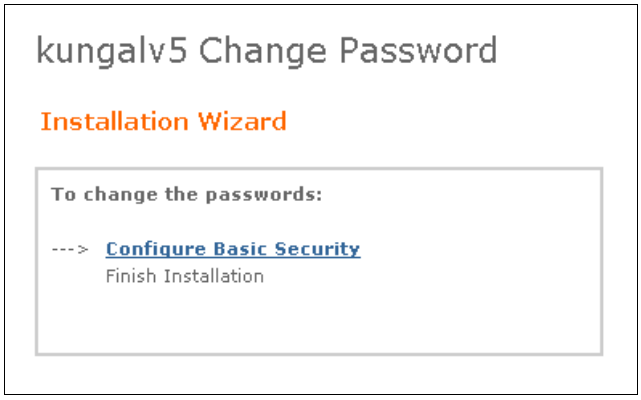


Figure 52 The Change Password page

Caution!

Use this function restrictively and only when you have lost the passwords to an already installed NE.

- **Configure Basic Security** — Opens the **Security** page, where passwords for the control_user and view_user are set, see Section 11.151 on page 380.
- **Finish Installation** — Opens the **Finish Installation** page, see Section 11.6 on page 163.
- **Back** — Navigates one step backward in the installation wizard.

  Note: Configurations that you have performed are not reversed.

See Also

- How to replace lost passwords on NPU 8x2, see Section 9.3 on page 136.

11.9 Emergency Fallback

This page provides a guided setup to activate the previous NPU software release.

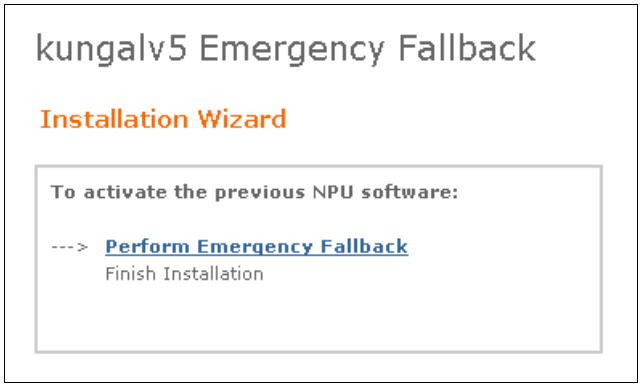


Figure 53 The Emergency Fallback page

- **Perform Emergency Fallback** — Opens the **Perform Emergency Fallback** page, see Section 11.10 on page 167.
- **Finish Installation** — Opens the **Finish Installation** page, see Section 11.6 on page 163.
- **Back** — Navigates one step backward in the installation wizard.

Note: Configurations that you have performed are not reversed.

See Also

- How to perform an emergency fallback for NPU2/NPU1 B, see Section 6.12.3 on page 95.
- How to perform an emergency fallback for NPU 8x2, see Section 6.12.4 on page 96.

11.10 Perform Emergency Fallback

This page is used to activate the previous NPU software release.

Figure 54 The Perform Emergency Fallback page

Caution!

Use this function restrictively and only in the unlikely event that you have performed a software upgrade to a software version, from which you cannot perform a full software upgrade back to a correct version.

- **OK** — Activates the previous NPU software.
- **Back** — Navigates one step backward in the installation wizard.

11.11 Factory Setting

This page provides a link to the **Delete Configuration File** page, used to delete an existing configuration file and revert the NE to factory setting, see Section 11.12 on page 169.

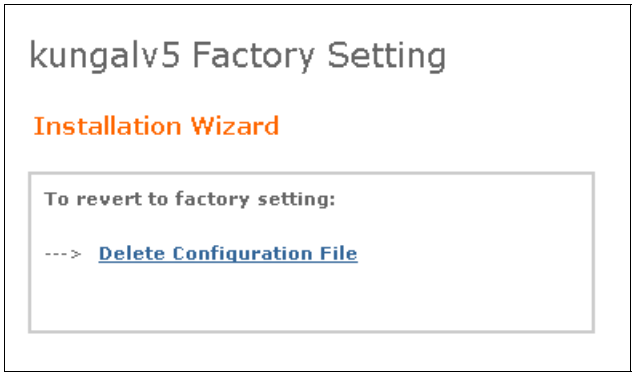


Figure 55 The Factory Setting page

11.12 Delete Configuration File

This page is used to delete an existing configuration file and revert the NE to factory setting.

Figure 56 The Delete Configuration File page

- **Apply** — Deletes the existing configuration file and opens the **Configuration File Deleted** page, see Section 11.13 on page 170. Only available if there is an existing configuration file.
- **Back** — Returns to the **Factory Setting** page, see Section 11.11 on page 168.

11.13 Configuration File Deleted

This page is displayed when a NE is restarting after a configuration file has been deleted.

Figure 57 The Configuration File Deleted page

11.14 Restore NPU Configuration

This page provides a guide to restore the NE configuration, residing on the NPU.

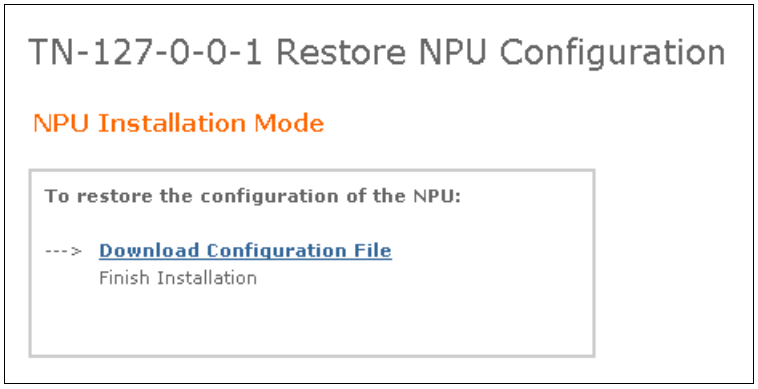


Figure 58 The Restore NPU Configuration page

- **Download Configuration File** — Opens the **Load Configuration** page, where you can download a configuration file from the default FTP server, see Section 11.87 on page 275. The default FTP server is located on the PC with IP address `10.0.0.2`. After the download an automatic software upgrade is performed if necessary.
- **Finish Installation** — Opens the **Finish Installation** page, see Section 11.6 on page 163.
- **Back** — Navigates one step backward in the installation wizard.

11.15 Basic NE Configuration

This page is used to set general NE parameters. It also allows configuration of the desired status of PFU/FAU.

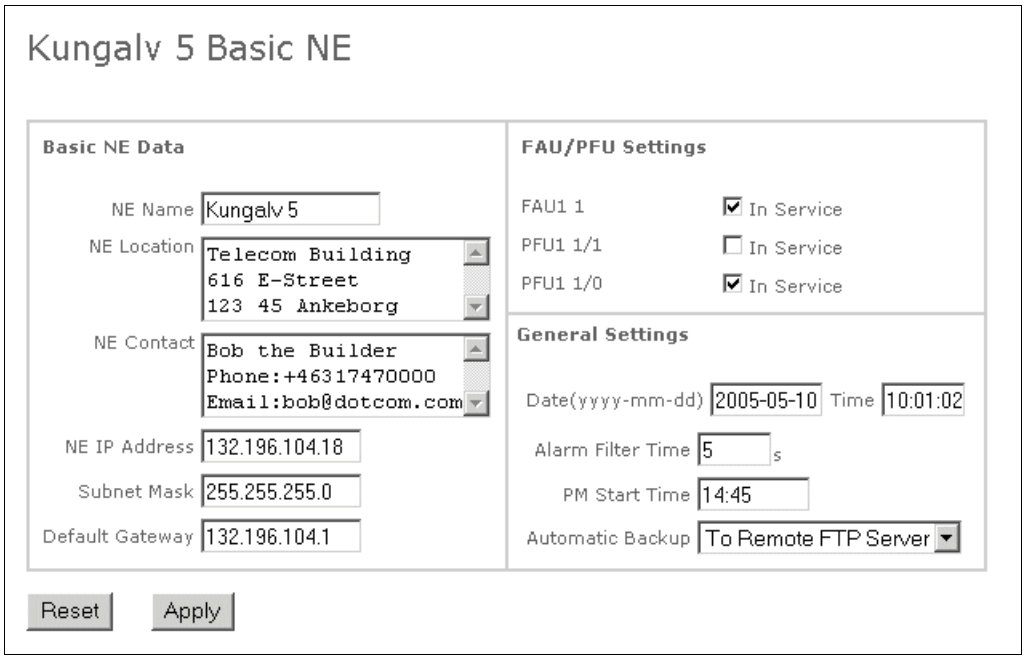


Figure 59 The Basic NE Configuration page

- **Basic NE Data** — Specifies general information about the NE.
  - **NE Name** — The name of the NE.
  - **NE Location** — The physical location of the NE.
  - **NE Contact** — Contact information such as name and telephone number of the system responsible person.
  - **NE IP Address** — The IP address of the NE, that is the internal router.
  - **Subnet Mask** — The subnet mask of the NE.
  - **Default Gateway** — Settings for the default gateway. Packets with unknown destination are sent to this IP address.
- **FAU/PFU Settings** — Specifies the desired status of the FAU and PFUs (AMM 20p/AMM 6p B only). At least one PFU must be In Service in case of redundant PFU.
  - **In Service** — Sets the unit in operating mode.
  - **Out of Service** — Sets the unit in non-operating mode. The unit is regarded as not present and will not be presented in the Navigation Tree, for example.
- **General Settings** — Specifies miscellaneous parameters of the NE.
  - **Date/Time** — The date (yyyy-mm-dd) and time (hh:mm) kept by the NE timer.

    Note: When an NTP server is available, this will adjust the NE date and time.

  - **Alarm Filter Time** — The time between the occurrence of a defect and the sending of an alarm. This applies also for sending a clear alarm when the defect ceases. The time can be set in the range 1.0 – 10.0 s, in steps of 0.5.
  - **PM Start Time** — The time when 24 hour performance interval starts. The time can be set in the range 00:00 – 23:45, in steps of 15 minutes.
  - **Automatic Backup** — Specifies that a backup of the configuration will be done each time the NE configuration is saved. The backup is saved on the specified FTP server.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.
- **Back** — Navigates one step backward in the installation wizard.

  Note: Configurations that you have performed are not reversed.

- **Next** — Navigates one step forward in the installation wizard.

11.16 Ethernet/LAN/Servers Configuration

This page is used to set parameters for Ethernet/LAN communication and DCN servers.

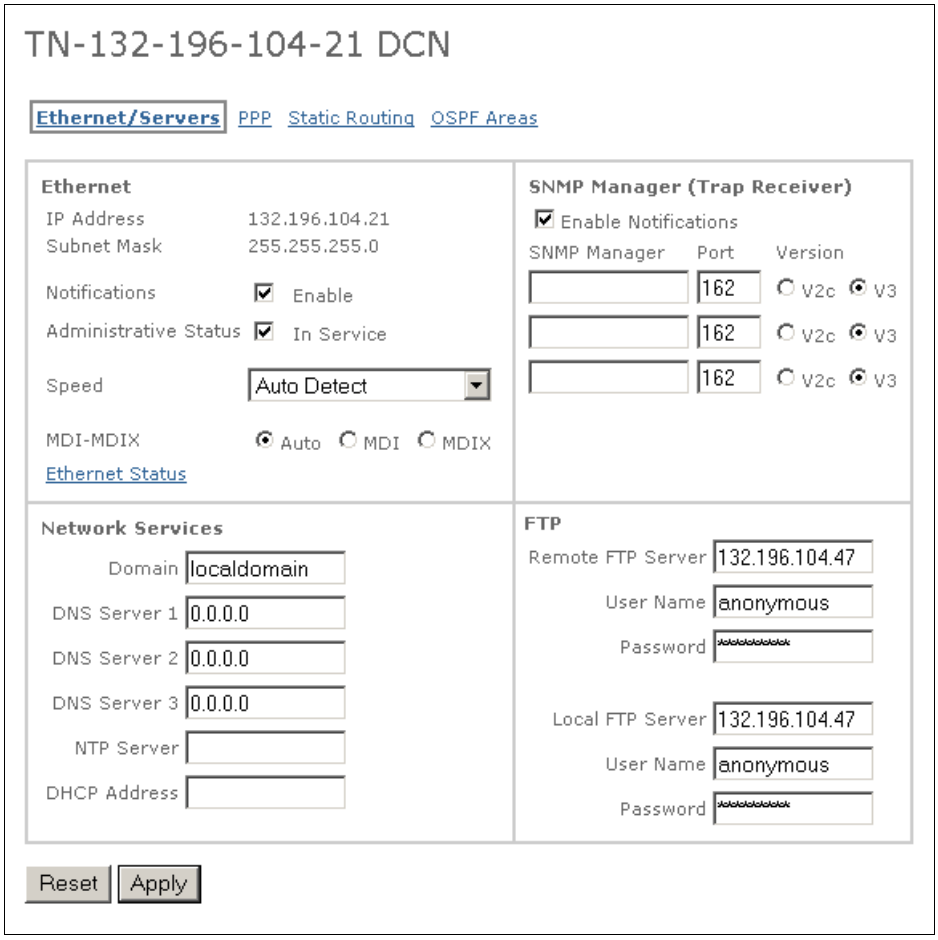


Figure 60 The Ethernet/LAN/Servers Configuration page

- **Ethernet/LAN** — Allows configuration of the Ethernet interface on the NPU2/NPU1 B or LAN interface ATU (B). For an NPU 8x2, this section only displays read-only values.
  - **IP Address** — The IP address of the interface, inheriting the address of the internal router.
  - **Subnet Mask** — The subnet mask of the interface, inheriting the subnet mask of the internal router.
  - **Notifications Enable** — Enables notifications from the interface.
  - **Administrative Status In Service** — Sets the interface in operating mode, enabling it for the site LAN or Ethernet Bridge traffic (NPU2 and ATU (B) only).
  - **Speed** — Specifies the speed in Mbit/s and duplex mode or detects it automatically.
  - **MDI-MDIX** — Specifies the MDI mode, that is selection of Rx/Tx.

        - **Auto** — The mode is detected automatically (default). A crossed or straight cable can be used independent of the connected device.
        - **MDI** — Manual mode with Rx and Tx not switched. Use a straight cable to connect to a router and a crossed cable to a PC.
        - **MDIX** — Manual mode with Rx and Tx switched. Use a straight cable to connect to a PC and a crossed cable to a router.
    - **Ethernet/LAN Status** — Opens the **Ethernet/LAN Status** page, see Section 11.94 on page 287.
- **SNMP Manager (Trap Receiver)** — Specifies the SNMP Managers that supervise the NE.
    - **Enable Notifications** — Enables traps sent to the SNMP Managers.
    - **SNMP Manager** — The IP address of an SNMP Manager.
    - **Port** — The port used for SNMP.
    - **Version** — The SNMP version.
- **Network Services** — Specifies network services parameters.
    - **Domain** — The domain name of the NE.
    - **DNS Server <nr>** — The first, second and third DNS server for the NE.
    - **NTP Server** — The host name or IP address of the NTP server.
    - **DHCP Address** — The host name or IP address of the DHCP server the NE is a relay for.
- **FTP** — Specifies parameters for the FTP servers used for software upgrade and loading of configuration files.
    - **Remote FTP Server** — The IP address of the remote FTP server. Normally this is the address of a permanent FTP server in the network, but it could also be an FTP server on the PC.
    - **User Name** — The user name used to log in to the remote FTP server.
    - **Password** — The password used to log in to the remote FTP server.
    - **Local FTP Server** — The IP address of the local FTP server. Normally this is the address of the PC, but it could also be a second remote FTP server.
    - **User Name** — The user name used to log in to the local FTP server.
    - **Password** — The password used to log in to the local FTP server.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.
- **Back** — Navigates one step backward in the installation wizard.

  Note: Configurations that you have performed are not reversed.

- **Next** — Navigates one step forward in the installation wizard.

11.17 Bridge Configuration

This page is used to set parameters for the Bridge interface on ATU (B).

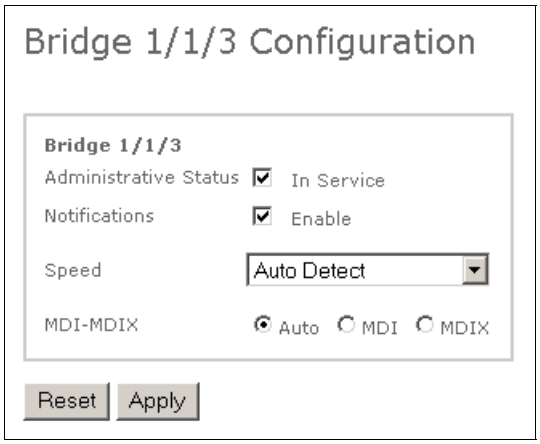


Figure 61 The Bridge Configuration page

- **Administrative Status In Service** — Specifies the desired status of the interface.
- **Notifications Enable** — Enables notifications from the interface.
- **Speed** — Specifies the speed in Mbit/s and duplex mode or detects it automatically.
- **MDI-MDIX** — Specifies the MDI mode, that is selection of Rx/Tx.
  - **Auto** — The mode is detected automatically (default). A crossed or straight cable can be used independent of the connected device.
  - **MDI** — Manual mode with Rx and Tx not switched. Use a straight cable to connect to a router and a crossed cable to a PC.
  - **MDIX** — Manual mode with Rx and Tx switched. Use a straight cable to connect to a PC and a crossed cable to a router.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.

11.18 PPP Configuration

This page is used to configure the PPP interfaces. It can specifically be used to change the default bandwidth of the STM-1 PPP interfaces and to set the number of DIG SC (2x64 kbit/s) for SMU2 in co-siting mode.

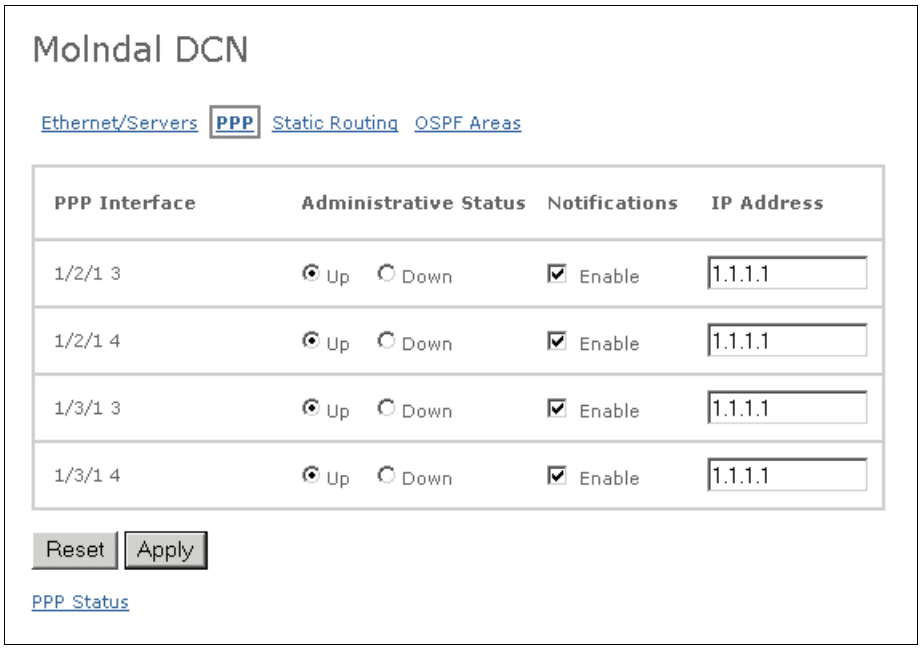


Figure 62 The PPP Configuration page

- **PPP Interface** — The name of the interface.
- **Administrative Status** — Specifies the desired status of the interface.
  - **Up** — Sets the interface in operating mode.
  - **Down** — Sets the interface in non-operating mode.

Caution!

Selecting **Down** will disable the DCN communication on the interface.

- **Notifications** — Specifies if the interface should send any notifications.
  - **Enable** — Enables notifications from the interface.
- **IP Address** — Specifies the IP address of a numbered interface. The box should be left empty for an un-numbered interface.

Caution!

It is recommended to set all interfaces destined to the same NE as either numbered or un-numbered. Mixing both types may cause DCN instability.

- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.
- **PPP Status** — Opens the **PPP Status** page, see Section 11.96 on page 290
- **Back** — Navigates one step backward in the installation wizard.

  Note: Configurations that you have performed are not reversed.

- **Next** — Navigates one step forward in the installation wizard.

See Also

- How to configure the PPP interfaces, see Section 6.10.2 on page 87.
- How to change the bandwidth of the STM-1 PPP interfaces, see Section 6.10.2.1 on page 87
- How to change the number of DIG SC (2x64 kbit/s) for SMU2 in co-siting mode, see Section 6.10.2.2 on page 88

11.19 Static Routing Configuration

This page is used to configure static routes. A maximum of 100 static routes is possible.

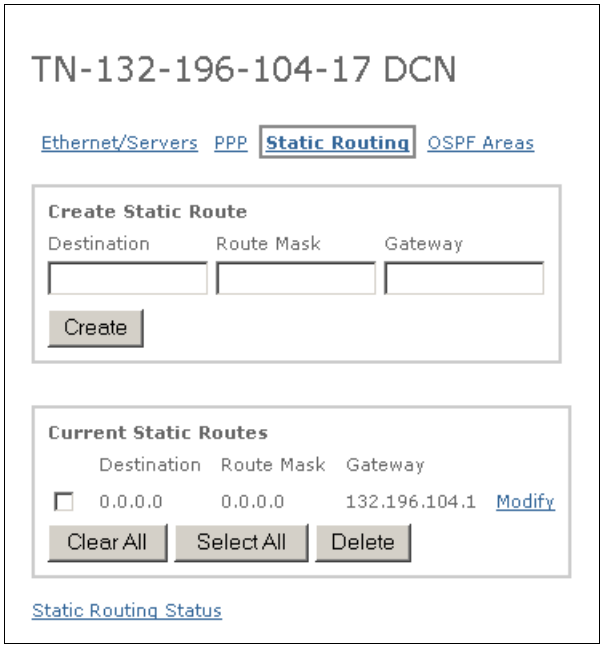


Figure 63 The Static Routing Configuration page

- **Create Static Route** — Specifies a new static route.
  - **Destination** — The destination IP address of this route.
  - **Route Mask** — The netmask for the destination IP address.
  - **Gateway** — The address of the next system on the route.
  - **Create** — Creates the static route and displays it under **Current Static Routes**.
- **Current Static Routes** — Displays the static routes. Selecting a check box enables deletion of the corresponding route.
  - **Modify** — Opens the **Modify Route** page, see Section 11.20 on page 180.
  - **Clear All** — Clears all check boxes.
  - **Select All** — Selects all check boxes.
  - **Delete** — Deletes the selected routes.
- **Static Routing Status** — Opens the **Static Routing Status** page, see Section 11.102 on page 299.
- **Back** — Navigates one step backward in the installation wizard.

  Note: Configurations that you have performed are not reversed.

- **Next** — Navigates one step forward in the installation wizard.

See Also

- How to configure static routes, see Section 6.10.5 on page 89.

11.20 Modify Static Route

This page is used to modify or delete a static route.

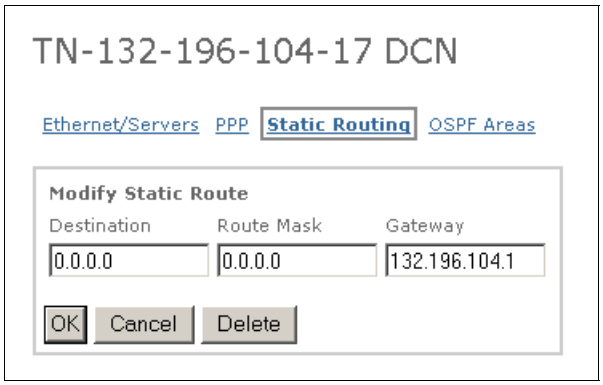


Figure 64 The Modify Static Route page

- **Destination** — The destination IP address of this route.
- **Route Mask** — The netmask for the destination IP address.
- **Gateway** — The address of the next system on the route.
- **OK** — Updates the static route and returns to the **Static Routing Configuration** page, see Section 11.19 on page 179.
- **Cancel** — Closes the page without modifying the static route and returns to the **Static Routing Configuration** page.
- **Delete** — Deletes the static route and returns to the **Static Routing Configuration** page.
- **Back** — Navigates one step backward in the installation wizard.

  Note: Configurations that you have performed are not reversed.

- **Next** — Navigates one step forward in the installation wizard.

See Also

- How to modify or delete static routes, see Section 6.10.6 on page 89.

11.21 OSPF Area Configuration

This page is used to create OSPF areas.

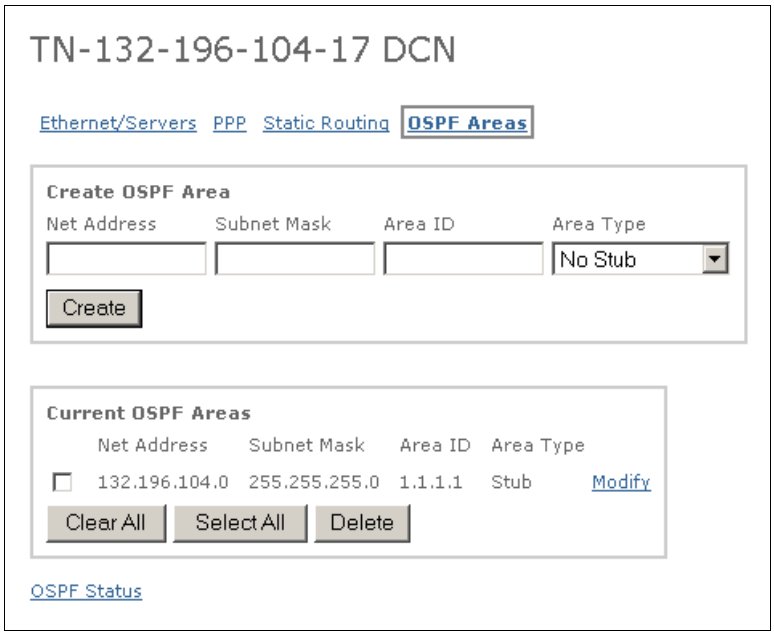


Figure 65 The OSPF Area Configuration page

- **Create OSPF Area** — Specifies a new OSPF area.
  - **Net Address** — The IP address of the subnet that is assigned the corresponding area ID.
  - **Subnet Mask** — The netmask of the subnet.
  - **Area ID** — The OSPF area of the subnet.
  - **Area Type** — The type of OSPF area.
  - **Create** — Creates the OSPF area and displays it under **Current OSPF Areas**.
- **Current OSPF Areas** — Displays the OSPF areas. Selecting a check box enables deletion of the corresponding area.
  - **Modify** — Opens the **Modify OSPF Area** page, see Section 11.22 on page 183.
  - **Clear All** — Clears all check boxes.
  - **Select All** — Selects all check boxes.
  - **Delete** — Deletes the selected routes.
- **OSPF Status** — Opens the **OSPF General Status** page, see Section 11.103 on page 300.
- **Back** — Navigates one step backward in the installation wizard.

  Note: Configurations that you have performed are not reversed.

- **Next** — Navigates one step forward in the installation wizard.

See Also

- How to configure OSPF areas, see Section 6.10.3 on page 88.

11.22 Modify OSPF Area

This page is used to modify or delete an OSPF area.

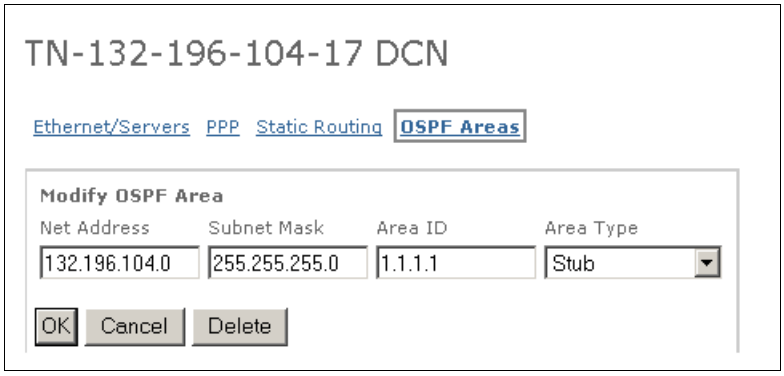


Figure 66 The Modify OSPF Area page

- **Net Address** — The IP address of the subnet that is assigned the corresponding area ID.
- **Subnet Mask** — The netmask of the subnet.
- **Area ID** — The OSPF area of the subnet.
- **Area Type** — The type of OSPF area.
- **OK** — Updates the OSPF area and returns to the **OSPF Area Configuration** page, see Section 11.21 on page 181.
- **Cancel** — Closes the page without modifying the OSPF area and returns to the **OSPF Area Configuration** page.
- **Delete** — Deletes the OSPF area and returns to the **OSPF Area Configuration** page.
- **Back** — Navigates one step backward in the installation wizard.

  Note: Configurations that you have performed are not reversed.

- **Next** — Navigates one step forward in the installation wizard.

See Also

- How to modify or delete OSPF areas, see Section 6.10.4 on page 88.

11.23 PFU1 Configuration

This page is used to configure a PFU1.

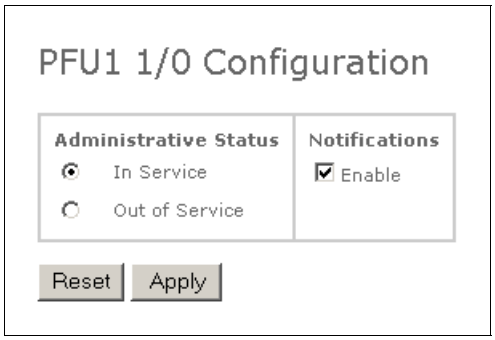


Figure 67 The PFU1 Configuration page

- **Administrative Status** — Specifies the desired status of the PFU1. At least one PFU1 must be In Service in case of redundant PFU1s.
  - **In Service** — Sets the unit in operating mode.
  - **Out of Service** — Sets the unit in non-operating mode. The unit is regarded as not present and will not be presented in the Navigation Tree, for example.
- **Notifications** — Specifies if the unit should send any notifications.
  - **Enable** — Enables notifications from the unit.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.

11.24 PFU2 Configuration

This page is used to configure a PFU2.

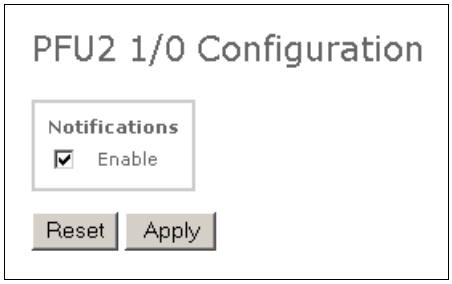


Figure 68 The PFU2 Configuration page

- **Notifications** — Specifies if the unit should send any notifications.
  - **Enable** — Enables notifications from the unit.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.

11.25 PFU3 Configuration

This page is used to configure a PFU3.

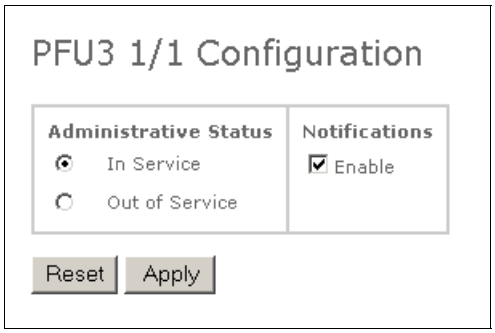


Figure 69 The PFU3 Configuration page

- **Administrative Status** — Specifies the desired status of the PFU3. At least one PFU3 must be In Service in case of redundant PFU3s.
  - **In Service** — Sets the unit in operating mode.
  - **Out of Service** — Sets the unit in non-operating mode. The unit is regarded as not present and will not be presented in the Navigation Tree, for example.
- **Notifications** — Specifies if the unit should send any notifications.
  - **Enable** — Enables notifications from the unit.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.

11.26 FAU Configuration

This page is used to configure an FAU.

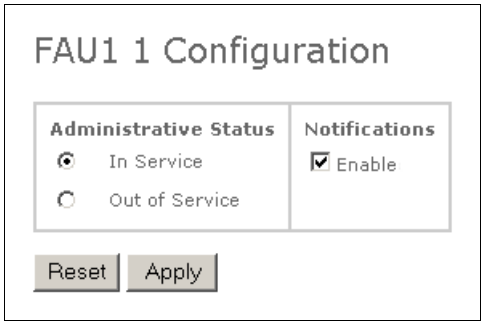


Figure 70 The FAU Configuration page

- **Administrative Status** — Specifies the desired status of the FAU.
  - **In Service** — Sets the unit in operating mode.
  - **Out of Service** — Sets the unit in non-operating mode. The unit is regarded as not present and will not be presented in the Navigation Tree, for example.
- **Notifications** — Specifies if the unit should send any notifications.
  - **Enable** — Enables notifications from the unit.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.

11.27 NPU1 B Configuration

Figure 71 The NPU1 B Configuration page

This page is used to configure an NPU1 B.

- **Notifications** — Specifies if the unit should send any notifications.
  - **Enable** — Enables notifications from the unit and lets through notifications from the unit's interfaces.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.

11.28 NPU 8x2 Configuration

This page is used to configure an NPU 8x2.

Figure 72 The NPU 8x2 Configuration page

- **Notifications** — Specifies if the unit should send any notifications.
  - **Enable** — Enables notifications from the unit and lets through notifications from the unit's interfaces.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.

11.29 NPU2/ATU NPU Configuration

This page is used to configure an NPU2 or an ATU NPU.

Figure 73 The NPU2/ATU NPU Configuration page

- **Notifications** — Specifies if the unit should send any notifications.
  - **Enable** — Enables notifications from the unit and lets through notifications from the unit's interfaces.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.

11.30 Ethernet Bridge Configuration

This page is used to select which E1 interfaces that will be used in the Ethernet Bridge, implemented in the NPU2 and ATU (B). A maximum of 16 E1s can be used for transmission of Ethernet traffic.

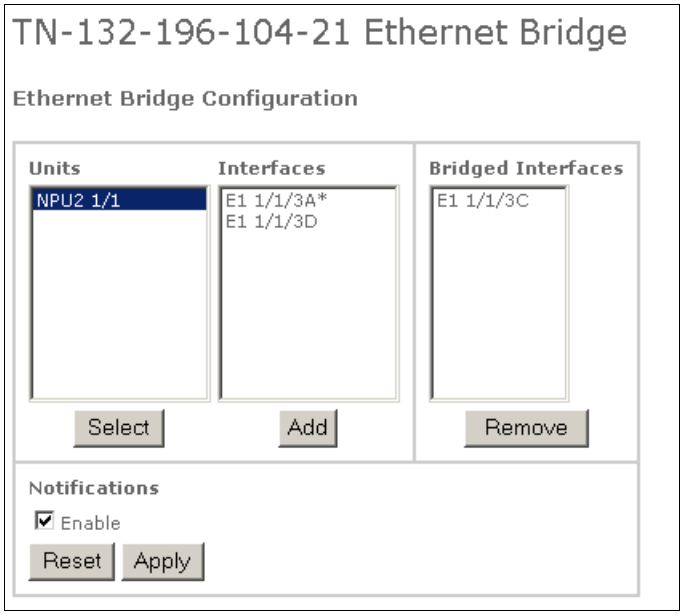


Figure 74 The Ethernet Bridge Configuration page

- **Units** — Displays the units that contain E1 interfaces. Select one unit from the list.
  - **Select** — Displays the available E1s for the selected unit under **Interfaces**.
- **Interfaces** — Displays E1s that can be bridged. An E1 can be bridged if it is not part of a traffic routing, used for DCN or already bridged. Select the E1s to be bridged. Use CTRL or SHIFT to select multiple items.
  - **Add** — Moves the selected E1s to **Bridged Interfaces**.
- **Bridged Interfaces** — Displays the bridged E1s. If E1s should be removed from the bridge, select them in the list. Use CTRL or SHIFT to select multiple items.
  - **Remove** — Removes the selected E1s from the bridge.
- **Notifications** — Specifies if the bridge should send any notifications for the HDLC encapsulation interface. Only displayed when at least one E1 is bridged.
  - **Enable** — Select the check box to enable notifications.
- **Reset** — Resets the settings of the check box.
- **Apply** — Applies notifications settings without leaving the page.

See Also

- How to configure the Ethernet Bridge, see Section 6.7 on page 79.

11.31 LTU 12x2 Configuration

This page is used to configure an LTU 12x2.

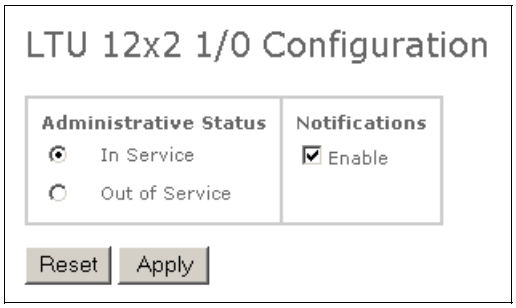


Figure 75 The LTU 12x2 Configuration page

- **Administrative Status** — Specifies the desired status of the unit.
  - **In Service** — Sets the unit in operating mode.
  - **Out of Service** — Sets the unit in non-operating mode.

Caution!

Selecting **Out of Service** will disturb the traffic.

Note: Notifications from the unit's interfaces are suppressed.

- **Notifications** — Specifies if the unit should send any notifications.
  - **Enable** — Enables notifications from the unit and lets through notifications from the unit's interfaces.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.

11.32 LTU 16x2 Configuration

This page is used to configure an LTU 16x2.

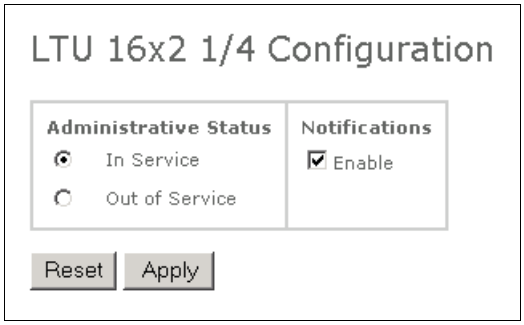


Figure 76 The LTU 16x2 Configuration page

- **Administrative Status** — Specifies the desired status of the unit.
  - **In Service** — Sets the unit in operating mode.
  - **Out of Service** — Sets the unit in non-operating mode.

Caution!

Selecting **Out of Service** will disturb the traffic.

Note: Notifications from the unit's interfaces are suppressed.

- **Notifications** — Specifies if the unit should send any notifications.
  - **Enable** — Enables notifications from the unit and lets through notifications from the unit's interfaces.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.

11.33 LTU 155 Configuration

This page is used to configure an LTU 155.

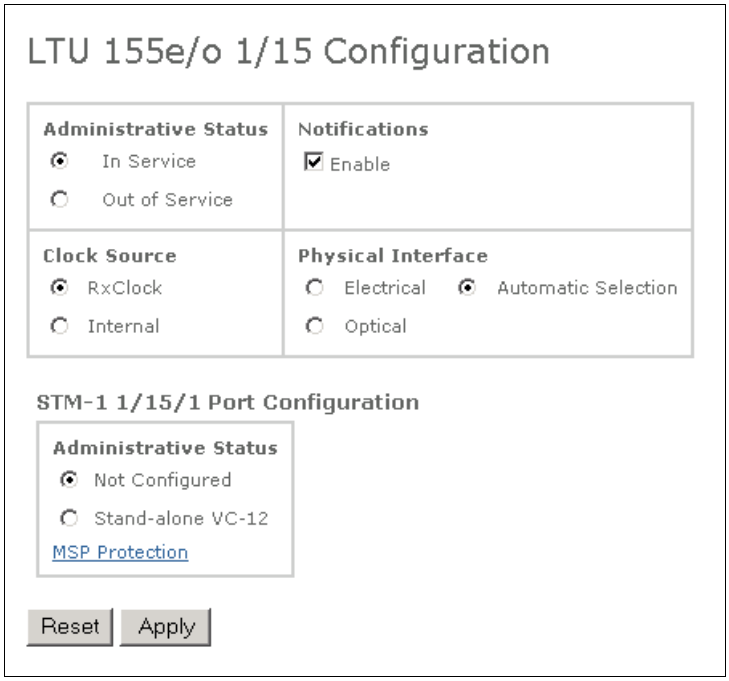


Figure 77 The LTU 155 Configuration page

- **Administrative Status** — Specifies the desired status of the unit.
  - **In Service** — Sets the unit in operating mode
  - **Out of Service** — Sets the unit in non-operating mode.

Caution!

Selecting **Out of Service** will disturb the traffic.

Note: Notifications from the unit's interfaces are suppressed.

- **Notifications** — Specifies if the unit should send any notifications.
  - **Enable** — Enables notifications from the unit and lets through notifications from the unit's interfaces.
- **Clock Source** — Selects the clock to be used as transmit clock.
  - **RxClock** — The recovered receive clock.
  - **Internal** — The local clock source.
- **Physical Interface** — Specifies the SDH connection to be used.
  - **Electrical** — Electrical interface.
  - **Optical** — Optical interface.
  - **Automatic Selection** — Selects the connected interface automatically.

- **STM-1 Port Configuration** — Specifies the properties of the STM-1 port.
  - **Administrative Status** — Specifies the administrative status of the STM-1 port.
    - **Not Configured** — The port does not provide traffic until it is configured.
    - **Stand-alone VC-12** — The port has 63 E1 interfaces and operates alone.
  - **MSP Protection** — Opens the **Create MSP Protection** page for the unit, see Section 11.68 on page 250.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.

11.34 MMU2 Configuration

This page is used to configure an MMU2.

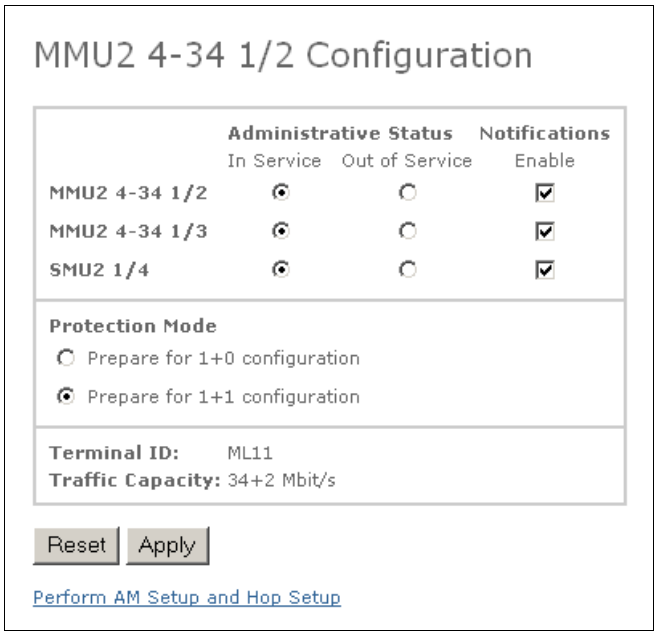


Figure 78 The MMU2 Configuration page

- **Administrative Status** — Specifies the desired status of the unit. For a 1+1 terminal it is possible to specify the status of all three units.
  - **In Service** — Sets the unit in operating mode.
  - **Out of Service** — Sets the unit in non-operating mode.

⚠ **Caution!**

Selecting **Out of Service** will disturb the traffic.

Note: Notifications from the unit's interfaces are suppressed.

- **Notifications** — Specifies if the unit should send any notifications. For a 1+1 terminal it is possible to disable notifications from all three indoor units.
  - **Enable** — Enables notifications from the unit and lets through notifications from the unit's interfaces.
- **Protection Mode** — Specifies the protection mode of the terminal.

  Note: Setting the protection mode is not applicable for ATU (B).

  - **Not Defined** — Indicates a mismatch regarding how the number of units per terminal are configured.
  - **Prepare for 1+0 configuration** — An unprotected Radio Terminal. This is the default value.

Note: If the terminal has been configured as 1+1, all three units must be left in the magazine until the terminal is configured as 1+0.

- **Prepare for 1+1 configuration** — A protected Radio Terminal. Only available if the units are placed in adjacent AMM positions according to specifications in *MINI-LINK TN ETSI Indoor Installation Manual*.

- **Terminal ID** — Displays the Radio Terminal identity.
- **Traffic Capacity** — The traffic capacity of the MMU2. The default value is 2x2 Mbit/s. `Not Defined` indicates a mismatch between the traffic capacities of the two MMU2 units in a 1+1 terminal.
- **Warnings** — Warnings about configuration mismatches, such as the number of units per terminal and the protection mode set in MSM.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.
- **Perform AM Setup and Hop Setup** — Starts MSM for further configuration of the Radio Terminal.

  Note: When using MINI-LINK Manager 7.1, the link **Perform Hop Setup** is present instead. Clicking the link starts MINI-LINK E Adapter. For MINI-LINK Manager 6.1 the link is replaced by the text “Use MINI-LINK Manager to view the hop”.

- **Back** — Navigates backward one step in the wizard. Only available in the installation wizard.

  Note: Configurations that you have performed are not reversed.

- **Next** — Navigates one step forward in the wizard. Only available in the installation wizard.

See Also

- How to configure an unprotected (1+0) Radio Terminal, see Section 6.4.3 on page 66.
- How to configure a protected (1+1) Radio Terminal, see Section 6.4.4 on page 66.

11.35 SMU2 Configuration

This page is used to configure an SMU2. The unit can be used for protection in a protected (1+1) Radio Terminal or as a traffic interface with co-sited MINI-LINK E terminals.

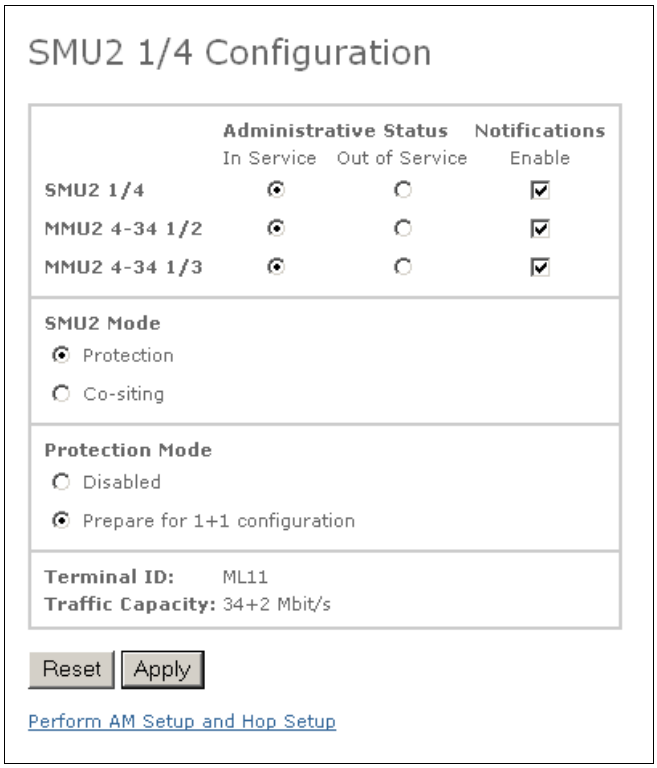


Figure 79 The SMU2 Configuration page

- **Administrative Status** — Specifies the desired status of the unit. For a 1+1 terminal it is possible to specify the status of all three units.
  - **In Service** — Sets the unit in operating mode.
  - **Out of Service** — Sets the unit in non-operating mode.

Caution!

Selecting **Out of Service** will disturb the traffic.

Note: Notifications from the unit's interfaces are suppressed.

- **Notifications** — Specifies if the unit should send any notifications. For a 1+1 terminal it is possible to disable notifications from all three indoor units.
  - **Enable** — Enables notifications from the unit and lets through notifications from the unit's interfaces.
- **SMU2 Mode** — Specifies the working mode of the unit.

- **Protection** — The unit is used for protection in a 1+1 Radio Terminal.

  Note: The unit must be set in **Protection** mode if the embedded software (CSS) in the unit should be updated using the Local Upgrade software.

- **Co-siting** — The unit is used as a traffic interface with co-sited MINI-LINK E terminals.

  Note: MSM cannot be used for configuration when the SMU2 is in co-siting mode.

  Note: If an SMU2 has been used for protection it is recommended to do a preset to factory settings before using it for co-siting. For more information on how to do a preset, see *MSM User Guide* or *MSM online Help*.

- **Protection Mode** — Specifies the protection mode of the terminal. Only available when **Protection** is selected.
  - **Not Defined** — Indicates a mismatch regarding how the number of units per terminal are configured.
  - **Disabled** — An unprotected Radio Terminal. This is the default value. This option is mainly used to disable the 1+1 configuration. The SMU2 has no practical application when it is set in this mode.

    Note: If the terminal has been configured as 1+1, all three units must be left in the magazine until the terminal is configured as 1+0.

  - **Prepare for 1+1 configuration** — A protected Radio Terminal. Only available if the units are placed in adjacent AMM positions according to specifications in *MINI-LINK TN ETSI Indoor Installation Manual*.
- **Terminal ID** — Displays the Radio Terminal identity.
- **Traffic Capacity** — Displays or sets the traffic capacity.
  - Protection: The traffic capacity of the MMU2s in the 1+1 terminal. The default value is 2x2 Mbit/s. `Not Defined` indicates a mismatch between the traffic capacities of the two MMU2 units.
  - Co-siting: Sets the traffic capacity of the unit.
- **Warnings** — Warnings about configuration mismatches, such as the number of units per terminal and the protection mode set in MSM.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.
- **Perform AM Setup and Hop Setup** — Starts MSM for further configuration of the Radio Terminal.

  Note: When using MINI-LINK Manager 7.1, the link **Perform Hop Setup** is present instead. Clicking the link starts MINI-LINK E Adapter. For MINI-LINK Manager 6.1 the link is replaced by the text “Use MINI-LINK Manager to view the hop”.

- **Back** — Navigates backward one step in the wizard. Only available in the installation wizard.

  Note: Configurations that you have performed are not reversed.

- **Next** — Navigates one step forward in the wizard. Only available in the installation wizard.

See Also

- How to configure a protected (1+1) Radio Terminal, see Section 6.4.4 on page 66.

11.36 MMU2 B/C Configuration

This page is used to configure the MMU2 B/Cs on the near-end Radio Terminal. For protected (1+1) Radio Terminals, both modems in the terminal are configured at the same time.

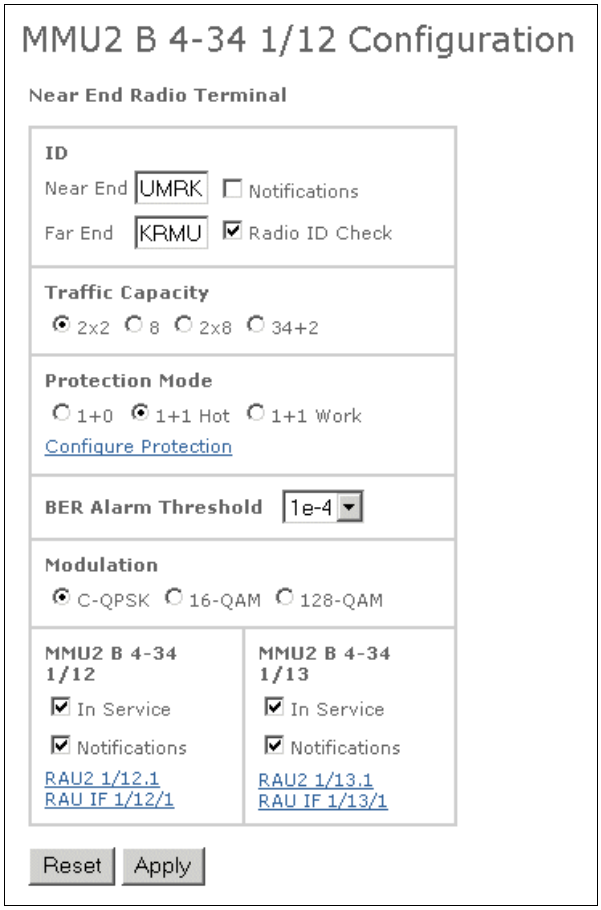


Figure 80 The MMU2 B/C Configuration page

- **ID** — Specifies the identity of the near-end Radio Terminal.
  - **Near End** — Specifies the identity of this Radio Terminal.
  - **Far End** — Specifies the expected identity of the Radio Terminal on the other end of the radio link. If **Radio ID Check** is enabled, this identity must match the identity of the far-end terminal.
  - **Notifications** — Specifies if the Radio Terminal should send any notifications.
  - **Radio ID Check** — Controls that the received traffic originates from the correct far-end Radio Terminal. If not, an alarm is generated.
- **Traffic Capacity** — Specifies the traffic capacity of the Radio Terminal. All supported capacities are displayed. `Unknown` indicates a mismatch between the two MMU2 B/C units in a protected Radio Terminal.
- **Protection Mode** — Specifies the protection mode of the Radio Terminal.

  - **Not Defined** — Indicates a mismatch in a protected Radio Terminal. For example, it has been configured as 1+1 Hot and then one MMU2 B/C is removed.
  - **1+0** — Specifies an unprotected Radio Terminal.
  - **1+1 Hot** — Specifies a protected Radio Terminal in hot standby mode. Only available if there are two units in the correct positions.
  - **1+1 Work** — Specifies a protected Radio Terminal in working standby mode. Only available if there are two units in the correct positions.
  - **Configure Protection** — Opens the **SWITCH Protection** page where the protection is configured. Only available for protected (1+1) Radio Terminals. Unavailable in the Installation Wizard.
- **BER Alarm Threshold** — Specifies the BER alarm threshold.
- **Modulation** — Specifies the modulation method.
- **MMU <ID>** — Specifies the desired status of the unit.
  - **In Service** — Selecting the check box sets the unit in operating mode.

Caution!

Clearing the check box will set the unit Out of Service and disturb the traffic.

Note: If the unit is set Out of Service, notifications from the unit's interfaces are suppressed.

  - **Notifications** — Specifies if the unit should send any notifications.
  - **RAU <ID>** — Clicking the link opens the **RAU Configuration** page, see Section 11.38 on page 204. Unavailable in the Installation Wizard.
  - **RAU IF <ID>** — Clicking the link opens the **RAU IF Configuration** page, see Section 11.37 on page 203. Unavailable in the Installation Wizard.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.
- **Back** — Navigates backward one step in the wizard. Only available in the Installation Wizard.

  Note: Configurations that you have performed are not reversed.

- **Next** — Navigates one step forward in the wizard. Only available in the Installation Wizard.

See Also

- How to configure an unprotected (1+0) Radio Terminal with MMU2 B/C, see Section 6.4.1 on page 63.
- How to configure a protected (1+1) Radio Terminal with MMU2 B/C, see Section 6.4.2 on page 64.

11.37 RAU IF Configuration

This page is used to configure an RAU IF interface for an MMU2 B/C.

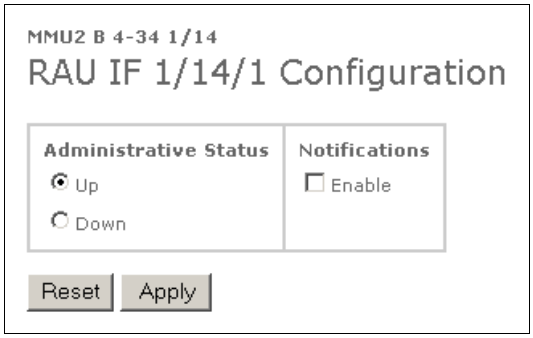


Figure 81 The RAU IF Configuration page

- **Administrative Status** — Specifies the desired status of the interface.
  - **Up** — Sets the interface in operating mode.
  - **Down** — Sends an AIS instead of traffic on the interface (in both directions). Notifications from this interface and higher layer interfaces are suppressed.
- **Notifications** — Specifies if the interface should send any notifications.
  - **Enable** — Enables notifications from the interface and lets through notifications from higher layer interfaces.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.

See Also

- How to configure an unprotected (1+0) Radio Terminal with MMU2 B/C, see Section 6.4.1 on page 63.
- How to configure a protected (1+1) Radio Terminal with MMU2 B/C, see Section 6.4.2 on page 64.

11.38 RAU Configuration

This page is used to configure the radio units on the near-end Radio Terminal.

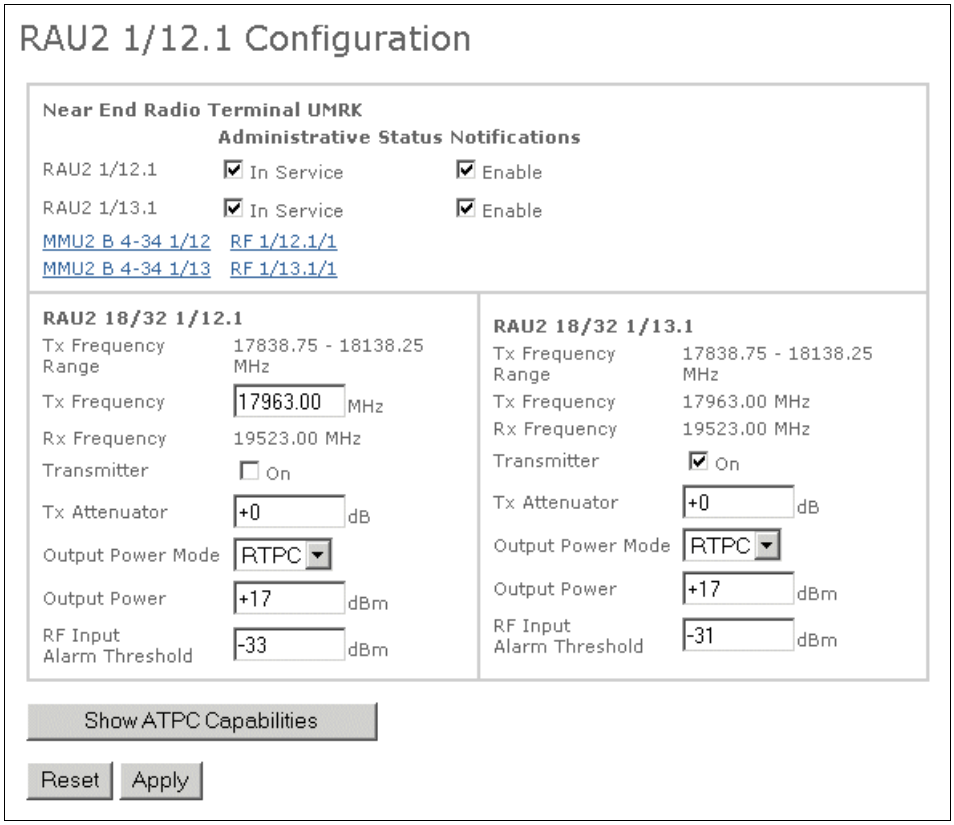


Figure 82 The RAU Configuration page

- **Near End Radio Terminal <ID>** — Displays the identity of the Radio Terminal. Both RAUs are available in a protected Radio Terminal.
  - **Administrative Status** — Specifies the desired status of the unit.
    - **In Service** — Selecting the check box sets the unit in operating mode.

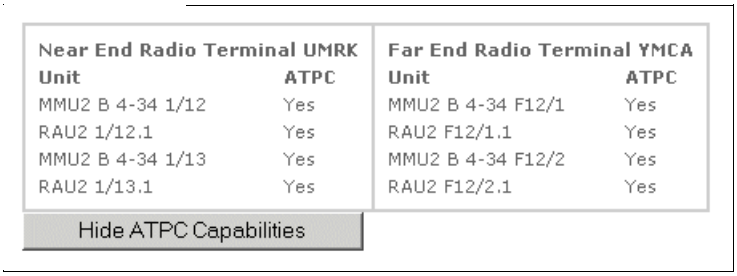
Caution!

Clearing the check box will set the unit Out of Service and disturb the traffic.

Note: If the unit is set Out of Service, notifications from the unit's interfaces are suppressed.

  - **Notifications** — Specifies if the unit should send any notifications.
    - **Enable** — Enables notifications from the unit and lets through notifications from the its interface.

  - **MMU2 B/C <ID>** — Clicking the link opens the **MMU2 B/C Configuration** page, see Section 11.36 on page 201.
  - **RF <ID>** — Clicking the link opens the **RF Configuration** page, see Section 11.39 on page 207.
- **RAU <ID>** — Displays the identity of the radio unit. In protected (1+1) configurations, both radios are shown side-by-side.
  - **Tx Frequency Range** — Displays the frequency range this RAU supports.
  - **Tx Frequency** — Specifies the transmitted frequency in MHz. Read-only for Ra2 in protected (1+1) terminals.
  - **Rx Frequency** — Indicates the received frequency in MHz, as determined by the **Tx Frequency**.
  - **Transmitter** — Selecting the check box turns the transmitter on. Clearing the check box turns the transmitter off.
  - **Tx Attenuator** — Specifies the value (in dB) of an optional fixed attenuator.
  - **Output Power Mode** — Specifies how the output power is controlled.
    - **RTPC** — The output power is set from a management application.
    - **ATPC** — The output power is set automatically depending on the received input power in the far-end RAU.
    - **Local** — The output power is set locally in the RAU.
  - **Output Power** — Specifies the output power (including **Tx Attenuator**) in dBm. Only available when **Output Power Mode** is set to **RTPC**.
  - **Max Output Power** — Specifies the maximum output power (including **Tx Attenuator**) in dBm. Only available when **Output Power Mode** is set to **ATPC**.
  - **Target Input Power (far-end)** — Specifies the target input power (in dBm) for the far-end RAU. Only available when **Output Power Mode** is set to **ATPC**.
  - **RF Input Alarm Threshold** — Specifies the input power threshold value (in dBm) used for 1+1 switching.
- **Show ATPC Capabilities** — Shows the ATPC capabilities for all units in the radio link. Click **Hide ATPC Capabilities** to hide them again.



- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.
- **Back** — Navigates backward one step in the wizard. Only available in the installation wizard.

Note: Configurations that you have performed are not reversed.

- **Next** — Navigates one step forward in the wizard. Only available in the installation wizard.

See Also

- How to configure an unprotected (1+0) Radio Terminal with MMU2 B/C, see Section 6.4.1 on page 63.
- How to configure a protected (1+1) Radio Terminal with MMU2 B/C, see Section 6.4.2 on page 64.

11.39 RF Configuration

This page is used to configure an RF interface, on an RAU connected to an MMU2 B/C.

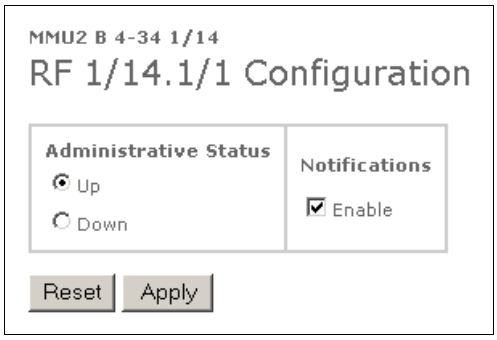


Figure 83 The RF Configuration page

- **Administrative Status** — Specifies the desired status of the interface.
  - **Up** — Sets the interface in operating mode.
  - **Down** — Turns the transmitter off and sends an AIS in the receive direction. Notifications from this interface and higher layer interfaces are suppressed.
- **Notifications** — Specifies if the interface should send any notifications.
  - **Enable** — Enables notifications from the interface and lets through notifications from higher layer interfaces.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.

See Also

- How to configure an unprotected (1+0) Radio Terminal with MMU2 B/C, see Section 6.4.1 on page 63.
- How to configure a protected (1+1) Radio Terminal with MMU2 B/C, see Section 6.4.2 on page 64.

11.40 Reset Configuration

This page is used to reset a Radio Terminal with MMU2 B/C to the default configuration. The configuration items on the MMU2 B/C, RAU, RAU IF, RF and SWITCH configuration pages will get default values. All units in the terminal must be `In Service` to be able to perform this operation.

Figure 84 The Reset Configuration page

Caution!

Resetting the configuration will disturb the traffic.

- **Apply** — Applies the default configuration without leaving the page.

See Also

- How to configure an unprotected (1+0) Radio Terminal with MMU2 B/C, see Section 6.4.1 on page 63.
- How to configure a protected (1+1) Radio Terminal with MMU2 B/C, see Section 6.4.2 on page 64.

11.41 Restore Configuration

This page is used to restore the configuration of a Radio Terminal with MMU2 B/C, which means:

- RF Loop, IF Loop and Rx Loop are disabled.
- Transmitter(s) is turned on.
- Switch mode is set to Auto.
- Notifications for the terminal are enabled.

All units in the terminal must be `In Service` to be able to perform this operation.

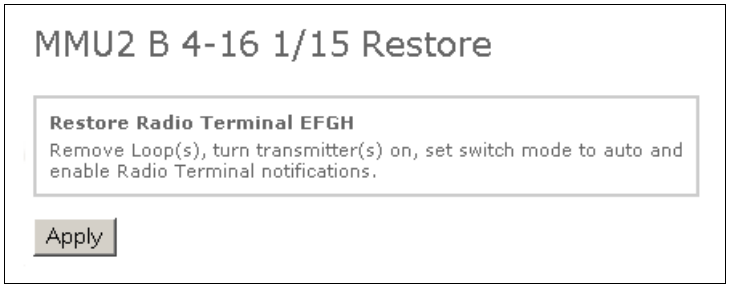


Figure 85 The Restore Configuration page

- **Apply** — Applies the restored configuration without leaving the page.

See Also

- How to configure an unprotected (1+0) Radio Terminal with MMU2 B/C, see Section 6.4.1 on page 63.
- How to configure a protected (1+1) Radio Terminal with MMU2 B/C, see Section 6.4.2 on page 64.

11.42 SWITCH Configuration

This page is used to configure the SWITCH interface for a Radio Terminal with MMU2 B or MMU2 C.

Figure 86 The SWITCH Configuration page

- **Notifications** — Specifies if the interface should send any notifications.
  - **Enable** — Enables notifications from the interface and lets through notifications from higher layer interfaces.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.

See Also

- How to configure an unprotected (1+0) Radio Terminal with MMU2 B/C, see Section 6.4.1 on page 63.
- How to configure a protected (1+1) Radio Terminal with MMU2 B/C, see Section 6.4.2 on page 64.

11.43 SWITCH Protection

This page is used to configure the protection parameters for a radio terminal with MMU2 B or MMU2 C.

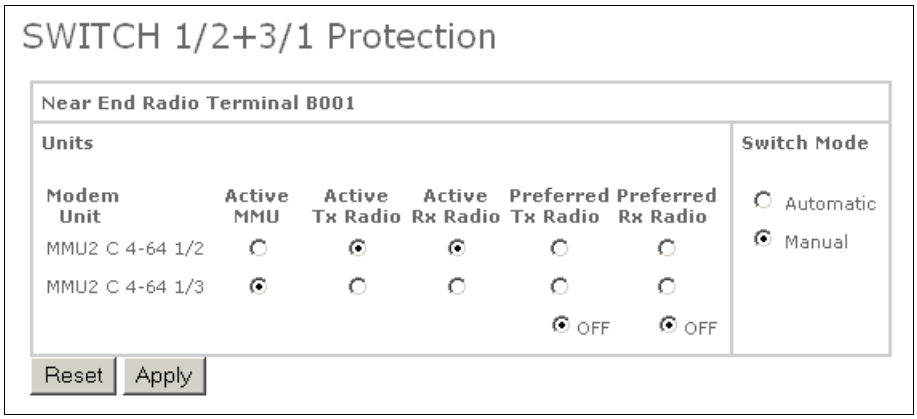


Figure 87 The SWITCH Protection page

- **Units** — Shows the MMUs in the protected Radio Terminal.
  - **Modem Unit** — Shows the names of the two MMUs.
  - **Active MMU** — Selects which MMU is used.
  - **Active Tx Radio** — Selects the transmitting RAU in a 1+1 Hot configuration.
  - **Active Rx Radio** — Selects the receiving RAU in a 1+1 Hot configuration.
  - **Preferred Tx Radio** — Selects the preferred RAU for transmitting in a 1+1 Hot configuration. If no RAU is preferred, set this option to **OFF**.
  - **Preferred Rx Radio** — Selects the preferred RAU for receiving in a 1+1 Hot configuration. If no RAU is preferred, set this option to **OFF**.
- **Switch Mode** — Specifies the switch mode for a protected Radio Terminal.
  - **Auto** — Specifies automatic switching. When **Switch Mode** is **Auto**, the options for **Active MMU**, **Active Tx Radio**, and **Active Rx Radio** are unavailable.
  - **Manual** — Specifies manual switching; all options are available.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.
- **Back** — Navigates backward one step in the wizard. Only available in the installation wizard.

  Note: Configurations that you have performed are not reversed.

- **Next** — Navigates one step forward in the wizard. Only available in the installation wizard.

See Also

- How to configure an unprotected (1+0) Radio Terminal with MMU2 B/C, see Section 6.4.1 on page 63.

- How to configure a protected (1+1) Radio Terminal with MMU2 B/C, see Section 6.4.2 on page 64.

11.44 MS/RS Configuration

This page is used to configure an MS/RS interface.

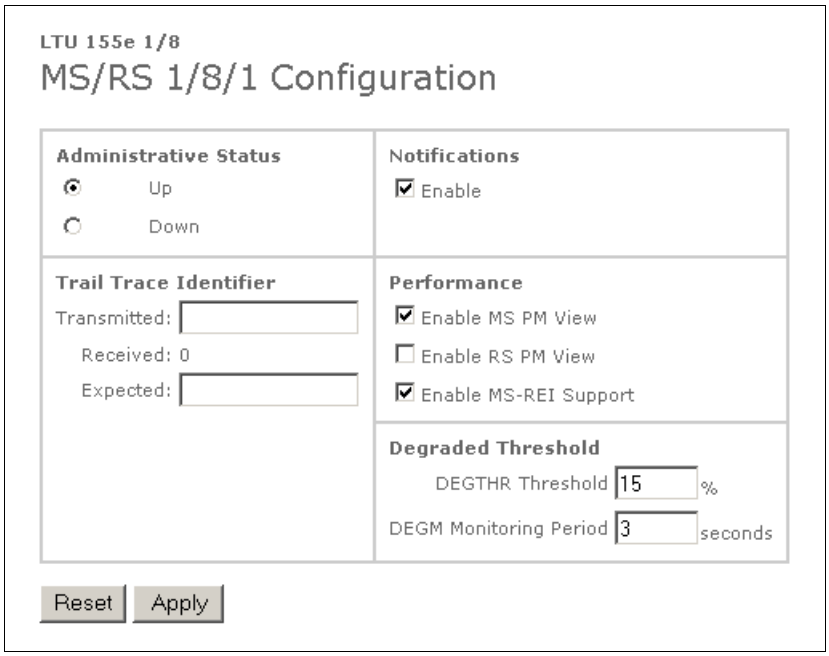


Figure 88 The MS/RS Configuration page

- **Administrative Status** — Specifies the desired status of the interface.
  - **Up** — Sets the interface in operating mode.
  - **Down** — Sends an AIS instead of traffic on the interface (in both directions). Notifications from this interface and higher layer interfaces are suppressed.
- **Notifications** — Specifies if the interface should send any notifications.
  - **Enable** — Enables notifications from the interface and lets through notifications from higher layer interfaces.
- **Trail Trace Identifier** — Specifies the identifier of the transmitted/received payload.
  - **Transmitted** — Specifies the identifier of the transmitted payload. Up to 15 characters (A – Z, a – z, 0 – 9 and white space) are allowed.
  - **Received** — Displays the identifier of the received payload.
  - **Expected** — Specifies the expected identifier of the received payload. Up to 15 characters (A – Z, a – z, 0 – 9 and white space) are allowed. If an identifier is specified, a comparison between the received and expected identifiers is done. If not equal, a Trail trace Identifier Mismatch (TIM) defect is generated.
- **Performance** — Specifies if performance data should be displayed and support of MS-REI.
  - **Enable MS PM View** — Selecting the check box enables display of MS performance data on the **MS/RS Performance** page, see Section 11.139 on page 359.

  - **Enable RS PM View** — Selecting the check box enables display of RS performance data on the **MS/RS Performance** page, see Section 11.139 on page 359.
  - **Enable MS-REI Support** — Clearing the check box secures compatibility with older SDH equipment which does not support MS-REI.
- **Degraded Threshold** — Specifies how DEGTHR and DEGM should be used.
  - **DEGTHR Threshold** — Specifies the DEGTHR threshold value used to detect a degraded defect at MS. Errored blocks are counted every second. A second is declared as degraded if the number of errored blocks during that second reaches or exceeds the threshold value. Value range is 1 – 100. Default value is 15.
  - **DEGM Monitoring Period** — Specifies the monitoring period, DEGM, used to declare DEG. DEG is declared as degraded if consecutive degraded seconds appear during a complete monitoring period. DEG is cleared if consecutive non-degraded seconds appear during a complete monitoring period. Value range is 2 – 10. Default value is 3.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.

11.45 MSP Configuration

This page is used to configure an MSP interface.

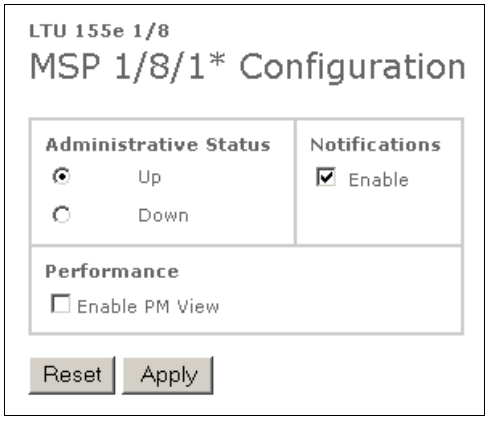


Figure 89 The MSP Configuration page

- **Administrative Status** — Specifies the desired status of the interface.
  - **Up** — Sets the interface in operating mode.
  - **Down** — Sends an AIS instead of traffic on the interface (in both directions). Notifications from this interface and higher layer interfaces are suppressed.
- **Notifications** — Specifies if the interface should send any notifications.
  - **Enable** — Enables notifications from the interface and lets through notifications from higher layer interfaces.
- **Performance** — Specifies if performance data should be displayed.
  - **Enable PM View** — Selecting the check box enables display of performance data for this MSP interface on the **MSP Performance** page, see Section 11.141 on page 363.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.

11.46 VC-4 Configuration

This page is used to configure a VC-4 interface.

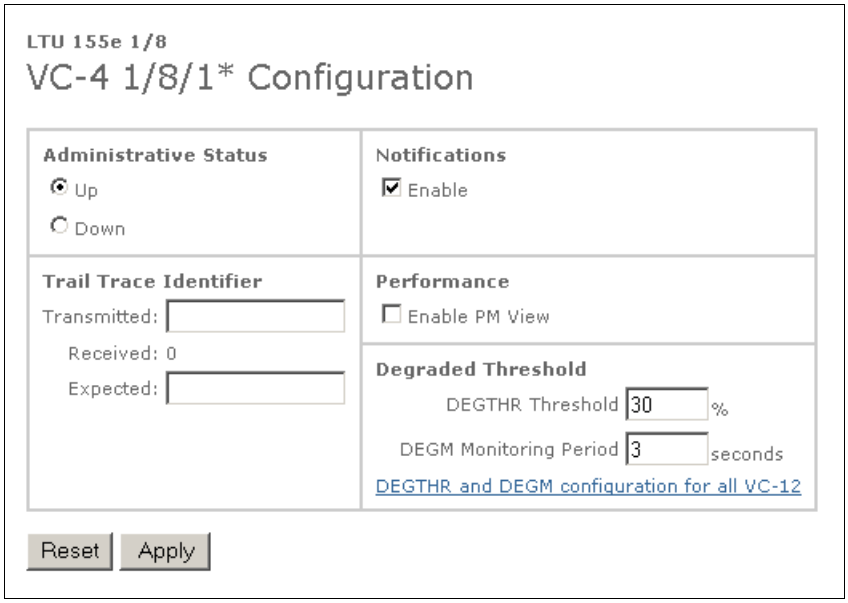


Figure 90 The VC-4 Configuration page

- **Administrative Status** — Specifies the desired status of the interface.
  - **Up** — Sets the interface in operating mode.
  - **Down** — Sends an AIS instead of traffic on the interface (in both directions). Notifications from this interface and higher layer interfaces are suppressed.
- **Notifications** — Specifies if the interface should send any notifications.
  - **Enable** — Enables notifications from the interface and lets through notifications from higher layer interfaces.
- **Trail Trace Identifier** — Specifies the identifier of the transmitted/received payload.
  - **Transmitted** — Specifies the identifier of the transmitted payload. Up to 15 characters (A – Z, a – z, 0 – 9 and white space) are allowed.
  - **Received** — Displays the identifier of the received payload.
  - **Expected** — Specifies the expected identifier of the received payload. Up to 15 characters (A – Z, a – z, 0 – 9 and white space) are allowed. If an identifier is specified, a comparison between the received and expected identifiers will be done. If not equal, a Trail trace Identifier Mismatch (TIM) defect is generated.
- **Performance** — Specifies if performance data should be displayed.
  - **Enable PM View** — Selecting the check box enables display of performance data for this VC-4 interface on the **VC-4 Performance** page, see Section 11.143 on page 367.
- **Degraded Threshold** — Specifies how DEGTHR and DEGM should be used.

  - **DEGTHR Threshold** — Specifies the DEGTHR threshold value used to detect a degraded defect at VC-4. Errored blocks are counted every second. A second is declared as degraded if the number of errored blocks during that second reaches or exceeds the threshold value. Value range is 1 – 100. Default value is 30.
  - **DEGM Monitoring Period** — Specifies the monitoring period, DEGM, used to declare DEG. DEG is declared as degraded if consecutive degraded seconds appear during a complete monitoring period. DEG is cleared if consecutive non-degraded seconds appear during a complete monitoring period. Value range is 2 – 10. Default value is 3.
  - **DEGTHR and DEGM configuration for all VC-12** — Opens the **All VC-12 Configuration** page, where the DEGTHR and DEGM thresholds for all VC-12 interfaces on the unit are configured, see Section 11.48 on page 220.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.

11.47 VC-12 Configuration

This page is used to configure a VC-12 interface.

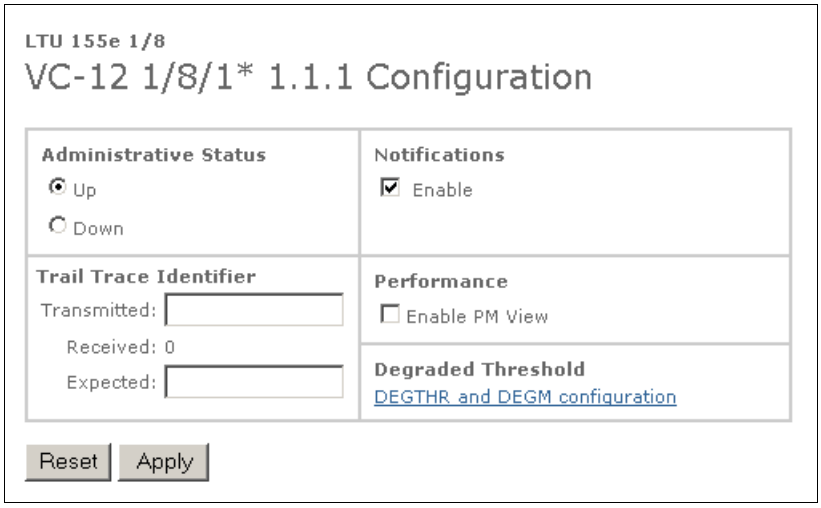


Figure 91 The VC-12 Configuration page

- **Administrative Status** — Specifies the desired status of the interface.
  - **Up** — Sets the interface in operating mode.
  - **Down** — Sends an AIS instead of traffic on the interface (in both directions). Notifications from this interface and higher layer interfaces are suppressed.
- **Notifications** — Specifies if the interface should send any notifications.
  - **Enable** — Enables notifications from the interface and lets through notifications from higher layer interfaces.
- **Trail Trace Identifier** — Specifies the identifier of the transmitted/received payload.
  - **Transmitted** — Specifies the identifier of the transmitted payload. Up to 15 characters (A – Z, a – z, 0 – 9 and white space) are allowed.
  - **Received** — Displays the identifier of the received payload.
  - **Expected** — Specifies the expected identifier of the received payload. Up to 15 characters (A – Z, a – z, 0 – 9 and white space) are allowed. If an identifier is specified, a comparison between the received and expected identifiers will be done. If not equal, a Trail trace Identifier Mismatch (TIM) defect is generated.
- **Performance** — Specifies if performance data should be displayed.
  - **Enable PM View** — Selecting the check box enables display of performance data for this VC-12 interface on the **VC-12 Performance** page, see Section 11.145 on page 371.
- **Degraded Threshold** — Provides a link for specification of how DEGTHR and DEGM should be used for all VC-12 interfaces on the unit.
  - **DEGTHR and DEGM configuration** — Opens the **All VC-12 Configuration** page, where the DEGTHR and DEGM thresholds for all VC-12 interfaces on the unit are configured, see Section 11.48 on page 220.

- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.

11.48 All VC-12 Configuration

This page is used to configure all VC-12 interfaces simultaneously on an LTU 155. One or several parameters can be included in the configuration.

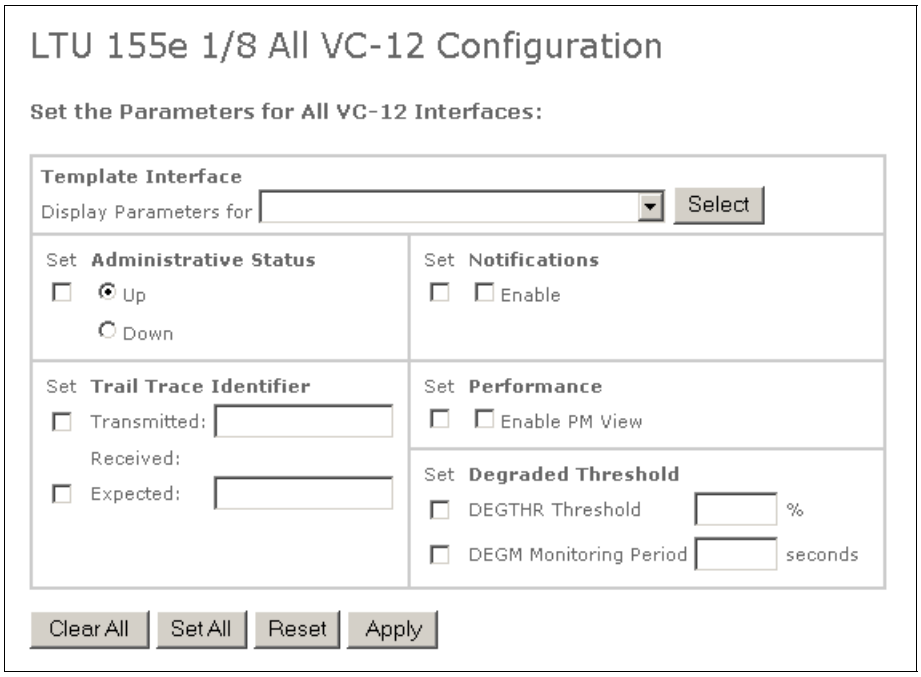


Figure 92 The All VC-12 Configuration page

The page initially displays no parameter values but it is possible to use one of the interfaces as template. If this page is opened by clicking the **DEGTHR and DEGM configuration** link on the configuration page for an individual VC-12 interface, the values for the interface are displayed as default values with **Set** selected.

- **Template Interface** — Specifies the VC-12 interface to be used as template. Select an interface from the list and click **Select** to display its configuration. If no interface is selected no values are displayed.
- **Set** — Specifies if a specific parameter should be set for all VC-12 interfaces on the unit. Available for all parameters on the page.
- **Administrative Status** — Specifies the desired status of the interface.
  - **Up** — Sets the interface in operating mode.
  - **Down** — Sends an AIS instead of traffic on the interface (in both directions). Notifications from this interface and higher layer interfaces are suppressed.
- **Notifications** — Specifies if the interface should send any notifications.
  - **Enable** — Enables notifications from the interface and lets through notifications from higher layer interfaces.
- **Trail Trace Identifier** — Specifies the identifier of the transmitted/received payload.
  - **Transmitted** — Specifies the identifier of the transmitted payload. Up to 15 characters (A – Z, a – z, 0 – 9 and white space) are allowed.

  - **Received** — Displays the identifier of the received payload.
  - **Expected** — Specifies the expected identifier of the received payload. Up to 15 characters (A – Z, a – z, 0 – 9 and white space) are allowed. If an identifier is specified, a comparison between the received and expected identifiers will be done. If not equal, a Trail trace Identifier Mismatch (TIM) defect is generated.
- **Performance** — Specifies if performance data should be displayed.
  - **Enable PM View** — Selecting the check box enables display of performance data for all VC–12 interfaces on the **VC-12 Performance** page, see Section 11.145 on page 371.
- **Degraded Threshold** — Specifies how DEGTHR and DEGM should be used.
  - **DEGTHR Threshold** — Specifies the DEGTHR threshold value used to detect a degraded defect at VC-4. Errored blocks are counted every second. A second is declared as degraded if the number of errored blocks during that second reaches or exceeds the threshold value. Value range is 1 – 100. Default value is 30.
  - **DEGM Monitoring Period** — Specifies the monitoring period, DEGM, used to declare DEG. DEG is declared as degraded if consecutive degraded seconds appear during a complete monitoring period. DEG is cleared if consecutive non-degraded seconds appear during a complete monitoring period. Value range is 2 – 10. Default value is 3.
- **Clear All** — Clears all **Set** check boxes.
- **Set All** — Selects all **Set** check boxes.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Opens a confirmation dialog box, where all configurations can be confirmed and applied.

11.49 E3 Configuration

This page is used to configure an E3 interface.

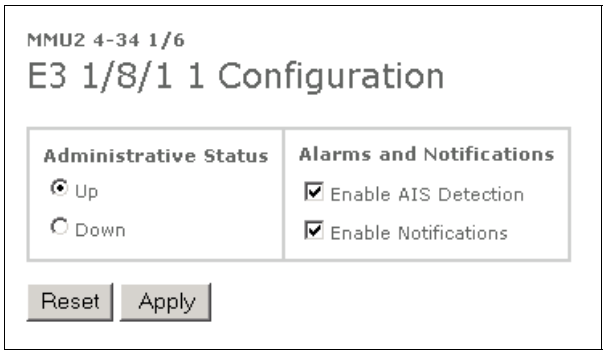


Figure 93 The E3 Configuration page

- **Administrative Status** — Specifies the desired status of the interface.
  - **Up** — Sets the interface in operating mode.
  - **Down** — Sends an AIS instead of traffic on the interface (in both directions). Notifications from this interface and higher layer interfaces are suppressed.
- **Alarms and Notifications** — Specifies alarms and notifications for the interface.
  - **Enable AIS Detection** — Enables the detection of AIS for the interface.
  - **Enable Notifications** — Enables notifications from the interface and lets through notifications from higher layer interfaces.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.

11.50 E2 Configuration

This page is used to configure an E2 interface.

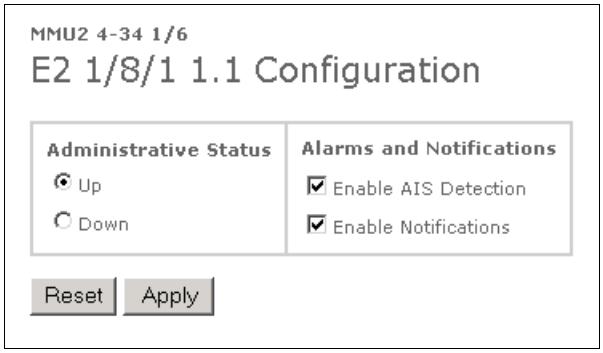


Figure 94 The E2 Configuration page

- **Administrative Status** — Specifies the desired status of the interface.
  - **Up** — Sets the interface in operating mode.
  - **Down** — Sends an AIS instead of traffic on the interface (in both directions). Notifications from this interface and higher layer interfaces are suppressed.
- **Alarms and Notifications** — Specifies alarms and notifications from the interface.
  - **Enable AIS Detection** — Enables the detection of AIS for the interface.
  - **Enable Notifications** — Enables notifications from the interface and lets through notifications from higher layer interfaces.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.

11.51 E1 Configuration

This page is used to configure an E1 interface.

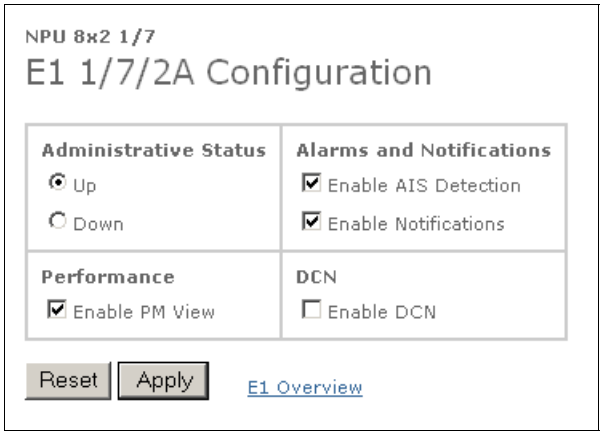


Figure 95 The E1 Configuration page

- **Administrative Status** — Specifies the desired status of the interface.
  - **Up** — Sets the interface in operating mode.
  - **Down** — Sends an AIS instead of traffic on the interface (in both directions) and suppresses notifications.
- **Alarms and Notifications** — Specifies alarms and notifications for the interface.
  - **Enable AIS Detection** — Enables the detection of AIS for the interface.
  - **Enable Notifications** — Enables notifications from the interface.
- **Performance** — Specifies if performance data should be displayed.
  - **Enable PM View** — Selecting the check box enables display of performance data for this E1 interface on the **E1 Performance** page, see Section 11.147 on page 375.
- **DCN** — Specifies if the E1 interface should serve as a DCN channel. Only available for an NPU 8x2/NPU1 B NE.

  Note: Not available for an interface which is part of a 1+1 E1 SNCP protection or traffic routing.

  - **Enable DCN** — Selecting the check box enables DCN traffic on the E1 interface. Only one E1 per NE can be enabled for DCN.
- **Configure Protected Interface** — Opens the **E1 Configuration** page for the protected interface. Only available for a protected interface.
- **Configure Unprotected Interface** — Opens the **E1 Configuration** page for the unprotected interface. Only available for a protected interface.
- **Back** — Returns to the page previously displayed. Only available if you reached this page from the **Modify 1+1 E1 SNCP** page.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.
- **E1 Overview** — Opens the **E1 Overview** page in a separate window, see Section 11.53 on page 226.

11.52 All E1 Configuration

This page is used to configure all physical E1 interfaces simultaneously, on a unit. One or several parameters can be included in the configuration by selecting the **Set** check box.

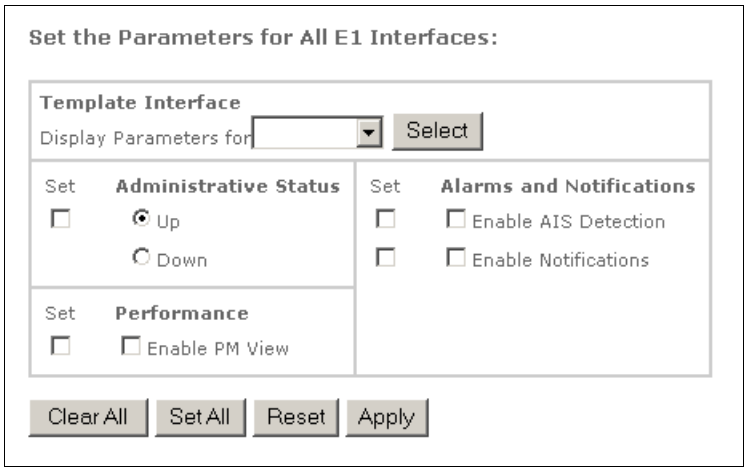


Figure 96 The All E1 Configuration page

The page initially displays no parameter values but it is possible to use one of the interfaces as template.

- **Template Interface** — Specifies the E1 interface to be used as template. Select an interface from the list and click **Select** to display its configuration. If no interface is selected no values are displayed.
- **Set** — Specifies if a specific parameter should be set for all E1 interfaces on the unit. Available for all parameters on the page.
- **Administrative Status** — Specifies the desired status of the interface.
  - **Up** — Sets the interface in operating mode.
  - **Down** — Sends an AIS instead of traffic on the interface (in both directions). Suppresses notifications from the unit's interfaces.
- **Alarms and Notifications** — Specifies alarms and notifications for the interface.
  - **Enable AIS Detection** — Enables the detection of AIS for the interface.
  - **Enable Notifications** — Enables notifications from the interface.
- **Performance** — Specifies if performance data should be displayed.
  - **Enable PM View** — Selecting the check box enables display of performance data for all E1 interfaces on the **E1 Performance** page, see Section 11.147 on page 375.
- **Clear All** — Clears all **Set** check boxes.
- **Set All** — Selects all **Set** check boxes.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Opens a confirmation dialog box, where all configurations can be confirmed and applied.

11.53 E1 Overview

This page is opened in a separate window where you can view and change the configuration of an E1 interface, as well as handle its 1+1 E1 SNCP protection and traffic routing. Furthermore, it is possible to handle the E1 as part of the Ethernet Bridge, when working with an NPU2 NE.

The upper part of the page displays the configuration of the related E1s. The top row is the E1 for which the page is opened. If this E1 is protected then the other two E1s in the 1+1 E1 SNCP protection is displayed in the next two rows. If the E1 is routed then the E1(s) to which it is routed is also displayed in the table.

The lower part gives a graphical view of how the different E1s are related.

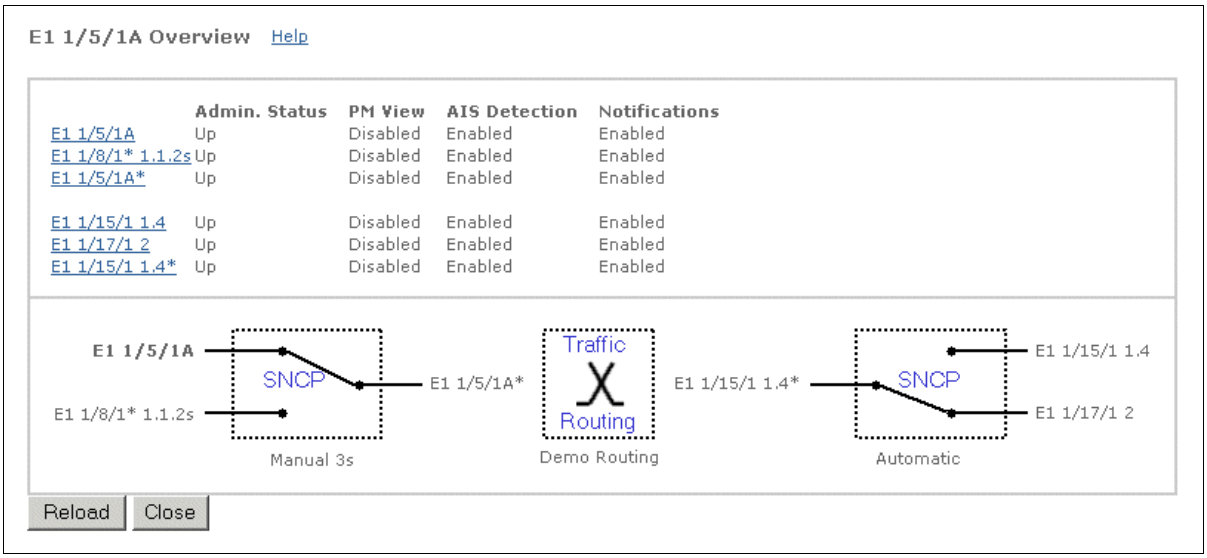


Figure 97 E1 Overview page

- **E1 <ID> Overview** — Displays for which E1 this page is opened.
- **Help** — Opens the Help section for this page.
- **E1 <ID>** — Clicking the link opens the **E1 Configuration** page for the interface, see Section 11.51 on page 224.
- **Admin. Status** — Displays the desired status of the interface.
- **PM View** — Displays if performance data should be displayed for the interface on the **E1 Performance** page, see Section 11.147 on page 375.
- **AIS Detection** — Displays if AIS should be detected for the interface.
- **Notifications** — Displays if alarm notifications are sent for the interface.
- **Create 1+1 E1 SNCP (left)** — Displayed when an E1 is unprotected. Clicking the link opens the **1+1 E1 SNCP List View** page where the E1 can be protected. The page is opened with this interface preselected, see Section 11.64 on page 243.
- **SCNP (left)** — This symbol is displayed when an E1 is protected. The two unprotected E1s are displayed to the left and the protected to the right. The symbol also illustrates the currently active E1. The E1 in bold typeface is the one for which the page is opened.

The switch mode is stated as Automatic or Manual including Hold-Off time in seconds.

Clicking the symbol opens the **Modify 1+1 E1 SNCP** page where the protection can be modified or deleted, see Section 11.67 on page 248.

- **Create Traffic Routing** — Displayed when an E1 is not routed and opens the **Traffic Routing List View** page where the E1 can be routed. The page is opened with this interface preselected, see Section 11.58 on page 234.
- **Traffic Routing** — This symbol is displayed when an E1 is routed, showing to which E1 it is routed and the name of the traffic routing stated below. Clicking the symbol opens the **Modify Traffic Routing** page where the traffic routing can be modified or deleted, see Section 11.61 on page 238.
- **Add E1 to Ethernet Bridge** — Clicking the link opens the **Ethernet Bridge Configuration** page where the E1 can be added to the Ethernet Bridge. The page is opened with this interface preselected, see Section 11.30 on page 191. Only available for an NPU2 and ATU (B).
- **Ethernet Bridge** — This symbol is displayed when an E1 is added to the Ethernet Bridge. Clicking the symbol opens the **Ethernet Bridge Configuration** page where the E1 can be removed from the Ethernet Bridge. Only available for an NPU2 and ATU (B).
- **Create 1+1 E1 SNCP (right)** — Clicking the link opens the **1+1 E1 SNCP List View** page where the E1 to the right of the Traffic Routing symbol can be protected. The page is opened with this interface preselected, see Section 11.64 on page 243.
- **SCNP (right)** — This symbol is displayed when the E1 to the right of the Traffic Routing symbol is protected. The two unprotected E1s are displayed to the right and the protected to the left. The symbol also illustrates the currently active interface.

  The switch mode is stated as Automatic or Manual including Hold-Off time in seconds.

  Clicking the symbol opens the **Modify 1+1 E1 SNCP** page where the protection can be modified or deleted, see Section 11.67 on page 248.
- **Reload** — Reloads the page with the latest information.
- **Close** — Closes the E1 Overview page.

See Also

- How to work with E1 Overview, see Section 6.9 on page 83.

11.54 User Input Configuration

This page is used to configure a User Input port.

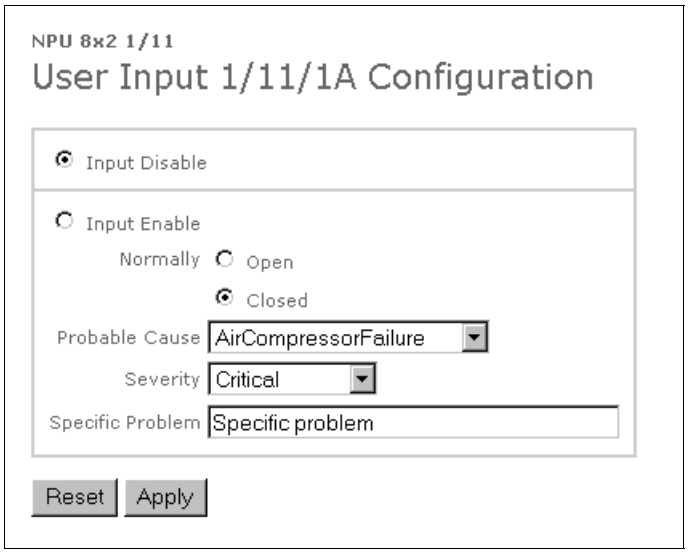


Figure 98 The User Input Configuration page

- **Input Disable** — The port is not used.
- **Input Enable** — The port is used.
  - **Normally Open** — The normal state of the port is open (active low).
  - **Normally Closed** — The normal state of the port is closed (active high).
  - **Probable Cause** — Specifies a probable cause of the alarm. The probable cause can be an environmental alarm or indeterminate.
  - **Severity** — Specifies the alarm severity. See also Section 7.2.4 on page 117.
  - **Specific Problem** — Specifies a detailed description of the alarm. Maximum 80 characters are allowed.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.

11.55 User Output Configuration

This page is used to configure a User Output port.

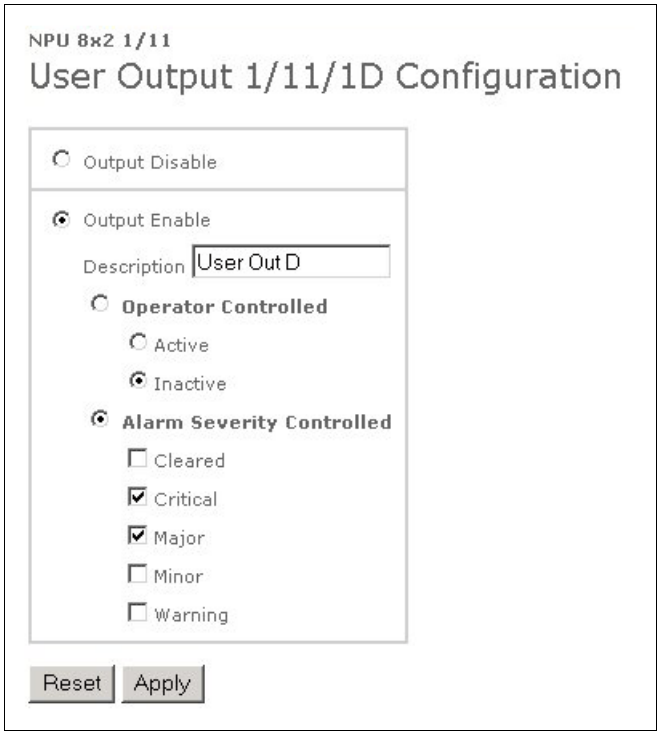


Figure 99 The User Output Configuration page

- **Output Disable** — The port is not used.
- **Output Enable** — The port is used.
  - **Description** — A name of the port that indicates its purpose. Maximum 16 characters are allowed.
  - **Operator Controlled** — The port is controlled on request from an operator.
    - **Active** — Sets the port in active (not normal) state.
    - **Inactive** — Sets the port in inactive (normal) state.
  - **Alarm Severity Controlled** — The port is automatically set in active (not normal) state, triggered by one or several alarm severities.
    - **Cleared/Critical/Major/Minor/Warning** — The severity or severities which set the port in active state.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.

11.56 Traffic Routing Select Interfaces

This page is used to select interfaces for creation or modification of traffic routing. Based on the selection, the actual configuration is made from either of two separate pages with different views.

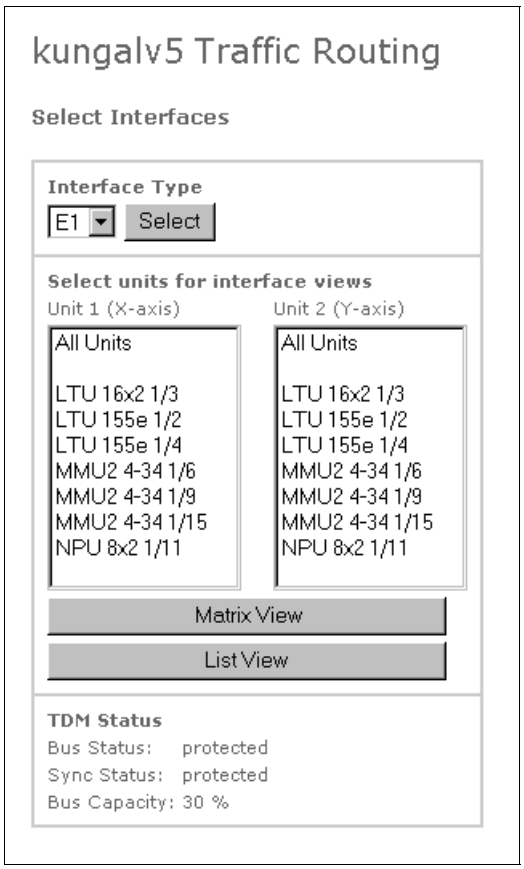


Figure 100 The Traffic Routing Select Interfaces page

- **Interface Type** — The available interface types.

  Note: This version of EEM allows only selection of E1.

- **Select** — Submits the selected interface type.
- **Select units for interface views** — Select the units from the two lists that hold the interfaces to be included in the traffic routing. Unit 1 and Unit 2 can be the same unit.
- **Matrix View** — Opens the **Traffic Routing Matrix View** page, displaying the selected interfaces in a matrix, see Section 11.57 on page 232.

  Note: It is not possible to display use Matrix View for All Units since each axis in the matrix can only show one unit.

- **List View** — Opens the **Traffic Routing List View** page, displaying the selected interfaces in a list, see Section 11.58 on page 234.

- **TDM Status** — Information about the TDM busses used for traffic routing. Fault tolerance is realized by a redundant TDM bus architecture where three busses provide a switching capacity of two busses. The third bus can be used for switching if one of the other busses fails.
  - **Bus Status** — Possible values are: `protected`, `not protected` and `failure`.
  - **Sync Status** — Possible values are: `protected`, `not protected` and `failure`.
  - **Bus Capacity** — A value in percent indicating how much of the available TDM bus capacity that is currently used.

See Also

- How to create traffic routing of E1 interfaces using the Matrix View, see Section 6.8.1.1 on page 80.
- How to create traffic routing of E1 interfaces using the List View, see Section 6.8.1.2 on page 80.

11.57 Traffic Routing Matrix View

This page is used to display, create, modify or delete traffic routing. It contains a matrix with the interfaces on two axes. An intersection point between two interfaces in the matrix is used to handle a certain traffic routing.

Note: If MINI-LINK Connexion is used to provision end-to-end E1 connections, then only use the EEM to *view* current connections. Creating, modifying, and deleting E1 connections shall in this case be done with MINI-LINK Connexion.

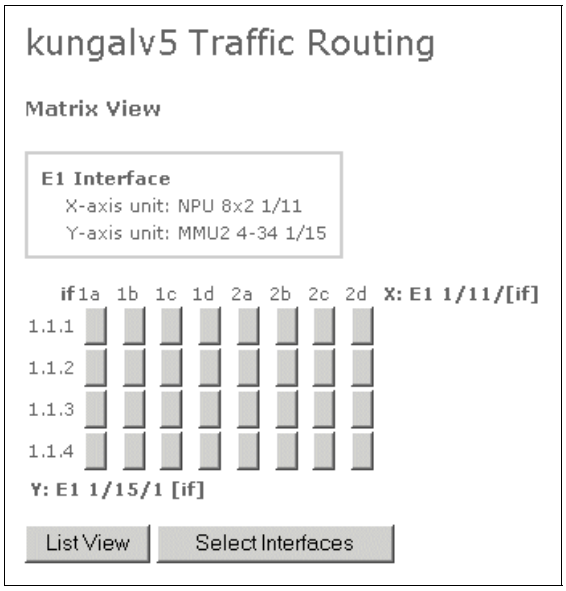


Figure 101 The Traffic Routing Matrix View page

Note: The interfaces on an MMU2 in a protected (1+1) Radio Terminal are denoted in accordance with the SMU2.

- **E1 Interface** — Displays the selected units.
  - **X-axis unit** — The name of the unit on the X-axis.
  - **Y-axis unit** — The name of the unit on the Y-axis.
- **Interface Matrix** — Each column and row in the matrix is labelled with an interface name. If the interface is included in a traffic routing and/or a 1+1 E1 SNCP protection the interface name is a link to the **E1 Overview page** page, see Section 11.53 on page 226. An intersection point in the matrix has a different appearance depending on the current status of the interface pair.
  - **Blank button** — There is no traffic routing between the interfaces but it is possible to create one. Clicking the button creates a nameless traffic routing.
  - **X button** — There is an existing traffic routing between the interfaces. Clicking the button opens the **Modify Traffic Routing** page, see Section 11.61 on page 238.

  - **Blank space** — It is not possible to create a traffic routing between the interfaces. A blank row or column indicates that the interface is routed to an interface not visible on the page. To see the interface, click the link on the interface name on the axis.

    If the same unit is selected for both the X-axis and the Y-axis all intersection points representing the same interface on both axes are blank, since an interface cannot be routed to itself.
  - **Horizontal line** — The interface labelling the row is routed to an interface on the X-axis. The line ends at an X button in the column labelled by the other interface.
  - **Vertical line** — The interface labelling the column is routed to an interface on the Y-axis. The line ends at an X button on the row labelled by the other interface.
  - **Interface interval link** 1.1.1-1.6.2 — Controls the displayed interface interval on the axis. The currently active interval is highlighted with bold text. Only displayed if the unit on an axis has more interfaces than will fit in the page.
- **List View** — Opens the **Traffic Routing List View** page for the selected interfaces, see Section 11.58 on page 234.
- **Select Interfaces** — Opens the **Traffic Routing Select Interfaces** page, see Section 11.56 on page 230.

See Also

- How to create traffic routing of E1 interfaces using the Matrix View, see Section 6.8.1.1 on page 80.

11.58 Traffic Routing List View

This page is used to display, create, modify or delete traffic routing.

Note: If MINI-LINK Connexion is used to provision end-to-end E1 connections, then only use the EEM to *view* current connections. Creating, modifying, and deleting E1 connections shall in this case be done with MINI-LINK Connexion.

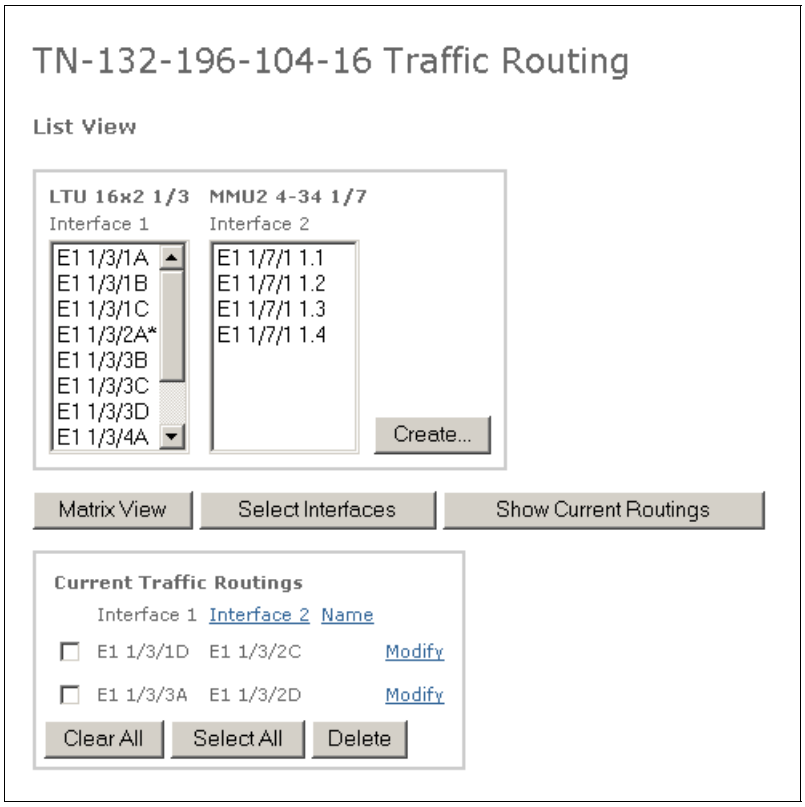


Figure 102 The Traffic Routing List View page

Note: The interfaces on an MMU2 in a protected (1+1) Radio Terminal are denoted in accordance with the SMU2.

- **<Unit 1>** — The name of the selected unit or All Units is displayed above the left list.
  - **Interface 1** — Displays the available interfaces. Select one or multiple items in the list. When selecting multiple items, the topmost selected interfaces in the two lists will form one interface pair and so on. Use CTRL or SHIFT to select multiple items.

    When this page is reached by clicking **Create** on the **Modify 1+1 E1 SNCP** page, the protected interface is the only available option.
- **<Unit 2>** — The name of the selected unit or All Units is displayed above the right list.

  - **Interface 2** — Displays the available interfaces. Select one or multiple items in the list. Use CTRL or SHIFT to select multiple items.

    When this page is reached by clicking **Create** on the **Modify 1+1 E1 SNCP** page, all available interfaces will be presented.
- **Create** — Opens the **Create Traffic Routing** or **Create Multiple Traffic Routing** pages depending on the number of selected items, see Section 11.59 on page 236 and Section 11.60 on page 237.
- **Matrix View** — Opens the **Traffic Routing Matrix View** page, see Section 11.57 on page 232.
- **Select Interfaces** — Opens the **Traffic Routing Select Interfaces** page, where interface type and units are selected, see Section 11.56 on page 230.
- **Show Current Routings** — Displays the **Current Traffic Routings** list below.
- **Current Traffic Routings** — All existing traffic routings that involve the items in the lists. Clicking the link in a column header sorts the list according to the items in that column and removes the link in the header.
  - **Interface 1** — The name of interface 1.
  - **Interface 2** — The name of interface 2.
  - **Name** — The name of the traffic routing.
  - **Modify** — Opens the **Modify Traffic Routing** page, where the traffic routing can be modified or deleted, see Section 11.61 on page 238.
- **Clear All** — Clears all check boxes.
- **Select All** — Selects all check boxes.
- **Delete** — Deletes the selected traffic routings.
- **Back** — Returns to the **Modify 1+1 E1 SNCP** page, see Section 11.67 on page 248. Only available when this page is reached from the **Modify 1+1 E1 SNCP** page.

See Also

- How to create traffic routing of E1 interfaces using the List View, see Section 6.8.1.2 on page 80.

11.59 Create Traffic Routing

This page is used to create traffic routing for one interface pair.

Note: If MINI-LINK Connexion is used to provision end-to-end E1 connections, then only use the EEM to *view* current connections. Creating, modifying, and deleting E1 connections shall in this case be done with MINI-LINK Connexion.

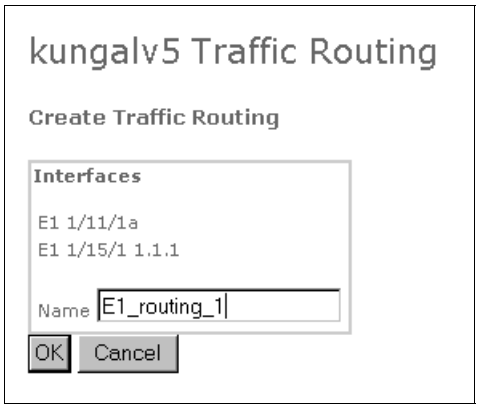


Figure 103 The Create Traffic Routing page

- **Interfaces** — The interfaces in the traffic routing.
- **Name** — The name of the traffic routing.
- **OK** — Creates the traffic routing and returns to the **Traffic Routing List View** page, see Section 11.58 on page 234.
- **Apply** — Creates the traffic routing without leaving the page. Only available when this page is opened from the **E1 Overview** page.
- **Cancel** — Closes the page without creating any traffic routing and returns to the **Traffic Routing List View** page, see Section 11.58 on page 234.

See Also

- How to create traffic routing of E1 interfaces using the List View, see Section 6.8.2.2 on page 82.

11.60 Create Multiple Traffic Routings

This page is used to create traffic routing for several interface pairs simultaneously.

Note: If MINI-LINK Connexion is used to provision end-to-end E1 connections, then only use the EEM to *view* current connections. Creating, modifying, and deleting E1 connections shall in this case be done with MINI-LINK Connexion.

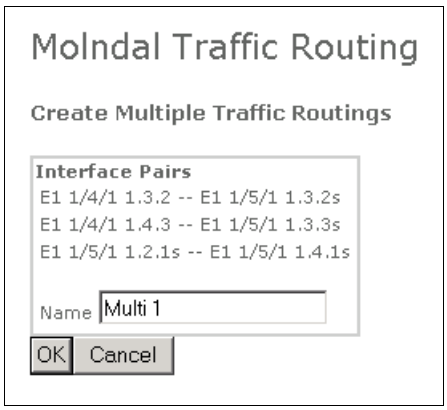


Figure 104 The Create Multiple Traffic Routings page

- **Interface Pairs** — The interface pairs in the traffic routings.
- **Name** — Specifies a common name for all traffic routings. An individual name can be set later by modifying an existing traffic routing.
- **OK** — Creates the traffic routings and returns to the **Traffic Routing List View** page, see Section 11.58 on page 234.
- **Cancel** — Closes the page without creating any traffic routings and returns to the **Traffic Routing List View** page, see Section 11.58 on page 234.

See Also

- How to create traffic routing of E1 interfaces using the List View, see Section 6.8.1.2 on page 80.

11.61 Modify Traffic Routing

This page is used to modify or delete an existing traffic routing.

Note: If MINI-LINK Connexion is used to provision end-to-end E1 connections, then only use the EEM to *view* current connections. Creating, modifying, and deleting E1 connections shall in this case be done with MINI-LINK Connexion.

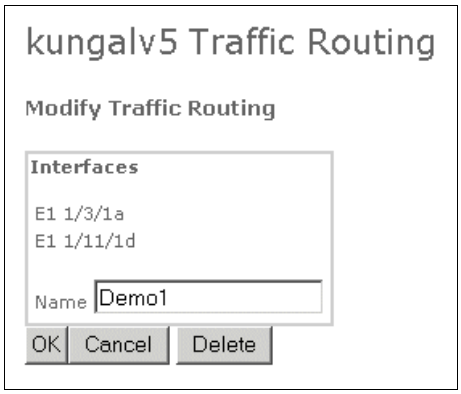


Figure 105 The Modify Traffic Routing page

- **Interfaces** — The interfaces in the traffic routing.
- **Name** — Specifies the name of the traffic routing.
- **OK** — Updates the traffic routing and returns to the page where this page was opened.
- **Apply** — Modifies the traffic routing without leaving the page. Only available when this page is opened from the **E1 Overview** page.
- **Cancel** — Closes the page without modifying the traffic routing and returns to the page where this page was opened.
- **Delete** — Deletes the traffic routing and returns to the page where this page was opened.

See Also

- How to modify or delete traffic routing of E1 interfaces using the Matrix View, see Section 6.8.2.1 on page 81.
- How to modify or delete traffic routing of E1 interfaces using the List View, see Section 6.8.2.2 on page 82.

11.62 1+1 E1 SNCP Select Interfaces

This page is used to select interfaces for creation or modification of 1+1 E1 SNCP protection. Based on the selection, the actual configuration is made from either of two separate pages with different views.

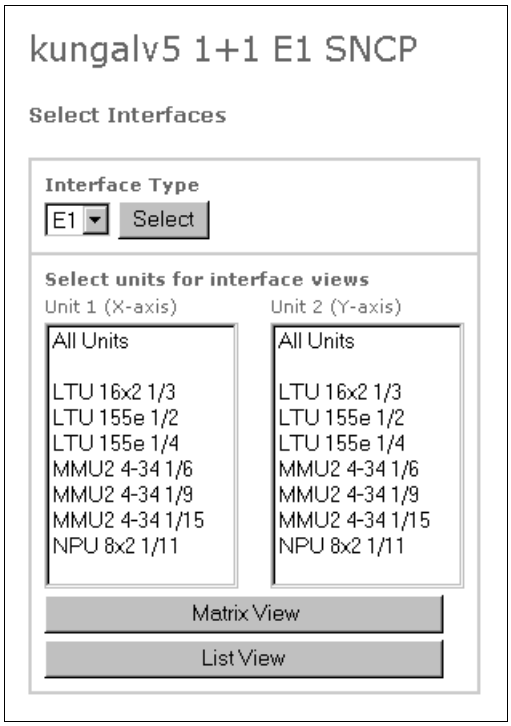


Figure 106 The 1+1 E1 SNCP Select Interfaces page

- **Interface Type** — The available interface type.

  Note: This version of EEM allows only selection of E1.

- **Select** — Submits the selected interface type.
- **Select units for interface views:** — Select the units from the two lists that hold the interfaces to be included in the protection(s). Unit 1 and Unit 2 can be the same unit.
- **Matrix View** — Opens the **1+1 E1 SNCP Matrix View** page, displaying the selected interfaces in a matrix, see Section 11.63 on page 241.

  Note: It is not possible to display a Matrix View if All Units is selected since each axis in the matrix can only show one unit.

- **List View** — Opens the **1+1 E1 SNCP List View** page, displaying the selected interfaces in a list, see Section 11.64 on page 243.

See Also

- How to create 1+1 E1 SNCP protection for E1 interfaces using the Matrix View, see Section 6.6.1.1 on page 70.

- How to create 1+1 E1 SNCP protection for E1 interfaces using the List View, see Section 6.6.1.2 on page 72.

11.63 1+1 E1 SNCP Matrix View

This page is used to display, create, modify or delete 1+1 E1 SNCP protection. It contains a matrix with the interfaces of the two selected units. An intersection point between two interfaces in the matrix is used to handle a certain protection.

Note: If MINI-LINK Connexion is used to provision end-to-end E1 connections, then only use the EEM to *view* current connections. Creating, modifying, and deleting E1 connections shall in this case be done with MINI-LINK Connexion.

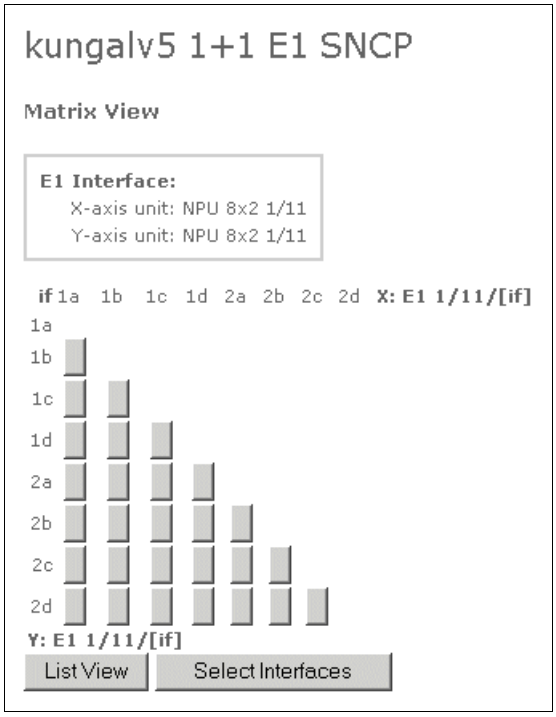


Figure 107 The 1+1 E1 SNCP Matrix View page

Note: The interfaces on an MMU2 in a protected (1+1) Radio Terminal are denoted in accordance with the SMU2.

- **E1 Interface** — Displays the names of the selected units.
  - **X-axis unit** — The name of the unit on the X-axis.
  - **Y-axis unit** — The name of the unit on the Y-axis.
- **Interface Matrix** — Each column and row in the matrix is labelled with an interface name. If the interface is included in a traffic routing and/or a 1+1 E1 SNCP protection the interface name is a link to the **E1 Overview** page, see Section 11.53 on page 226. An intersection point in the matrix has different appearance depending on the current status of the of the interface pair.
  - **Blank button** — No 1+1 E1 SNCP protection exists but it is possible to create one with default settings by clicking the button.

  - **P button**  — There is an existing 1+1 E1 SNCP protection. Clicking the button opens the **Modify 1+1 E1 SNCP** page, where the settings for the protection can be changed, see Section 11.67 on page 248.
  - **Blank space** — It is not possible to create a 1+1 E1 SNCP protection. A blank row or column indicates that the interface is protected with an interface not visible on the page. To see the interface, click the link on the interface name on the axis.

    A blank space can also indicate that both interfaces are traffic routed. Then it is not possible to use them in the same 1+1 E1 SNCP protection.

    If the same unit is selected for both the X-axis and the Y-axis all intersection points representing the same interface on both axes are blank, since an interface cannot be protected with itself.
  - **Horizontal line** — The interface labelling the row is protected with an interface on the X-axis unit. The line ends at a P button in the column labelled by the other interface.
  - **Vertical line** — The interface labelling the column is protected with an interface on the Y-axis unit. The line ends at a P button on the row labelled by the other interface.
  - **Interface interval link** 1.1.1-1.6.2 — Controls the displayed interface interval on the axis. The currently active interval is highlighted with bold text. Only available if the unit on an axis has more interfaces than will fit in the page.
- **List View** — Opens the **1+1 E1 SNCP List View** page for the selected units, see Section 11.64 on page 243.
- **Select Interfaces** — Opens the **1+1 E1 SNCP Select Interfaces** page, see Section 11.62 on page 239.

See Also

- How to create 1+1 E1 SNCP protection for E1 interfaces using the Matrix View, see Section 6.6.1.1 on page 70.

11.64 1+1 E1 SNCP List View

This page is used to display, create, modify or delete 1+1 E1 SNCP protection.

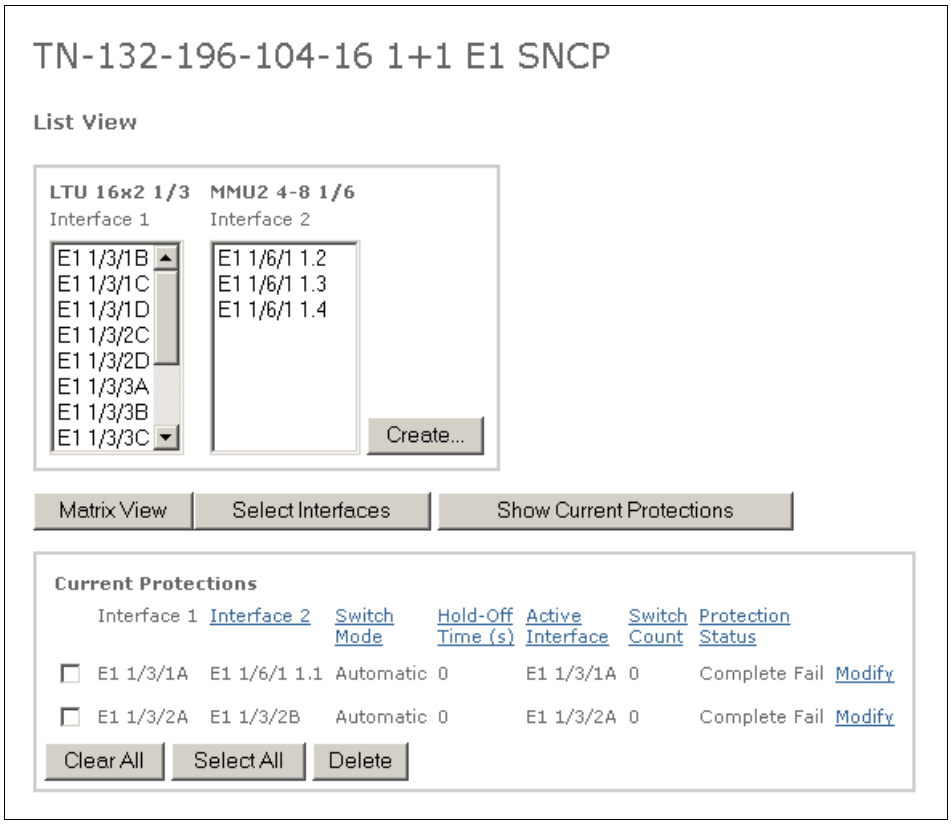


Figure 108 1+1 E1 SNCP List View page

Note: The interfaces on an MMU2 in a protected (1+1) Radio Terminal are denoted in accordance with the SMU2.

- **<Unit 1>** — The name of the selected unit or All Units is displayed above the left list.
  - **Interface 1** — Displays the available interfaces. Select one or multiple items in the list. When selecting multiple items, the topmost selected interfaces in the two lists will form one interface pair and so on. Use CTRL or SHIFT to select multiple items.
- **<Unit 2>** — The name of the selected unit or All Units is displayed above the right list.
  - **Interface 2** — Displays the available interfaces. Select one or multiple items in the list. Use CTRL or SHIFT to select multiple items.
- **Create** — Opens the **Create 1+1 E1 SNCP** or **Create Multiple 1+1 E1 SNCP** pages depending on the number of selected items, see Section 11.65 on page 245 and Section 11.66 on page 247.
- **Matrix View** — Opens the **1+1 E1 SNCP Matrix View** page, see Section 11.63 on page 241.

- **Select Interfaces** — Opens the **1+1 E1 SNCP Select Interfaces** page, see Section 11.62 on page 239.
- **Show Current Protections** — Displays the **Current Protections** list below.
- **Current Protections** — All existing protections that involve the interfaces in the lists. Clicking the link in a column header sorts the list according to the items in that column and removes the link in the header.
  - **Interface 1** — The name of interface 1.
  - **Interface 2** — The name of interface 2.
  - **Switch Mode** — Specifies the way the traffic is switched between the interfaces.
    - **Automatic** — The traffic is automatically switched between the interfaces if a disturbance occurs.
    - **Manual** — An operator has to switch interfaces manually.
  - **Hold-Off Time** — The time in seconds before an interface switch is initiated.
  - **Active Interface** — The name of the currently active interface.
  - **Switch Count** — The number of switches since the last restart.
  - **Protection Status** — The status of the protection.
    - **Fully Protected** — Both interfaces are operating.
    - **Unprotected** — The active interface is operating but the passive interface fails.
    - **Complete Fail** — Both interfaces fail.
    - **Lock To Fail** — The active interface fails but the passive is operating and the switch is locked to the active interface.
    - **Interface Mismatch** — The interfaces on both sides of the network connection are incompatible. This status is set only when this can be detected.
  - **Modify** — Opens the **Modify 1+1 E1 SNCP** page, where the protection can be modified or deleted, see Section 11.67 on page 248.
- **Clear All** — Clears all check boxes.
- **Select All** — Selects all check boxes.
- **Delete** — Deletes the selected traffic routings.

See Also

- How to create 1+1 E1 SNCP protection for E1 interfaces using the List View, see Section 6.6.1.2 on page 72.

11.65 Create 1+1 E1 SNCP

This page is used to create 1+1 E1 SNCP protection for one interface pair.

Note: If MINI-LINK Connexion is used to provision end-to-end E1 connections, then only use the EEM to *view* current connections. Creating, modifying, and deleting E1 connections shall in this case be done with MINI-LINK Connexion.

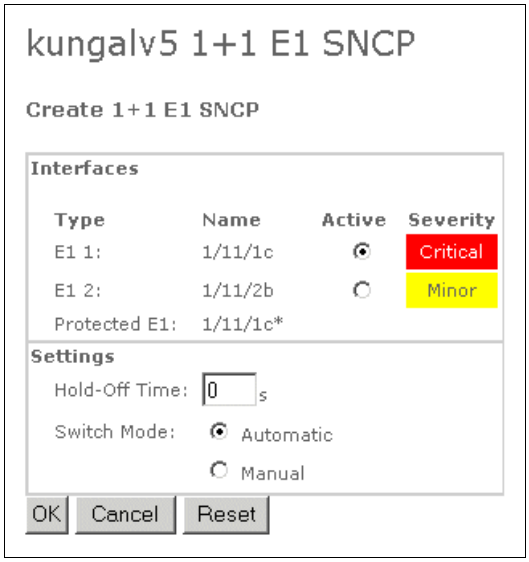


Figure 109 The Create 1+1 E1 SNCP page

- **Interfaces** — Specifies the interfaces in the protection.
  - **Type** — The type or role of the interface in the protection.
    - **E1 1** — One of the interfaces selected for the protection.
    - **E1 2** — The other interface selected for the protection.
    - **Protected E1** — The resulting "virtual" protected interface.
  - **Name** — The name of the interface.

    Note: An asterisk (*) at the end of the name indicates a protected interface.

  - **Active** — The interface to carry traffic.
  - **Severity** — The alarm severity of the interface. See also Section 7.2.4 on page 117.
- **Settings** — Specifies parameters for the protection.
  - **Hold-Off Time** — The time in seconds before an interface switch is initiated. Value range is 0.0 – 10.0.
  - **Switch Mode** — Specifies the way the traffic is switched between the interfaces.
    - **Automatic** — The traffic is automatically switched between the interfaces if a disturbance occurs.
    - **Manual** — An operator has to switch interfaces manually using the **Modify 1+1 E1 SNCP** page, see Section 11.67 on page 248.

- **OK** — Creates the protection and returns to the **1+1 E1 SNCP List View** page, see Section 11.64 on page 243.
- **Apply** — Creates the protection without leaving the page. Only available when this page is opened from the **E1 Overview** page.
- **Cancel** — Closes the page without creating any protection and returns to the **1+1 E1 SNCP List View** page, see Section 11.64 on page 243.
- **Reset** — Resets all settings to their initial values.

See Also

- How to create 1+1 E1 SNCP protection for E1 interfaces using the List View, see Section 6.6.1.2 on page 72.

11.66 Create Multiple 1+1 E1 SNCP

This page is used to create 1+1 E1 SNCP protection for several interface pairs simultaneously.

Note: If MINI-LINK Connexion is used to provision end-to-end E1 connections, then only use the EEM to *view* current connections. Creating, modifying, and deleting E1 connections shall in this case be done with MINI-LINK Connexion.

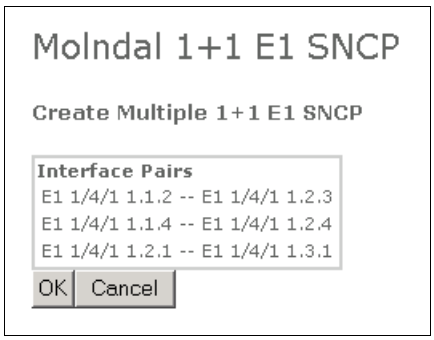


Figure 110 The Create Multiple 1+1 E1 SNCP page

- **Interface Pairs** — The names of the interfaces in the protections.
- **OK** — Creates the protections with default settings and returns to the **1+1 E1 SNCP List View** page, see Section 11.64 on page 243. The settings can be changed later by modifying an existing protection.
- **Cancel** — Closes the page without creating any protections and returns to the **1+1 E1 SNCP List View** page, see Section 11.64 on page 243.

See Also

- How to create 1+1 E1 SNCP protection for E1 interfaces using the List View, see Section 6.6.1.2 on page 72.

11.67 Modify 1+1 E1 SNCP

This page is used to modify or delete a 1+1 E1 SNCP protection.

Note: If MINI-LINK Connexion is used to provision end-to-end E1 connections, then only use the EEM to *view* current connections. Creating, modifying, and deleting E1 connections shall in this case be done with MINI-LINK Connexion.

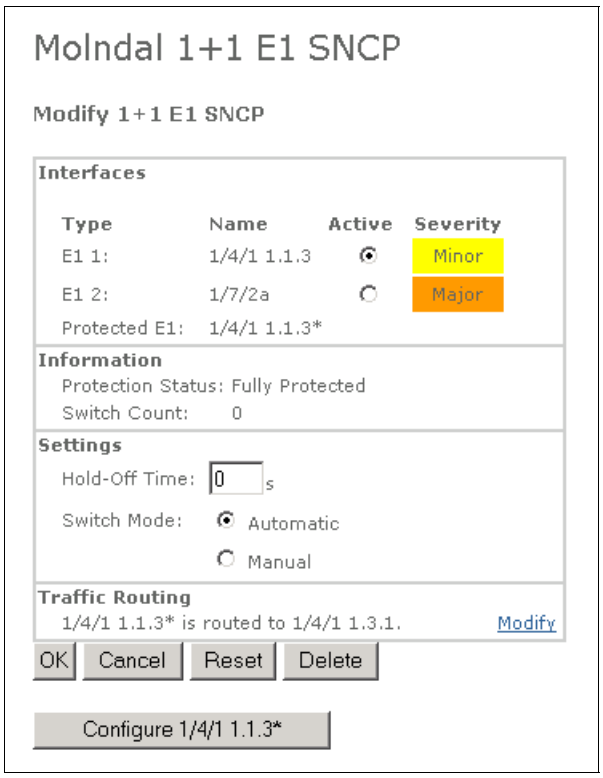


Figure 111 The Modify 1+1 E1 SNCP page

- **Interfaces** — Specifies the interfaces in the protection.
  - **Type** — The type or role of the interface in the protection.
    - **E1 1** — One of the interfaces selected for the protection.
    - **E1 2** — The other interface selected for the protection.
    - **Protected E1** — The resulting "virtual" protected interface.
  - **Name** — The name of the interface.

    Note: An asterisk (*) at the end of the name indicates a protected interface.

  - **Active** — The interface to carry traffic.
  - **Severity** — The alarm severity of the interface. See also Section 7.2.4 on page 117.
- **Information** — Information about the protection.
  - **Protection Status** — The status of the protection.
    - **Fully Protected** — Both interfaces are operating.

        - **Unprotected** — The active interface is operating but the passive interface fails.
        - **Complete Fail** — Both interfaces fail.
        - **Lock To Fail** — The active interface fails but the passive is operating and the switch is locked to the active interface.
        - **Interface Mismatch** — The interfaces on both sides of the network connection are incompatible. This status is set only when this can be detected.
    - **Switch Count** — The number of protection switches since the last restart.
- **Settings** — Specifies protection parameters.
    - **Hold-Off Time** — The time in seconds before an interface switch is initiated. Value range is 0.0 – 10.0.
    - **Switch Mode** — Specifies the way the traffic is switched between the interfaces.
        - **Automatic** — The traffic is automatically switched between the interfaces if a disturbance occurs.
        - **Manual** — An operator has to switch interfaces manually using the **Active** option on this page.
- **Traffic Routing** — Enables traffic routing of the protected interface or a modification of an existing traffic routing.
    - **Create** — Opens the **Traffic Routing List View** page, where the traffic routing is created, see Section 11.58 on page 234.
    - **Modify** — Opens the **Modify Traffic Routing** page, where the traffic routing can be modified or deleted, see Section 11.61 on page 238.
- **OK** — Updates the protection configuration and returns to the page from which this page was opened.
- **Apply** — Modifies the protection routing without leaving the page. Only available when this page is opened from the **E1 Overview** page.
- **Cancel** — Closes the page without changes and returns to the page from which this page was opened.
- **Reset** — Resets all settings to their initial values.
- **Delete** — Deletes the protection and returns to the page from which this page was opened.
- **Configure <Protected E1 Interface>** — Opens the **E1 Configuration** page for the protected interface, see Section 11.51 on page 224.

See Also

- How to modify or delete 1+1 E1 SNCP protection using the Matrix View, see Section 6.6.2.1 on page 75.
- How to modify or delete 1+1 E1 SNCP protection using the List View, see Section 6.6.2.2 on page 77.

11.68 Create MSP Protection

This page is used to create MSP protection including two adjacent LTU 155s.

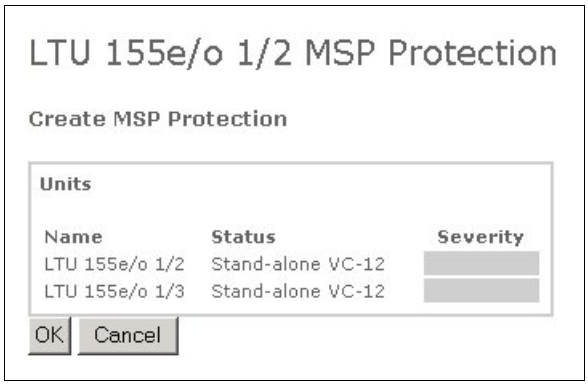


Figure 112 The Create MSP Protection page

Note: The page is only displayed when the units are not included in an MSP protection.

Note: The two LTU 155s have to be placed in adjacent AMM positions according to specifications in *MINI-LINK TN ETSI Indoor Installation Manual*.

Note: Creating MSP protection will remove the existing traffic routings on the LTU 155.

- **Units** — Information about the two adjacent LTU 155s.
  - **Name** — The name of the unit.
  - **Status** — The status of the unit's STM-1 port.
    - **Not Configured** — The port does not provide traffic until it is configured.
    - **Stand-alone VC-12** — The port has 63 E1 interfaces and operates alone.
  - **Severity** — The severity for the unit. See also Section 7.2.4 on page 117.
- **OK** — Starts the MSP creation process and opens the **Creating Protection** page, see Section 11.69 on page 251.
- **Cancel** — Closes the page without creating any MSP protection and returns to the page where this page was opened.

See Also

- How to create MSP protection, see Section 6.5.1 on page 68.

11.69 Creating Protection

This page displays the progress of an ongoing creation of MSP protection. It is automatically refreshed every fifth second to give an up-to-date status of the progress. When both units are ready this page is replaced by the **Modify MSP Protection** page, see Section 11.70 on page 252.

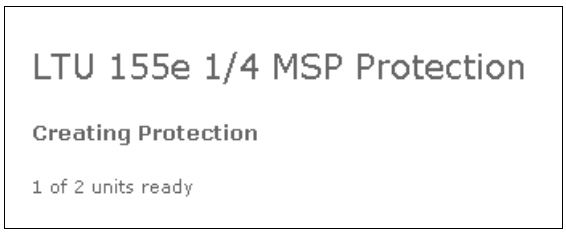


Figure 113 The Creating Protection page

- **0 of 2 units ready/1 of 2 units ready** — The progress of the MSP protection creation process.

See Also

- How to create MSP protection, see Section 6.5.1 on page 68.

11.70 Modify MSP Protection

This page is used to modify or delete an existing MSP protection.

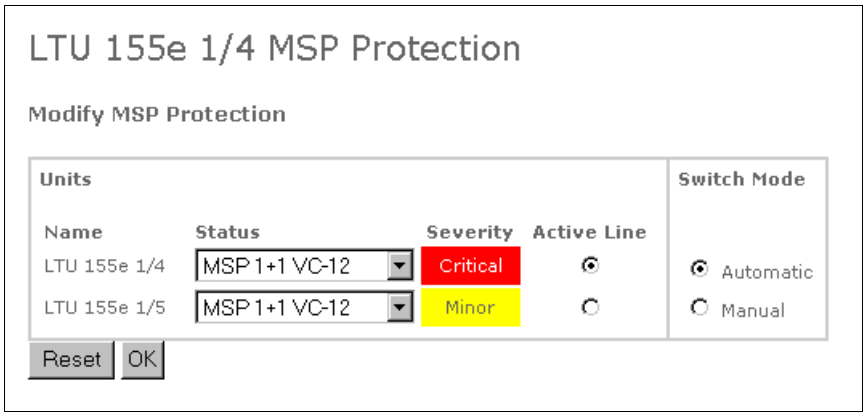


Figure 114 The Modify MSP Protection page

- **Units** — Specifies information about two adjacent LTU 155s.
  - **Name** — The name of the unit.
  - **Status** — The status of the unit's STM-1 port.
    - **Not Configured** — The port does not provide traffic until it is configured.
    - **MSP 1+1 VC-12** — The unit is protected sharing 63 E1 interfaces with its adjacent unit. The unit with the currently active line is the one carrying traffic. This is the status both units in the MSP protection will always have when this page is displayed.

Caution!

If the status is changed from `MSP 1+1 VC-12` for either of the units the MSP protection will be deleted and the **Deleting Protection** page will be displayed, see Section 11.71 on page 254.

  - **Severity** — The severity for the unit. See also Section 7.2.4 on page 117.
  - **Active Line** — The unit with the line interface that should carry traffic in the receive direction. If the selected unit has alarms it will not be used as the active line.
- **Switch Mode** — Specifies how the active line should be switched when a failure occurs on the unit with the currently active line.
  - **Automatic** — A switch is made when a failure occurs on the unit with the active line or when you change the active line.
  - **Manual** — A switch is only made when you change the active line.
- **Reset** — Reloads the page with its initial values.
- **OK** — Updates the MSP configuration.

See Also

- How to modify MSP protection, see Section 6.5.2 on page 69.

11.71 Deleting Protection

This page displays the progress of an ongoing deletion of MSP protection. It is automatically refreshed every fifth second to give an up-to-date status of the progress. When both units are ready this page is replaced by the **Create MSP Protection** page, see Section 11.68 on page 250.

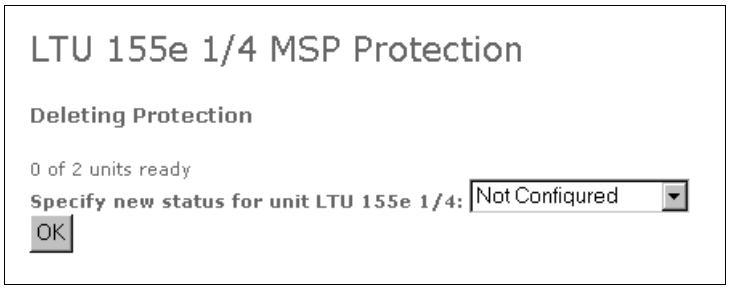


Figure 115 The Deleting Protection page

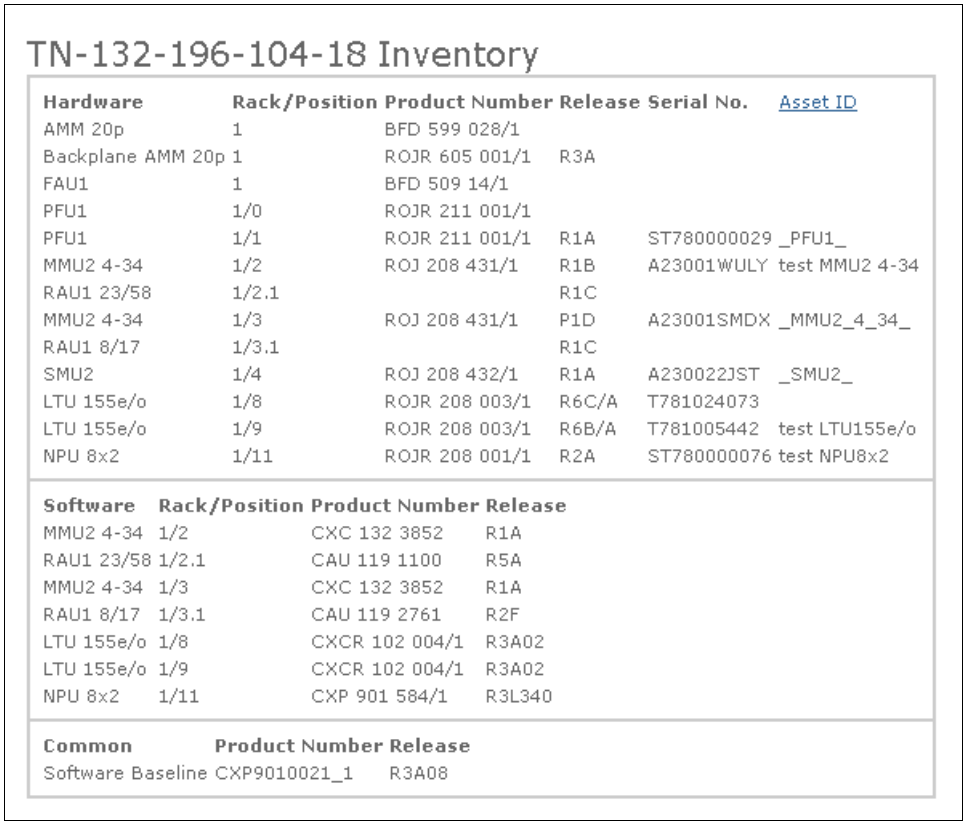
- **0 of 2 units ready/1 of 2 units ready** — The progress of the MSP protection deletion process.
- **Specify new status for unit** — Re-specifies the desired status of the second unit's STM-1 port in the MSP protection. This list and the **OK** button will appear only if you leave the page and later on re-enter it by clicking the **MSP Protection** link on the **LTU 155 Configuration** page, see Section 11.33 on page 194. In this case the NE has lost the information about the selected status of the second unit and you have to specify it again.
  - **Not Configured** — The port does not provide traffic until it is configured.
- **OK** — Submits the specified status.

See Also

- How to delete MSP protection, see Section 6.5.3 on page 69.

11.72 Inventory

This page displays hardware and software information about the NE. Units without software modules will not be present in the software table.



TN-132-196-104-18 Inventory

Hardware	Rack/Position	Product Number	Release	Serial No.	Asset ID
AMM 20p	1	BFD 599 028/1			
Backplane AMM 20p	1	ROJR 605 001/1	R3A		
FAU1	1	BFD 509 14/1			
PFU1	1/0	ROJR 211 001/1			
PFU1	1/1	ROJR 211 001/1	R1A	ST780000029	_PFU1_
MMU2 4-34	1/2	ROJ 208 431/1	R1B	A23001WULY	test MMU2 4-34
RAU1 23/58	1/2.1		R1C		
MMU2 4-34	1/3	ROJ 208 431/1	P1D	A23001SMDX	_MMU2_4_34_
RAU1 8/17	1/3.1		R1C		
SMU2	1/4	ROJ 208 432/1	R1A	A230022JST	_SMU2_
LTU 155e/o	1/8	ROJR 208 003/1	R6C/A	T781024073	
LTU 155e/o	1/9	ROJR 208 003/1	R6B/A	T781005442	test LTU155e/o
NPU 8x2	1/11	ROJR 208 001/1	R2A	ST780000076	test NPU8x2

Software	Rack/Position	Product Number	Release
MMU2 4-34	1/2	CXC 132 3852	R1A
RAU1 23/58	1/2.1	CAU 119 1100	R5A
MMU2 4-34	1/3	CXC 132 3852	R1A
RAU1 8/17	1/3.1	CAU 119 2761	R2F
LTU 155e/o	1/8	CXCR 102 004/1	R3A02
LTU 155e/o	1/9	CXCR 102 004/1	R3A02
NPU 8x2	1/11	CXP 901 584/1	R3L340

Common	Product Number	Release
Software Baseline	CXP9010021_1	R3A08

Figure 116 The Inventory page

- **Hardware** — The name of the hardware unit.
  - **Rack/Position** — The rack and position number.
  - **Product Number** — The product number of the hardware unit.
  - **Release** — The release state of the hardware unit.
  - **Serial No.** — The serial number of the hardware unit.
  - **Asset ID** — A user specified identity of the hardware unit. Clicking the link opens the **Edit Asset ID** page, see Section 11.73 on page 256.
- **Software** — The name of the hardware unit containing a software module.
  - **Rack/Position** — The rack and position number.
  - **Product Number** — The product number of the software module.
  - **Release** — The release state of the software module.
- **Common** — Information about the software baseline. If version control is disabled, N/A will be displayed.
  - **Product Number** — The product number of the baseline.
  - **Release** — The release state of the baseline.

11.73 Edit Asset ID

This page is used to specify identities of indoor hardware units.

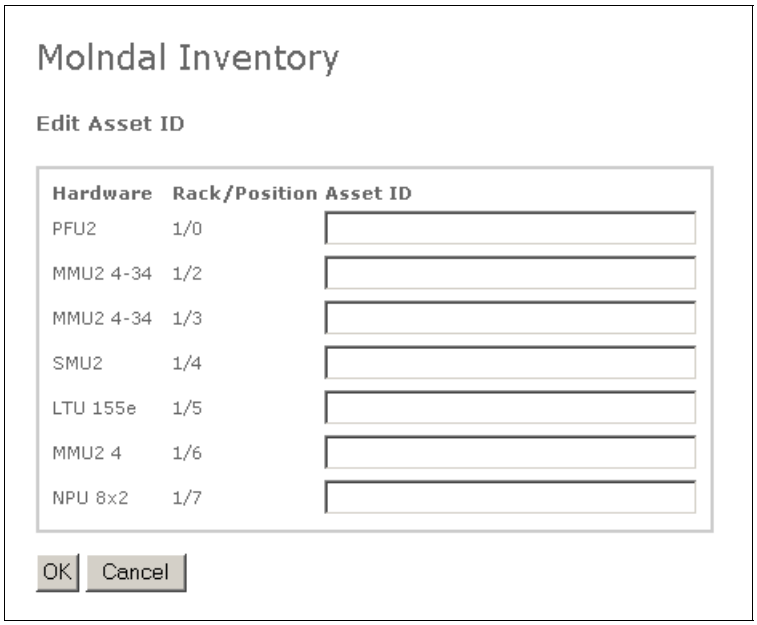


Figure 117 The Edit Asset ID page

- **Hardware** — The name of the unit.
- **Rack/Position** — The rack and position number.
- **Asset ID** — A user specified identity of the unit.
- **OK** — Saves and returns to the **Inventory** page, see Section 11.72 on page 255.
- **Cancel** — Closes the page without saving and returns to the **Inventory** page, see Section 11.72 on page 255.

11.74 Report

This page is used to generate a report of the configuration and inventory data of the NE. Select the check boxes for the items to be included in the configuration report. The contents of the report are further described in Section 11.75 on page 258.

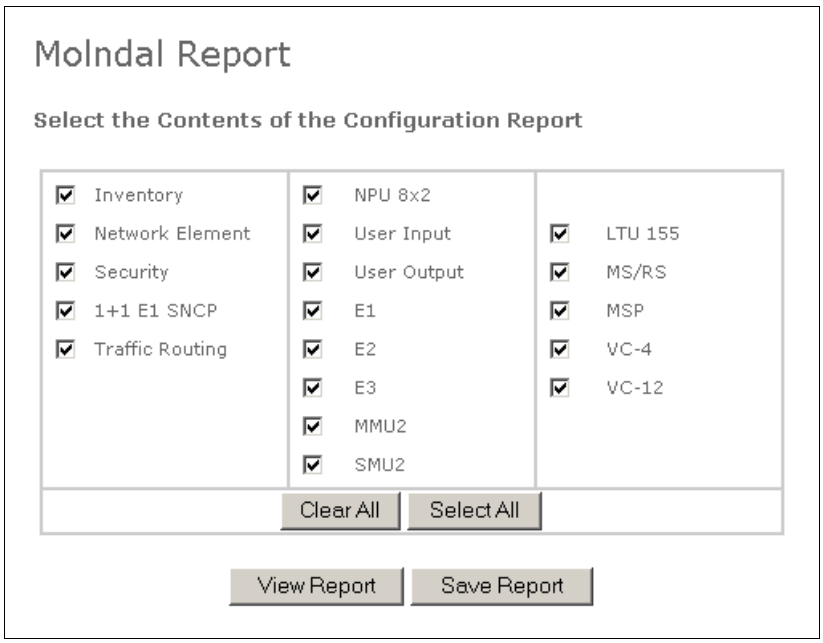
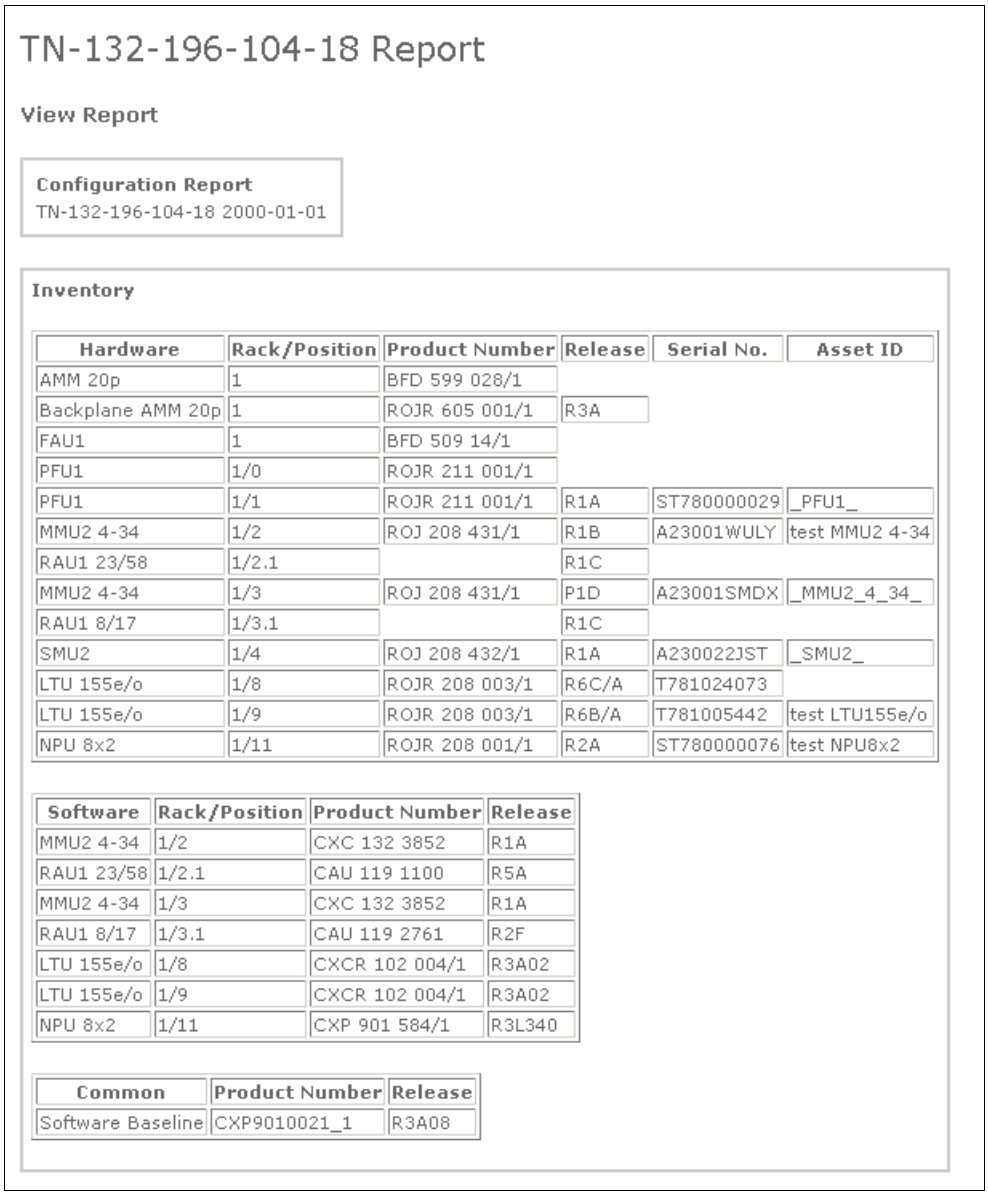


Figure 118 The Report page

- **Clear All** — Clears all check boxes.
- **Select All** — Selects all check boxes.
- **View Report** — Generates the report.
- **Save Report** — Saves the report to a file. The format of the file is HTML 4 and it can be opened in a number of different applications such as Microsoft Excel and Microsoft Word.

11.75 View Report

This page displays a configuration and inventory report. References are provided to help texts for the different parts of the report.



TN-132-196-104-18 Report

View Report

Configuration Report
TN-132-196-104-18 2000-01-01

Inventory

Hardware	Rack/Position	Product Number	Release	Serial No.	Asset ID
AMM 20p	1	BFD 599 028/1			
Backplane AMM 20p	1	ROJR 605 001/1	R3A		
FAU1	1	BFD 509 14/1			
PFU1	1/0	ROJR 211 001/1			
PFU1	1/1	ROJR 211 001/1	R1A	ST780000029	_PFU1_
MMU2 4-34	1/2	ROJ 208 431/1	R1B	A23001WULY	test MMU2 4-34
RAU1 23/58	1/2.1		R1C		
MMU2 4-34	1/3	ROJ 208 431/1	P1D	A23001SMDX	_MMU2_4_34_
RAU1 8/17	1/3.1		R1C		
SMU2	1/4	ROJ 208 432/1	R1A	A230022JST	_SMU2_
LTU 155e/o	1/8	ROJR 208 003/1	R6C/A	T781024073	
LTU 155e/o	1/9	ROJR 208 003/1	R6B/A	T781005442	test LTU155e/o
NPU 8x2	1/11	ROJR 208 001/1	R2A	ST780000076	test NPU8x2

Software	Rack/Position	Product Number	Release
MMU2 4-34	1/2	CXC 132 3852	R1A
RAU1 23/58	1/2.1	CAU 119 1100	R5A
MMU2 4-34	1/3	CXC 132 3852	R1A
RAU1 8/17	1/3.1	CAU 119 2761	R2F
LTU 155e/o	1/8	CXCR 102 004/1	R3A02
LTU 155e/o	1/9	CXCR 102 004/1	R3A02
NPU 8x2	1/11	CXP 901 584/1	R3L340

Common	Product Number	Release
Software Baseline	CXP9010021_1	R3A08

Figure 119 The View Report page. Note that the figure shows only the beginning of the report.

The list below provides references to the pages where the data is set.

- **Inventory** — See Section 11.72 on page 255.
- **Network Element Configuration** — The following configurations on NE level are available.
  - **Basic NE Configuration** — See Section 11.15 on page 172.

  - **Ethernet/LAN/Servers Configuration** — See Section 11.16 on page 174.
  - **PPP Configuration** — See Section 11.18 on page 177.
  - **Static Routing Configuration** — See Section 11.19 on page 179.
  - **OSPF Area Configuration** — See Section 11.21 on page 181.
- **Security** — See Section 11.151 on page 380.
- **1+1 E1 SNCP Protection** — See Section 11.64 on page 243.
- **Traffic Routing** — See Section 11.58 on page 234.
- **NPU1 B Configuration** — See Section 11.27 on page 188.
- **NPU 8x2 Configuration** — See Section 11.28 on page 189.
- **NPU2/ATU NPU Configuration** — See Section 11.29 on page 190.
- **User Input Configuration** — See Section 11.54 on page 228.
- **User Output Configuration** — See Section 11.55 on page 229.
- **E3 Configuration** — See Section 11.49 on page 222.
- **E2 Configuration** — See Section 11.50 on page 223.
- **E1 Configuration** — See Section 11.51 on page 224.
- **MMU2 Configuration** — See Section 11.34 on page 196.
- **SMU2 Configuration** — See Section 11.35 on page 198.
- **MMU2 B/C Configuration** — See Section 11.36 on page 201.
- **RAU IF Configuration** — See Section 11.37 on page 203.
- **RAU Configuration** — See Section 11.38 on page 204.
- **RF Configuration** — See Section 11.39 on page 207.
- **SWITCH Configuration** — See Section 11.42 on page 210.
- **SWITCH Protection** — See Section 11.43 on page 211.
- **LTU 16x2 Configuration** — See Section 11.32 on page 193.
- **LTU 12x2 Configuration** — See Section 11.31 on page 192.
- **LTU 155 Configuration** — See Section 11.33 on page 194.
- **MSP Protection** — See Section 11.70 on page 252.
- **MS/RS Configuration** — See Section 11.44 on page 213.
- **MSP Configuration** — See Section 11.45 on page 215.
- **VC-4 Configuration** — See Section 11.46 on page 216.
- **VC-12 Configuration** — See Section 11.47 on page 218.
- **Ethernet Bridge Configuration** — See Section 11.30 on page 191.
- **Bridge Configuration** — See Section 11.17 on page 176.
- **Back** — Navigates one step backward in the wizard. Only available in the installation wizard.
- **Next** — Navigates one step forward in the wizard. Only available in the installation wizard.

11.76 Upgrade of Baseline

This page is the start page of a wizard providing a software upgrade to a desired baseline of load modules, defined in a Software Baseline Description File (SBDF).

Note: MMU2 and SMU2 (protection) are upgraded using MSM, Local Upgrade or MINI-LINK Manager.

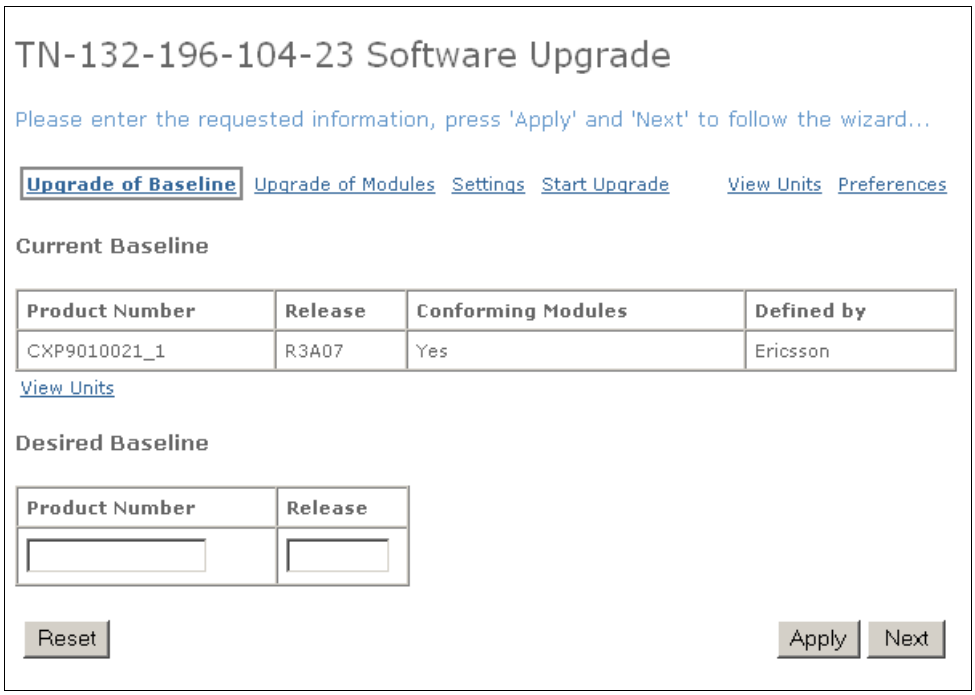


Figure 120 The Upgrade Baseline page

- **Current Baseline** — Information about the current baseline. If version control is disabled, N/A will be displayed.
  - **Product Number** — The product number of the current baseline.
  - **Release** — The release state (version) of the current baseline.
  - **Conforming Modules** — Displays if the current software configuration is compliant with the current baseline.
  - **Defined by** — Displays if the baseline is defined by Ericsson or not.
  - **View Units** — Opens the **View Units** page showing information about all load modules in the units.
- **Desired Baseline** — Information about the desired baseline.

  Note: The SBDF and the load modules must be stored in specific folders under: `<drive:>\tn_ftp_home\tn_system_release\ml_tn_software`, see Section 3.2.1.2 on page 18.

  - **Product Number** — The product number of the desired baseline.
  - **Release** — The release state (version) of the desired baseline.
- **Reset** — Resets all settings to their initial values.

- **Apply** — Applies all changes you have made without leaving the page.
- **Next** — Opens the **Settings** page, see Section 11.78 on page 263.

See Also

- How to perform an upgrade of baseline, see Section 6.12.1 on page 91.

11.77 Upgrade of Modules

This page is the start page of a wizard providing software upgrade of specific load modules.

Note: MMU2 and SMU2 (protection) are upgraded using MSM, Local Upgrade or MINI-LINK Manager.

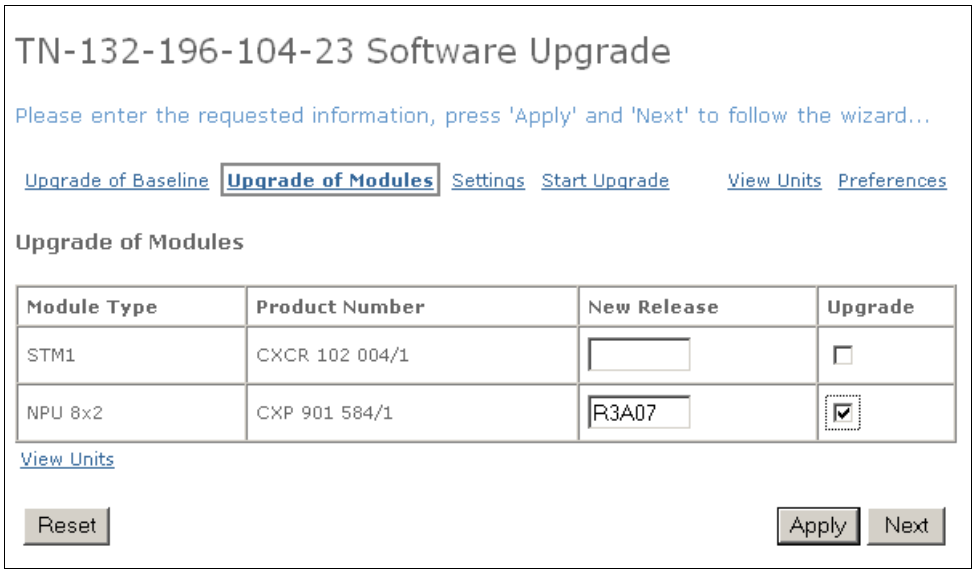


Figure 121 The Upgrade of Modules page

- **Upgrade of Modules** — Specifies which load modules that should be included in the software upgrade.

  Note: The load modules must be stored in specific folders under: `<drive:>\tn_ftp_home\tn_system_release\ml_tn_software`, see Section 3.2.1.2 on page 18.

  - **Module Type** — The name of the load module.
  - **Product Number** — The product number of the load module.
  - **New Release** — The release state (version) of the new load module.
  - **Upgrade** — Select the check box to include the load module in the software upgrade.
  - **View Units** — Opens the **View Units** page showing information about all load modules in the units.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.
- **Next** — Opens the **Settings** page, see Section 11.78 on page 263.

See Also

- How to perform an upgrade of modules, see Section 6.12.2 on page 93.

11.78 Settings

This page is used to define software upgrade settings.

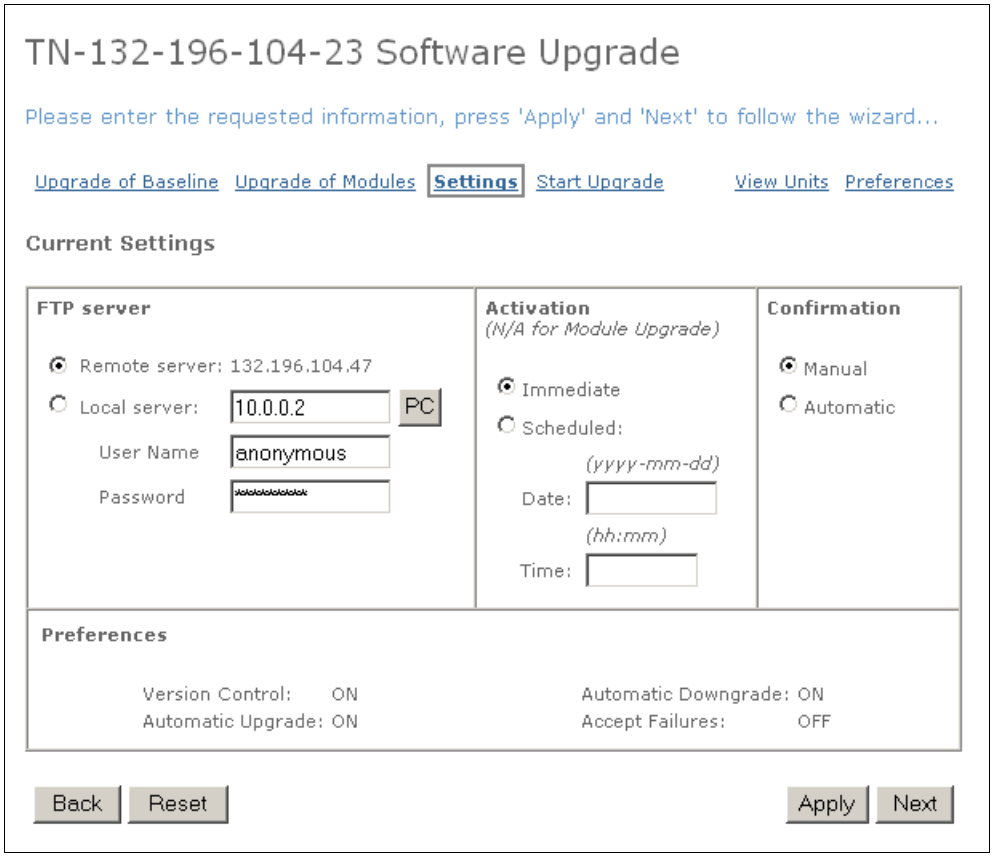


Figure 122 The Settings page

- **FTP server** — The FTP server from which the new software should be downloaded.
  - **Remote server** — A permanent FTP server in the network.
  - **Local server** — The FTP server on the local PC.
    - **PC** — Enters the IP address of the local PC.
    - **User Name** — The user name used by the NE to log in to the FTP server. The FTP server must be configured accordingly.
    - **Password** — The password used by the NE to log in to the FTP server. The FTP server must be configured accordingly.
- **Activation** — Specifies the point of time when the new software configuration should be activated after it has been downloaded to the NE.
  - **Immediate** — The new software configuration will be activated directly after all load modules have been received successfully.
  - **Scheduled** — The new software will be activated at a specified occasion. Only to be used for an upgrade of baseline and for automatic confirmation.
    - **Date** — The activation date (yyyy-mm-dd).
    - **Time** — The activation time (hh:mm).

- **Confirmation** — Specifies the way the new software should be confirmed or rejected after it has been activated.
  - **Manual** — The operator has to confirm the new software configuration within 15 minutes after activation.
  - **Automatic** — The NE will confirm the new software configuration automatically.
- **Preferences** — Displays the software upgrade preferences, specified on the **Preferences** page, see Section 11.81 on page 267. Preferences are only applicable for baseline upgrade.
- **Back** — Opens the **Upgrade of Baseline** page or **Upgrade of Modules** page, see Section 11.76 on page 260 and Section 11.77 on page 262.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.
- **Next** — Opens the **Start Upgrade** page, see Section 11.79 on page 265.

11.79 Start Upgrade

This page is used to start a software upgrade, summarizing the requested actions.

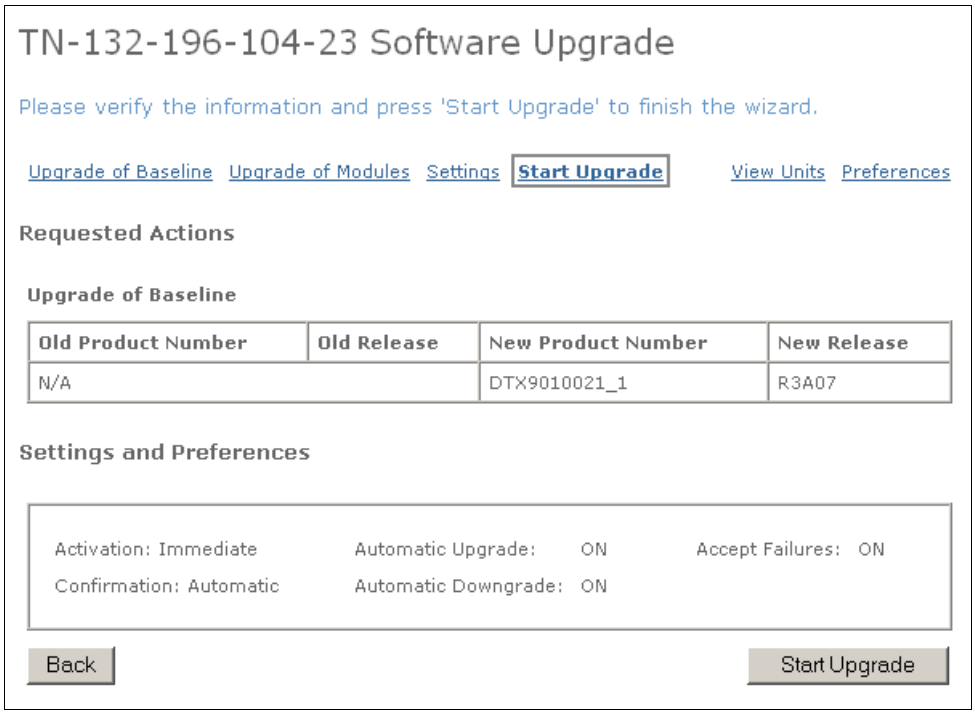
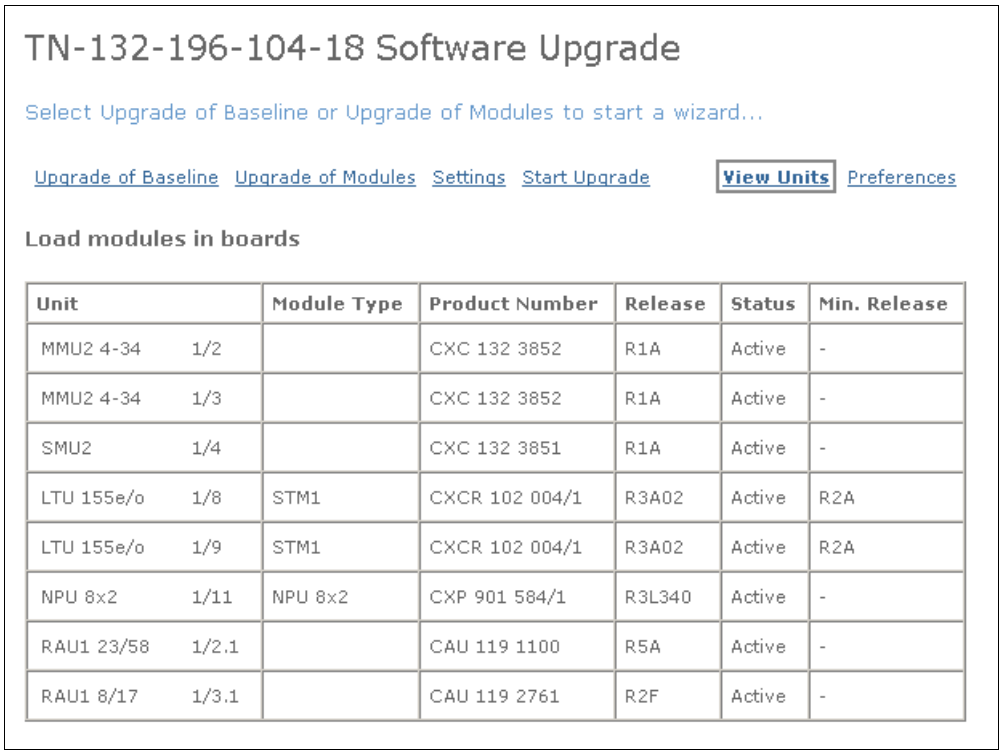


Figure 123 The Start Upgrade page, when an upgrade of baseline is performed

- **Requested Actions** — Displays information of the upgrade to be performed.
  - **Upgrade of Baseline** — Displays the product number and release of the old and new baseline. If version control is disabled, N/A will be displayed.
  - **Upgrade of Modules** — Displays the module type, product number and release of the old and new load module.
- **Settings and Preferences** — Displays the software upgrade settings and preferences, see Section 11.78 on page 263 and Section 11.81 on page 267.
- **Back** — Opens the **Settings** page, see Section 11.78 on page 263.
- **Start Upgrade** — Initiates the software upgrade. Opens the **Upgrade Progress – Baseline** page or **Upgrade Progress – Modules** page, see Section 11.82 on page 269 or Section 11.83 on page 271.

11.80 View Units

This page shows information about the load modules in all units.



Unit		Module Type	Product Number	Release	Status	Min. Release
MMU2 4-34	1/2		CXC 132 3852	R1A	Active	-
MMU2 4-34	1/3		CXC 132 3852	R1A	Active	-
SMU2	1/4		CXC 132 3851	R1A	Active	-
LTU 155e/o	1/8	STM1	CXCR 102 004/1	R3A02	Active	R2A
LTU 155e/o	1/9	STM1	CXCR 102 004/1	R3A02	Active	R2A
NPU 8x2	1/11	NPU 8x2	CXP 901 584/1	R3L340	Active	-
RAU1 23/58	1/2.1		CAU 119 1100	R5A	Active	-
RAU1 8/17	1/3.1		CAU 119 2761	R2F	Active	-

Figure 124 The View Units page

- **Load modules in boards** — Information about the load modules in the units.
  - **Unit** — The name of the unit.
  - **Module Type** — The name of the load module.
  - **Product Number** — The product number of the load module.
  - **Release** — The release state (version) of the load module.
  - **Status** — The status of the load module.
  - **Min. Release** — The minimum required release state (version) of the unit.

11.81 Preferences

This page is used to define software upgrade preferences. Preferences are only applicable for a baseline upgrade.

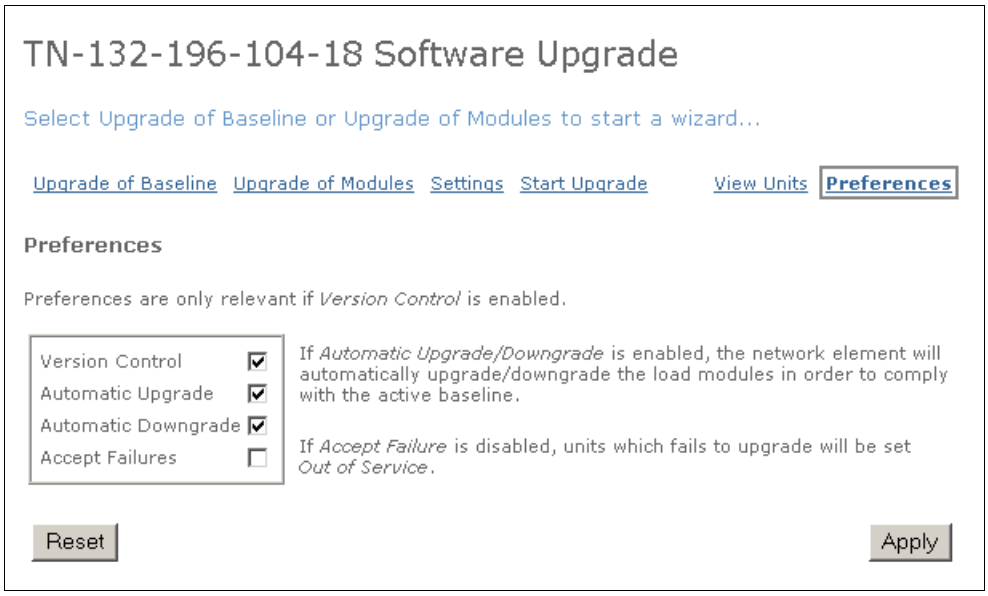


Figure 125 The Preferences page

- **Preferences** — Specifies the software upgrade preferences.
  - **Version Control** — Checks if load modules comply to a certain baseline. Clearing the check box disables version control. An upgrade of baseline enables version control. An upgrade of modules disables version control. Version control is enabled (ON) by default.
  - **Automatic Upgrade** — Selecting the check box enables automatic software upgrade of units with a software revision older than the one specified by the baseline. If version control is enabled a check against the baseline will be performed and an automatic software upgrade will be performed if needed. Automatic upgrade is enabled (ON) by default.
  - **Automatic Downgrade** — Selecting the check box enables automatic software downgrade of units with newer software revision than the one specified by the baseline. If version control is enabled a check against the baseline will be performed and an automatic software downgrade will be performed if needed. Automatic downgrade is enabled (ON) by default.

    Note: If neither **Automatic Upgrade** nor **Automatic Downgrade** is selected when performing an upgrade of baseline, then no units will be upgraded or downgraded.

  - **Accept Failures** — Selecting the check box sets units In Service after failing a software upgrade/downgrade. Clearing the check box will set inserted or cold restarted units in Out of Service if any automatic software upgrade/downgrade failed. Units that are already In Service

will be set to Reduced Service in order not to disturb traffic as a result of a failing software upgrade. Accept failures is disabled (OFF) by default.

- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.

11.82 Upgrade Progress – Baseline

This page shows the progress of a baseline upgrade.

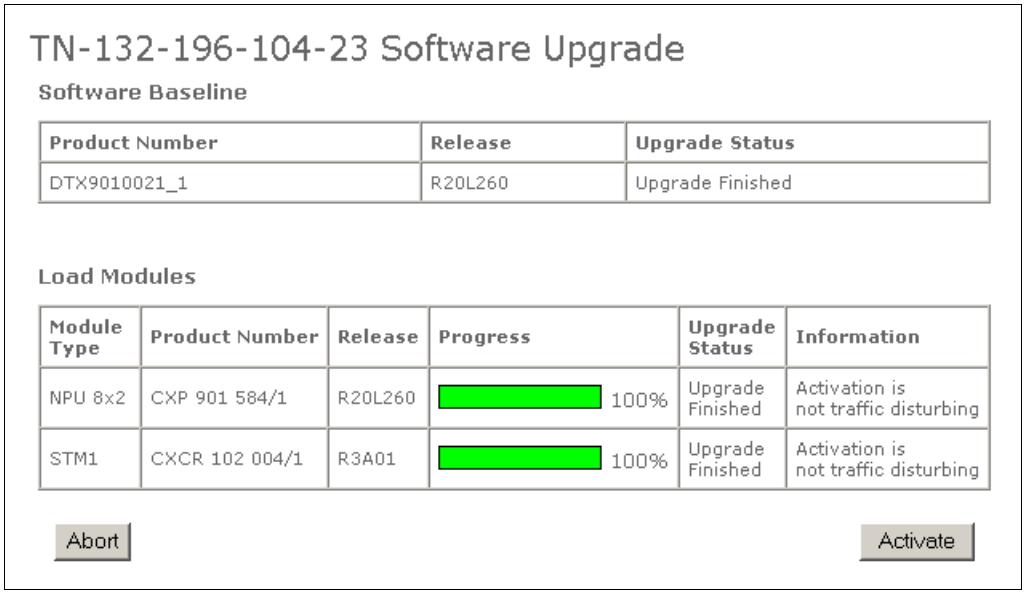


Figure 126 The Upgrade Progress – Baseline page

- **Software Baseline** — Displays information about the baseline.
  - **Product Number** — The product number of the baseline.
  - **Release** — The release state (version) of the baseline.
  - **Upgrade Status** — The status of the upgrade. When status `Upgrade Finished` is reached for all load modules the **Activate** button appears on the page.

    If the software upgrade gets aborted check the Event Log, see Section 11.134 on page 351. It is also useful to check the following for the FTP server:
    - It is up and running.
    - The IP address is correct, see Section 11.16 on page 174.
    - The correct directory structure is defined, see Section 3.2.1 on page 18.
    - The correct product number and release is defined for the desired baseline.
- **Load Modules** — Displays information about the load modules.
  - **Module Type** — The name of the load module.
  - **Product Number** — The product number of the load module.
  - **Release** — The release state (version) of the load module.
  - **Progress** — Indicates the progress of the download of the load module.
  - **Upgrade Status** — The status of the upgrade of the load module.
  - **Information** — Displays information about download, activation and failures.

- **Abort** — Aborts the upgrade and returns to the **Upgrade of Baseline** page, see Section 11.76 on page 260.
- **Activate** — Activates the new software configuration (immediate activation). The **Activation in Progress page** is displayed during the activation, see Section 11.85 on page 273.

  If manual configuration was selected, the **Confirm New Software Configuration** page is opened when the activation is finished, see Section 11.86 on page 274.

11.83 Upgrade Progress – Modules

This page shows the progress of a load module upgrade.

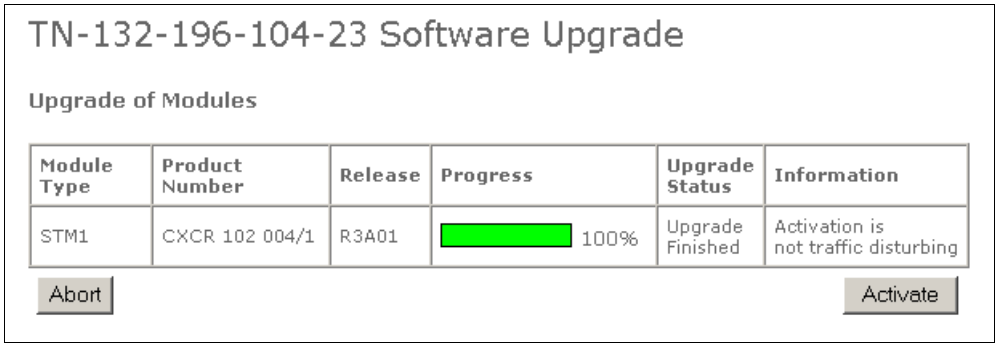


Figure 127 The Upgrade Progress – Modules page

- **Upgrade Modules** — Displays information about the upgrade of load modules.
  - **Module Type** — The name of the load module.
  - **Product Number** — The product number of the load module.
  - **Release** — The release state (version) of the load module.
  - **Progress** — Indicates the progress of the download of the load module.
  - **Upgrade Status** — The status of the upgrade of the load module.

    If the software upgrade gets aborted check the Event Log, see Section 11.134 on page 351. It is also useful to check the following for the FTP server:
    - It is up and running.
    - The IP address is correct, see Section 11.16 on page 174.
    - The correct directory structure is defined, see Section 3.2.1 on page 18.
    - The correct product number and release is defined for the load modules.
  - **Information** — Displays information about download, activation and failures.
- **Abort** — Aborts the upgrade and returns to the **Upgrade of Baseline** page, see Section 11.76 on page 260.
- **Activate** — Activates the new software configuration (immediate activation). The **Activation in Progress** page is displayed during the activation, see Section 11.85 on page 273.
- **Fallback** — Reverts to the old software configuration.
- **Confirm** — Manually confirms the new software configuration.

11.84 Scheduled Activation

This page is displayed when the NE is scheduled for an activation of a new software configuration (only upgrade of baseline).

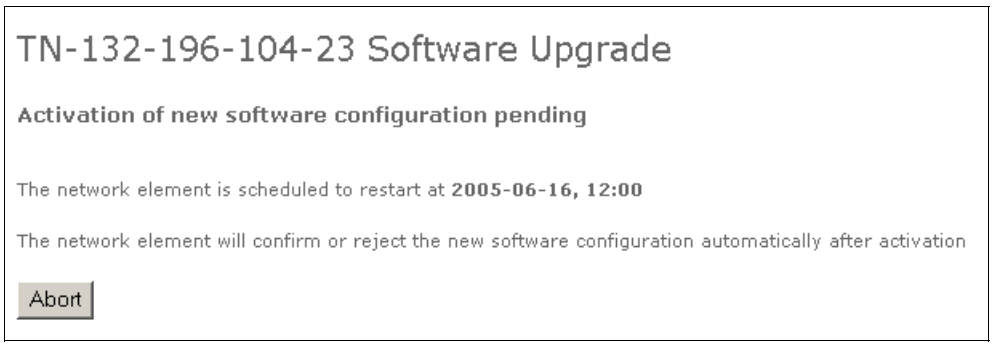


Figure 128 The Scheduled Activation page

- **Abort** — Aborts the scheduled activation and returns to the **Upgrade of Baseline** page, see Section 11.76 on page 260.

11.85 Activation in Progress

This page is displayed when a new software configuration is activated.

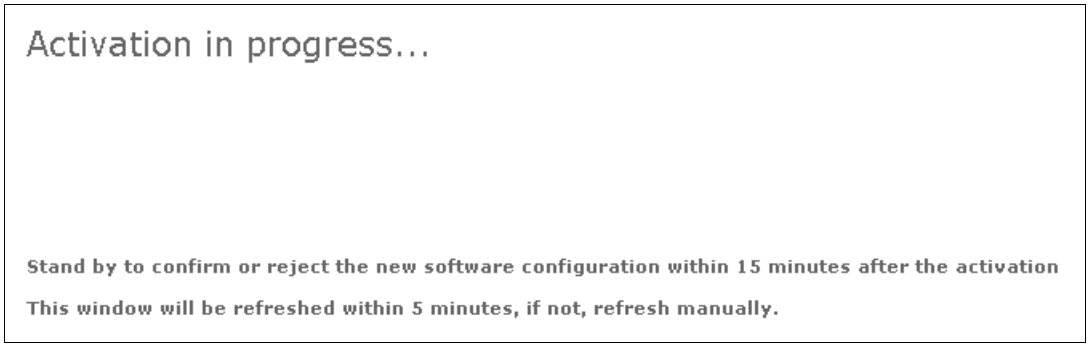


Figure 129 The Activation in Progress page

11.86 Confirm New Software Configuration

This page is used to manually confirm the activation of the new software configuration, when performing an upgrade of baseline.

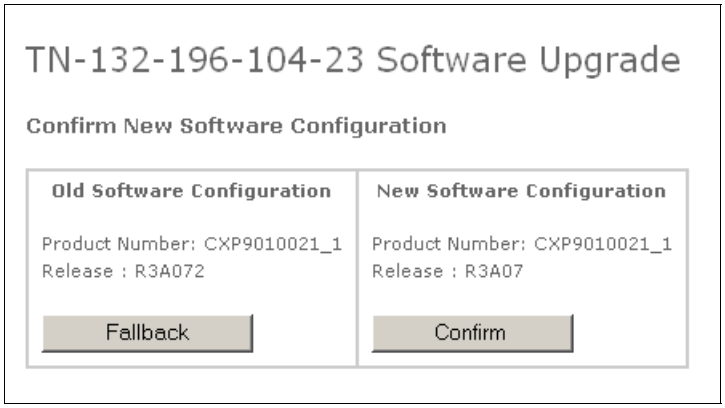


Figure 130 The Confirm New Software Configuration page

Caution!

If no button is clicked on this page within 15 minutes the NE will revert to the old software configuration.

- **Old Software Configuration** — The product number and release state (version) of the previous software configuration.
- **Fallback** — Reverts to the old software configuration.
- **New Software Configuration** — The product number and release state (version) of the new software configuration.
- **Confirm** — Confirms the new software configuration.

11.87 Load Configuration

This page is used to save a backup file of a configuration on an FTP server or to restore a configuration using a backup file.

Note: Activating a configuration file that has been fetched from another NE will revert the user passwords to default factory settings. See also Section 9.1 on page 135.

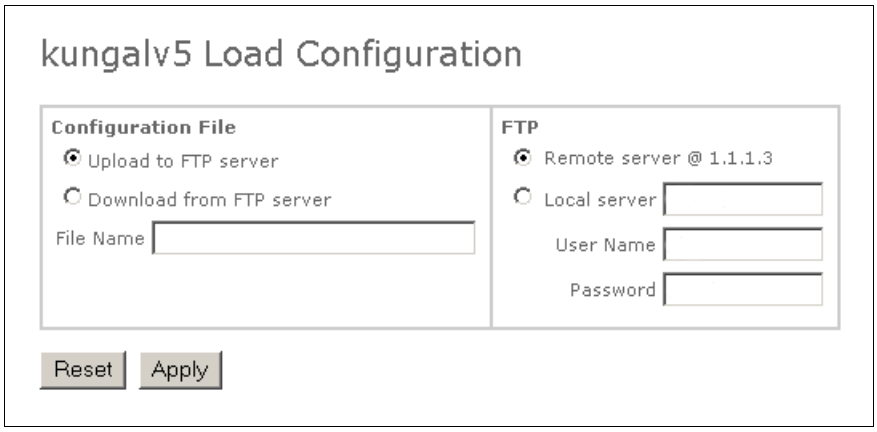


Figure 131 The Load Configuration page

- **Configuration File** — Specifies the load to be performed.
  - **Upload to FTP server** — A configuration file is uploaded to an FTP server to be used as backup configuration.
  - **Download from FTP server** — A configuration file is downloaded from an FTP server to be used to restore a configuration.
  - **File Name** — The name of the configuration file. It can be maximum 80 characters long. The configuration files are located in the *<drive:>*\tn_ftp_home\tn_backup_configuration folder on the FTP server. A configuration file is named *<hostname>*.cfg where *<hostname>* is typically the name or IP address of an NE. The file extension .cfg.old is used when a configuration file is uploaded using a file name that already exists.

    Note: Since tn_backup_configuration is likely to hold configuration files belonging to several NEs it is important to use file names that can easily be identified.

- **FTP** — Specifies the FTP server to be used. Only available in Normal mode.
  - **Remote server @ <IP address>** — Specifies that the permanent FTP server in the network should be used. See also Section 11.16 on page 174.
  - **Local server** — Specifies that the local FTP server should be used.
    - **User Name** — The user name used by the NE to log in to the FTP server. The FTP server must be configured accordingly.
    - **Password** — The password used by the NE to log in to the FTP server. The FTP server must be configured accordingly.

- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.
- **Back** — Navigates one step backward in the wizard. Only available in the installation wizard.

  Note: Configurations that you have performed are not reversed.

11.88 Load Configuration Progress

This page is used to display the progress of an ongoing upload or download of a configuration file.

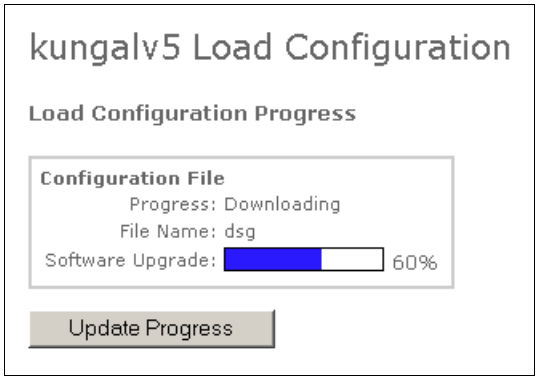


Figure 132 The Load Configuration Progress page

- **Configuration File** — Information about the ongoing process.
  - **Progress** — Displays the status of the upload or download.
  - **File Name** — The name of the configuration file.
  - **Software Upgrade** — Displays the progress of a software upgrade started automatically in NPU or Node Installation mode, if the configuration file specified a different NPU software release than the one currently active. Only available if a software upgrade is in progress.
- **Update Progress** — Updates the page with the latest information about the progress. Only available when status is `Downloading` or `Uploading`.
- **OK** — Opens the **Load Configuration** page, where a new configuration file can be loaded, see Section 11.87 on page 275. Only available when status is `Upload Failed` or `Download Failed`.
- **Back** — Navigates one step backward in the wizard. Only available in the installation wizard.

  Note: Configurations that you have performed are not reversed.

- **Next** — Navigates one step forward in the wizard. Only available in the installation wizard.

11.89 Restart

This page is used to perform a restart of the NE or a single unit.

Figure 133 The Restart page

Note: A restart of the NE or NPU will clear the Alarm List, Performance and Event Logs. Configurations that have not been saved, active loops and running BERTs will be lost.

Note: During a restart of the NE, the PC will lose contact with the Web server. Click **Refresh** or **Reload** in your browser after the NE has restarted to connect to the Web server.

- **Restart** — Selects the type of restart.
  - **Cold Restart** — Initiates a complete restart of the NE or unit.

Caution!

A cold restart will disturb the traffic.

  - **Warm Restart** — Restarts the control and management system of all units. Only available on NE level.
- **Apply** — Applies all changes you have made without leaving the page.

11.90 Help Setup

This page is used to specify the location of the Help file by typing the path in the text box. For more information on how to set up and use the Help, see Section 4.6 on page 42.

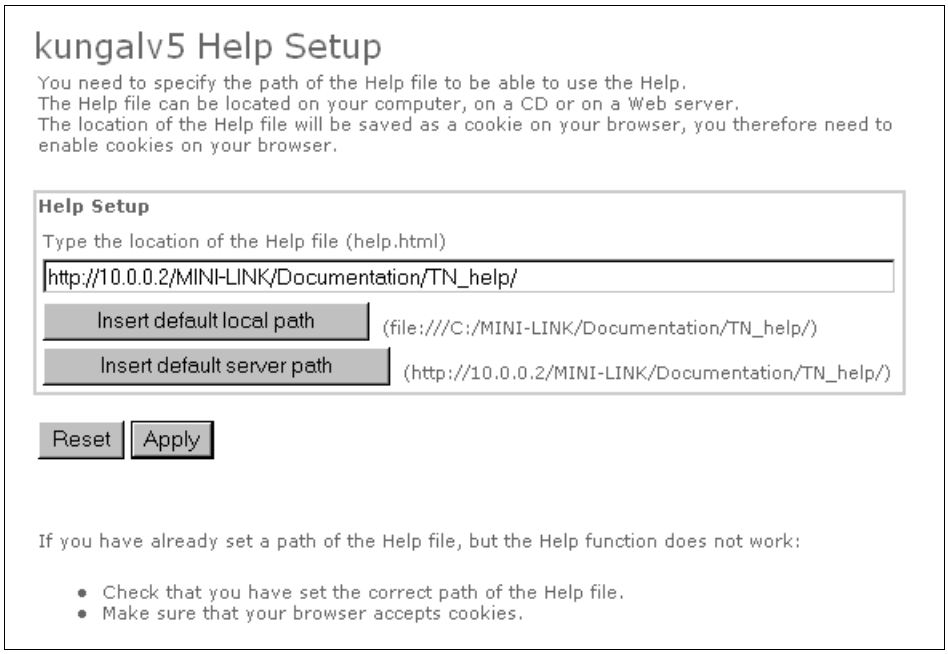


Figure 134 The Help Setup page

- **Help Setup** — Specifies the location of the Help file.
  - **Type the location of the Help file** — The path of the Help file.
  - **Insert default local path** — Inserts the default location on the local hard drive, `file:///C:/MINI-LINK/Documentation/TN_help/`, where MINI-LINK TN Help files are stored. Add the remaining part, `ETSI_<revision>/help.html`, manually to get the complete path of the file.
  - **Insert default server path** — Inserts the default folder, `http://10.0.0.2/MINI-LINK/Documentation/TN_help/`, on the local hard drive where MINI-LINK TN Help files are stored. Add the remaining part, `ETSI_<revision>/help.html`, manually to get the complete path of the file.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.

Note: A security feature in Internet Explorer 6 SP1 sometimes denies the browser to access the Help on your PC. Should this occur do the following in your browser: Click **Tools->Internet Options->Security->** and add `http://<IP address of the NE>` as a “Trusted Site”.

11.91 NE Alarms and Status

This page gives an overview of the alarms and status of the NE and its plug-in units.

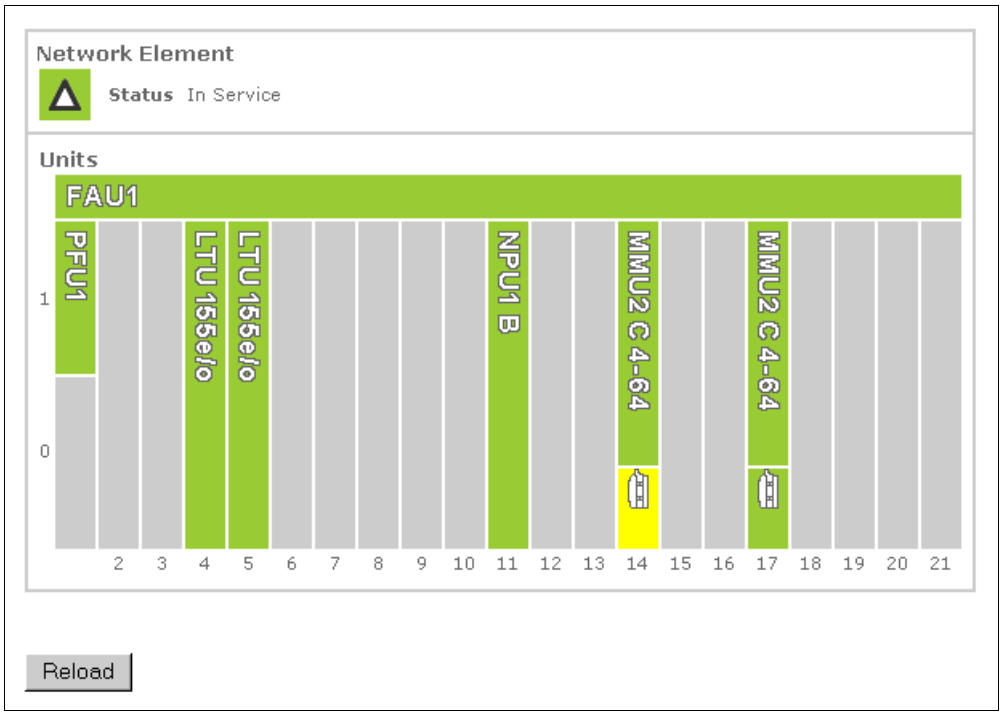


Figure 135 The NE Alarms and Status page for an AMM 20p

The position of a plug-in unit is indicated by a figure. Each unit is identified by a label and its accumulated status is indicated by a color. A bluish-green color indicates that a unit has notifications disabled or administration status set to Out of Service. Moving the pointer over a unit will display a tool tip with information on unit type, operational status and severity. Clicking a unit will open the **Alarms and Status** page for the unit.

Equipment protection is indicated by the text 1+1. The active LTU 155 and MMU2 B/C is indicated by a label, while the active MMU2 is indicated in MSM.

A warning will be displayed if notifications from the NE are disabled.

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **Network Element** — Displays alarms and status information related to the NE.
  - **Status** — Displays the status of the NE.
    - **In Service** — The NE is operating properly.
    - **Reduced Service** — Traffic is running, but the management functionality is reduced or unavailable.
    - **Out of Service** — The NE is not operating.

  - **Alarms** — Displays the NE alarms. See Section 7.2.5 on page 118 for alarm descriptions.
  - **NTP Status** — Displays the operational status of an NTP service. Only available if the NE is configured to use an NTP server.
    - **Up** — Contact established with NTP server.
    - **Down** — Contact lost with NTP server.
- **Units** — Displays the accumulated status of each unit in the AMM. MMUs are shown together with their RAUs.
- **Reload** — Reloads the page with the latest information.

11.92 Ethernet Bridge Alarms and Status

This page displays the alarms and status of the Ethernet Bridge, implemented in the NPU2 and ATU (B). It also displays counters for the HDLC and Ethernet interfaces, if desired.

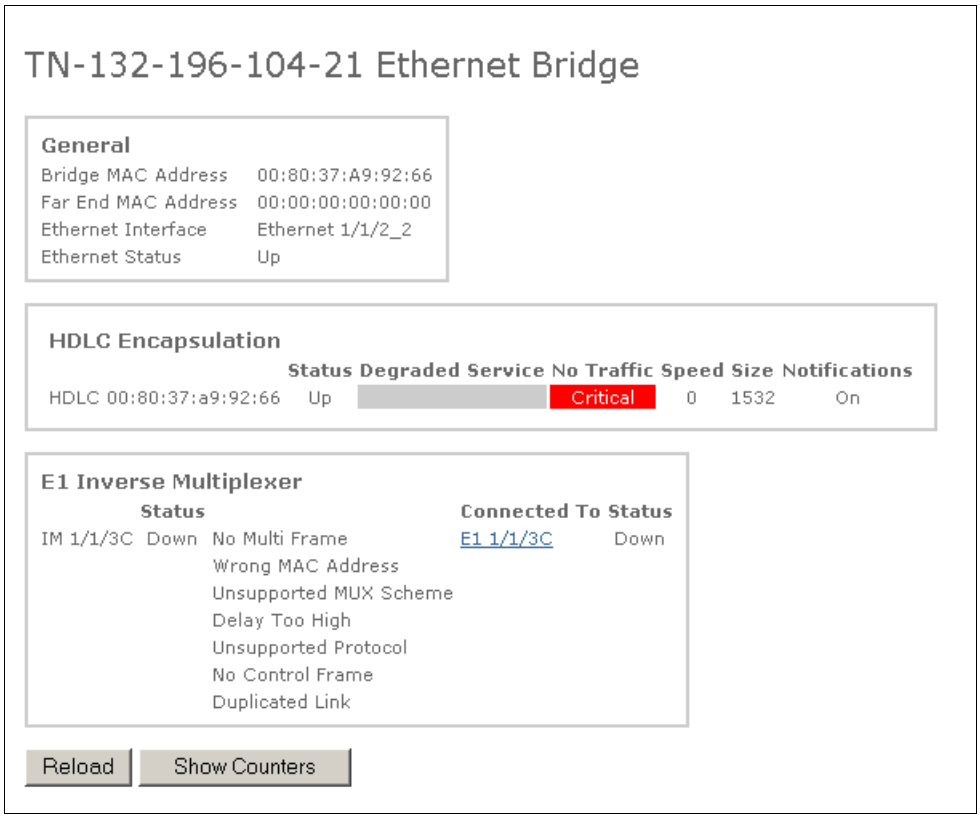


Figure 136 The Ethernet Bridge Alarms and Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **General** — Displays general bridge information.
  - **Bridge MAC Address** — The physical address of the Ethernet port.
  - **Far End MAC Address** — The physical address of the far end port.
  - **Ethernet/Bridge Interface** — The identity of the bridge's internal Ethernet interface.
  - **Ethernet/Bridge Status** — The status of the bridge's internal Ethernet interface.
    - **Up** — Ethernet carrier detected.
    - **Down** — Ethernet carrier not detected.
- **HDLC Encapsulation** — Displays information about the HDLC encapsulation interface. This interface holds 1 to 16 Inverse Multiplexer (IM) interfaces, that is one IM interface per E1 in the bridge.
  - **Status** — The status of the interface.

    - **Up** — Payload is passing on the interface.
    - **Down** — A defect is detected on the interface.
  - **Alarms** — Lists active alarms on the interface. See Section 7.2.5 on page 118 for alarm descriptions.
  - **Speed** — The speed in Mbit/s.
  - **Size** — The size of the largest protocol data unit, in octets, that can be sent or received on the interface.
  - **Notifications** — Indicates if notifications are enabled on the interface.
- **E1 Inverse Multiplexer** — Displays information about the Inverse Multiplexer (IM) interfaces. One IM interface is associated with one E1 interface.
  - **IM <ID>** — The name of the IM interface.
  - **Status** — The status of the interface.
    - **Up** — Payload is passing on the interface.
    - **Down** — A defect is detected on the interface.
    - **No Multi Frame** — Can also be displayed for the far end.
    - **Wrong MAC Address** — Can also be displayed for the far end.
    - **Unsupported MUX Scheme** — Can also be displayed for the far end.
    - **Link Degraded (Too much CRC4)** — Can also be displayed for the far end.
    - **Unsupported Protocol** — Can also be displayed for the far end.
    - **Delay Too High/Low** — Can also be displayed for the far end.
    - **No Control Frame** — Can also be displayed for the far end.
    - **Duplicated Link** — Only displayed for the near end.
  - **Connected To** — Displays the associated E1. Clicking a link opens the **E1 Alarms and Status** page for the interface, see Section 11.124 on page 337.
  - **Status** — Displays the status of the E1 interfaces associated with the IM interfaces.
- **Counters** — Displays counters for the HDLC and Ethernet interfaces.
  - **Received** — Counters for the received packets.
    - **Octets** — The number of octets received on the interface, including framing characters.
    - **Unicast** — The number of sub-network unicast packets delivered to a higher layer protocol.
    - **Multicast** — The number of sub-network multicast packets delivered to a higher layer protocol.
    - **Broadcast** — The number of sub-network broadcast packets delivered to a higher layer protocol.
    - **Discarded** — The number of inbound packets discarded, even though no error was detected, preventing them from being delivered to a higher layer protocol (for example buffer overflow).
    - **Error** — The number of inbound packets that contain error, preventing them from being delivered to a higher layer protocol.
  - **Transmitted** — Counters for the transmitted packets.

    - **Octets** — The number of octets transmitted on the interface, including framing characters.
    - **Unicast** — The number of packets that higher layer protocols requested to be transmitted to a sub-network unicast address, including those that were discarded or otherwise not sent.
    - **Multicast** — The number of multicast packets that higher layer protocols requested to be transmitted to a sub-network multicast address, including those that were discarded or otherwise not sent.
    - **Broadcast** — The number of packets that higher layer protocols requested to be transmitted to a sub-network broadcast address, including those that were discarded or otherwise not sent.
    - **Discarded** — The number of outbound packets discarded, even through no errors had been detected, preventing them from being transmitted (for example buffer overflow).
    - **Error** — The number of outbound packets that could not be transmitted because of error.
- **Reload** — Reloads the page with the latest information.
- **Show Counters** — Enables the display of counters. The display is disabled by default.
- **Clear HDLC Counters** — Clears the HDLC counters.
- **Clear Ethernet Counters** — Clears the Ethernet counters.
- **Hide Counters** — Disables the display of counters.

See Also

- How to configure the Ethernet Bridge, see Section 6.7 on page 79.

11.93 Bridge Alarm and Status

This page displays the status of the Bridge interface on ATU (B).

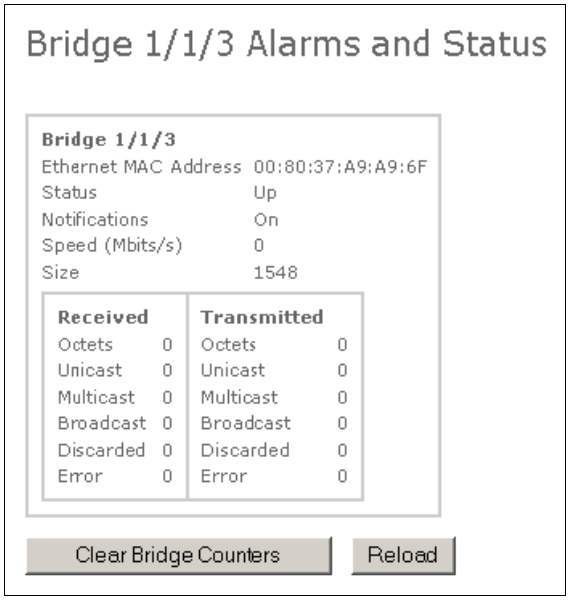


Figure 137 The Bridge Alarm and Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **Ethernet MAC Address** — The MAC address.
- **Status** — The operational status of the interface.
  - **Up** — Ethernet carrier detected.
  - **Down** — Ethernet carrier not detected.
- **Notifications** — Displays if notifications from the interface are enabled (on) or disabled (off).
- **Speed (Mbit/s)** — The speed in Mbit/s.
- **Size** — The size of the largest protocol data unit, in octets that can be sent or received on the interface.
- **Received** — Displays counters for the received packets.
  - **Octets** — The number of octets received on the interface, including framing characters.
  - **Unicast** — The number of sub-network unicast packets delivered to a higher layer protocol.
  - **Multicast** — The number of sub-network multicast packets delivered to a higher layer protocol.
  - **Broadcast** — The number of sub-network broadcast packets delivered to a higher layer protocol.
  - **Discarded** — The number of inbound packets discarded, even though no error was detected, preventing them from being delivered to a higher layer protocol (for example buffer overflow).

  - **Error** — The number of inbound packets that contain error, preventing them from being delivered to a higher layer protocol.
- **Transmitted** — Displays counters for the transmitted packets.
  - **Octets** — The number of octets transmitted on the interface, including framing characters.
  - **Unicast** — The number of packets that higher layer protocols requested to be transmitted to a sub-network unicast address, including those that were discarded or otherwise not sent.
  - **Multicast** — The number of multicast packets that higher layer protocols requested to be transmitted to a sub-network multicast address, including those that were discarded or otherwise not sent.
  - **Broadcast** — The number of packets that higher layer protocols requested to be transmitted to a sub-network broadcast address, including those that were discarded or otherwise not sent.
  - **Discarded** — The number of outbound packets discarded, even through no errors had been detected, preventing them from being transmitted (for example buffer overflow).
  - **Error** — The number of outbound packets that could not be transmitted because of error.
- **Clear Bridge Counters** — Clears the Bridge counters.
- **Reload** — Reloads the page with the latest information.

11.94 Ethernet/LAN Status

This page displays the status of the Ethernet/LAN interface.

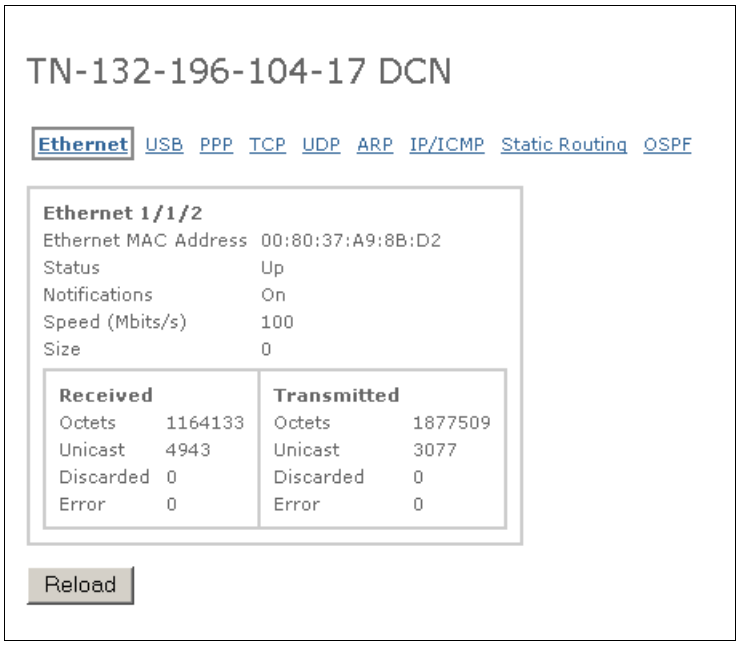


Figure 138 The Ethernet/LAN Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **Ethernet/LAN <ID>** — The name of the Ethernet/LAN interface.
  - **Ethernet MAC Address** — The MAC address.
  - **Status** — The operational status of the interface.
    - **Up** — Ethernet carrier detected.
    - **Down** — Ethernet carrier not detected.
  - **Notifications** — Displays if notifications from the interface are enabled (on) or disabled (off).
  - **Speed (Mbit/s)** — The speed in Mbit/s.
  - **Size** — The size of the largest protocol data unit, in octets that can be sent or received on the interface.
- **Received** — Parameters for received packets.
  - **Octets** — The number of octets received on the interface, including framing characters.
  - **Unicast** — The number of sub-network unicast packets delivered to a higher layer protocol.
  - **Discarded** — The number of inbound packets discarded, even though no error was detected, preventing them from being delivered to a higher layer protocol (for example buffer overflow).
  - **Error** — The number of inbound packets that contain error, preventing them from being delivered to a higher layer protocol.

- **Transmitted** — Parameters for transmitted packets.
  - **Octets** — The number of octets transmitted on the interface, including framing characters.
  - **Unicast** — The number of packets that higher layer protocols requested to be transmitted to a sub-network unicast address, including those that were discarded or otherwise not sent.
  - **Discarded** — The number of outbound packets discarded, even through no errors had been detected, preventing them from being transmitted (for example buffer overflow).
  - **Error** — The number of outbound packets that could not be transmitted because of error.
- **Reload** — Reloads the page with the latest information.

11.95 USB Status

This page displays the status of the USB interface on the NPU2/NPU1 B.

Figure 139 The USB Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **Local Access <ID>** — The name of the interface. N/A indicates Not Applicable.
- **Status** — Indicates if a PC is connected or not.
- **Reload** — Reloads the page with the latest information.

11.96 PPP Status

This page displays the status of the PPP and ML-PPP interfaces.

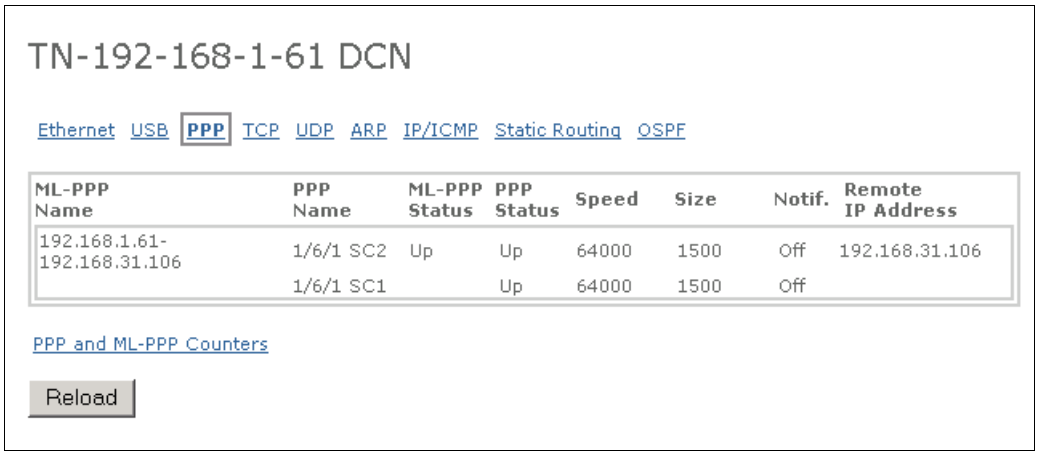


Figure 140 The PPP Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **ML-PPP Name** — The name of a Multilink PPP interface, that is all PPP interfaces destined to the same IP address. A Multilink PPP interface is indicated by a frame. N/A indicates not applicable.
- **PPP Name** — The name of the PPP interface.
- **ML-PPP Status** — The status of the Multilink PPP interface.
  - **Up** — The interface can be used for DCN communication.
  - **Down** — The interface can not be used for DCN communication.
- **PPP Status** — The status of the PPP interface.
- **Speed** — The speed in bit/s.
- **Size** — The size of the largest protocol data unit, in octets that can be sent or received on the interface.
- **Notif.** — Displays if notifications from the interface are enabled (on) or disabled (off).
- **Remote IP Address** — The remote IP address.
- **PPP and ML-PPP Counters** — Opens the **PPP and ML-PPP Counters** page, see Section 11.97 on page 291.
- **Reload** — Reloads the page with the latest information.

See Also

- How to configure the PPP interfaces, see Section 6.10.2 on page 87.

11.97 PPP and ML-PPP Counters

This page displays the status of the PPP and ML-PPP counters.

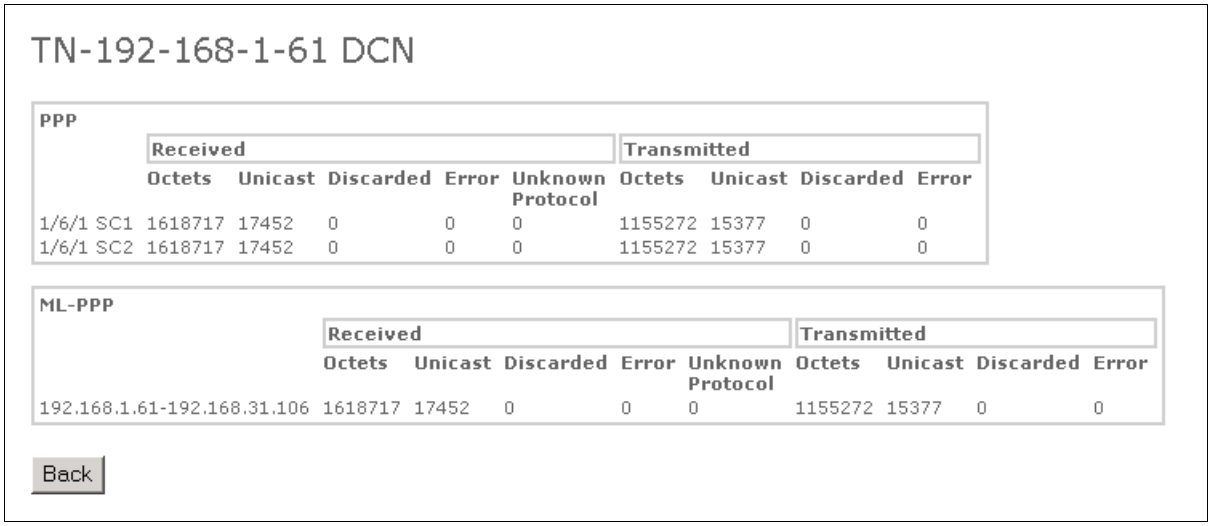


Figure 141 The PPP and ML-PPP Counters page

- **PPP** — Displays the status of the PPP counters.
  - **Received** — The received PPP counters.
    - **Octets** — The number of octets received on the interface, including framing characters.
    - **Unicast** — The number of sub-network unicast packets delivered to a higher layer protocol.
    - **Discarded** — The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent them from being delivered to a higher layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
    - **Error** — The number of inbound packets that contained errors preventing them from being deliverable to a higher layer protocol.
    - **Unknown Protocol** — The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.
  - **Transmitted** — The transmitted PPP counters.
    - **Octets** — The number of octets transmitted out of the interface, including framing characters.
    - **Unicast** — The number of packets that higher level protocols requested to be transmitted to a sub-network unicast address, including those that were discarded or not sent.
    - **Discarded** — The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent them from being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
    - **Error** — The number of outbound packets that could not be transmitted because of errors.

- **ML-PPP** — Displays the ML-PPP counters, as described above.
- **Back** — Opens the **PPP Status** page, see Section 11.96 on page 290.

11.98 TCP Status

This page displays the status of the TCP parameters.

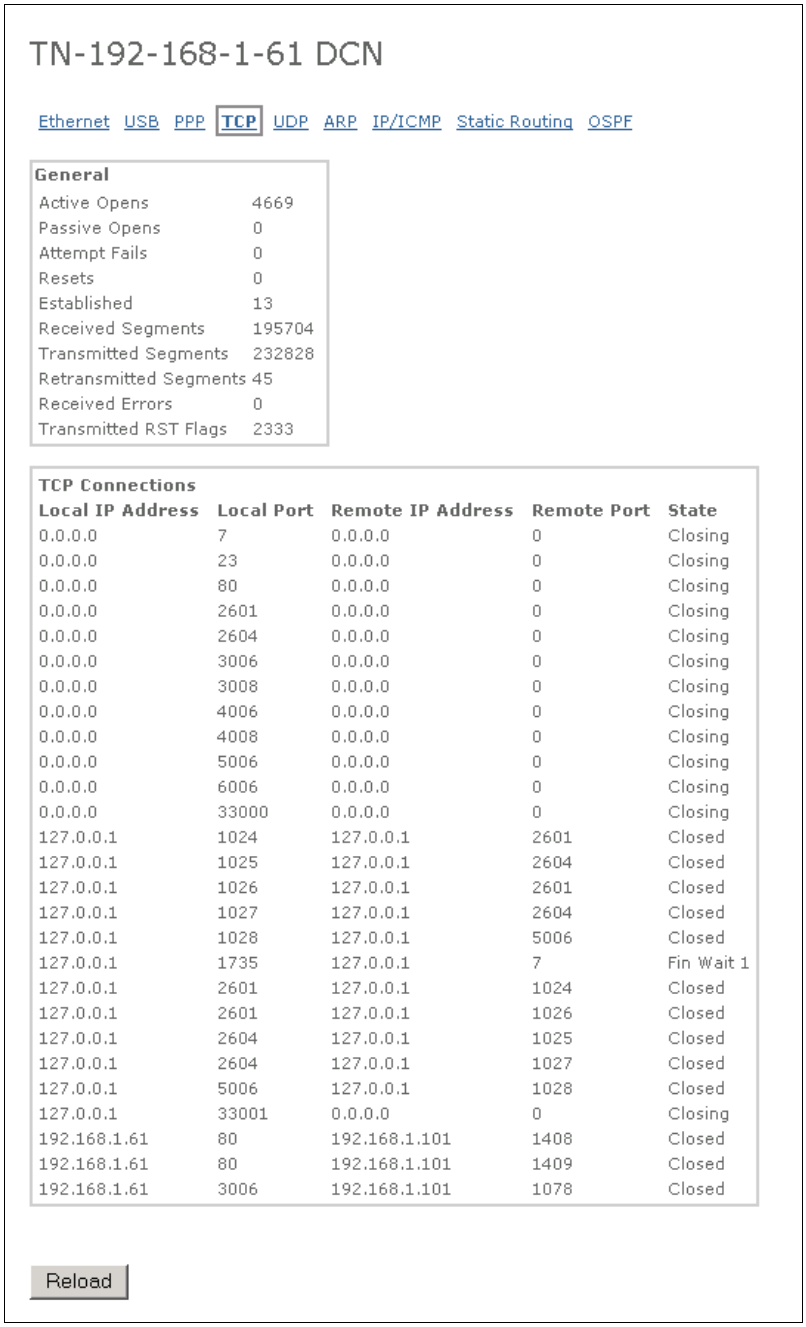


Figure 142 The TCP Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **General** — Displays general TCP parameters.

  - **Active Opens** — The number of active open TCP ports.
  - **Passive Opens** — The number of passive TCP ports.
  - **Attempt Fails** — The number of failed connection attempts.
  - **Resets** — The number of resets that have occurred.
  - **Established** — The number of TCP connections for which the current state is either `Established` or `Close Wait`.
  - **Received Segments** — The number of received segments, including those received in error.
  - **Transmitted Segments** — The number of transmitted segments, excluding those containing only retransmitted octets.
  - **Retransmitted Segments** — The number of retransmitted segments.
  - **Received Errors** — The number of segments received in error.
  - **Transmitted RST flags** — The number of TCP segments sent containing the RST (reset) flag.
- **TCP Connections** — Displays the TCP connections.
  - **Local IP Address** — The local IP address of the TCP connection.
  - **Local Port** — The local port number.
  - **Remote IP Address** — The remote IP address of the TCP connection.
  - **Remote Port** — The remote port number.
  - **State** — The state of the TCP connection.
- **Reload** — Reloads the page with the latest information.

11.99 UDP Status

This page displays the status of the UDP parameters.

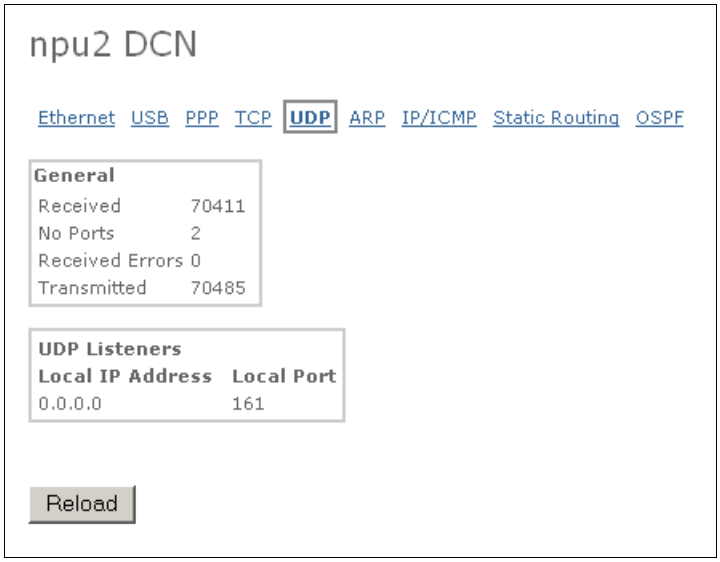


Figure 143 The UDP Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **General** — Displays general UDP parameters.
  - **Received** — The number of UDP datagrams delivered to UDP users.
  - **No Ports** — The number of received UDP datagrams for which there was no application at the destination port.
  - **Received Errors** — The number of received UDP datagrams that could not be delivered for reasons other than lack of application at the destination port.
  - **Transmitted** — The number of UDP datagrams sent from this entity.
- **UDP Listeners** — Displays general UDP parameters.
  - **Local IP Address** — The local IP address of this UDP listener.
  - **Local Port** — The local port number of this UDP listener.
- **Reload** — Reloads the page with the latest information.

11.100 ARP Status

This page displays the status of the ARP parameters for the effected Ethernet interfaces.

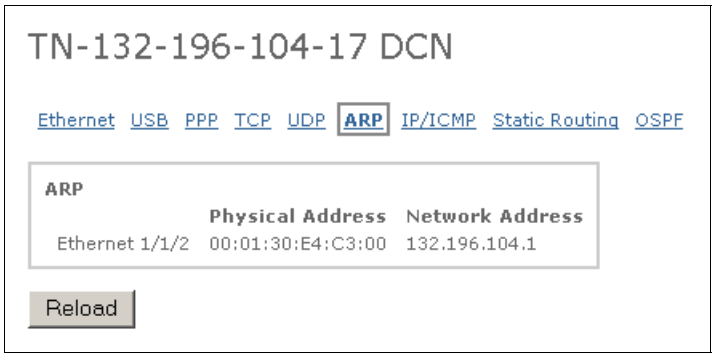


Figure 144 The ARP Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **Physical Address** — The physical (MAC) address of the Ethernet interface.
- **Network Address** — The network address of the Ethernet interface.
- **Reload** — Reloads the page with the latest information.

11.101 IP/ICMP Status

This page displays the status of the IP/ICMP parameters.

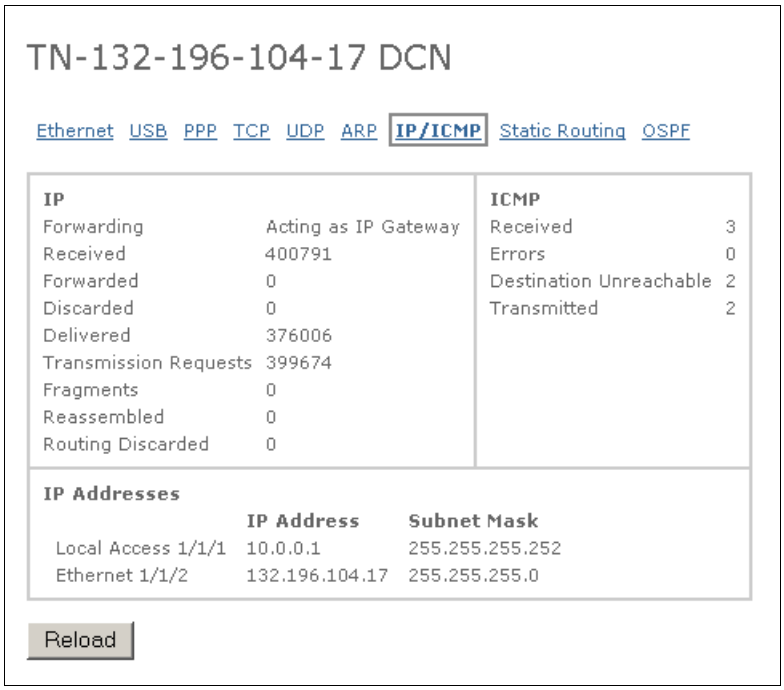


Figure 145 The IP/ICMP Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **IP** — Displays IP parameters.
  - **Forwarding** — Indicates whether this entity is acting as an IP router in respect to the forwarding of datagrams received by, but not addressed to, this entity.
  - **Received** — The number of input datagrams received from interfaces, including those received in error.
  - **Forwarded** — The number of input datagrams that have been forwarded.
  - **Discarded** — The number of input datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example due to lack of buffer space).
  - **Delivered** — The number of input datagrams successfully delivered.
  - **Transmission Requests** — The number of datagrams that local IP user protocols supplied to IP in requests for transmission.
  - **Fragments** — The number of IP fragments received which needed to be reassembled at this entity.
  - **Reassembled** — The number of IP datagrams successfully reassembled.

  - **Routing Discarded** — The number of routing entries discarded even though valid.
- **ICMP** — Displays ICMP parameters.
  - **Received** — The number of ICMP messages.
  - **Errors** — The number of ICMP messages with ICMP errors.
  - **Destination Unreachable** — The number of ICMP destination unreachable messages received.
  - **Transmitted** — The number of ICMP messages that this entity attempted to send.
- **IP Addresses** — Displays an address table for the Ethernet and ML-PPP interfaces.
  - **IP Address** — The IP address of the interface.
  - **Subnet Mask** — The subnet mask of the interface.
- **Reload** — Reloads the page with the latest information.

11.102 Static Routing Status

This page displays static routing parameters.

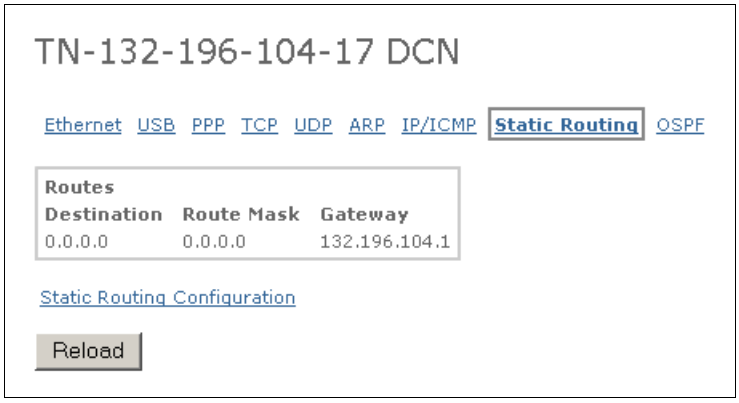


Figure 146 The Static Routing Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **Destination** — The destination IP address of this route.
- **Route Mask** — The netmask for the destination IP address.
- **Gateway** — The address of the next system on the route (only used for remote routes, 0.0.0.0 otherwise).
- **Static Routing Configuration** — Opens the **Static Routing Configuration** page, see Section 11.19 on page 179.
- **Reload** — Reloads the page with the latest information.

See Also

- How to configure static routes, see Section 6.10.5 on page 89.

11.103 OSPF General Status

This page displays general OSPF parameters.

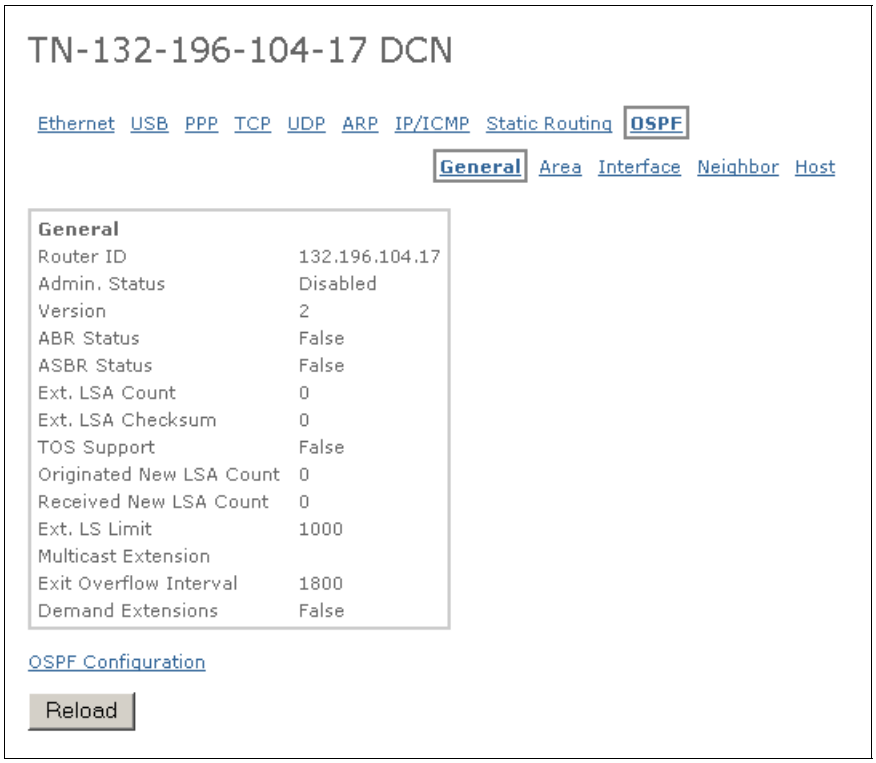


Figure 147 The OSPF General Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **Router ID** — A unique identifier of the router in the Autonomous System (AS).
- **Admin. Status** — The administrative status of OSPF in the router. `Enabled` denotes that the OSPF process is active on at least one interface. `Disabled` denotes that the OSPF process is disabled on all interfaces.
- **Version** — The current version of the OSPF protocol.
- **Status** — Indicates whether this is an Area Border Router (ABR).
- **ASBR Status** — Indicates whether this is an Autonomous System Border Router (ASBR)
- **Ext. LSA Count** — The number of external (LS type 5) Link State Advertisements (LSA) in the link state database.
- **Ext. LSA Checksum** — Checksums of the external link state advertisements contained in the link state database. This sum can be used to determine if there has been a change in a router's link state database, and to compare the link state database of two routers.
- **TOS Support** — The router's support for Type Of Service (TOS) routing.

- **Originated New LSA Count** — The number of new LSAs that have been originated. This number is incremented each time the router originates a new LSA.
- **Received New LSA Count** — The number of LSAs received, determined to be new instantiations. This number does not include newer instantiations of self-originated LSAs.
- **Ext. LS Limit** — The maximum number of non-default AS-external-LSAs entries that can be stored in the link state database. If the value is –1, then there is no limit. When the number of non-default AS-external-LSAs in a router's link state database reaches Ext. LS Limit, the router enters Overflow State. The router never holds more than Ext. LS Limit non-default AS-external-LSAs in its database. Ext. LS Limit must be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area (that is, OSPF stub areas and NSSAs are excluded).
- **Multicast Extension** — A bit mask indicating whether the router is forwarding IP multicast (Class D) datagrams based on the algorithms defined in the multicast extensions to OSPF.

  Bit 0, if set, indicates that the router can forward IP multicast datagrams in the router's directly attached areas (called intra-area multicast routing).

  Bit 1, if set, indicates that the router can forward IP multicast datagrams between OSPF areas (called inter-area multicast routing).

  Bit 2, if set, indicates that the router can forward IP multicast datagrams between Autonomous Systems (called inter-AS multicast routing).

  Only certain combinations of bit settings are allowed, namely:

  0 No multicast forwarding is enabled. This is the default value.

  1 Intra-area multicasting only.

  3 Intra-area and inter-area multicasting.

  5 Intra-area and inter-AS multicasting.

  7 Multicasting everywhere.
- **Exit Overflow Interval** — The number of seconds that, after entering Overflow State, a router will attempt to leave Overflow State. This allows the router to again originate non-default AS-external-LSAs. When set to 0, the router will not leave Overflow State until restarted.
- **Demand Extensions** — The router's support for demand routing.
- **OSPF Configuration** — Opens the **OSPF Area Configuration** page, see Section 11.21 on page 181.
- **Reload** — Reloads the page with the latest information.

11.104 OSPF Area Status

This page displays OSPF area parameters.

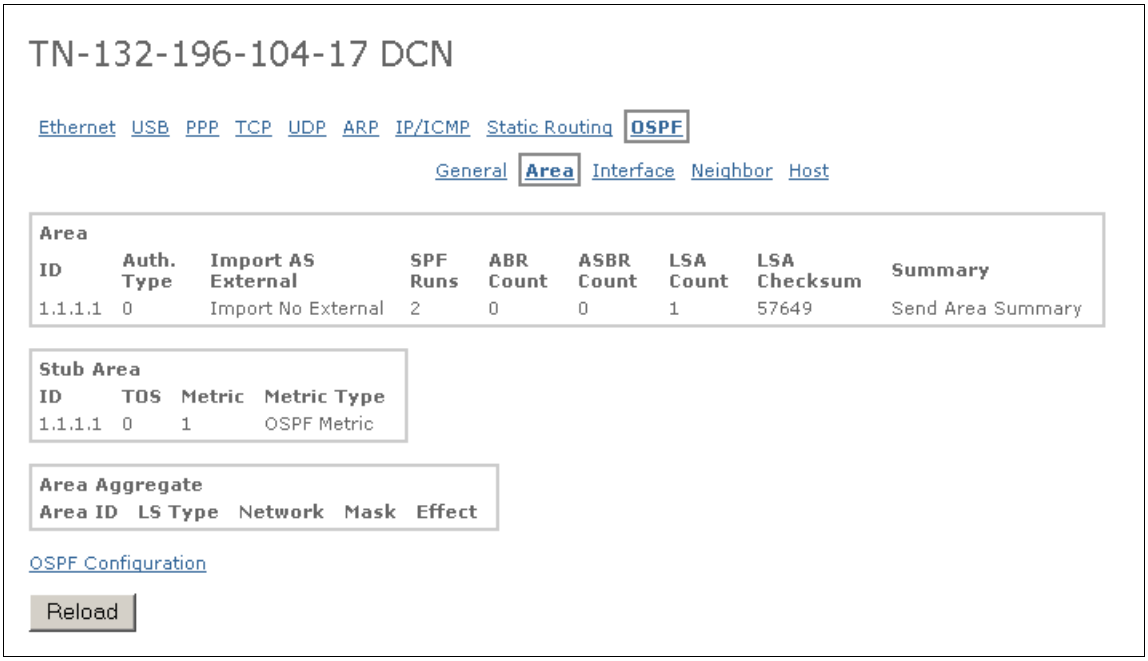


Figure 148 The OSPF Area Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **Area** — Displays area parameters.
  - **ID** — A unique identifier of the area. Area ID 0.0.0.0 is used for the OSPF backbone.
  - **Auth. Type** — The authentication type specified for an area. Additional authentication types may be assigned locally on a per area basis.
  - **Import AS External** — The area's support for importing AS-external-LSAs.
  - **SPF Runs** — The number of times that the intra-area route table has been calculated using this area's link state database.
  - **ABR Count** — The total number of ABRs reachable within this area. This is initially 0, and is calculated in each SPF pass.
  - **ASBR Count** — The total number of ASBRs reachable within this area. This is initially 0, and is calculated in each SPF pass.
  - **LSA Count** — The total number of LSAs in this area's link state database, excluding AS-external-LSAs.
  - **LSA Checksum** — The 32-bit unsigned sum of the LSA's LS checksums contained in this area's link state database. This sum excludes external (LS type 5) LSAs. The sum can be used to determine if there has been a change in a router's link state database, and to compare the link state database of two routers.

  - **Summary** — Controls the import of summary LSAs into stub areas. It has no effect on other areas. If it is no `Area Summary`, the router will neither originate nor propagate summary LSAs into the stub area. It will rely entirely on its default route. If it is `Send Area Summary`, the router will both summarize and propagate summary LSAs.
- **Stub Area** — Displays stub area parameters.
  - **ID** — A unique identifier of the stub area.
  - **TOS** — The Type Of Service (TOS) associated with the metric.
  - **Metric** — The metric value applied at the indicated TOS. By default, this equals the least metric at the TOS among the interfaces with other areas.
  - **Metric Type** — The type of metric advertised as a default route.
- **Area Aggregate** — Displays area aggregate parameters.
  - **Area ID** — The area the address aggregate is to be found within.
  - **LS Type** — The type of link state this address aggregate applies to.
  - **Network** — The IP address of the net or subnet indicated by the range.
  - **Mask** — The subnet mask that pertains to the net or subnet.
  - **Effect** — Subnets subsumed by ranges either trigger the advertisement of the indicated aggregate (Advertise Matching), or result in the subnets not being advertised at all outside the area.
- **OSPF Configuration** — Opens the **OSPF Area Configuration** page, see Section 11.21 on page 181.
- **Reload** — Reloads the page with the latest information.

See Also

- How to configure OSPF areas, see Section 6.10.3 on page 88.

11.105 OSPF Interface Status

This page displays OSPF interface parameters.

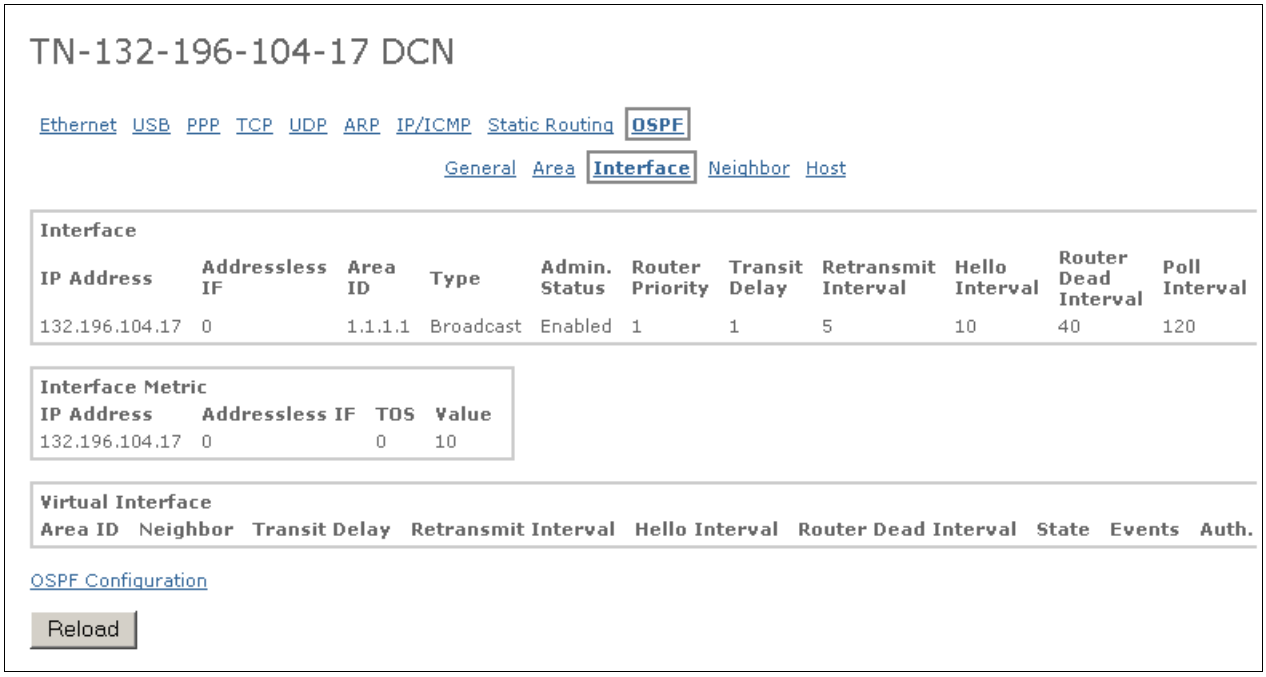


Figure 149 The OSPF Interface Status page. Note that the figure does not show all parameters that will be displayed on the screen.

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **Interface** — Displays interface parameters.
  - **IP Address** — The IP address of the OSPF interface
  - **Addressless IF** — Differentiates the addressless interfaces from the addressed interfaces. The value 0 signifies that the interface has an IP address.
  - **Area ID** — A unique identifier of the area. Area ID 0.0.0.0 is used for the OSPF backbone.
  - **Type** — The OSPF interface type.
  - **Admin. Status** — The administrative status of the OSPF interface. When the value is set to `Enabled`, it signifies that the neighbor relationships may be formed on the interface, and the interface is advertised as an internal route to some area. When the value is set to `Disabled`, it signifies that the interface is external to OSPF.
  - **Router Priority** — The priority of this interface. When the value is set to 0, it signifies that the router is not eligible to become the designated router on this particular network.
  - **Transit Delay** — The estimated number of seconds it takes to transmit a link state update packet over this interface.

- **Retransmit Interval** — The number of seconds between the link state advertisement retransmissions, for adjacencies belonging to this interface. This value is also used when retransmitting database description and link state request packets.
- **Hello Interval** — The time interval, in seconds, between the Hello packets that the router sends on the interface. This value must be the same for all the routers attached to a common network.
- **Router Dead Interval** — The number of seconds that a router's Hello packets have not been seen before it's neighbors declare the router down. This should be some multiple of the Hello Interval. This value must be the same for all routers attached to a common network.
- **Poll Interval** — The larger time interval, in seconds, between the Hello packets sent to an inactive non-broadcast multi-access neighbor.
- **State** — The OSPF interface state.
- **Designated Router** — The IP address of the designated router.
- **Backup Designated Router** — The IP address of the backup designated router.
- **Events** — The number of times this OSPF interface has changed its state, or an error has occurred.
- **Auth. Key** — The authentication key.
- **Multicast Forwarding** — The way multicasts should be forwarded on this interface, not forwarded, forwarded as datalink multicasts or forwarded as data link unicasts. Data link multicasting is not meaningful on PPP and NBMA interfaces. The value 0 effectively disables all multicast forwarding.
- **Demand** — Indicates whether demand OSPF procedures (Hello suppression to FULL neighbors and setting the DoNotAge flag on propagated LSAs) should be performed on this interface.
- **Auth. Type** — The authentication type specified for an area. Additional authentication types may be assigned locally on a per area basis.

• **Interface Metric** — Displays interface metric parameters.
- **IP Address** — The IP address of the OSPF interface
- **Addressless IF** — Differentiates the addressless interfaces from the addressed interfaces. The value 0 signifies that the interface has an IP address.
- **TOS** — The Type Of Service (TOS) metric being referenced.
- **Value** — The metric of using this TOS on this interface. The default value of the TOS 0 metric is 10^8/Speed.

• **Virtual Interface** — Displays virtual interface parameters.
- **Area ID** — The transit area that the virtual link traverses. By definition, this is not 0.0.0.0.
- **Neighbor** — The router ID of the virtual neighbor.
- **Transit Delay** — The estimated number of seconds it takes to transmit a link state update packet over this interface.
- **Retransmit Interval** — The number of seconds between link state advertisement retransmissions, for adjacencies belonging to this interface. This value is also used when retransmitting the database

description and link state request packets. This value should be greater than the expected round-trip time.

- **Hello Interval** — The time interval, in seconds, between the Hello packets that the router sends on the interface. This value must be the same for the virtual neighbor.
- **Router Dead Interval** — The time interval, in seconds, during which a router's Hello packets are not received before its neighbors declare the router down. This is a multiple of the Hello interval. This value must be the same for the virtual neighbor.
- **State** — Signifies the OSPF virtual interface states.
- **Events** — The number of state changes or error events on this virtual link.
- **Auth. Key** — The authentication key.
- **Auth. Type** — The authentication type specified for a virtual interface. Additional authentication types may be assigned locally.

- **OSPF Configuration** — Opens the **OSPF Area Configuration** page, see Section 11.21 on page 181.
- **Reload** — Reloads the page with the latest information.

11.106 OSPF Neighbor Status

This page displays OSPF neighbor parameters.

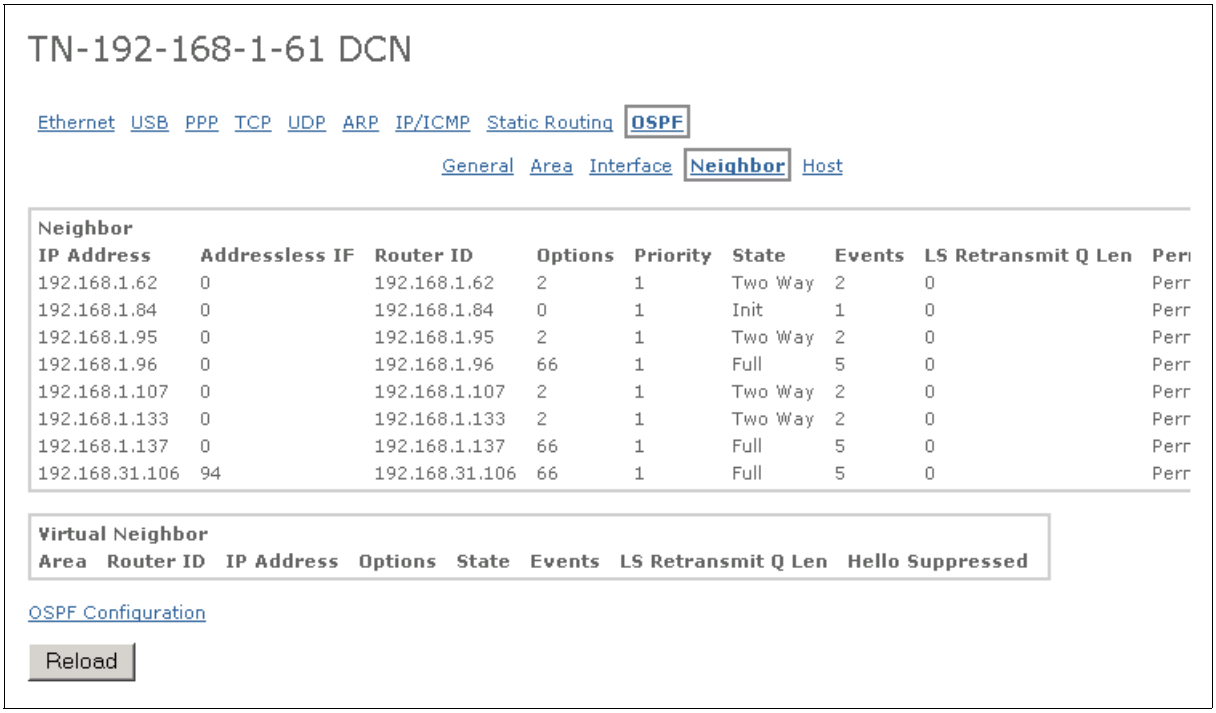


Figure 150 The OSPF Neighbor Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **Neighbor** — Displays neighbor parameters.
  - **IP Address** — The IP address this neighbor is using in its IP source address. Note that on addressless links, this will not be 0.0.0.0, but the address of another of the neighbor's interfaces.
  - **Addressless Interface** — Differentiates the addressless interfaces from the addressed interfaces. When the value is set to 0, it signifies that the interface has an IP address.
  - **Router ID** — A unique identifier of the neighboring router in the Autonomous System (AS).
  - **Options** — A bit mask corresponding to the neighbor's options field.

    Bit 0, if set, indicates that the system will operate on TOS metrics other than TOS 0. If the value is 0, the neighbor will ignore all metrics except the TOS 0 metric.

    Bit 1, if set, indicates that the associated area accepts and operates on external information. If the value is 0, it is a stub area.

    Bit 2, if set, indicates that the system is capable of routing IP multicast datagrams, implementing the multicast extensions to OSPF.

Bit 3, if set, indicates that the associated area is a Not So Stubby Area (NSSA). These areas are capable of carrying type 7 external advertisements, which are translated into type 5 external advertisements at NSSA borders.

- **Priority** — Signifies the priority of this neighbor in the designated router. When the value is set to 0, it signifies that the neighbor is not eligible to become the designated router on this particular network.
- **State** — The state of the relationship with this neighbor.
- **Events** — The number of times this neighbor relationship has changed state, or an error has occurred.
- **LS Retransmit Q Len** — The current length of the retransmission queue.
- **Permanence** — This variable displays the status of the entry. `Dynamic` and `Permanent` refer to how the neighbor became known.
- **Hello Suppressed** — Indicates whether Hellos are being suppressed to the neighbor.

- **Virtually Neighbor** — Displays virtual neighbor parameters.
  - **Area** — The transit area identifier.
  - **Router ID** — A unique identifier of the neighboring router in the Autonomous System (AS).
  - **IP Address** — The IP address this virtual neighbor is using.
  - **Options** — A bit mask corresponding to the neighbor's options field.

    Bit 1, if set, indicates that the system will operate on TOS metrics other than TOS 0. If the value is 0, the neighbor will ignore all metrics except the TOS 0 metric.

    Bit 2, if set, indicates that the system is network multicast capable, that is implementing OSPF multicast routing.
  - **State** — The state of the virtual neighbor relationship.
  - **Events** — The number of times this virtual link has changed its state, or an error has occurred.
  - **LS Retransmit Q Len** — The current length of the retransmission queue.
  - **Hello Suppressed** — Indicates whether Hellos are being suppressed to the neighbor.
- **OSPF Configuration** — Opens the **OSPF Area Configuration** page, see Section 11.21 on page 181.
- **Reload** — Reloads the page with the latest information.

11.107 OSPF Host Status

This page displays OSPF host parameters.

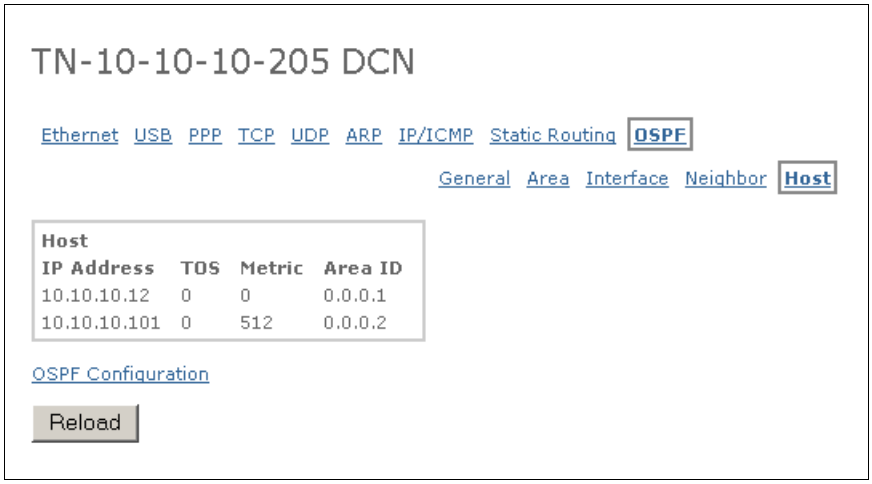


Figure 151 The OSPF Host Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **IP Address** — The IP Address of the host.
- **TOS** — The Type Of Service of the route being configured.
- **Metric** — The metric to be advertised.
- **Area ID** — The area the host entry is to be found within. By default, the area that a subsuming OSPF interface is in, or 0.0.0.0.
- **OSPF Configuration** — Opens the **OSPF Area Configuration** page, see Section 11.21 on page 181.
- **Reload** — Reloads the page with the latest information.

11.108 PFU Alarms and Status

This page displays the alarms and status of a PFU. A warning will be displayed if notifications from the unit are disabled.

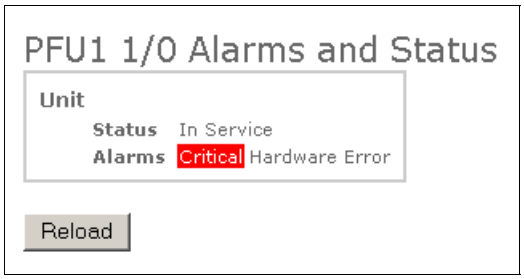


Figure 152 PFU Alarms and Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **Unit** — Alarms and status of the unit.
  - **Status** — Displays the operational status of the unit.
    - **In Service** — The unit is operating properly.
    - **Out of Service** — The unit is not operating or not present.
  - **Alarms** — Lists active alarms in the unit. See Section 7.2.5 on page 118 for alarm descriptions.
- **Reload** — Reloads the page with the latest information.

11.109 FAU Alarms and Status

This page displays the alarms and status of an FAU. A warning will be displayed if notifications from the unit are disabled.

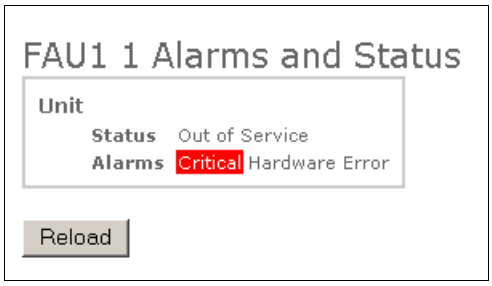


Figure 153 The FAU Alarms and Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **Unit** — Alarms and status of the unit.
  - **Status** — Displays the operational status of the unit.
    - **In Service** — The unit is operating properly.
    - **Out of Service** — The unit is not operating or not present.
  - **Alarms** — Lists active alarms in the unit. See Section 7.2.5 on page 118 for alarm descriptions.
- **Reload** — Reloads the page with the latest information.

11.110 NPU1 B Alarms and Status

This page displays the alarms and status of the NPU1 B and provides links to the E1 interfaces and user I/O ports. A warning will be displayed if notifications from the unit are disabled.

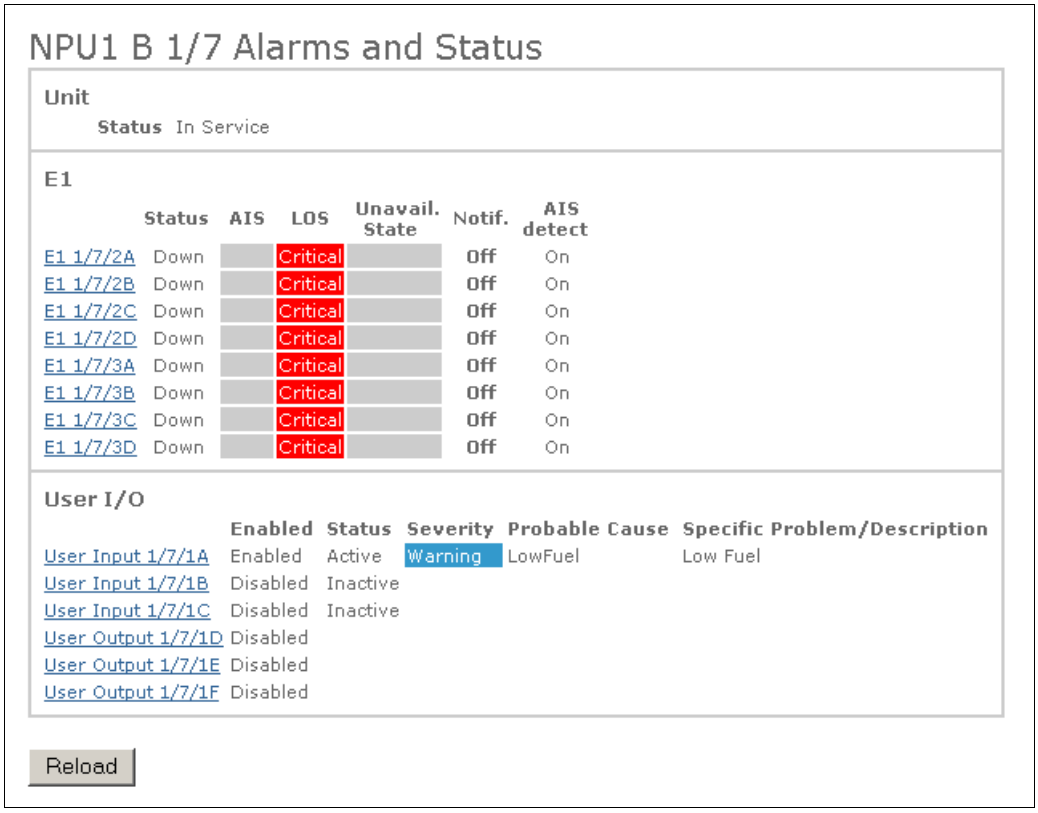


Figure 154 The NPU1 B Alarms and Status

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **Unit** — Alarms and status of the unit.
  - **Status** — Displays the operational status of the unit.
    - **In Service** — The unit is operating properly.
    - **Reduced Service** — Traffic is running but the management functionality is reduced or unavailable. The unit is in a warm reset state where all control and management logic is reset.
    - **Out of Service** — The unit is not operating. The unit is in a cold reset state where all traffic, control and management logics are reset.
  - **Alarms** — Lists active alarms in the unit. See Section 7.2.5 on page 118 for alarm descriptions.
- **E1** — Alarms and status of the E1 interfaces. See Section 7.2.5 on page 118 for alarm descriptions. Clicking a link opens the **E1 Alarms and Status**

page, where a complete alarm description can be found, see Section 11.124 on page 337.

- **User I/O** — Alarms and status of the User Input/Output ports. See Section 7.2.5 on page 118 for alarm descriptions. Clicking a link opens the **User Input Alarms and Status** and **User Output Alarms and Status** pages, where complete alarm descriptions can be found, see Section 11.131 on page 347 and Section 11.132 on page 348.
- **Reload** — Reloads the page with the latest information.

11.111 NPU 8x2 Alarms and Status

This page displays the alarms and status of the NPU 8x2 and provides links to the E1 interfaces and user I/O ports. A warning will be displayed if notifications from the unit are disabled.

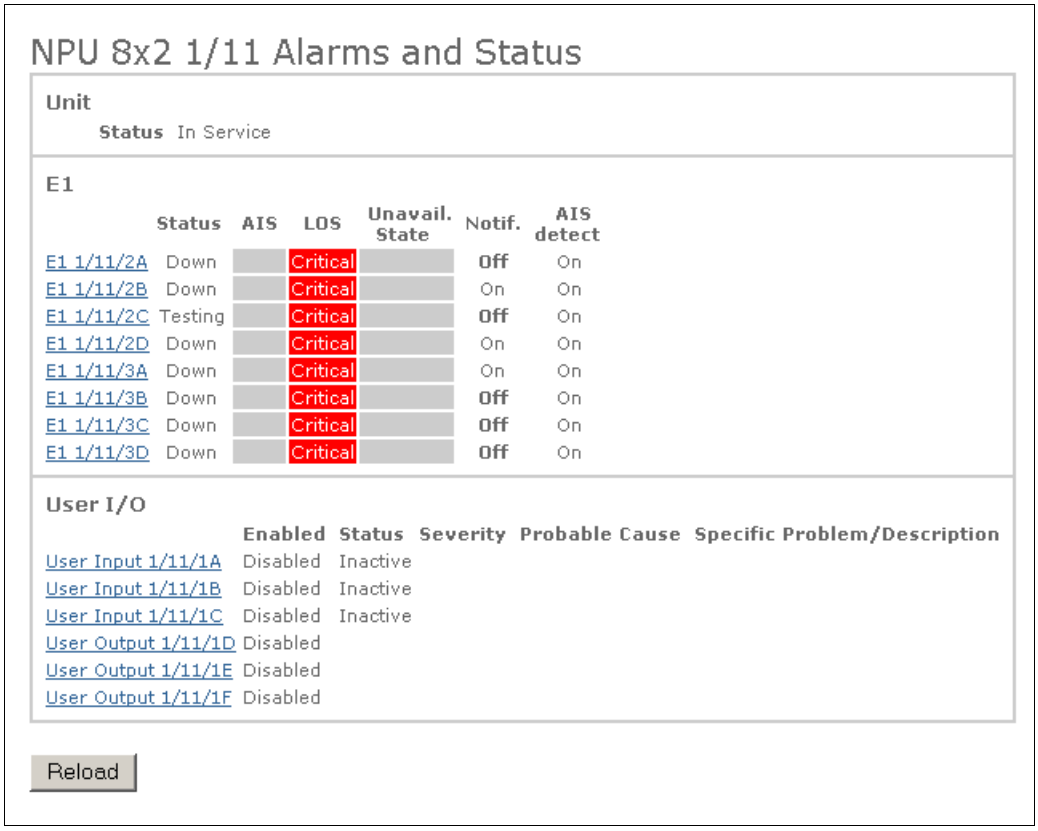


Figure 155 The NPU 8x2 Alarms and Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **Unit** — Alarms and status of the unit.
  - **Status** — Displays the operational status of the unit.
    - **In Service** — The unit is operating properly.
    - **Reduced Service** — Traffic is running but the management functionality is reduced or unavailable. The unit is in a warm reset state where all control and management logic is reset.
    - **Out of Service** — The unit is not operating. The unit is in a cold reset state where all traffic, control and management logics are reset.
  - **Alarms** — Lists active alarms in the unit. See Section 7.2.5 on page 118 for alarm descriptions.
- **E1** — Alarms and status of the E1 interfaces. See Section 7.2.5 on page 118 for alarm descriptions. Clicking a link opens the **E1 Alarms and Status**

page, where a complete alarm description can be found, see Section 11.124 on page 337.

- **User I/O** — Alarms and status of the User Input/Output ports. See Section 7.2.5 on page 118 for alarm descriptions. Clicking a link opens the **User Input Alarms and Status** and **User Output Alarms and Status** pages, where complete alarm descriptions can be found, see Section 11.131 on page 347 and Section 11.132 on page 348.
- **Reload** — Reloads the page with the latest information.

11.112 NPU2/ATU NPU Alarms and Status

This page displays the alarms and status of the NPU2 or ATU NPU and provides links to its interfaces. A warning will be displayed if notifications from the unit are disabled.

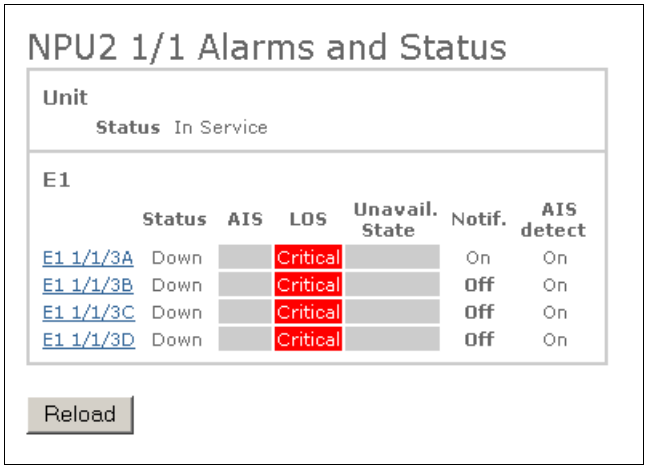


Figure 156 The NPU2/ATU NPU Alarms and Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **Unit** — Alarms and status of the unit.
  - **Status** — Displays the operational status of the unit.
    - **In Service** — The unit is operating properly.
    - **Reduced Service** — Traffic is running but the management functionality is reduced or unavailable. The unit is in a warm reset state where all control and management logic is reset.
    - **Out of Service** — The unit is not operating. The unit is in a cold reset state where all traffic, control and management logics are reset.
  - **Alarms** — Lists active alarms in the unit. See Section 7.2.5 on page 118 for alarm descriptions.
- **E1** — Alarms and status of the E1 interfaces. See Section 7.2.5 on page 118 for alarm descriptions. Clicking a link opens the **E1 Alarms and Status** page, where a complete alarm description can be found, see Section 11.124 on page 337.
- **Bridge** — Alarms and status of the Bridge interface on ATU (B). See Section 7.2.5 on page 118 for alarm descriptions. Clicking the link opens the **Bridge Alarms and Status** page, where a complete status description can be found, see Section 11.93 on page 285.
- **Reload** — Reloads the page with the latest information.

11.113 LTU 16x2 Alarms and Status

This page displays the alarms and status of the LTU 16x2 and provides links to the E1 interfaces. A warning will be displayed if notifications from the unit are disabled.

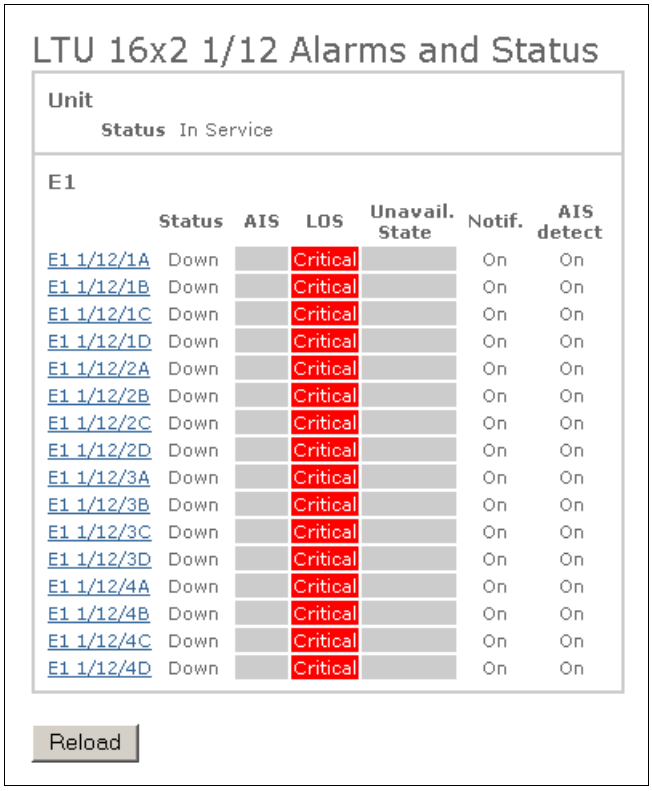


Figure 157 The LTU 16x2 Alarms and Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **Unit** — Alarms and status of the unit.
  - **Status** — Displays the operational status of the unit.
    - **In Service** — The unit is operating properly.
    - **Reduced Service** — Traffic is running but the management functionality is reduced or unavailable. The unit is in a warm reset state where all control and management logic is reset.
    - **Out of Service** — The unit is not operating. The unit is in a cold reset state where all traffic, control and management logics are reset.
  - **Severity** — Displays a color-coded severity for each active alarm. See also Section 7.2.4 on page 117.
  - **Alarms** — Lists active alarms in the unit. See Section 7.2.5 on page 118 for alarm descriptions.
- **E1** — Alarms and status of the E1 interfaces. See Section 7.2.5 on page 118 for alarm descriptions. Clicking a link opens the **E1 Alarms and Status**

page, where a complete alarm description can be found, see Section 11.124 on page 337.

- **Reload** — Reloads the page with the latest information.

11.114 LTU 12x2 Alarms and Status

This page displays the alarms and status of the LTU 12x2 and provides links to the E1 interfaces. A warning will be displayed if notifications from the unit are disabled.

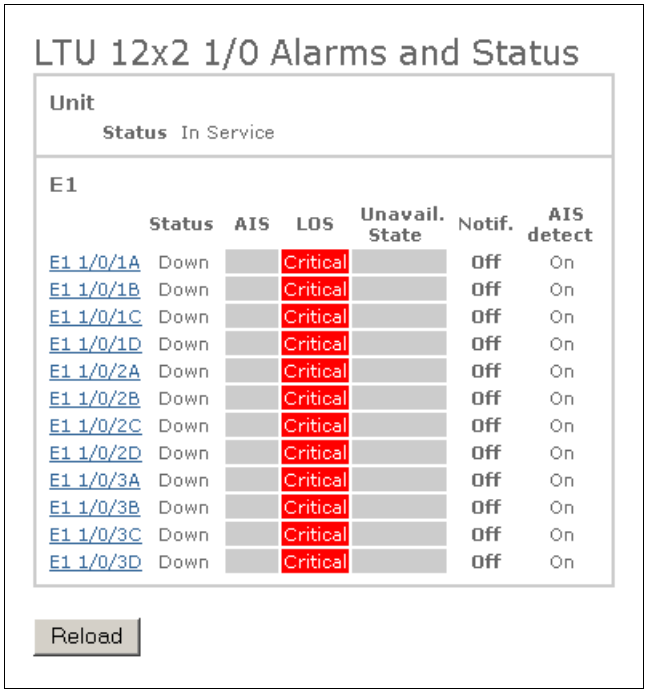


Figure 158 The LTU 12x2 Alarms and Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **Unit** — Alarms and status of the unit.
  - **Status** — Displays the operational status of the unit.
    - **In Service** — The unit is operating properly.
    - **Reduced Service** — Traffic is running but the management functionality is reduced or unavailable. The unit is in a warm reset state where all control and management logic is reset.
    - **Out of Service** — The unit is not operating. The unit is in a cold reset state where all traffic, control and management logics are reset.
  - **Alarms** — Lists active alarms in the unit. See Section 7.2.5 on page 118 for alarm descriptions.
- **E1** — Alarms and status of the E1 interfaces. See Section 7.2.5 on page 118 for alarm descriptions. Clicking a link opens the **E1 Alarms and Status** page, where a complete alarm description can be found, see Section 11.124 on page 337.
- **Reload** — Reloads the page with the latest information.

11.115 LTU 155 Alarms and Status

This page displays the alarms and status of the LTU 155 and its STM-1 port and provides a link to the MS/RS interface. A warning will be displayed if notifications from the unit are disabled.

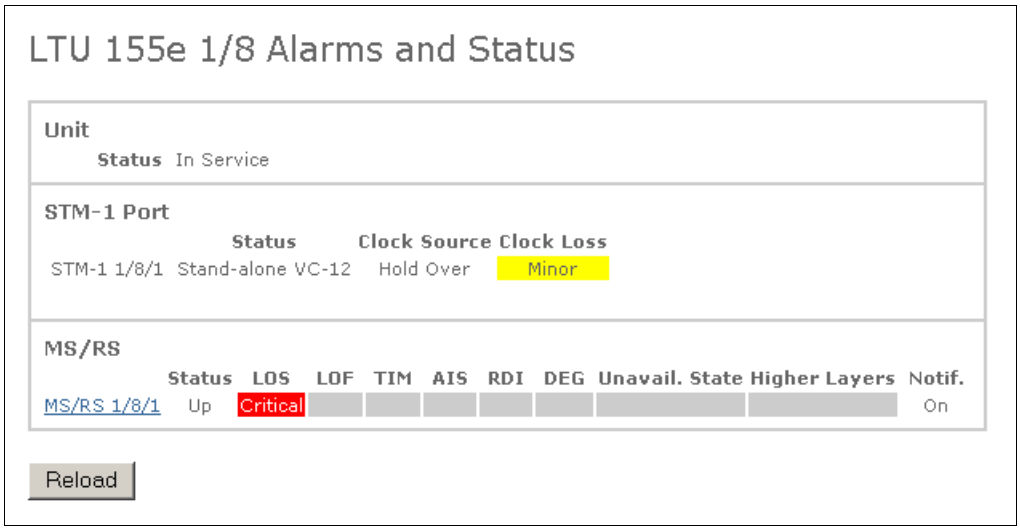


Figure 159 The LTU 155 Alarms and Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **Unit** — Alarms and status of the unit.
  - **Status** — Displays the operational status of the unit.
    - **In Service** — The unit is operating properly.
    - **Reduced Service** — Traffic is running but the management functionality is reduced or unavailable. The unit is in a warm reset state where all control and management logic is reset.
    - **Out of Service** — The unit is not operating. The unit is in a cold reset state where all traffic, control and management logics are reset.
  - **Alarms** — Lists active alarms in the unit. See Section 7.2.5 on page 118 for alarm descriptions.
- **STM-1 Port** — Displays the alarms and status of the STM-1 port. Only available if the administrative status of the MS/RS interface is Up.
  - **Status** — Displays the operational status of the STM-1 port.
    - **Not Configured** — The port does not provide traffic until it is configured.
    - **Stand-alone VC-12** — The port has 63 E1 interfaces and operates alone.
    - **MSP 1+1 VC-12** — The port is protected sharing 63 E1 interfaces with the port on the adjacent unit.

    - **Wait For Neighbour** — Indicates that the port in the adjacent unit should be configured as `MSP 1+1 VC-12`, but it is not yet ready or the unit is being repaired, removed or otherwise faulty.
  - **Clock Source** — Displays the operational status of the clock source.
    - **Rx Clock** — The recovered receive clock is used as the transmit clock.
    - **Internal** — The local clock source is used as the transmit clock.
    - **Hold Over** — The last reference is preserved.
    - **Free Running** — The clock source from the SEC module is used (SEC accuracy).
    - **SEC Passive** — The SEC module is passive.
  - **Alarms** — Lists active alarms on the port. See Section 7.2.5 on page 118 for alarm descriptions.
- **MS/RS** — Alarms and status of the MS/RS interface. See Section 7.2.5 on page 118 for alarm descriptions. Clicking a link opens the **MS/RS Alarms and Status** page, where a complete alarm description can be found, see Section 11.127 on page 340. **Unavail. State** indicates the worst severity of the near-end and far-end Unavailable State alarms. **Higher Layer** indicates the worst severity of the alarms on higher layer interfaces.
- **Reload** — Reloads the page with the latest information.

11.116 Radio Terminal Alarms and Status

This page gives alarms and status information for a near-end Radio Terminal based on MMU2 B and MMU2 C.

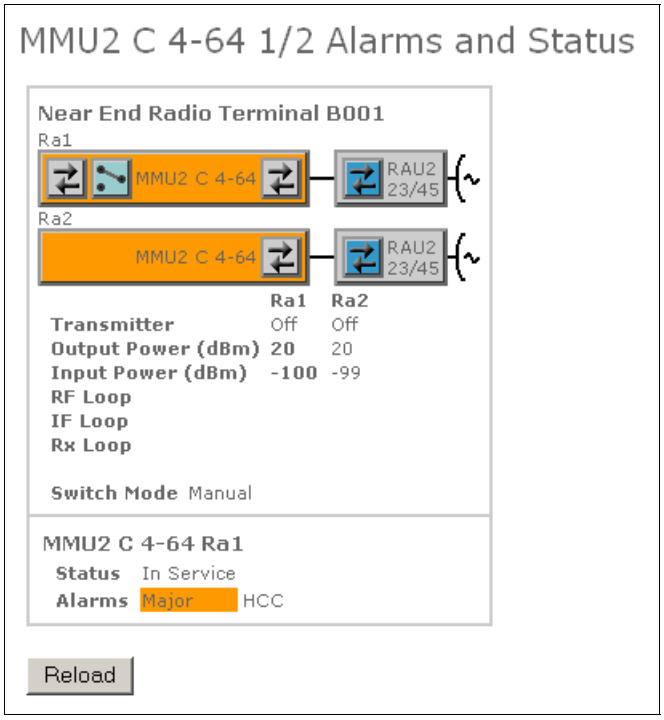


Figure 160 The Radio Terminal Alarms and Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

The upper part of the page illustrates the Radio Terminal, with rectangles representing the units and framed arrows representing the different interfaces. The MMU holds the traffic interfaces (E1, E2 and E3) and the RAU IF. The RAU holds the RF interface. For a protected Radio Terminal, a SWITCH interface is available on the active MMU.

The highest alarm severity for each entity is indicated by a color and detailed information is displayed in the lower part when clicking a specific entity. Tool tips are provided when the pointer is moved over a unit or an interface.

- **Radio Terminal <ID>** — The identity of the Radio Terminal.
  - **Transmitter** — Displays the status of the transmitter in the RAU.
  - **RF Loop** — Displays if an RF loop is set.
  - **IF Loop** — Displays if an IF loop is set.
  - **Active Tx** — For a protected Radio Terminal. Displays the active TDM Tx (Ra1/Ra2).
  - **Switch Mode** — For a protected Radio Terminal. Displays if manual or automatic switch mode is set.

  - **Active Rx** — For a protected Radio Terminal. Displays the active TDM Rx (Ra1/Ra2).
- **MMU2 B/C <ID>** — Displays alarms and status information for the MMU. A warning will be displayed if notifications are disabled.
  - **Status** — Displays the operational status of the unit.
    - **In Service** — The unit is operating properly.
    - **Reduced Service** — Traffic is running but the management functionality is reduced or unavailable. The unit is in a warm reset state where all control and management logic is reset.
    - **Out of Service** — The unit is not operating. The unit is in a cold reset state where all traffic, control and management logics are reset.
  - **Alarms** — Lists active alarms in the unit. See Section 7.2.5 on page 118 for alarm descriptions.
- **E3** — Displays alarms and status for the E3 interface, if applicable. See Section 7.2.5 on page 118 for alarm descriptions. Clicking an interface link opens the **E3 Alarms and Status** page, see Section 11.126 on page 339.
  - **Status** — Displays the operational status of the interface.
    - **Up** — Payload is passing on the interface and one or more of the active lower layers have operational status Up.
    - **Down** — A defect is detected on the interface or administrative status is set to Down.
    - **Unknown** — The unit is in cold reset, warm reset or repair state.
  - **Alarms** — Displays active alarms in the interface. See Section 7.2.5 on page 118 for alarm descriptions.
  - **Notif.** — Displays if notifications from the interface are enabled or disabled.
  - **AIS detect** — Displays if AIS detection is enabled or disabled.
- **E2** — Displays alarms and status for the E2 interface(s), if applicable. See Section 7.2.5 on page 118 for alarm descriptions. Clicking an interface link opens the **E2 Alarms and Status** page, see Section 11.125 on page 338.
  - **Status** — Displays the operational status of the interface.
    - **Up** — Payload is passing on the interface and one or more of the active lower layers have operational status Up.
    - **Down** — A defect is detected on the interface or administrative status is set to Down.
    - **Unknown** — The unit is in cold reset, warm reset or repair state.
    - **Lower Layer Down** — The interface is Down due to lower layer interfaces. Payload is passing on the interface but not all active lower layers have operational status Up.
  - **Alarms** — Displays active alarms in the interface. See Section 7.2.5 on page 118 for alarm descriptions.
  - **Notif.** — Displays if notifications from the interface are enabled or disabled.
  - **AIS detect** — Displays if AIS detection is enabled or disabled.

- **E1** — Displays alarms and status for the E1 interfaces. See Section 7.2.5 on page 118 for alarm descriptions. Clicking an interface link opens the **E1 Alarms and Status** page, see Section 11.124 on page 337.
  - **Status** — Displays the operational status of the interface.
    - **Up** — Payload is passing on the interface.
    - **Down** — A defect is detected on the interface or administrative status is set to Down.
    - **Lower Layer Down** — The interface is Down due to lower layer interfaces. Payload is passing on the interface but not all active lower layers have operational status Up.
    - **Testing** — The interface is in test mode, for example a loop is active or a BERT is running.
    - **Unknown** — The unit is in cold reset, warm reset or repair state.
  - **Alarms** — Displays active alarms in the interface. See Section 7.2.5 on page 118 for alarm descriptions.
  - **Notif.** — Displays if notifications from the interface are enabled or disabled.
  - **AIS detect** — Displays if AIS detection is enabled or disabled.
- **RAU IF** — Displays alarms and status information for the MMU's interface with the RAU. See Section 7.2.5 on page 118 for alarm descriptions. A warning will be displayed if notifications are disabled.
  - **Status** — Displays the operational status of the interface.
    - **Up** — Payload is passing on the interface.
    - **Down** — A defect is detected on the interface or administrative status is set to Down.
    - **Lower Layer Down** — The interface is Down due to lower layer interfaces. Payload is passing on the interface but not all active lower layers have operational status Up.
    - **Testing** — The interface is in test mode, for example a loop is active or a BERT is running.
    - **Unknown** — The unit is in cold reset, warm reset or repair state.
  - **Alarms** — Lists active alarms in the interface. See Section 7.2.5 on page 118 for alarm descriptions.
- **RAU** — Displays alarms and status information for the RAU. See Section 7.2.5 on page 118 for alarm descriptions. A warning will be displayed if notifications are disabled.
  - **Status** — Displays the operational status of the unit.
    - **In Service** — The unit is operating properly.
    - **Reduced Service** — Traffic is running but the management functionality is reduced or unavailable.
    - **Out of Service** — The unit is not operating. The transmitter is turned off.
  - **Alarms** — Lists active alarms in the unit. See Section 7.2.5 on page 118 for alarm descriptions.
- **RF** — Displays alarms and status information for the RF interface. See Section 7.2.5 on page 118 for alarm descriptions. A warning will be displayed if notifications are disabled.

  - **Status** — Displays the operational status of the interface.
    - **Up** — The transmitter is on, no loop is set and no RCC alarm is active.
    - **Down** — The transmitter is off or an RCC alarm is active.
    - **Testing** — The transmitter is on and a loop is set.
  - **Alarms** — Lists active alarms in the interface. See Section 7.2.5 on page 118 for alarm descriptions.
- **SWITCH** — Displays alarms and status information for the SWITCH interface in a protected Radio Terminal. See Section 7.2.5 on page 118 for alarm descriptions. A warning will be displayed if notifications are disabled.
  - **Status** — Displays the operational status of the interface.
    - **Up** — Payload is passing on the interface.
    - **Down** — A defect is detected on the interface or administrative status is set to Down.
    - **Lower Layer Down** — The interface is Down due to lower layer interfaces. Payload is passing on the interface but not all active lower layers have operational status Up.
    - **Testing** — The interface is in test mode, for example a loop is active or a BERT is running.
  - **Alarms** — Lists active alarms in the interface. See Section 7.2.5 on page 118 for alarm descriptions.
- **Reload** — Reloads the page with the latest information.

11.117 MMU2 Alarms and Status

This page provides alarms and status information for the MMU2.

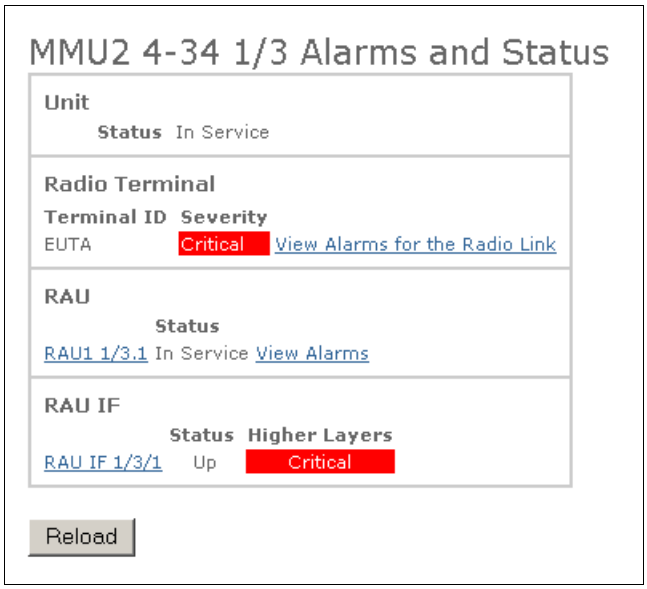


Figure 161 The MMU2 Alarms and Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

Note: It is important to use MSM or MINI-LINK E Adapter to get the complete set of alarms for the terminal.

A warning will be displayed if notifications from the unit are disabled.

- **Unit** — Alarms and status of the unit.
  - **Status** — Displays the operational status of the unit.
    - **In Service** — The unit is operating properly.
    - **Reduced Service** — Traffic is running but the management functionality is reduced or unavailable. The unit is in a warm reset state where all control and management logic is reset.
    - **Out of Service** — The unit is not operating. The unit is in a cold reset state where all traffic, control and management logics are reset.
  - **Alarms** — Lists active alarms in the unit. See Section 7.2.5 on page 118 for alarm descriptions.
- **Radio Terminal** — Provides a summary alarm for the Radio Terminal.
  - **Terminal ID** — The terminal identity.
  - **Severity** — The severity of the summary alarm.
  - **View Alarms for the Radio Link** — Starts MSM or MINI-LINK E Adapter for the selected terminal providing complete alarm information.
- **RAU** — Links associated with the RAU.

  - **RAU <ID>** — Opens the **RAU Alarms and Status** page, see Section 11.118 on page 328.
  - **Status** — The status of the unit.
  - **View Alarms** — Starts MSM or MINI-LINK E Adapter displaying the alarms for the RAU.
- **RAU IF** — Provides a link to the interface with the RAU.
  - **RAU IF <ID>** — Opens the **RAU IF Alarms and Status** page, see Section 11.120 on page 331.
  - **Status** — The status of the interface.
  - **Higher Layers** — Indicates the worst severity of the alarms on higher layer interfaces.
- **Reload** — Reloads the page with the latest information.

11.118 RAU Alarms and Status for MMU2

This page provides alarms and status information for an RAU connected to an MMU2.

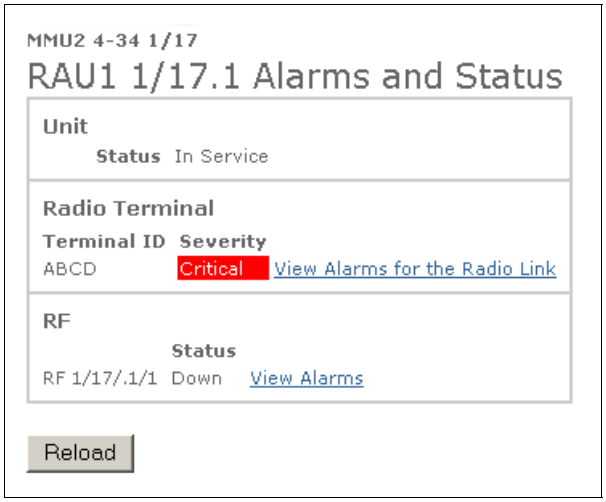


Figure 162 The RAU Alarms and Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

Note: It is important to use MSM or MINI-LINK E Adapter to get the complete set of alarms for the terminal. There are alarms on the RAU that will not be displayed on this page.

A warning will be displayed if notifications from the unit are disabled.

- **Unit** — Alarms and status of the unit.
  - **Status** — Displays the operational status of the unit.
    - **In Service** — The unit is operating properly.
    - **Reduced Service** — Traffic is running but the management functionality is reduced or unavailable.
    - **Out of Service** — The unit is not operating. The transmitter is turned off.
  - **Alarms** — Lists active alarms in the unit. See Section 7.2.5 on page 118 for alarm descriptions.
- **Radio Terminal** — Provides a summary alarm for the Radio Terminal.
  - **Terminal ID** — The terminal identity.
  - **Severity** — The severity of the summary alarm.
  - **View Alarms for the Radio Link** — Starts MSM or MINI-LINK E Adapter for the selected terminal providing complete alarm information.
- **RF** — Information about the interface with the antenna.
  - **RF <ID>** — The RF interface identity.
  - **Status** — The status of the interface.
  - **View Alarms** — Starts MSM or MINI-LINK E Adapter displaying the alarms for the interface.

- **Reload** — Reloads the page with the latest information.

11.119 RF Alarms and Status for MMU2

This page displays the status of the RF interface, on an RAU connected to an MMU2, which is the interface between the RAU and antenna.

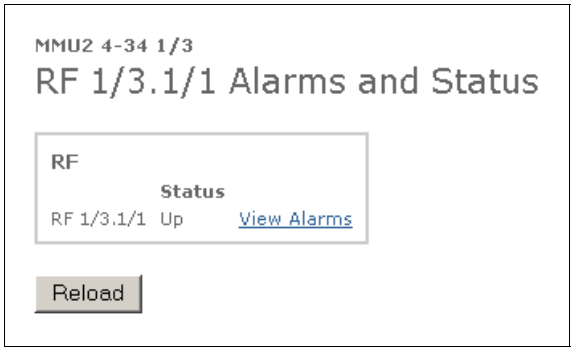


Figure 163 The RF Alarms and Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **RF** — Provides a link to MSM or MINI-LINK E Adapter.
  - **RF <ID>** — The RF interface identity.
  - **Status** — Displays the operational status of the interface.
    - **Up** — The transmitter is on, no loop is set and no RCC alarm is active.
    - **Down** — The transmitter is off or an RCC alarm is active.
    - **Testing** — The transmitter is on and a loop is set.
  - **View Alarms** — Starts MSM or MINI-LINK E Adapter displaying the alarms for the interface.
- **Reload** — Reloads the page with the latest information.

11.120 RAU IF Alarms and Status for MMU2

This page provides alarm and status information for RAU IF on an MMU2, which is the MMU2's interface with the RAU.

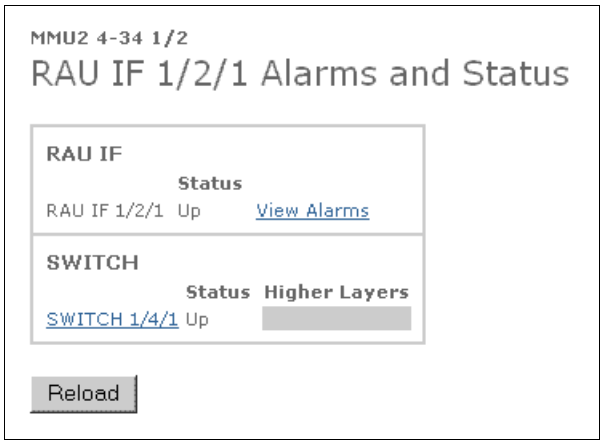


Figure 164 The RAU IF Alarms and Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **RAU IF** — Provides a link to MSM or MINI-LINK E Adapter.
  - **RAU IF <ID>** — The RAU IF interface identity.
  - **Status** — Displays the operational status of the interface. For this release the status will always be Up.
  - **View Alarms** — Starts MSM or MINI-LINK E Adapter displaying the alarms for the interface.
- **SWITCH** — Provides a link to the SWITCH interface for a 1+1 terminal.
  - **SWITCH <ID>** — Opens the **SWITCH Alarms and Status** page, see Section 11.121 on page 333.
  - **Status** — The status of the interface.
  - **Higher Layer** — Indicates the worst severity of the alarms on higher layer interfaces.
- **E3** — Alarms and status information for the E3 interface. See Section 7.2.5 on page 118 for alarm descriptions. Only available for a 1+0 terminal using this traffic rate.
  - **E3 <ID>** — Opens the **E3 Alarms and Status** page, where a complete alarm description can be found, see Section 11.126 on page 339. **Higher Layer** indicates the worst severity of the alarms on higher layer interfaces.
- **E2** — Alarms and status information for the E2 interfaces. See Section 7.2.5 on page 118 for alarm descriptions. Only available for a 1+0 terminal using this traffic rate.
  - **E2 <ID>** — Opens the **E2 Alarms and Status** page, where a complete alarm description can be found, see Section 11.125 on page 338. **Higher Layer** indicates the worst severity of the alarms on higher layer interfaces.

- **E1** — Alarms and status information for the E1 interfaces. See Section 7.2.5 on page 118 for alarm descriptions. Only available for a 1+0 terminal using this traffic rate.
  - **E1 <ID>** — Opens the **E1 Alarms and Status** page, where a complete alarm description can be found, see Section 11.124 on page 337.
- **Reload** — Reloads the page with the latest information.

11.121 SWITCH Alarms and Status for MMU2

This page provides alarm and status information for the SWITCH interface in a protected Radio Terminal with MMU2 and SMU2.

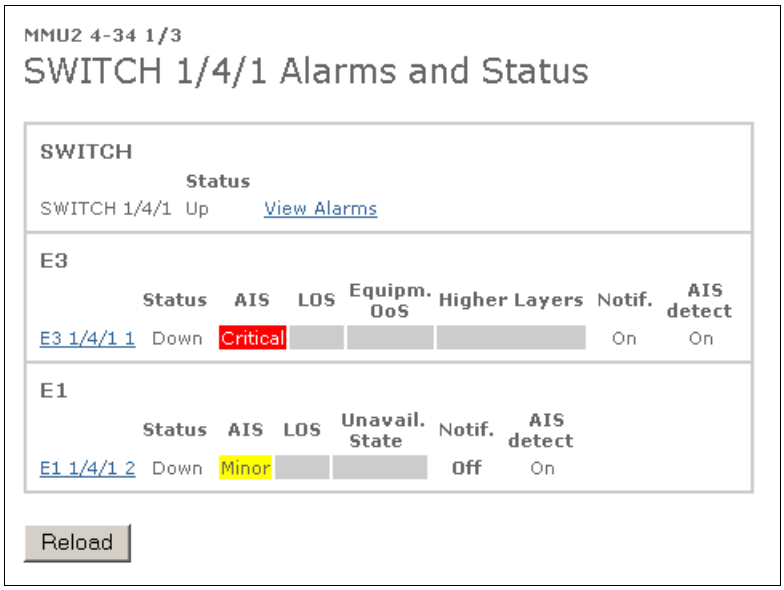


Figure 165 The SWITCH Alarms and Status page

- **SWITCH** — Provides a link to MSM or MINI-LINK E Adapter.
  - **SWITCH <ID>** — The SWITCH interface identity.
  - **Status** — Displays the operational status of the interface. For this release the status will always be Up.
  - **View Alarms** — Starts MSM or MINI-LINK E Adapter.
- **E3** — Alarms and status information for the E3 interface. See Section 7.2.5 on page 118 for alarm descriptions. Only available when this traffic rate is used.
  - **E3 <ID>** — Opens the **E3 Alarms and Status** page, where a complete alarm description can be found, see Section 11.126 on page 339. **Higher Layer** indicates the worst severity of the alarms on higher layer interfaces.
- **E2** — Alarms and status information for the E2 interfaces. See Section 7.2.5 on page 118 for alarm descriptions. Only available when this traffic rate is used.
  - **E2 <ID>** — Opens the **E2 Alarms and Status** page, where a complete alarm description can be found, see Section 11.125 on page 338. **Higher Layer** indicates the worst severity of the alarms on higher layer interfaces.
- **E1** — Alarms and status information for the E1 interfaces. See Section 7.2.5 on page 118 for alarm descriptions. Only available when this traffic rate is used.
  - **E1 <ID>** — Opens the **E1 Alarms and Status** page, where a complete alarm description can be found, see Section 11.124 on page 337.
- **Reload** — Reloads the page with the latest information.

11.122 SMU2 Alarms and Status

This page provides alarms and status information for the SMU2.

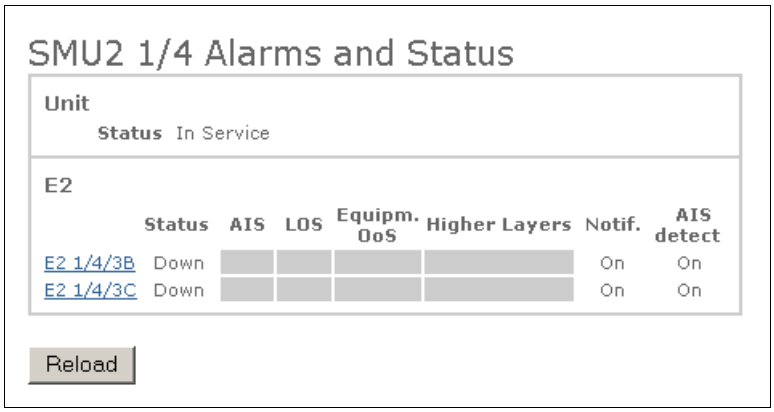


Figure 166 The SMU2 Alarms and Status page (co-siting)

Note: The page is not updated automatically. Click **Reload** to display the latest information.

Note: When SMU2 is used for protection, it is important to use MSM or MINI-LINK E Adapter to get the complete set of alarms for the terminal.

A warning will be displayed if notifications from the unit are disabled.

- **Unit** — Alarms and status of the unit.
  - **Status** — Displays the operational status of the unit.
    - **In Service** — The unit is operating properly.
    - **Reduced Service** — Traffic is running but the management functionality is reduced or unavailable. The unit is in a warm reset state where all control and management logic is reset.
    - **Out of Service** — The unit is not operating. The unit is in a cold reset state where all traffic, control and management logics are reset.
  - **Alarms** — Lists active alarms in the unit. See Section 7.2.5 on page 118 for alarm descriptions.
- **Radio Terminal** — Provides a summary alarm for the Radio Terminal. Only available if the SMU2 is configured for protection.
  - **Terminal ID** — The terminal identity.
  - **Severity** — The severity of the summary alarm.
  - **View Alarms for the Radio Link** — Starts MSM or MINI-LINK E Adapter for the selected terminal providing complete alarm information.
- **E3** — Alarms and status information for the E3 interface. See Section 7.2.5 on page 118 for alarm descriptions. Only available if the SMU is configured for co-siting using this traffic rate.
  - **E3 <ID>** — Opens the **E3 Alarms and Status** page, where a complete alarm description can be found, see Section 11.126 on page 339. **Higher Layer** indicates the worst severity of the alarms on higher layer interfaces.

- **E2** — Alarms and status information for the E2 interfaces. See Section 7.2.5 on page 118 for alarm descriptions. Only available if the SMU is configured for co-siting using this traffic rate. **Higher Layer** indicates the worst severity of the alarms on higher layer interfaces.
  - **E2 <ID>** — Opens the **E2 Alarms and Status** page, where a complete alarm description can be found, see Section 11.125 on page 338.
- **E1** — Alarms and status information for the E1 interfaces. See Section 7.2.5 on page 118 for alarm descriptions. Only available if the SMU is configured for co-siting using this traffic rate.
  - **E1 <ID>** — Opens the **E1 Alarms and Status** page, where a complete alarm description can be found, see Section 11.124 on page 337.
- **Reload** — Reloads the page with the latest information.

11.123 Unsupported Unit Alarms and Status

This page displays the alarms and status of a unit not supported by the currently installed software. Make sure you have installed the latest software version. For information on how to perform a software upgrade, see Section 6.12 on page 91.

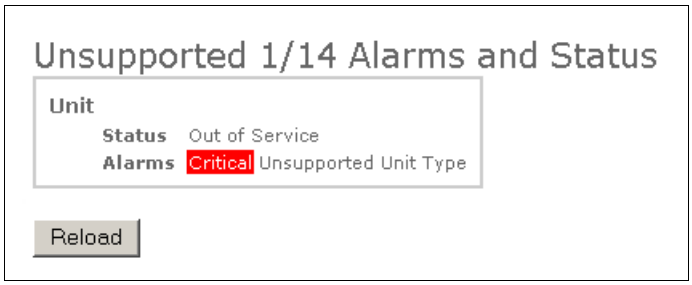


Figure 167 The Unsupported Unit Alarms and Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

A warning will be displayed if notifications from the unit are disabled.

- **Status** — Displays the operational status of the unit.
  - **In Service** — The unit is operating properly.
  - **Reduced Service** — Traffic is running but the management functionality is reduced or unavailable. The unit is in a warm reset state where all control and management logic is reset.
  - **Out of Service** — The unit is not operating. The unit is in a cold reset state where all traffic, control and management logics are reset.
- **Alarms** — Lists active alarms in the unit. See Section 7.2.5 on page 118 for alarm descriptions.
- **Reload** — Reloads the page with the latest information.

11.124 E1 Alarms and Status

This page displays the alarms and status of the interface. If the E1 interface is part of a 1+1 E1 SNCP protection the operational status and alarms on the protected E1 interface is displayed as well. A protected interface is denoted with an asterisk (*) at the end of the name.

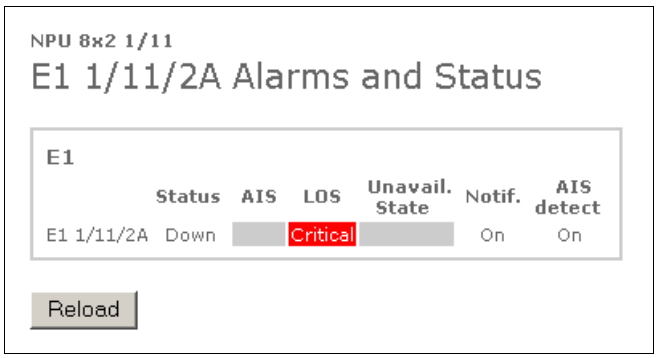


Figure 168 The E1 Alarms and Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **Status** — Displays the operational status of the interface.
  - **Up** — Payload is passing on the interface.
  - **Down** — A defect is detected on the interface or administrative status is set to Down.
  - **Lower Layer Down** — The interface is Down due to lower layer interfaces. Payload is passing on the interface but not all active lower layers have operational status Up.
  - **Testing** — The interface is in test mode, for example a loop is active or a BERT is running.
  - **Unknown** — The unit is in cold reset, warm reset or repair state.
- **Alarms** — Lists active alarms on the interface. See Section 7.2.5 on page 118 for alarm descriptions.
- **Notif.** — Displays if notifications from the interface are enabled or disabled.
- **AIS detect** — Displays if AIS detection is enabled or disabled.
- **Reload** — Reloads the page with the latest information.

11.125 E2 Alarms and Status

This page displays the alarms and status of the interface and provides links to the E1 interfaces.

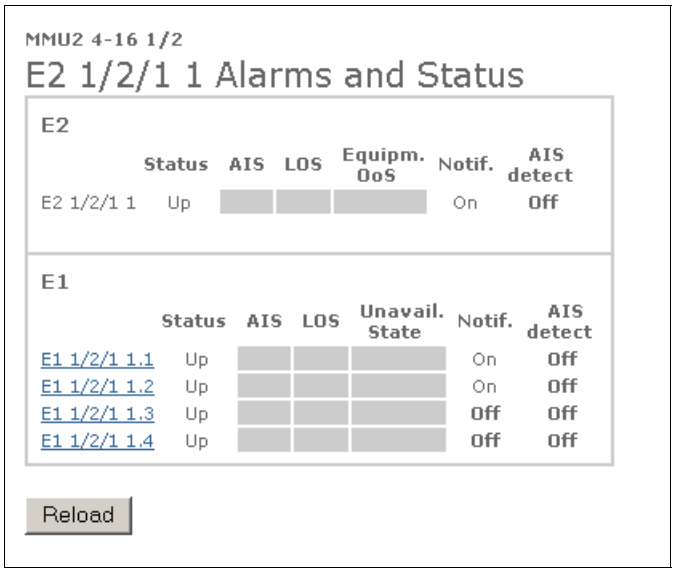


Figure 169 The E2 Alarms and Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **E2** — Alarms and status of the selected E2 interface.
  - **Status** — Displays the operational status of the interface.
    - **Up** — Payload is passing on the interface and one or several of the active lower layers have operational status Up.
    - **Down** — A defect is detected on the interface or administrative status is set to Down.
    - **Unknown** — The unit is in cold reset, warm reset or repair state.
    - **Lower Layer Down** — The interface is Down due to lower layer interfaces. Payload is passing on the interface but not all active lower layers have operational status Up.
  - **Alarms** — Lists active alarms on the interface. See Section 7.2.5 on page 118 for alarm descriptions.
  - **Notif.** — Displays if notifications from the interface are enabled or disabled.
  - **AIS detect** — Displays if AIS detection is enabled or disabled.
- **E1** — Alarms and status of the E1 interfaces. See Section 7.2.5 on page 118 for alarm descriptions. Clicking a link opens the **E1 Alarms and Status** page, where a complete alarm description can be found, see Section 11.124 on page 337.
- **Reload** — Reloads the page with the latest information.

11.126 E3 Alarms and Status

This page displays the alarms and status of the interface and provides links to the E2 interfaces.

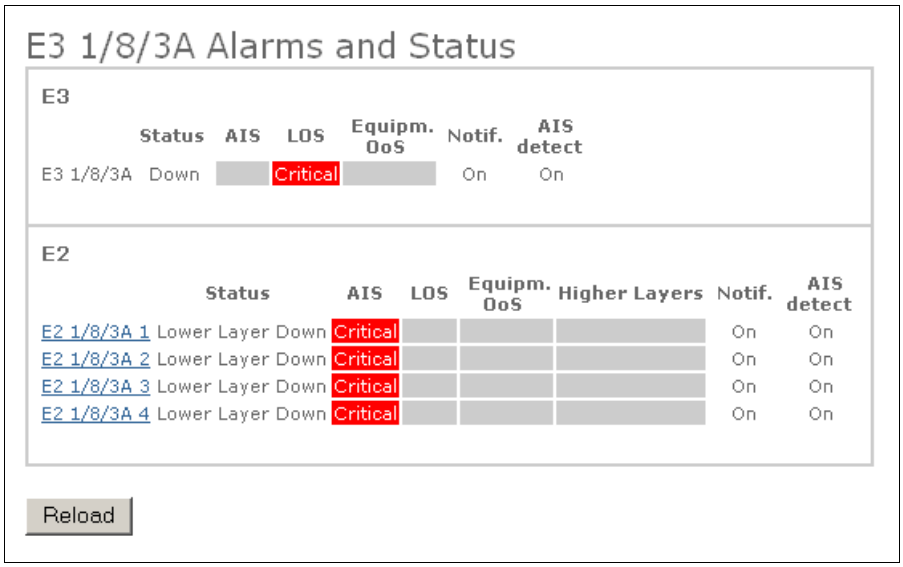


Figure 170 The E3 Alarms and Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **E3** — Alarms and status of the selected E3 interface.
  - **Status** — Displays the operational status of the interface.
    - **Up** — Payload is passing on the interface and one or more of the active lower layers have operational status Up.
    - **Down** — A defect is detected on the interface or administrative status is set to Down.
    - **Unknown** — The unit is in cold reset, warm reset or repair state.
  - **Alarms** — Lists active alarms on the interface. See Section 7.2.5 on page 118 for alarm descriptions.
  - **Notif.** — Displays if notifications from the interface are enabled or disabled.
  - **AIS detect** — Displays if AIS detection is enabled or disabled.
- **E2** — Alarms and status of the E2 interfaces. See Section 7.2.5 on page 118 for alarm descriptions. Clicking a link opens the **E2 Alarms and Status** page, where a complete alarm description can be found, see Section 11.125 on page 338. **Higher Layer** indicates the worst severity of the alarms on higher layer interfaces.
- **Reload** — Reloads the page with the latest information.

11.127 MS/RS Alarms and Status

This page displays the alarms and status of the interface and provides links to the next higher layer interface level.

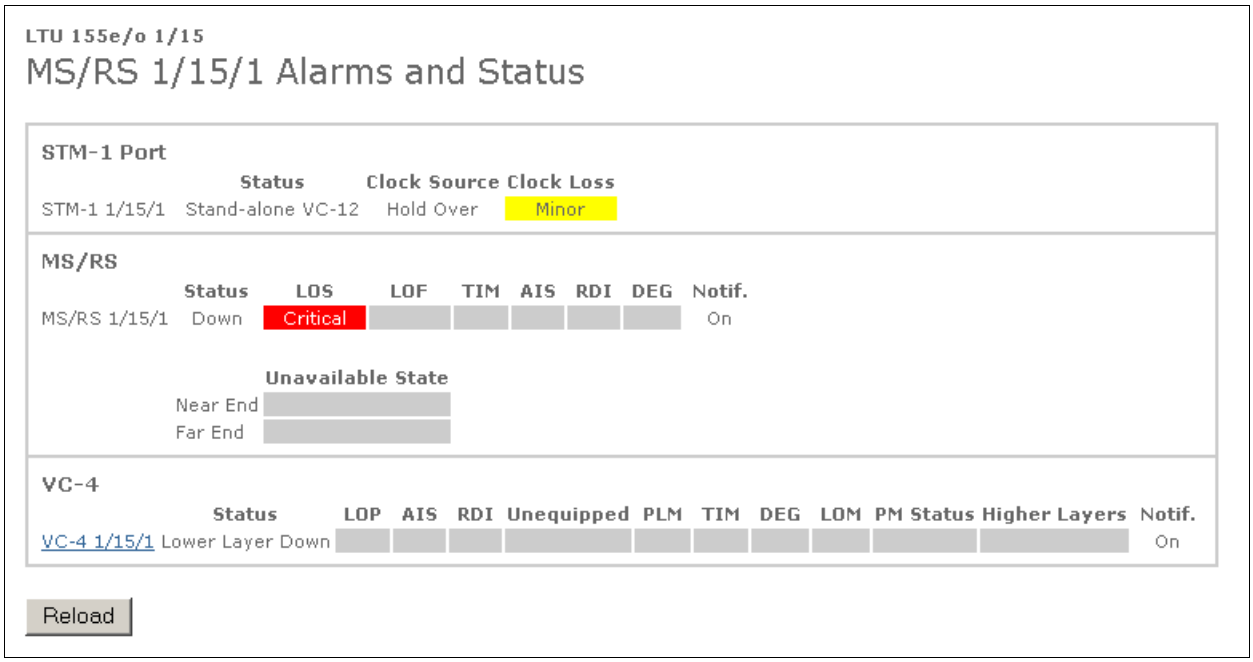


Figure 171 The MS/RS Alarms and Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **STM-1 Port** — The status and alarms of the STM-1 port. Only available if the administrative status of the MS/RS interface is Up.
  - **Status** — The operational status of the unit's STM-1 port.
    - **Not Configured** — The port does not provide traffic until it is configured.
    - **Stand-alone VC-12** — The port has 63 E1 interfaces and operates alone.
    - **MSP 1+1 VC-12** — The port is protected sharing 63 E1 interfaces with the port in the adjacent unit.
    - **Wait For Neighbour** — The port in the adjacent unit should be configured as `MSP 1+1 VC-12`, but it is not yet ready or the unit is being repaired, removed or otherwise faulty.
  - **Clock Source** — The operational status of the clock source.
    - **Rx Clock** — The recovered receive clock is used as the transmit clock.
    - **Internal** — The local clock source is used as the transmit clock.
    - **Hold Over** — The last reference is preserved.
    - **Free Running** — The clock source from the SEC module is used (SEC accuracy).

    - **SEC Passive** — The SEC module is passive.
  - **Alarms** — Lists active alarms on the port. See Section 7.2.5 on page 118 for alarm descriptions.
- **MS/RS** — Status and alarms for the MS/RS interface. Performance alarms for both near and far end MS/RS interfaces are also displayed. Only available if the administrative status of the interface is Up.
  - **Status** — Displays the operational status of the interface.
    - **Up** — Payload is passing on the interface and one or several of the active lower layers have operational status Up.
    - **Down** — A defect is detected on the interface or administrative status is set to Down.
    - **Unknown** — The unit is in cold reset, warm reset or repair state.
    - **Lower Layer Down** — The interface is Down due to lower layer interfaces. Payload is passing on the interface but not all active lower layers have operational status Up.
  - **MS/RS Status** — Indicates if the line is active or passive. Only available if the STM-1 port is configured as `MSP 1+1 VC-12`.
  - **Alarms** — Lists active alarms on the interface. See Section 7.2.5 on page 118 for alarm descriptions.
  - **Notif.** — Displays if notifications from the interface are enabled or disabled.
- **VC-4** — Alarms and status of the VC-4 interface. See Section 7.2.5 on page 118 for alarm descriptions. Clicking a link opens the **VC-4 Alarms and Status** page, where a complete alarm description can be found, see Section 11.129 on page 344. **PM Status** indicates the worst severity of the near-end and far-end Unavailable State alarms. **Higher Layer** indicates the worst severity of the alarms on higher layer interfaces. Only available if the STM-1 port is configured as `Stand-alone VC-12`.
- **MSP** — Alarms and status of the MSP interface. See Section 7.2.5 on page 118 for alarm descriptions. Clicking a link opens the **MSP Alarms and Status** page, where a complete alarm description can be found, see Section 11.128 on page 342. **PM Status** indicates the worst severity of the near-end and far-end Unavailable State alarms. **Higher Layer** indicates the worst severity of the alarms on higher layer interfaces. Only available if the STM-1 port is configured as `MSP 1+1 VC-12`.
- **Reload** — Reloads the page with the latest information.

11.128 MSP Alarms and Status

This page displays the alarms and status of the interface and provides links to the next higher layer interface level. It also displays information on which unit is active in the MSP protection.

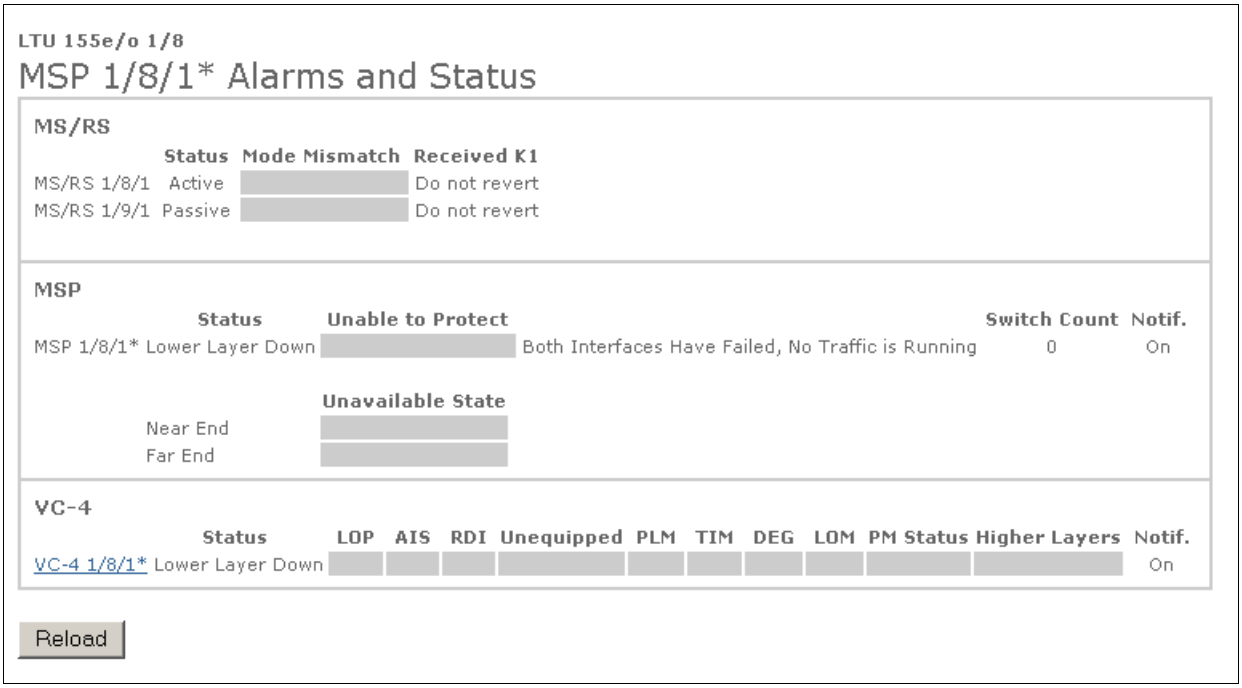


Figure 172 The MSP Alarms and Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **MS/RS** — Alarms and status of the two MS/RS interfaces constituting the MSP interface. Only available if the administrative status of the MSP interface is Up.
  - **Status** — Indicates active and passive line.
  - **Alarms** — Lists active alarms on the interface. See Section 7.2.5 on page 118 for alarm descriptions.
  - **Received K1** — The received K1 byte.
- **MSP** — Alarms and status of the of the MSP interface. Performance alarms for the near and far end MSP interfaces are also displayed. Only available if the administrative status of the interface is Up.
  - **Status** — Displays the operational status of the interface.
    - **Up** — Payload is passing on the interface and one or several of the active lower layers have operational status Up.
    - **Down** — A defect is detected on the interface or administrative status is set to Down.
    - **Unknown** — The unit is in cold reset, warm reset or repair state.

    - **Lower Layer Down** — The interface is Down due to lower layer interfaces. Payload is passing on the interface but not all active lower layers have operational status Up.
  - **Alarms** — Lists active alarms on the interface. See Section 7.2.5 on page 118 for alarm descriptions.
  - **Switch Count** — The number of protection switching events in the multiplex section caused by external events. Equipment protection switching is not included in this counter.
  - **Notif.** — Displays if notifications from the interface are enabled or disabled.
- **VC-4** — Alarms and status of the VC-4 interface. Clicking a link opens the **VC-4 Alarms and Status** page, where a complete alarm description can be found, see Section 11.129 on page 344. **PM Status** indicates the worst severity of the near-end and far-end Unavailable State alarms. **Higher Layer** indicates the worst severity of the alarms on higher layer interfaces.
- **Reload** — Reloads the page with the latest information.

11.129 VC-4 Alarms and Status

This page displays the alarms and status of the interface and provides links to the next higher layer interface level.

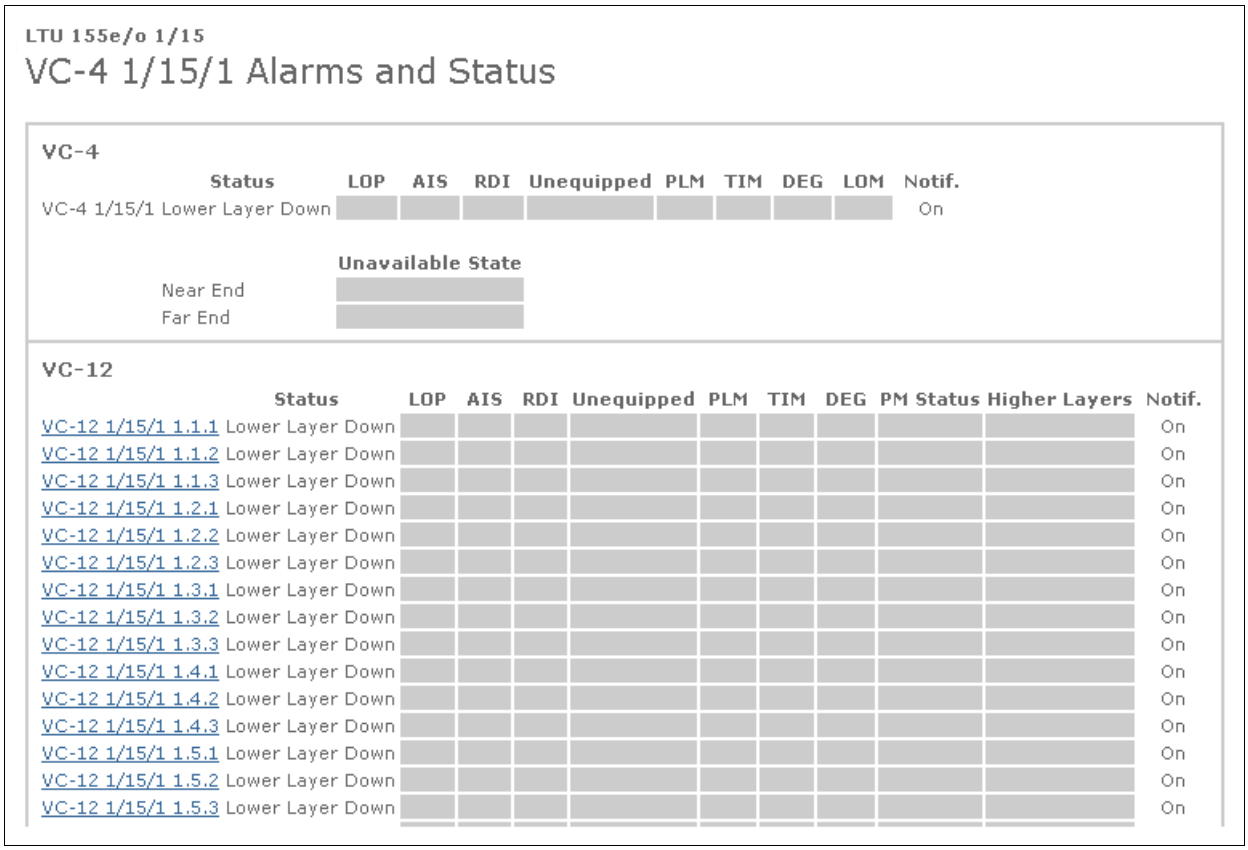


Figure 173 The VC-4 Alarms and Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **VC-4** — Alarms and status of the VC-4 interface. Performance alarms for the near and far end VC-4 interfaces are also displayed. The alarms are only available if the administrative status of the interface is Up.
  - **Status** — Displays the operational status of the interface.
    - **Up** — Payload is passing on the interface and one or several of the active lower layers have operational status Up.
    - **Down** — A defect is detected on the interface or administrative status is set to Down.
    - **Unknown** — The unit is in cold reset, warm reset or repair state.
    - **Lower Layer Down** — The interface is Down due to lower layer interfaces. Payload is passing on the interface but not all active lower layers have operational status Up.
  - **Alarms** — Lists active alarms on the interface. See Section 7.2.5 on page 118 for alarm descriptions.

  - **Notif.** — Displays if notifications from the interface are enabled or disabled.
- **VC-12** — Alarms and status of the VC-12 interfaces. See Section 7.2.5 on page 118 for alarm descriptions. Clicking a link opens the **VC-12 Alarms and Status** page, where a complete alarm description can be found, see Section 11.130 on page 346. **PM Status** indicates the worst severity of the near-end and far-end Unavailable State alarms. **Higher Layer** indicates the worst severity of the alarms on higher layer interfaces.
- **Reload** — Reloads the page with the latest information.

11.130 VC-12 Alarms and Status

This page displays the alarms and status of the interface and provides links to the next higher layer interface level.

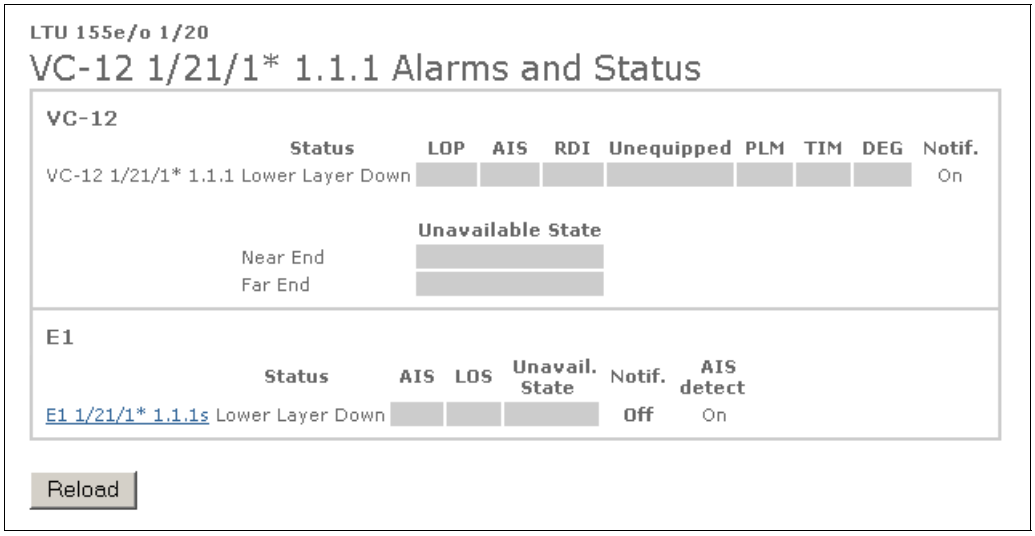


Figure 174 The VC-12 Alarms and Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **VC-12** — Alarms and status of the VC-12 interface. Performance alarms for the near and far end VC-12 interfaces are also displayed. The alarms are only available if the administrative status of the interface is Up.
  - **Status** — Displays the operational status of the interface.
    - **Up** — Payload is passing on the interface and one or several of the active lower layers have operational status Up.
    - **Down** — A defect is detected on the interface or administrative status is set to Down.
    - **Unknown** — The unit is in cold reset, warm reset or repair state.
    - **Lower Layer Down** — The interface is Down due to lower layer interfaces. Payload is passing on the interface but not all active lower layers have operational status Up.
  - **Alarms** — Lists active alarms on the interface. See Section 7.2.5 on page 118 for alarm descriptions.
  - **Notif.** — Displays if notifications from the interface are enabled or disabled.
- **E1** — Alarms and status of the E1 interfaces. See Section 7.2.5 on page 118 for alarm descriptions. Clicking a link opens the **E1 Alarms and Status** page, where a complete alarm description can be found, see Section 11.124 on page 337.
- **Reload** — Reloads the page with the latest information.

11.131 User Input Alarms and Status

This page displays the alarms and status of the user input.

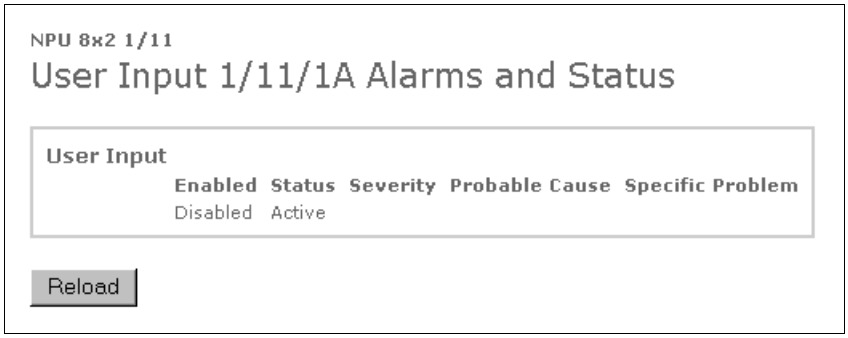


Figure 175 The User Input Alarms and Status page

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **Enabled** — Displays if the user input is enabled.
- **Status** — Indicates if the user input alarm is active.
- **Severity** — The severity of the alarm. See also Section 7.2.4 on page 117.
- **Probable Cause** — Displays the cause of the user input alarm.
- **Specific Problem** — Details on the user input alarm.
- **Reload** — Reloads the page with the latest information.

11.132 User Output Alarms and Status

This page displays the alarms and status of the user output.

Figure 176 The User Output Alarms and Status

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **Enabled** — Displays if the user output is enabled.
- **Status** — Indicates if the user output alarm is active.
- **Description** — Details on the user output alarm.
- **Reload** — Reloads the page with the latest information.

11.133 Alarm List

This page displays all active alarms for the NE, a single unit or interface. When opened for an interface, the higher layer interface alarms are also displayed.

The maximum number of alarms is 200.

Note: A restart of the NE or NPU will clear the Alarm List.

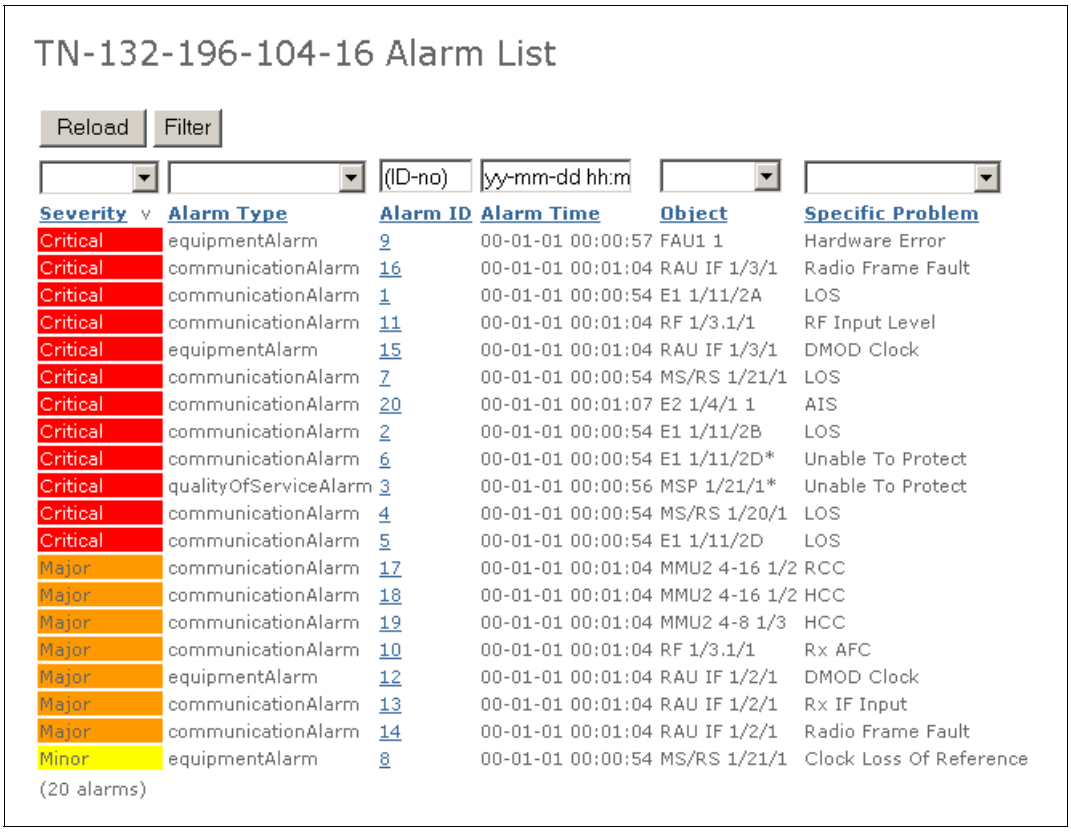


Figure 177 The Alarm List page

Filter functionality for each column is available above each heading. Combinations of several filter criteria are possible.

Sorting on a column is possible by clicking its heading, illustrated by '^'. Next click gives the opposite sorting, illustrated by 'v'.

Note: The page is not updated automatically. Click **Reload** to display the latest information.

- **Reload** — Reloads the page with the latest information, that is all active alarms that fulfil the filter criteria (if any).
- **Filter** — Applies one or several filter criteria to all displayed alarms. No new alarms are fetched.
- **Severity** — The severity of an alarm. See also Section 7.2.4 on page 117.

- **Alarm Type** — Displays the category of an alarm. Five basic categories of alarm are specified:
  - **Communications alarm** — An alarm associated with the procedures and/or processes required to convey information from one point to another.
  - **Quality of service alarm** — An alarm associated with a degradation in the quality of a service.
  - **Processing error alarm** — An alarm associated with a software or processing fault.
  - **Equipment alarm** — An alarm associated with an equipment fault.
  - **Environmental alarm** — An alarm associated with a condition related to an enclosure in which the equipment resides.
- **Alarm ID** — Displays the identity of an alarm. Clicking a link displays more detailed information about a particular ID.
- **Alarm Time** — The time when the alarm occurred.
- **Object** — Indicating from where the alarm was generated.
- **Specific Problem** — The specific problem of the alarm. See also Section 7.2.5 on page 118.

11.134 Event Log

This page is used to display the Event Log, holding a maximum of 400 entries of events and alarms.

Note: A restart of the NE or NPU will clear the Event Log.

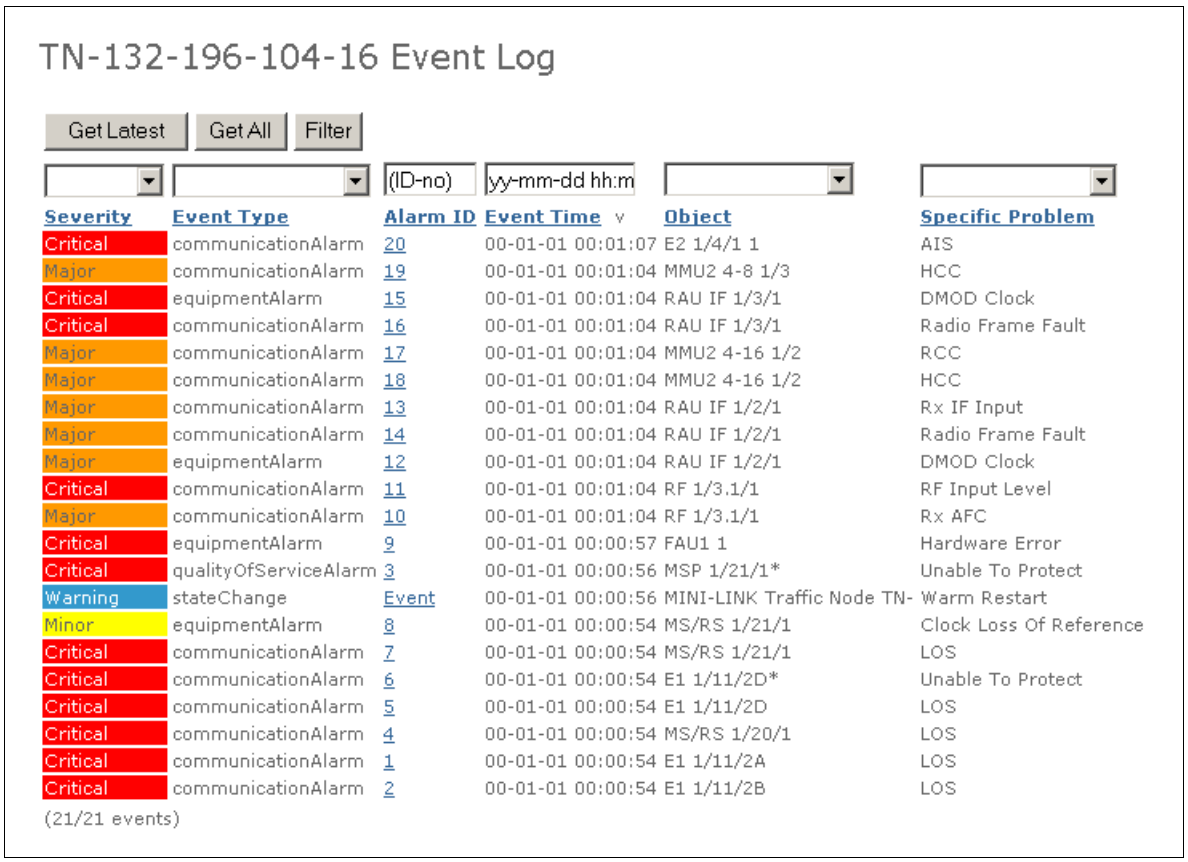


Figure 178 The Event Log page

Filter functionality for each column is available above each heading. Combinations of several filter criteria are possible.

Sorting on a column is possible by clicking its heading, illustrated by '^'. Next click gives the opposite sorting, illustrated by 'v'.

Note: The page is not updated automatically. Click **Get Latest** or **Get All** to display the latest information.

- **Get Latest** — Reloads the page with the 50 latest entries that fulfil the filter criteria (if any).
- **Get All** — Reloads the page with all entries that fulfil the filter criteria (if any).
- **Filter** — Applies one or several filter criteria to the displayed entries. No new entries are fetched.
- **Severity** — The severity of an entry. See also Section 7.2.4 on page 117.

- **Event Type** — Displays the category of an entry.
- **Alarm ID** — Displays the identity of an entry. Alarms have an ID number while an event is identified as `Event`. Clicking a link displays more detailed information about a particular ID.
- **Event Time** — The time when the entry occurred.
- **Object** — Indicating where the entry was generated.
- **Specific Problem** — The specific problem of the entry. See also Section 7.2.5 on page 118.

11.135 Load Error Log

This page is used to load the Error Log from the NE to an FTP server or to delete the Error Log from the NE. The Error Log contains information about internal HW and SW errors as well as restarts and equipment alarms. It comprises two files, `<hostname>_active.elog` and `<hostname>_passive.elog`.

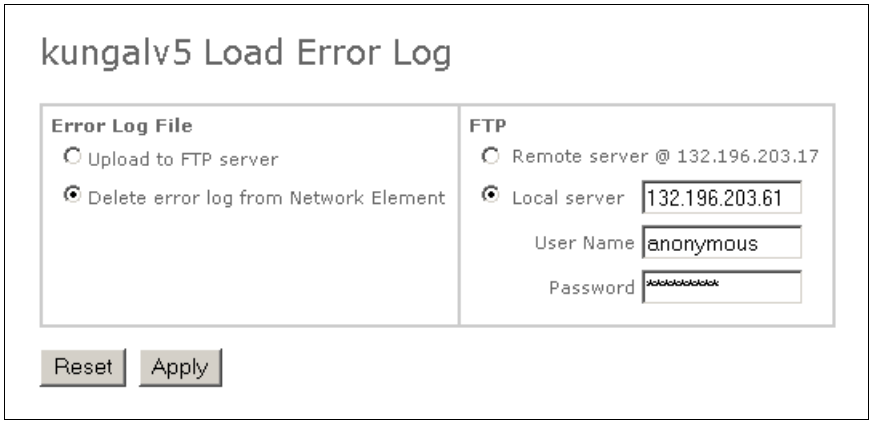


Figure 179 The Load Error Log page

- **Error Log File** — Specifies the action to perform regarding the Error Log.
  - **Upload to FTP server** — Uploads the `<hostname>_active.elog` and `<hostname>_passive.elog` files to the FTP server. The files will be stored in the `<drive:>\tn_ftp_home\tn_error_log` folder.

    Note: To avoid overwriting an existing Error Log from the same NE, add the extension `.old` to the existing files, for example `<hostname>_active.elog.old`.

  - **Delete error log from Network Element** — Deletes the `<hostname>_active.elog` file from the NE.
- **Remote server @ <IP address>** — Specifies that the permanent FTP server in the network should be used. See also Section 11.16 on page 174.
- **Local server** — Specifies that the local FTP server should be used.
  - **User Name** — The user name used by the NE to log in to the FTP server. The FTP server must be configured accordingly.
  - **Password** — The password used by the NE to log in to the FTP server. The FTP server must be configured accordingly.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.

See Also

- Error log handling, see Section 7.5 on page 129.

11.136 Activities

This page gives an overview of all ongoing activities in the NE, in terms of software upgrade, loops and BER Tests (BERT).

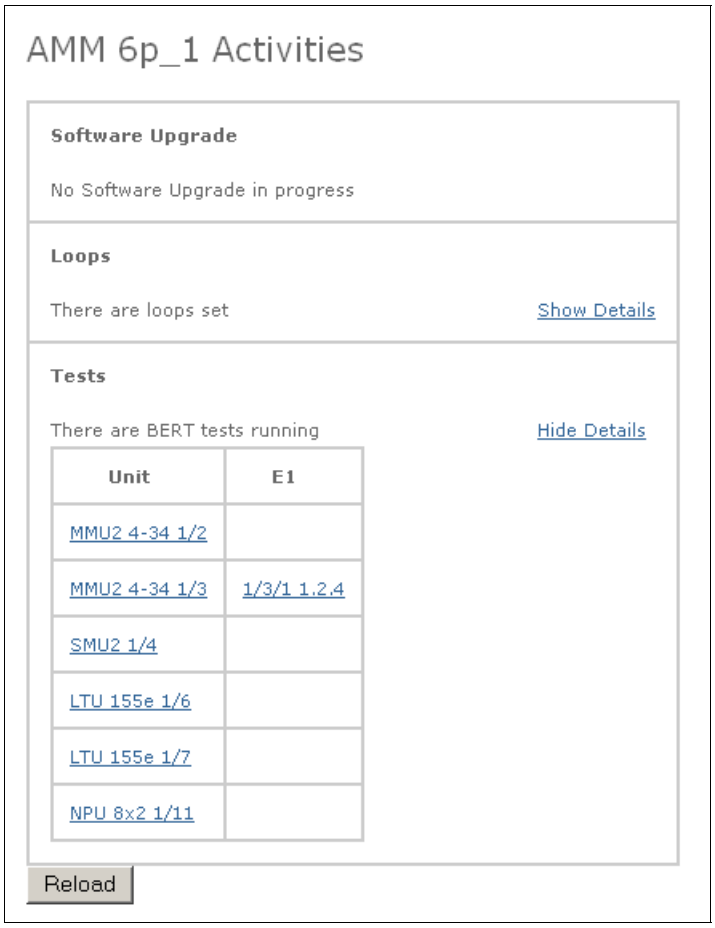


Figure 180 The Activities page

- **Software Upgrade** — Displays if a software upgrade is in progress. If so, it is stated if it is a Load Module Upgrade or a Software Baseline Upgrade.
  - **Upgrade Progress** — Opens the **Upgrade Progress – Baseline** or **Upgrade Progress – Baseline** page, see Section 11.82 on page 269 and Section 11.83 on page 271. Only available when a software upgrade is in progress.
- **Loops** — Displays if there are loops set. A link is provided showing more details about the loops. No details are displayed by default.
  - **Show Details** — Displays a table with links to the **Loops** page for all units where loops can be set, see Section 11.138 on page 357. The table also holds links to the **Loops** page for all interfaces where loops are set. Interfaces on equipment protected units are present for both units in the protected pair.
  - **Hide Details** — Hides the table with details about the loops.

- **Tests** — Displays if there are BERTs on E1 interfaces running. A link is provided showing more details about the BERTs. No details are displayed by default.
  - **Show Details** — Displays a table with links to the **Test** page for all units where BERTs can be set, see Section 11.150 on page 378. The table also holds links to the **Test** page for all interfaces where BERTs are running. Interfaces on equipment protected units are present for both units in the protected pair.
  - **Hide Details** — Hides the table with details about the BERTs.
- **Reload** — Reloads the page with the latest information.

11.137 NE Loops

This page provides links to the **Loops** page on plug-in unit and interface level, see Section 11.138 on page 357.

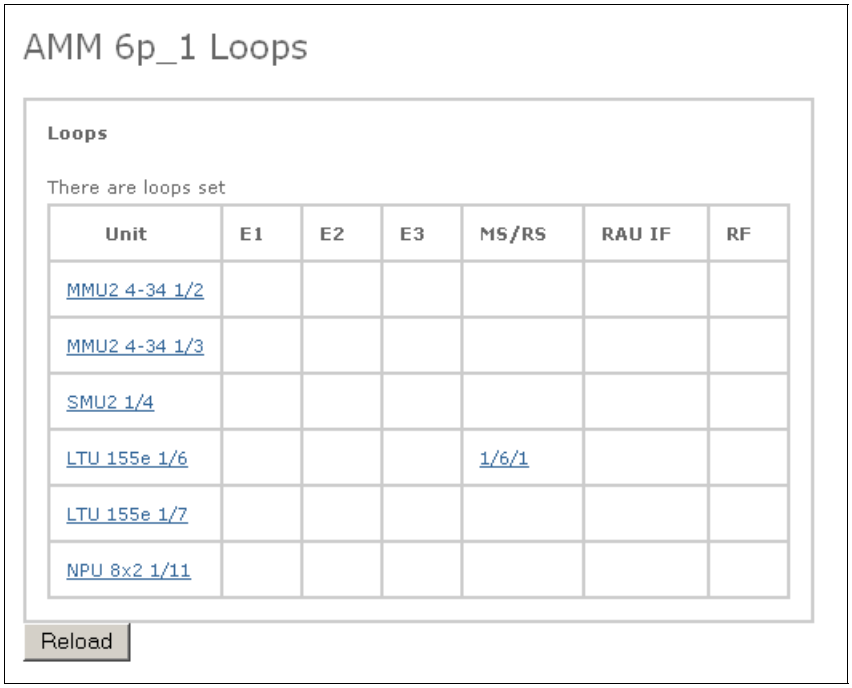


Figure 181 The NE Loops page

- **Unit** — Provides links to the **Loops** page for all available units, where loops can be set.
- **<IF type>** — Each column provides links to the **Loops** page for all interfaces of a certain type, with active loops.
- **Reload** — Reloads the page with the latest information.

11.138 Loops

This page is used to set loops for fault localization. It can be opened for a single interface or for a unit, enabling loops to be set on all applicable interfaces on the unit.

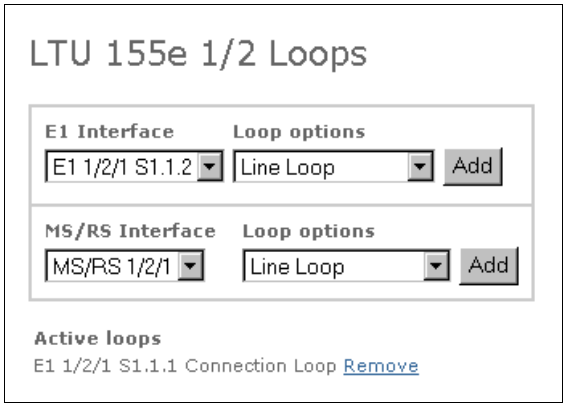


Figure 182 The Loops page when an LTU 155e is selected.

Caution!

If an interface is used, the loop will disturb the traffic.

Note: An active loop will disable notifications from the interface and suppress notifications from higher layer interfaces.

- **<IF type> Interface** — Selects the interface to be looped. If the page is opened for an interface, this interface is the only option in the list. An interface with an already active loop is not present in the list.
- **Loop options** — Selects the type of loop for the interface. The options available for the different interface types are described in Table 22 on page 357.
- **Add** — Sets the selected loop on the selected interface.
- **Active loops** — The currently active loops on the unit or interface.
- **Remove** — Removes an active loop.
- **Remove All** — Removes all active loops. Only available if more than one loop are active.

Table 22 Loop types

Interface	Loop
E1 line interface	Line Loop, Local Loop, Connection Loop(1)
E1 non-line interface, for example a protected E1 (1+1 E1 SNCP)	Connection Loop (1)

Interface	Loop
E2 line interface	Line Loop, Local Loop
E3 line interface	Line Loop, Local Loop
MS/RS	Line Loop, Local Loop, Line Loop + Local Loop
RAU IF	IF Loop, Rx Loop
RF	RF Loop

(1) Connection Loop cannot be set for an interface with an active BERT.

See Also

- How to set a loop on an interface, see Section 7.4.2 on page 128.

11.139 MS/RS Performance

This page displays near end and far end MS/RS performance data for the current and previous 15 minute/24 hour error counting intervals. The text `Invalid` or a grey background indicates invalid performance data.

Note: Display of performance data is enabled on the **MS/RS Configuration** page, see Section 11.44 on page 213. Performance data can be enabled for MS and RS separately.

Note: A restart of the LTU 155 will cause a loss of all performance data.

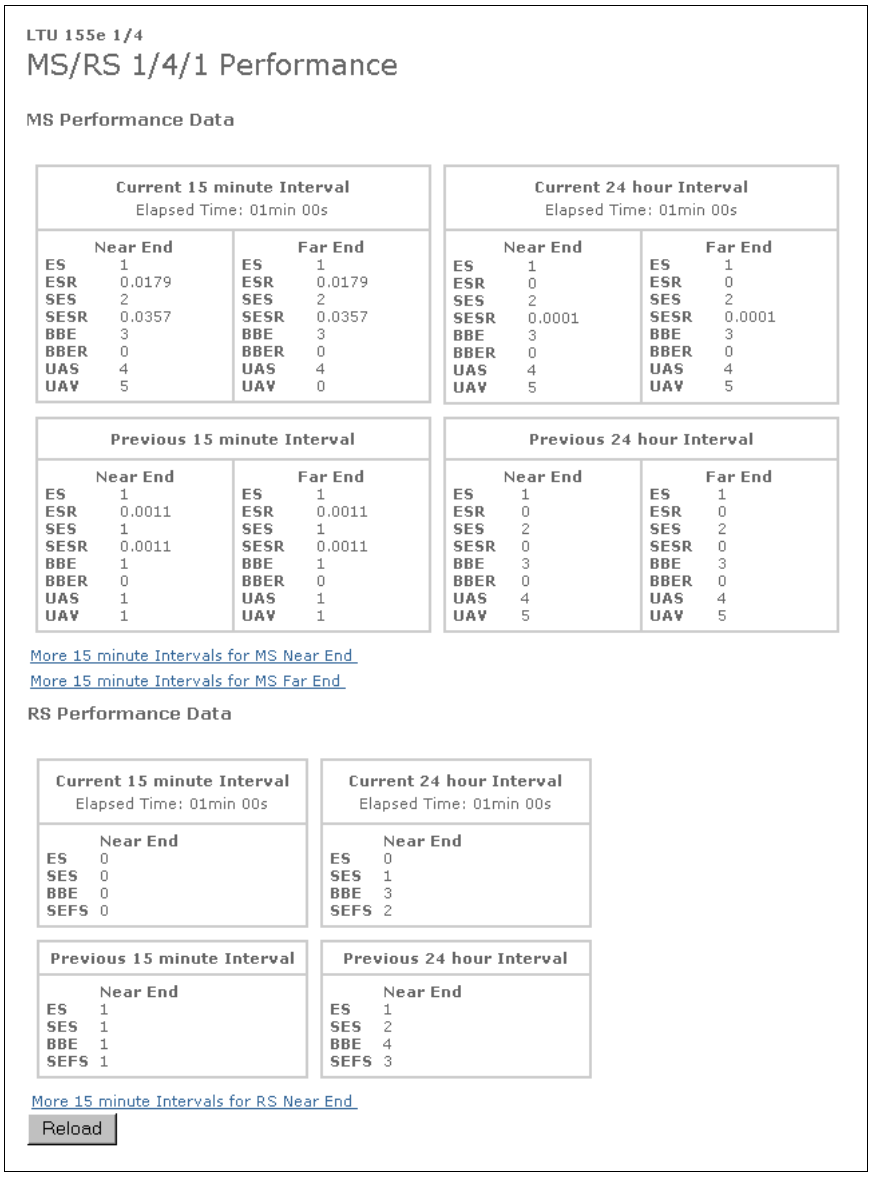


Figure 183 The MS/RS Performance page

- **MS Performance Data** — The MS interface performance data.

  - **ES** — The number of Errored Seconds that were counted during the Elapsed Time of the interval.
  - **ESR** — The Errored Second Ratio (value range 0 to 1). Calculated as ESR = ES/(P-UAS), where P is the Elapsed Time of the interval.
  - **SES** — The number of Severely Errored Seconds that were counted during the Elapsed Time of the interval.
  - **SESR** — The Severely Errored Seconds Ratio (value range 0 to 1). Calculated as SESR = SES/(P-UAS), where P is the Elapsed Time of the interval.
  - **BBE** — The number of Background Block Errors that were counted during the Elapsed Time of the interval.
  - **BBER** — The Background Block Error Ratio (value range 0 to 1). Calculated as BBER = BBE/[(P-UAS-SES)×blocks per second], where P is the Elapsed Time of the interval. Blocks per second for the MS interface is 192000.
  - **UAS** — The number of Unavailable Seconds that were counted during the Elapsed Time of the interval.
  - **UAV** — The number of Unavailable Events that were counted during the Elapsed Time of the interval.
  - **More 15 minute Intervals for MS Near End** — Opens the **MS/RS Performance 15 minute Intervals** page, see Section 11.140 on page 361. The link locates all previous MS Near End data on the page.
  - **More 15 minute Intervals for MS Far End** — Opens the **MS/RS Performance 15 minute Intervals** page, see Section 11.140 on page 361. The link locates all previous MS Far End data on the page.
- **RS Performance Data** — The RS Interface performance data.
  - **ES** — The number of Errored Seconds that were counted during the Elapsed Time of the interval.
  - **SES** — The number of Severely Errored Seconds that were counted during the Elapsed Time of the interval.
  - **BBE** — The number of Background Block Errors that were counted during the Elapsed Time of the interval.
  - **SEFS** — The number of Severely Errored Framing Seconds that were counted during the Elapsed Time of the interval.
  - **Elapsed Time** — The Elapsed Time (in seconds) of the interval.
  - **More 15 minute Intervals for RS Near End** — Opens the **MS/RS Performance 15 minute Intervals** page, see Section 11.140 on page 361. The link locates all previous RS Near End data on the page.
- **Reload** — Reloads the page with the latest information.

11.140 MS/RS Performance 15 Minute Intervals

This page displays near end and far end MS/RS performance for all previous 15 minute intervals for which data was collected. The text `Invalid` or a grey background indicates invalid performance data.

Note: Display of performance data is enabled on the **MS/RS Configuration** page, see Section 11.44 on page 213. Performance data can be enabled for MS and RS separately.

Note: A restart of the LTU 155 will cause a loss of all performance data.

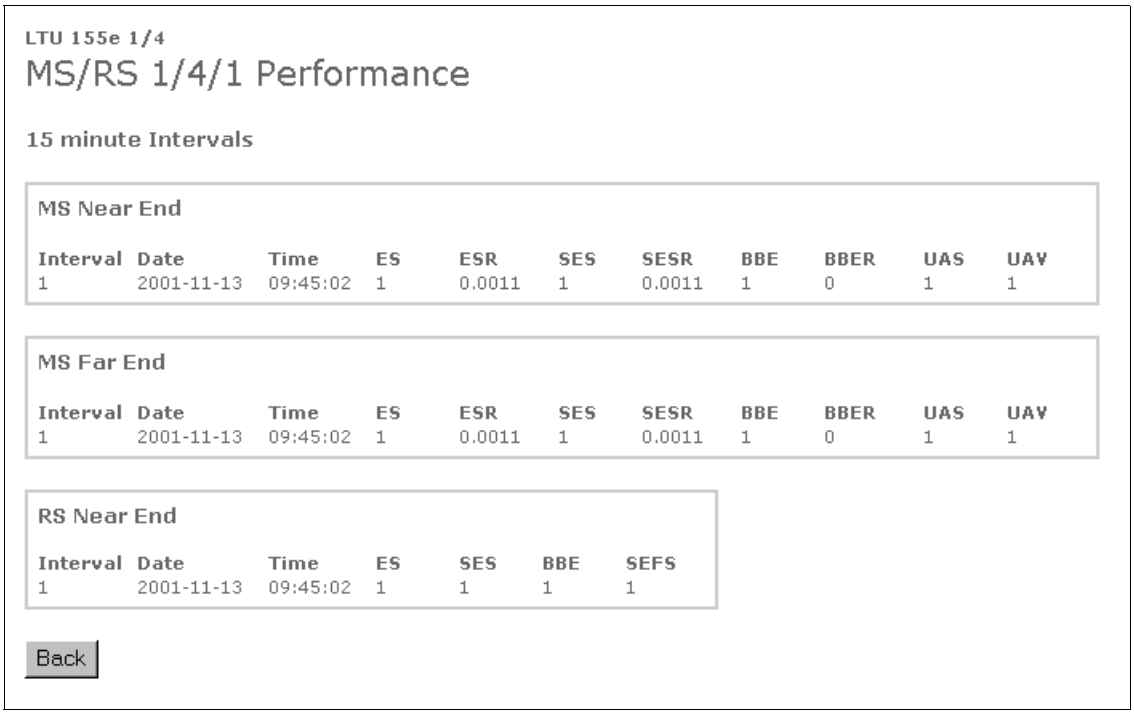


Figure 184 The MS/RS Performance 15 minute Intervals page

The duration of an invalid interval is not known, therefore the **Date** and **Time** parameters cannot be displayed for intervals following an invalid interval. In this case the parameters will be displayed as `Unknown`.

- **MS Near End/MS Far End** — The MS Interface performance data for the Near End and Far End.
  - **Interval** — The 15 minute interval number from 1 up to 96.
  - **Date** — The date (yyyy-mm-dd) when the 15 minute interval started
  - **Time** — The time (hh:mm:ss) when the 15 minute interval started.
  - **ES** — The number of Errored Seconds that were counted during the 15 minute interval.
  - **ESR** — The Errored Second Ratio (value range 0 to 1). Calculated as ESR = ES/(P-UAS), where P is the number of seconds in a complete interval.

  - **SES** — The number of Severely Errored Seconds that were counted during the 15 minute interval.
  - **SESR** — The Severely Errored Seconds Ratio (value range 0 to 1). Calculated as SESR = SES/(P-UAS), where P is the number of seconds in a complete interval.
  - **BBE** — The number of Background Block Errors that were counted during the 15 minute interval.
  - **BBER** — The Background Block Error Ratio (value range 0 to 1). Calculated as BBER = BBE/[(P-UAS-SES)×blocks per second], where P is the number of seconds in a complete interval. Blocks per second for the MS interface is 192000.
  - **UAS** — The number of Unavailable Seconds that were counted during the 15 minute interval.
  - **UAV** — The number of Unavailable Events that were counted during the 15 minute interval.
- **RS Near End** — The RS Interface performance data for the Near End and Far End.
  - **Interval** — The 15 minute interval number from 1 up to 96.
  - **Date** — The date (yyyy-mm-dd) when the 15 minute interval started.
  - **Time** — The time (hh:mm:ss) when the 15 minute interval started
  - **ES** — The number of Errored Seconds that were counted during the 15 minute interval.
  - **SES** — The number of Severely Errored Seconds that were counted during the 15 minute interval.
  - **BBE** — The number of Background Block Errors that were counted during the 15 minute interval.
  - **SEFS** — The number of Severely Errored Framing Seconds that were counted during the 15 minute interval.
- **Back** — Returns to the **MS/RS Performance Data** page, see Section 11.139 on page 359.

11.141 MSP Performance

This page displays near end and far end MSP performance data for the current and previous 15 minute/24 hour error counting intervals. The text `Invalid` or a grey background indicates invalid performance data.

Note: Display of performance data is enabled on the **MSP Configuration** page, see Section 11.45 on page 215.

Note: A restart of the LTU 155 will cause a loss of all performance data.

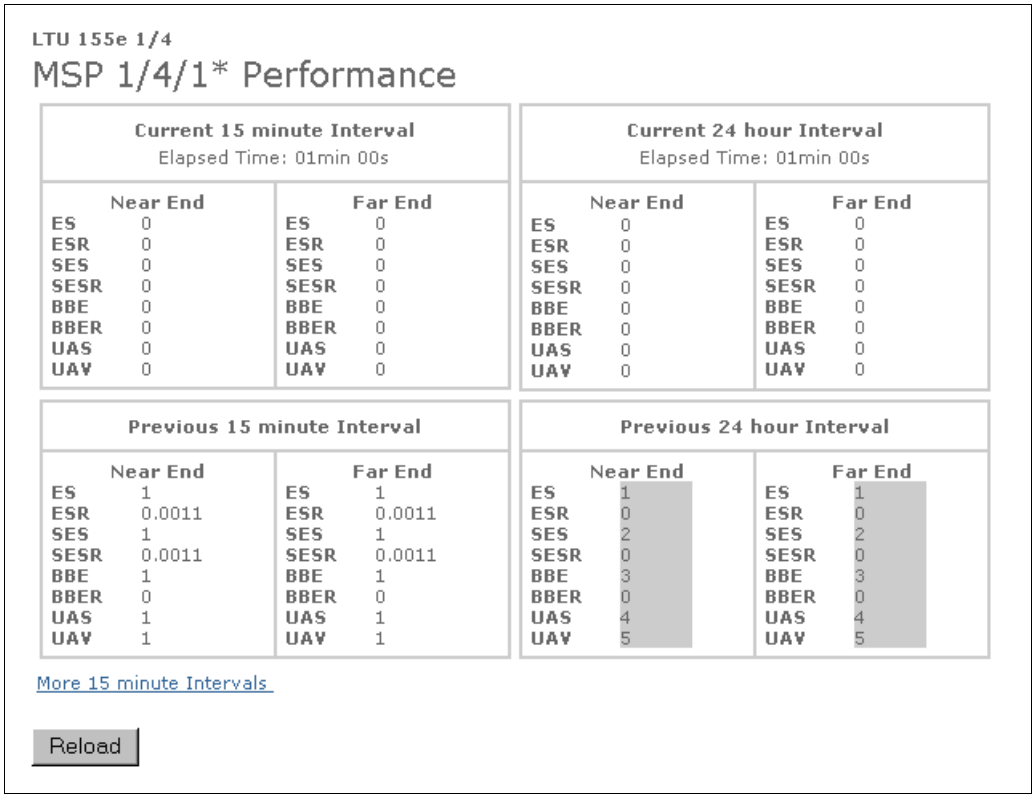


Figure 185 The MSP Performance page

Note: The MSP interface is only available if the unit configured as `MSP 1+1 VC-12`.

- **ES** — The number of Errored Seconds that were counted during the Elapsed Time of the interval.
- **ESR** — The Errored Second Ratio (value range 0 to 1). Calculated as ESR = ES/(P-UAS), where P is the Elapsed Time of the interval.
- **SES** — The number of Severely Errored Seconds that were counted during the Elapsed Time of the interval.
- **SESR** — The Severely Errored Seconds Ratio (value range 0 to 1). Calculated as SESR = SES/(P-UAS), where P is the Elapsed Time of the interval.

- **BBE** — The number of Background Block Errors that were counted during the Elapsed Time of the interval.
- **BBER** — The Background Block Error Ratio (value range 0 to 1). Calculated as BBER = BBE/[(P-UAS-SES)×blocks per second], where P is the Elapsed Time of the interval. Blocks per second for the MSP interface is 192000.
- **UAS** — The number of Unavailable Seconds that were counted during the Elapsed Time of the interval.
- **UAV** — The number of Unavailable Events that were counted during the Elapsed Time of the interval.
- **More 15 minute Intervals** — Opens the **MSP Performance 15 minute Intervals** page, which displays all previous 15 minute intervals, see Section 11.142 on page 365.
- **Reload** — Reloads the page with the latest information.

11.142 MSP Performance 15 minute Intervals

This page displays near end and far end MSP performance data for all previous 15 minute intervals for which data was collected. The text `Invalid` or a grey background indicates invalid performance data.

Note: Display of performance data is enabled on the **MSP Configuration** page, see Section 11.45 on page 215.

Note: A restart of the LTU 155 will cause a loss of all performance data.

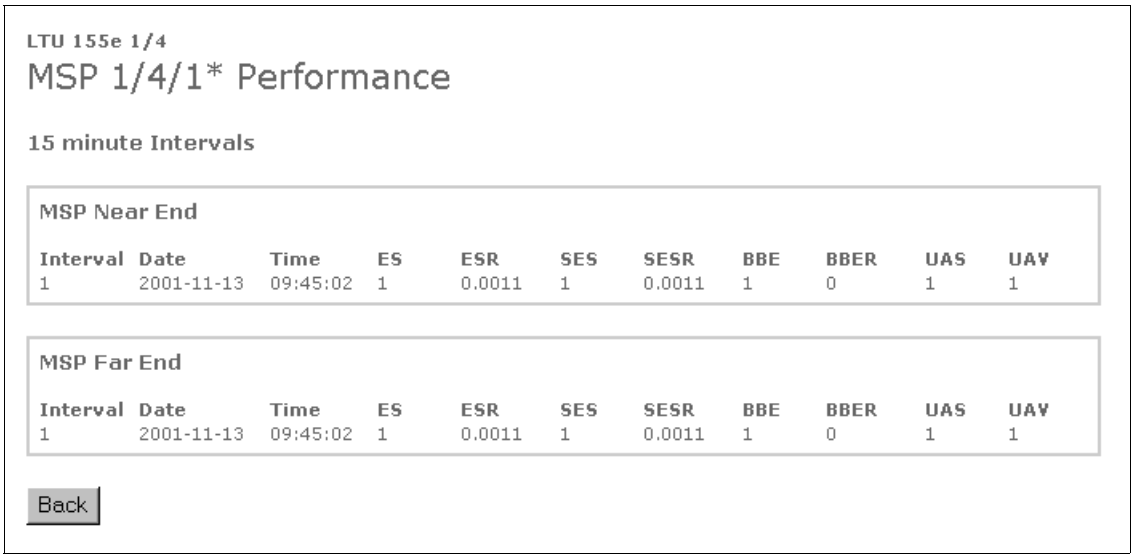


Figure 186 The MSP Performance 15 minute Intervals page

The duration of an invalid interval is not known, therefore the **Date** and **Time** parameters cannot be displayed for intervals following an invalid interval. In this case the parameters will be displayed as `Unknown`.

- **Interval** — The 15 minute interval number from 1 up to 96.
- **Date** — The date (yyyy-mm-dd) when the 15 minute interval started
- **Time** — The time (hh:mm:ss) when the 15 minute interval started.
- **ES** — The number of Errored Seconds that were counted during the 15 minute interval.
- **ESR** — The Errored Second Ratio (value range 0 to 1). Calculated as ESR = ES/(P-UAS), where P is the number of seconds in a complete interval.
- **SES** — The number of Severely Errored Seconds that were counted during the 15 minute interval.
- **SESR** — The Severely Errored Seconds Ratio (value range 0 to 1). Calculated as SESR = SES/(P-UAS), where P is the number of seconds in a complete interval
- **BBE** — The number of Background Block Errors that were counted during the 15 minute interval.
- **BBER** — The Background Block Error Ratio (value range 0 to 1). Calculated as BBER = BBE/[(P-UAS-SES)×blocks per second], where P

is the number of seconds in a complete interval. Blocks per second for the MSP interface is 192000.

- **UAS** — The number of Unavailable Seconds that were counted during the 15 minute interval.
- **UAV** — The number of Unavailable Events that were counted during the 15 minute interval.
- **Back** — Returns to the **MSP Performance Data** page, see Section 11.141 on page 363.

11.143 VC-4 Performance

This page displays near end and far end VC-4 performance data for the current and previous 15 minute/24 hour error counting intervals. The text `Invalid` or a grey background indicates invalid performance data.

Note: Display of performance data is enabled on the **VC-4 Configuration** page, see Section 11.46 on page 216.

Note: A restart of the LTU 155 will cause a loss of all performance data.

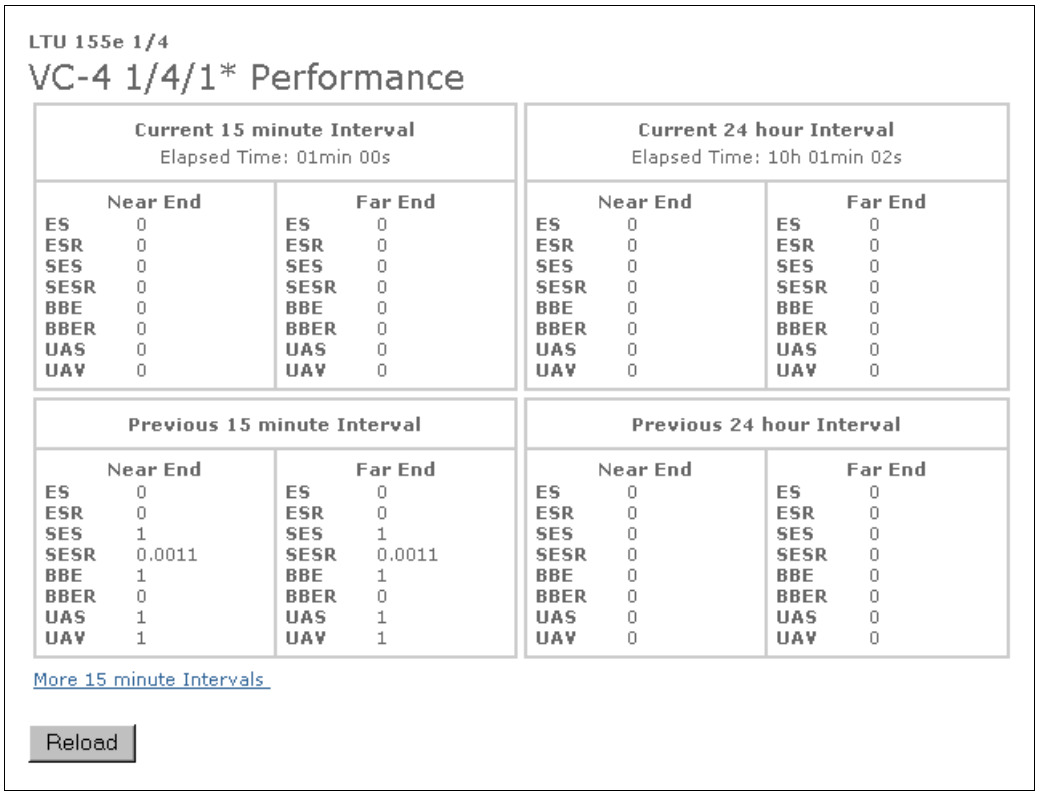


Figure 187 The VC-4 Performance page

- **ES** — The number of Errored Seconds that were counted during the Elapsed Time of the interval.
- **ESR** — The Errored Seconds Ratio (value range 0 to 1). Calculated as ESR = ES/(P-UAS), where P is the Elapsed Time of the interval.
- **SES** — The number of Severely Errored Seconds that were counted during the Elapsed Time of the interval.
- **SESR** — The Severely Errored Seconds Ratio (value range 0 to 1). Calculated as SESR = SES/(P-UAS), where P is the Elapsed Time of the interval.
- **BBE** — The number of Background Block Errors that were counted during the Elapsed Time of the interval.
- **BBER** — The Background Block Error Ratio (value range 0 to 1). Calculated as BBER = BBE/[(P-UAS-SES)×blocks per second], where P is

the Elapsed Time of the interval. Blocks per second for the VC-4 interface is 8000.

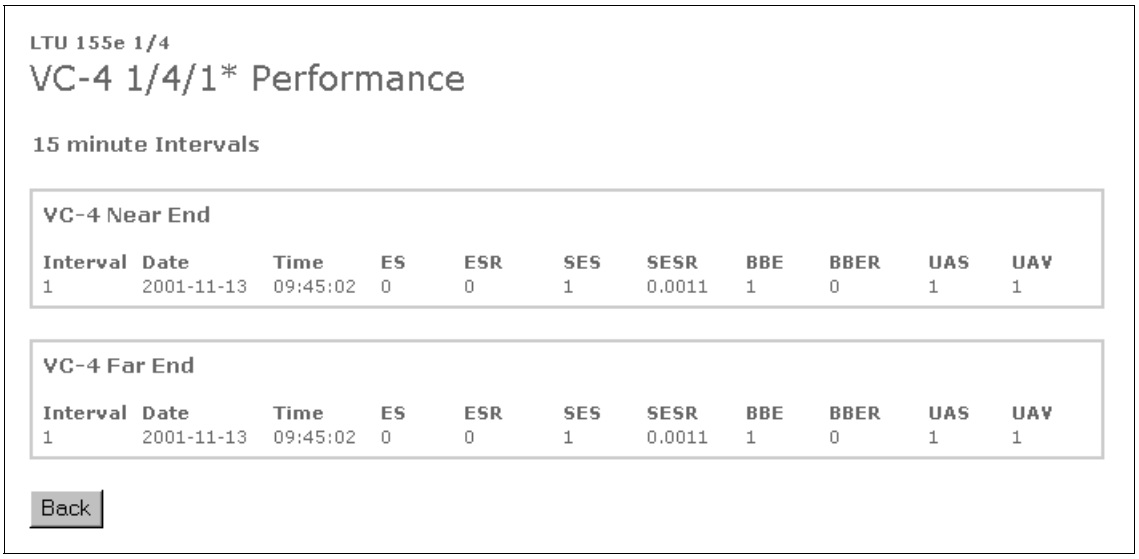
- **UAS** — The number of Unavailable Seconds that were counted during the Elapsed Time of the interval.
- **UAV** — The number of Unavailable Events that were counted during the Elapsed Time of the interval.
- **More 15 minute Intervals** — Opens the **VC–4 Performance 15 minute Intervals** page, which displays all previous 15 minute intervals, see Section 11.144 on page 369.
- **Reload** — Reloads the page with the latest information.

11.144 VC-4 Performance 15 minute Intervals

This page displays near end and far end VC-4 performance data for all previous 15 minute intervals for which data has been collected. The text `Invalid` or a grey background indicates invalid performance data.

Note: Display of performance data is enabled on the **VC-4 Configuration** page, see Section 11.46 on page 216.

Note: A restart of the LTU 155 will cause a loss of all performance data.


LTU 155e 1/4

VC-4 1/4/1* Performance

15 minute Intervals

VC-4 Near End

Interval	Date	Time	ES	ESR	SES	SESR	BBE	BBER	UAS	UAV
1	2001-11-13	09:45:02	0	0	1	0.0011	1	0	1	1

VC-4 Far End

Interval	Date	Time	ES	ESR	SES	SESR	BBE	BBER	UAS	UAV
1	2001-11-13	09:45:02	0	0	1	0.0011	1	0	1	1

Back

Figure 188 The VC-4 Performance 15 minute Intervals page

The duration of an invalid interval is not known, therefore the **Date** and **Time** parameters cannot be displayed for intervals following an invalid interval. In this case the parameters will be displayed as `Unknown`.

- **Interval** — The 15 minute interval number from 1 up to 96.
- **Date** — The date (yyyy-mm-dd) when the 15 minute interval started.
- **Time** — The time (hh:mm:ss) when the 15 minute interval started.
- **ES** — The number of Errored Seconds that were counted during the 15 minute interval.
- **ESR** — The Errored Second Ratio (value range 0 to 1). Calculated as ESR = ES/(P-UAS), where P is the number of seconds in a complete interval.
- **SES** — The number of Severely Errored Seconds that were counted during the 15 minute interval.
- **SESR** — The Severely Errored Seconds Ratio (value range 0 to 1). Calculated as SESR = SES/(P-UAS), where P is the number of seconds in a complete interval
- **BBE** — The number of Background Block Errors that were counted during the 15 minute interval.
- **BBER** — The Background Block Error Ratio (value range 0 to 1). Calculated as BBER = BBE/[(P-UAS-SES)×blocks per second], where P

is the number of seconds in a complete interval. Blocks per second for the VC-4 interface is 8000.

- **UAS** — The number of Unavailable Seconds that were counted during the 15 minute interval.
- **UAV** — The number of Unavailable Events that were counted during the 15 minute interval.
- **Back** — Returns to the **VC-4 Performance Data** page, see Section 11.143 on page 367.

11.145 VC-12 Performance

This page displays near end and far end VC-12 performance data for the current and previous 15 minute/24 hour error counting intervals. The text `Invalid` or a grey background indicates invalid performance data.

Note: Display of performance data is enabled on the **VC-12 Configuration** page, see Section 11.47 on page 218.

Note: A restart of the LTU 155 will cause a loss of all performance data.

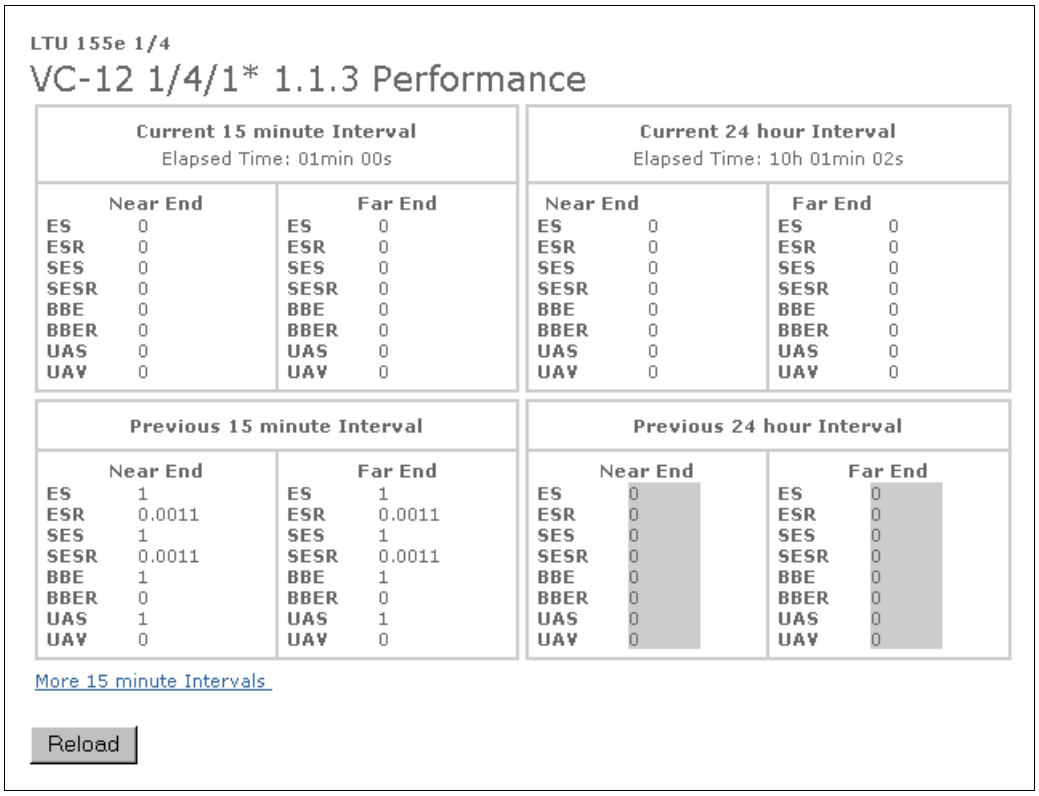


Figure 189 The VC-12 Performance page

- **ES** — The number of Errored Seconds that were counted during the Elapsed Time of the interval.
- **ESR** — The Errored Second Ratio (value range 0 to 1). Calculated as ESR = ES/(P-UAS), where P is the Elapsed Time of the interval.
- **SES** — The number of Severely Errored Seconds that were counted during the Elapsed Time of the interval.
- **SESR** — The Severely Errored Seconds Ratio (value range 0 to 1). Calculated as SESR = SES/(P-UAS), where P is the Elapsed Time of the interval.
- **BBE** — The number of Background Block Errors that were counted during the Elapsed Time of the interval.
- **BBER** — The Background Block Error Ratio (value range 0 to 1). Calculated as BBER = BBE/[(P-UAS-SES)×blocks per second], where P

is the Elapsed Time in seconds for the interval. Blocks per second for the VC-12 interface is 2000.

- **UAS** — The number of Unavailable Seconds that were counted during the Elapsed Time of the interval.
- **UAV** — The number of Unavailable Events that were counted during the Elapsed Time of the interval.
- **More 15 minute Intervals** — Opens the **VC-12 Performance 15 minute Intervals** page, which displays all previous 15 minute intervals, see Section 11.146 on page 373.
- **Reload** — Reloads the page with the latest information.

11.146 VC-12 Performance 15 minute Intervals

This page displays near end and far end VC-12 performance data for all previous 15 minute intervals for which data was collected. The text `Invalid` or a grey background indicates invalid performance data.

Note: Display of performance data is enabled on the **VC-12 Configuration** page, see Section 11.47 on page 218.

Note: A restart of the LTU 155 will cause a loss of all performance data.

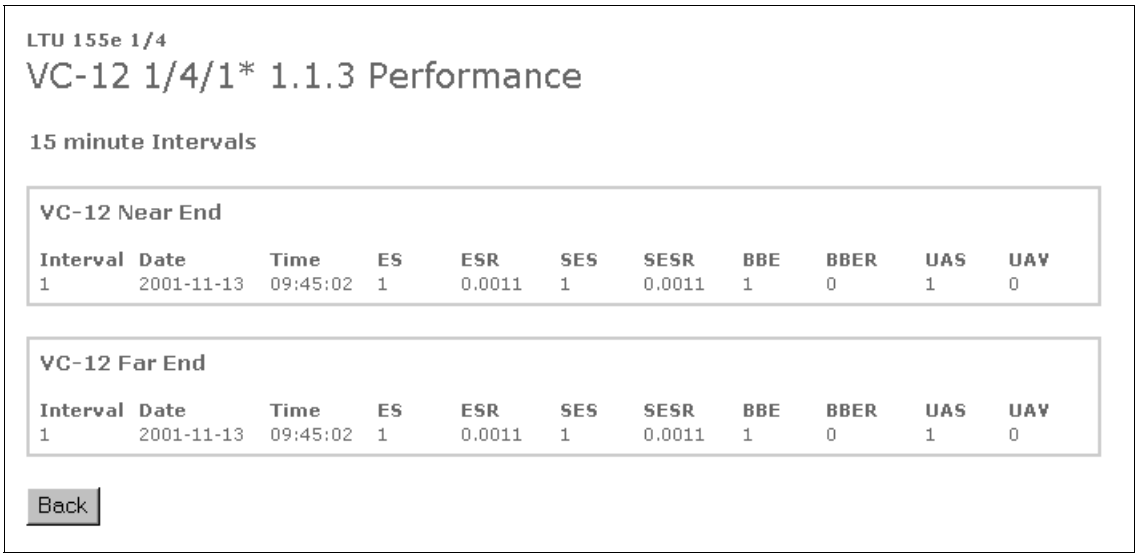


Figure 190 The VC-12 Performance 15 minute Intervals page

The duration of an invalid interval is not known, therefore the **Date** and **Time** parameters cannot be displayed for intervals following an invalid interval. In this case the parameters will be displayed as `Unknown`.

- **Interval** — The 15 minute interval number from 1 up to 96.
- **Date** — The date (yyyy-mm-dd) when the 15 minute interval started.
- **Time** — The time (hh:mm:ss) when the 15 minute interval started.
- **ES** — The number of Errored Seconds that were counted during the 15 minute interval.
- **ESR** — The Errored Second Ratio (value range 0 to 1). Calculated as ESR = ES/(P-UAS), where P is the number of seconds in a complete interval.
- **SES** — The number of Severely Errored Seconds that were counted during the 15 minute interval.
- **SESR** — The Severely Errored Seconds Ratio (value range 0 to 1). Calculated as SESR = SES/(P-UAS), where P is the number of seconds in a complete interval.
- **BBE** — The number of Background Block Errors that were counted during the 15 minute interval.
- **BBER** — The Background Block Error Ratio. Calculated as BBER = BBE/[(P-UAS-SES)×blocks per second], where P is the number of seconds in a complete interval. Blocks per second for the VC-12 interface is 2000.

- **UAS** — The number of Unavailable Seconds that were counted during the 15 minute interval.
- **UAV** — The number of Unavailable Events that were counted during the 15 minute interval.
- **Back** — Returns to the **VC-12 Performance Data** page, see Section 11.145 on page 371.

11.147 E1 Performance

This page displays E1 performance data for the current and previous 15 minute/24 hour error counting intervals. If the selected E1 is part of a 1+1 E1 SNCP protection the performance data for the E1 and the protected E1 will be displayed. The text `Invalid` or a grey background indicates invalid performance data.

Note: Display of performance data is enabled on the **E1 Configuration** page and **All E1 Configuration** page, see Section 11.51 on page 224 and Section 11.28 on page 189.

Note: A restart of the NE or NPU will cause a loss of all E1 performance data.

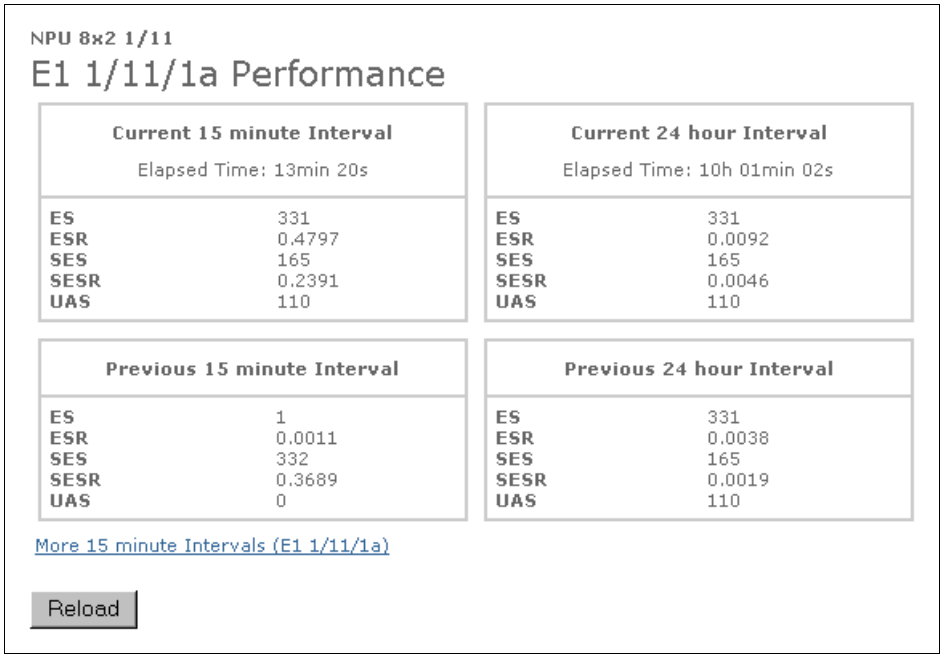


Figure 191 The E1 Performance page

- **ES** — The number of Errored Seconds that were counted during the Elapsed Time of the interval.
- **ESR** — The Errored Second Ratio (value range 0 to 1). Calculated as ESR = ES/(P-UAS), where P is the Elapsed Time in seconds for the interval.
- **SES** — The number of Severely Errored Seconds that were counted during the Elapsed Time of the interval.
- **SESR** — The Severely Errored Seconds Ratio (value range 0 to 1). Calculated as SESR = SES/(P-UAS), where P is the Elapsed Time in seconds for the interval.
- **UAS** — The number of Unavailable Seconds that were counted during the Elapsed Time of the interval.
- **More 15 minute Intervals** — Opens the **E1 Performance 15 minutes Intervals** page, which displays all previous 15 minute intervals for which data was collected, see Section 11.148 on page 376.
- **Reload** — Reloads the page with the latest information.

11.148 E1 Performance 15 Minute Intervals

This page displays E1 performance data for all previous 15 minute intervals for which data was collected. The text `Invalid` or a grey background indicates invalid performance data.

Note: Display of performance data is enabled on the **E1 Configuration** page and **All E1 Configuration** page, see Section 11.51 on page 224 and Section 11.28 on page 189.

Note: A restart of the NE or NPU will cause a loss of all E1 performance data.

Figure 192 The E1 Performance 15 minute Intervals page

The duration of an invalid interval is not known, therefore the **Date** and **Time** parameters cannot be displayed for intervals following an invalid interval. In this case the parameters will be displayed as `Unknown`.

- **Display Intervals for...** — Switches between the **E1 Performance 15 minute Intervals** page for the E1 (which is part of a 1+1 E1 SNCP protection) and the protected E1. This link appears only if the selected E1 is part of a 1+1 E1 SNCP protection.
- **Interval** — The 15 minute interval number from 1 up to 96.
- **Date** — The date (yyyy-mm-dd) when the 15 minute interval started.
- **Time** — The time (hh:mm:ss) when the 15 minute interval started.
- **ES** — The number of Errored Seconds that were counted during the previous 15 minute interval.
- **ESR** — The Errored Second Ratio. Calculated as ESR = ES/(P-UAS), where P is the number of seconds in a complete interval.
- **SES** — The number of Severely Errored Seconds that were counted during the previous 15 minute interval.
- **SESR** — The Severely Errored Seconds Ratio (value range 0 to 1). Calculated as SESR = SES/(P-UAS), where P is the number of seconds in a complete interval.
- **UAS** — The number of Unavailable Seconds that were counted during the previous 15 minute interval.
- **Back** — Returns to the **E1 Performance Data** page, see Section 11.147 on page 375.

11.149 RF Power

This page shows input and output power performance data for the RF interface.

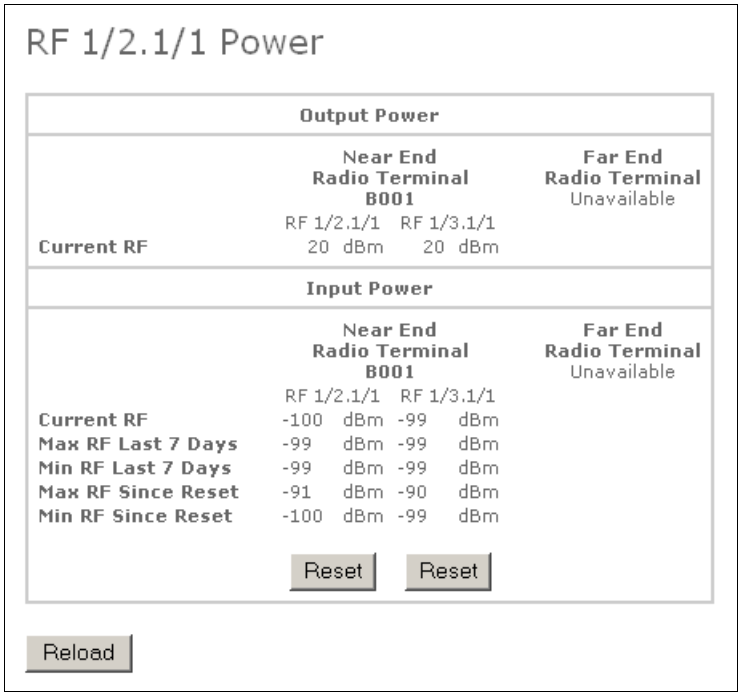


Figure 193 The RF Power page

- **Output Power** — Shows the current output power on the near-end. For protected (1+1) terminals, data for both RF interfaces are shown.
  - **Current RF** — Shows the current RF output power in dBm.
- **Input Power** — Shows current and historical input power on the near-end. For protected (1+1) terminals, data for both RF interfaces are shown.
  - **Current RF** — Shows the current input power in dBm.
  - **Max RF Last 7 Days** — Shows the highest input power (in dBm) during the last 7 days.
  - **Min RF Last 7 Days** — Shows the lowest input power (in dBm) during the last 7 days.
  - **Max RF Since Reset** — Shows the highest input power (in dBm) since the counters were reset.
  - **Min RF Since Reset** — Shows the lowest input power (in dBm) since the counters were reset.
  - **Reset** — Resets the counters. For protected (1+1) terminals, the counters can be reset separately for each RF interface.

11.150 Bit Error Ratio Test (BERT)

This page is used to run a Bit Error Ratio Test (BERT) on E1 interfaces for performance measurement. The page can be accessed on NE, unit or E1 interface level. A Pseudo Random Bit Sequence (PRBS) with test pattern $2^{15} - 1$ is sent on the selected interface.

For an illustration of the BERT functionality, see Section 8.3 on page 132.

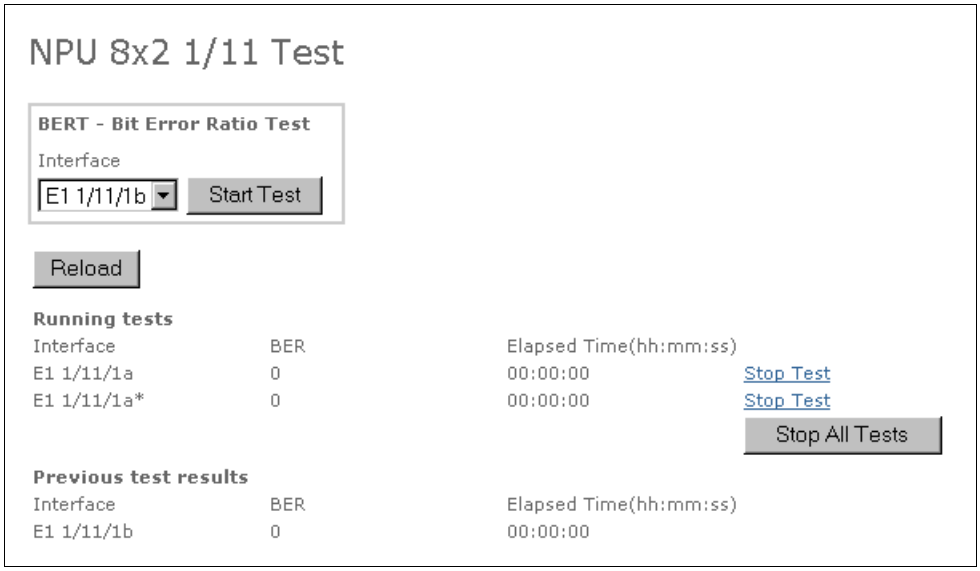


Figure 194 The Test page

Caution!

If the interface is used, the BERT will disturb the traffic.

- **BERT – Bit Error Ratio Test** — Allows selection and start of a BERT. Only available if a BERT resource is available.
  - **Interface** — Selects the E1 interface to test or displays the selected interface when the page is opened for a specific interface.

    Note: It is not possible to select an interface that already has a running BERT, an active Connection Loop or administrative status set to Down.

  - **Start Test** — Starts a BERT on the selected interface.
- **Reload** — Reloads the current page with the latest information.
- **Running tests** — All tests that are currently running.
  - **Interface** — The name of the interface.
  - **BER** — The result of the test (Bit Error Ratio).

  - **Elapsed Time** — The elapsed time since the start of the BERT. The timer is only started if a valid traffic signal (no LOS) is present.
  - **Stop Test** — Stops the BERT on the selected interface
  - **Stop All Tests** — Stops all BERTs. Only available if more than one BERT are running.
- **Previous test results** — Displays previous test results.
  - **Interface** — The name of the interface.
  - **BER** — The result of the test (Bit Error Ratio).
  - **Elapsed Time** — The duration of the test.

See Also

- How to run a BERT on an E1 interface, see Section 8.3 on page 132.

11.151 Security

This page is used to configure security parameters.

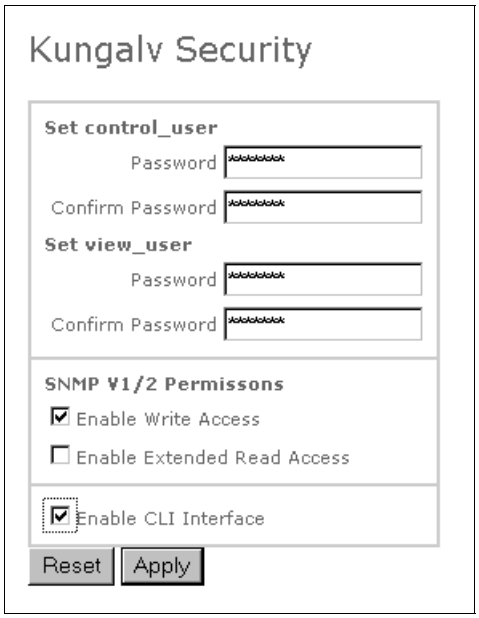


Figure 195 The Security page

- **Set control_user** — Specifies the control_user password.
  - **Password** — Has to be 8 – 16 characters long.
  - **Confirm Password** — Identical to the password entered in the password box.
- **Set view_user** — Specifies the view_user password.
  - **Password** — Has to be 8 – 16 characters long.
  - **Confirm Password** — Identical to the password entered in the password box.
- **SNMP V1/2 Permissions** — Specifies permissions for the read and write SNMP communities that can be used by an external management system.
  - **Enable Write Access** — Enables read and write access to all managed objects for community string 'private'. When not enabled, no access is granted to any managed object.
  - **Enable Read Access** — Enables read access to all managed objects for community string 'public'. When not enabled, read access is granted only to the managed objects in the system branch. Only available in Normal mode.
- **Enable CLI Interface** — Enables the CLI interface. The CLI interface is accessed using telnet and allows configuration of IP parameters. Only available in Normal mode.
- **Reset** — Resets all settings to their initial values.
- **Apply** — Applies all changes you have made without leaving the page.

11.152 Select Option

When this page is displayed you have to click a menu command to open a specific page.

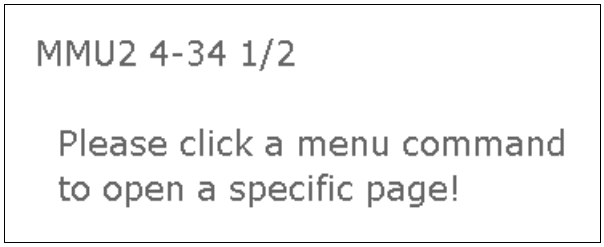


Figure 196 The Select Option page

Glossary

10/100BASE-T
Ethernet traffic at 10 Mbit/s or 100 Mbit/s.

ABR
Area Border Router

AIS
Alarm Indication Signal. A signal that replaces the normal traffic signal when an error occurs, preventing cascading alarms being generated downstream.

AM
Access Module

AMM
Access Module Magazine

ARP
Address Resolution Protocol

AS
Autonomous System

ASBR
Autonomous System Border Router

BBE
Background Block Error. An errored block that does not occur as part of an SES.

BBER
Background Block Error Ratio.

BER
Bit Error Ratio

BERT
Bit Error Ratio Test

BR
Board Removal

CD
Compact Disc

CD-ROM
Compact Disc Read-Only Memory

CLI
Command Line interface

Cold reset state
A state of a plug-in unit when all traffic, control and management logics are reset. The operational status is Out of Service, that is the unit is not operating.

Cold restart
A restart of the control and management system as well as the traffic system. This type of restart will disturb all traffic within the scope of the restart.

CRC
Cyclic Redundancy Check

CSS
Control and Supervision System. The embedded software in an MMU2 or SMU2.

DB
Database

DCC
Data Communication Channel

DCN
Data Communication Network

DEG
Degraded Signal

DEGM
Degraded Monitoring

DEGTHR
Degraded Threshold

DHCP
Dynamic Host Configuration Protocol

DIG SC
Digital Service Channel (64 kbit/s). Applies to SMU2 in co-siting mode for DCN connection to MINI-LINK E equipment

DNS
Domain Name Server

DP
Device Processor

E1
PDH traffic at 2 Mbit/s (2 048 kbit/s)

E2
PDH traffic at 8 Mbit/s (8 448 kbit/s)

E3
PDH traffic at 34 Mbit/s (34 368 kbit/s)

EB
Errored Block

EBER
Excessive Bit Error Ratio

EEM
Embedded Element Manager

ES
Errored Second. A one-second period with one or more errored blocks or at least one defect.

ESR
Errored Second Ratio

FAU
Fan Unit

FEC
Forward Error Correction

FTP
File Transfer Protocol

HDLC
High level Data Link Control

HW
Hardware

I/O
Input/Output

ICMP
Internet Control Message Protocol

ID
Identity

IM
Inverse Multiplexer

IP
Internet Protocol

LAN
Local Area Network

LCT
Local Craft Terminal

LED
Light Emitting Diode

Load module
Software for a plug-in unit.

LOF
Loss Of Frame

LOM
Loss Of Multiframe

LOP
Loss Of Pointer

LOS
Loss Of Signal

LS
Link State

LSA
Link State Advertisement

LSID
Link State Identity

LTU
Line Termination Unit

MAC
Media Access Control

MB
Megabyte

MDI
Medium Dependent Interface

MDIX
Medium Dependent Interface Crossover

MHz
Megahertz

ML-PPP
Multilink Point-to-Point Protocol

MMU
Modem Unit

MS
Multiplex Section

MS-REI
Multiplex Section Remote Error Indication

MSM
MINI-LINK Service Manager

MSOH
Multiplexer Section Overhead

MSP
Multiplex Section Protection, providing 1+1 protection of STM-1 traffic.

N/A
Not Applicable

NBMA
Non-Broadcast Multi-Access

NE
Network Element

NMS
Network Management System

Node Installation mode
A state used for initial setup of an NPU 8x2 NE, allowing a limited set of parameters to be set.

Normal mode
A state of the NE used for normal operation, allowing complete configuration possibilities.

NPU
Node Processor Unit

NPU Installation mode
A fault state of the NE. Also used for NPU repair.

NSSA
Not So Stubby Area

NTP
Network Time Protocol

O&M
Operation and Maintenance

OSPF
Open Shortest Path First. A dynamic routing protocol for IP networks.

PC
Personal Computer

PFU
Power Filter Unit

PLM
Payload Mismatch

PM
Performance Management

PPP
Point-to-Point Protocol

PRBS
Pseudo Random Bit Sequence

Radio Terminal (1+0)
One side of an unprotected radio link at traffic rate 4-34 Mbit/s. The indoor part comprises an MMU2.

Radio Terminal (1+1)
One side of a protected radio link at traffic rate 4-34 Mbit/s. The indoor part comprises two MMU2 units and one SMU2 (protection).

RAU
Radio Unit

RCC
Radio Communication Channel

RDI
Remote Defect Indication

RF
Radio Frequency

RS
Regenerator Section

RSOH
Regenerator Section Overhead

RST
Reset

SBDF
Software Baseline Description File

SBL
Software Baseline

SDH
Synchronous Digital Hierarchy

SEC
SDH Equipment Clock

SEFS
Severely Errored Framing Second. A second containing one or more SEF events. This counter is only at the RS layer. An SEF is the occurrence of four contiguous errored frame alignment words. A frame alignment word occupies the A1 and A2 bytes of an SDH STM-1 frame. The SEF defect is terminated when two contiguous error-free frame words are detected.

SES
Severely Errored Second. A one-second period which contains X% errored blocks or at least one defect, where X is 15 for MS/MSP and 30 for RS/VC-4/VC-12.

SESR
Severely Errored Second Ratio.

SMU
Switch Multiplexer Unit

SNCP
Sub-Network Connection Protection. 1+1 E1 SNCP is used to create a protected E1 interface from two unprotected E1 interfaces.

SNMP
Simple Network Management Protocol

SPF
Shortest Path First

Startup configuration file
The configuration of the NE is saved into a non-volatile memory on the NPU. Configuration changes (running configuration) are stored in the startup configuration file. NE and NPU restarts will revert from the running to the startup configuration.

STM-1
Synchronous Transport Module level 1. SDH traffic at 155 Mbit/s.

System release
Software package used in MINI-LINK TN 2.0 and earlier.

SW
Software

TCP
Transmission Control Protocol

TDM
Time Division Multiplex

TIM
Trace Identifier Mismatch

TOS
Type Of Service

TULOM
Tributary Unit Loss Of Multiframe

UAS
Unavailable Seconds. The time interval in seconds from the first of 10 consecutive SES to the first of 10 consecutive non-SES.

UAV
Unavailable Events

UDP
User Datagram Protocol

URL
Universal Resource Locator

USB
Universal Serial Bus

VC-n
Virtual Container -n. In the SDH hierarchy, one VC-4 contains 63 VC-12.

Warm reset state
A state of a plug-in unit when the control and management logic is reset. The unit's operational status is `Reduced Service`, that is the traffic is in operation but the management functionality is reduced or unavailable.

Warm restart
A restart of the control and management system. Traffic is not disturbed by this type of restart.

Index

1+1 E1 SNCP List View page....243
1+1 E1 SNCP Matrix View page....241
1+1 E1 SNCP protection....70
creating....70
list view....72
matrix view....70
modifying or deleting....75
list view....77
matrix view....75
1+1 E1 SNCP Select Interfaces page....239

A

ABR....88
defining stub areas....107
Access Module Magazine, *See* AMM
Access Termination Unit, *See* ATU
Activation page....273
Activities page....354
Adding plug-in units....140
Administrative status....60
of a plug-in unit....60
of an interface....60
Alarm List
active alarms....115
displaying....116
Alarm List page....349
Alarms....115
list of....118
sending notifications....115
severity levels....117
viewing active....115
viewing logged....116
Alarms and Status page....115
All E1 Configuration page....225
All VC-12 Configuration page....220
AMM....8
AMM 20p....10
AMM 2p....8
AMM 6p....9
AMM 6p B....9
Antennas....15
Area Border Router, *See* ABR
ARP Status page....296
ATU....14
ATU (cont.)
ATU NPU emergency fallback....95
configuring interfaces....62
configuring Radio Terminals....50, 66
configuring the ATU NPU....62
configuring the Ethernet Bridge....79
loops....127
replacing....152
starting LCT....30
working with E1 interfaces....83
ATU Installation Instruction....2
ATU NPU Alarms and Status page....316
ATU NPU Configuration page....190
Automatic configuration
of NE parameters....53
Automatic Configuration page....159

B

Baseline, *See* SBDF
Baseline upgrade....91
Basic NE Configuration page....172
BERT
running on an E1 interface....132
Bit Error Ratio Test, *See* BERT
Bit Error Ratio Test (BERT) page....378
BR button
on NPU 8x2....28
on NPU1 B....23
Bridge Alarm and Status page....285
Bridge Configuration page....176

C

Change Password page....165
Changing
passwords....136
traffic capacity
of Radio Terminal....153–154
of SMU2 (co-siting)....156
unprotected to protected Radio Terminal....154–155
Cleared, severity....117
CLI....16
command modes....99

CLI (cont.)
commands
Exec mode....103
Global Configuration mode....105
Interface Configuration mode....106
Privileged Exec mode....104
Router Configuration mode....106
confirming configuration....98
defining stub areas....107
editing features....101
Exec mode....100
Global Configuration mode....101
help facility....98
important commands....103
Interface Configuration mode....101
introduction....97
OSPF configuration commands....108
OSPF show commands....109
overview....97
Privileged Exec mode....100
Router Configuration mode....101
static routing....110
Command Line Interface, *See* CLI
Configuration
generating reports....111
Management....59
typical workflow....59
uploading file to FTP server....90
Configuration File Deleted page....170
Configuration files
stored on FTP server....19
uploading file to FTP server....90
Configuring
DCN....85
E1
all interfaces in one unit....225
single interface....224
E2....223
E3....222
Ethernet Bridge....79
FAU....172, 187
FTP server....20
Internet Explorer not to use a proxy server....33
IP address
in Windows 2000....32
in Windows XP....33
LTU 12x2....192
LTU 155....194
LTU 16x2....193
MS/RS....213
MSP....215
Configuring (cont.)
NE parameters automatically....53
NE parameters manually....54
NPU 8x2....189
NPU1 B....188
NPU2....190
PFU1....184
PFU2....185
PFU3....186
PPP interfaces....87, 177
protected Radio Terminals with MMU2....66
protected Radio Terminals with MMU2 B/C....64
SMU2....198
static routes....110
static routing....110, 179
creating....89
unprotected Radio Terminals with ATU....66
unprotected Radio Terminals with MMU2....66
unprotected Radio Terminals with MMU2 B/C....63
User Input....228
User Output....229
VC-12, all interfaces on one unit....220
VC-12, single interface....218
VC-4....216
Confirm
button....42
configuration, CLI....98
Confirm New Software Configuration page....274
Connection loop....126
control_user....135
Conventions....3
for safety information....3
typographic....3
Copyright....4
Create 1+1 E1 SNCP page....245
Create MSP Protection page....250
Create Multiple 1+1 E1 SNCP page....247
Create Multiple Traffic Routings page....237
Create Traffic Routing page....236
Creating
1+1 E1 SNCP protection....70
list view....72
matrix view....70
MSP protection....68
OSPF areas....88
static routes....89
traffic routing of E1....79
list view....80
matrix view....80

Creating Protection page....251
Critical, severity....117

D

DCN
configuration....85
status, viewing....126
Default password
FTP server....21
Default passwords
for control_user....135
for view_user....135
Delete Configuration File page....169
Deleting
1+1 E1 SNCP protection....75
list view....77
matrix view....75
MSP protection....69
OSPF areas....88
static routes....89
traffic routing of E1....81
list view....82
matrix view....81
Deleting Protection page....254
DHCP server
ATU....30
NPU 8x2....26
NPU1 B....23
NPU2....23
DIG SC (64 kbit/s)....87
setting number of....88
Directory structure
FTP server....18
MINI-LINK TN 2.0....20
MINI-LINK TN 2.1 and later....20

E

E1
adding to Ethernet Bridge....85
configuration, all interfaces in one unit....225
Overview, working with....83
traffic routing
creating, list view....80
creating, matrix view....80
modifying or deleting, list view....82
modifying or deleting, matrix view....81
E1 Alarms and Status page....337
E1 Configuration page....224
E1 DCN Configuration page....162
E1 Overview page....226
E1 Performance 15 minute Intervals page....376
E1 Performance page....375
E2 Alarms and Status page....338
E2 Configuration page....223
E3 Alarms and Status page....339
E3 Configuration page....222
Edit Asset ID page....256
EEM....1, 16
basics....35
troubleshooting....47
Embedded Element Manager, *See* EEM
Emergency fallback
ATU NPU....95
NPU 8x2....96
NPU1 B....95
NPU2....95
Emergency Fallback page....166
Error log
deleting from NE....130
files stored on FTP server....19
uploading from FTP server....129
Ethernet Bridge
adding E1 to....85
configuring....79
Ethernet Bridge Alarms and Status page....282
Ethernet Bridge Configuration page....191
Ethernet configuration....174
Ethernet Status page....287
Ethernet/LAN/Servers Configuration page....174
Ethernet/Servers Configuration page....174
Event Log page....351
Events....115
list of....125
Exec mode....100

F

Factory Setting page....168
Fan Unit, *See* FAU
FAU....13
FAU Alarms and Status page....311
FAU Configuration page....187
FAU1....13
FAU2....13
FAU4....13

Fault Management....113
Finish Installation page....163
FTP server
activating on startup....21
configuring....20
default password....21
default user name....21
directory structure....18
installing and configuring....18
specifying root directory....21
starting....21
uninstalling....34

G

Getting started....17
Global Configuration mode....101
Graphical layout problems in browser....47

H

Hardware maintenance....139
Help....42
Help Setup page....279

I

IF loop....127
Indeterminate, severity....117
Indoor part
with AMM....8
with ATU....14
Initial setup....49
automatic configuration of NE parameters....53
manual configuration of NE parameters....54
configuring basic NE parameters....55
configuring DCN parameters....56
configuring E1 for DCN....57
creating OSPF areas....57
creating static routes....57
finishing the installation....58
performing a Local Software Upgrade....54
setting passwords....55
Radio Terminal configuration....49
Installation Finished page....164
Installation wizard....49
menus....36
Installing
Installing (cont.)
FTP server on PC....18
load modules on PC....22
MSM on PC....21
software on PC....18
USB driver on PC....21
Interface Configuration mode....101
Interface loops....128
Inventory page....255
Inventory report, generating....111
IP address
configuring in Windows 2000....32
configuring in Windows XP....33
NE default
ATU....30
NPU 8x2....26
NPU1 B....23
NPU2....23
PC default
NPU 8x2....26
NPU1 B....23
NPU2....23
IP/ICMP Status page....297

L

LAN/Servers Configuration page....174
LCT....1
starting
for ATU....30
for NPU 8x2....26
for NPU1 B....22
for NPU2....22
Line loop....126
Line Termination Unit, *See* LTU
List of
alarms....118
events....125
List view
1+1 E1 SNCP protection
creating....72
modifying or deleting....77
traffic routing
E1, creating....80
E1, modifying or deleting....81
Load Configuration page....275
Load Configuration Progress page....277
Load Error Log page....353
Load modules
installing on PC....22

Load modules (cont.)
stored on FTP server 19
uninstalling 34
Local Craft Terminal, *See* LCT
Local loop 127
Loops 126
setting 128
Loops page 357
LTU 12
replacing 140
LTU 12x2 12
LTU 12x2 Alarms and Status page 319
LTU 12x2 Configuration page 192
LTU 155 12
LTU 155 Alarms and Status page 320
LTU 155 Configuration page 194
LTU 155e, *See* LTU 155
LTU 155e/o, *See* LTU 155
LTU 16x2 12
LTU 16x2 Alarms and Status page 317
LTU 16x2 Configuration page 193

M

Maintenance 139
Major, severity 117
Management 16
CLI 16
EEM 16
MINI-LINK Connexion 16
MINI-LINK Manager 16
Manual configuration of NE parameters 54
configuring basic NE parameters 55
configuring DCN parameters 56
configuring E1 for DCN 57
creating OSPF areas 57
creating static routes 57
finishing the installation 58
performing a Local Software Upgrade 54
setting passwords 55
Manual Configuration page 160
Manuals 2
Matrix view
1+1 E1 SNCP protection
creating 70
modifying or deleting 75
traffic routing
E1, creating 80
E1, modifying or deleting 81
Menus 36
Menus (cont.)
installation wizard 36
Normal mode 38
NPU Installation mode 38
MINI-LINK Connexion 16
MINI-LINK DCN Guideline 2
MINI-LINK Manager 16
MINI-LINK Service Manager, *See* MSM
MINI-LINK TN 7
MINI-LINK TN ETSI Indoor Installation Manual 2
MINI-LINK TN ETSI Technical Description 2
MINI-LINK TN, MINI-LINK HC, MINI-LINK E ETSI Product Catalog 2
MINI-LINK TN, MINI-LINK HC, MINI-LINK E Outdoor Installation Manual 2
Minor, severity 117
ML-PPP, *See* PPP
MMU2 12
configuring Radio Terminals 50
replacing 142
MMU2 Alarms and Status page 326
MMU2 B/C
configuring 1+0 Radio Terminals 63
configuring 1+1 Radio Terminals 64
configuring Radio Terminals 51
replacing 143
MMU2 B/C Configuration page 201
MMU2 Configuration page 196
Modem Unit, *See* MMU2
Modify 1+1 E1 SNCP page 248
Modify MSP Protection page 252
Modify OSPF Area page 183
Modify Static Route page 180
Modify Traffic Routing page 238
Modifying
1+1 E1 SNCP protection 75
list view 77
matrix view 75
MSP protection 69
OSPF areas 88
static routes 89
traffic routing of E1 81
list view 82
matrix view 81
Modules upgrade 93
MS/RS Alarms and Status page 340
MS/RS Configuration page 213
MS/RS Performance 15 Minute Intervals page 361
MS/RS Performance page 359
MSM
installing on PC 21

MSM (cont.)
launch failure....47
uninstalling....34
MSM 6.4 Installation Guide....2
MSM 6.4 User Guide....2
MSP
protection....68
creating....68
deleting....69
modifying....69
MSP Alarms and Status page....342
MSP Configuration page....215
MSP Performance 15 Minute Intervals page....365
MSP Performance page....363

N

Naming principles....44
Navigation Tree....36
NE....7
NE Alarms and Status page....280
NE Loops page....356
Network Element, *See* NE
Node Installation mode....26
Node Processor Unit, *See* NPU
Normal mode
menus....38
NPU 8x2....27
NPU1 B....23
NPU2....23
Notifications....115
NPU....11
Installation mode....23
NPU 8x2....11
emergency fallback....96
replacing....147
starting LCT in Node/NPU Installation mode....28
starting LCT in Normal mode....29
NPU 8x2 Alarms and Status page....314
NPU 8x2 Configuration page....189
NPU Installation mode....27
menus....38
NPU1 B....12
emergency fallback....95
replacing....149
starting LCT....22
NPU1 B Alarms and Status page....312
NPU1 B Configuration page....188
NPU2....11
emergency fallback....95
NPU2 (cont.)
replacing....151
starting LCT....22
NPU2 Alarms and Status page....316
NPU2 Configuration page....190

O

Open Shortest Path First, *See* OSPF
Operational status....113
equipment....113
interfaces....114
OSPF....86
areas
creating....57, 88
deleting or modifying....88
configuration and troubleshooting....107
configuration commands....108
show commands....109
stub areas....88
OSPF Area Configuration page....181
OSPF Area Status page....302
OSPF General Status page....300
OSPF Host Status page....309
OSPF Interface Status page....304
OSPF Neighbor Status page....307
Outdoor part....15

P

Passwords
changing....136
default
for control_user....135
for FTP server....21
for view_user....135
replacing lost....136
PC requirements, *See* System requirements
Perform Emergency Fallback page....167
Performance
E1 15 Minute Intervals page....376
E1 page....375
enabling view of....131
Management....131
MS/RS, 15 Minute Intervals page....361
MS/RS, page....359
MSP, 15 Minute Intervals page....365
MSP, page....363
start time, specifying....131

Performance (cont.)
VC-12, 15 Minute Intervals page....373
VC-12, page....371
VC-4, 15 Minute Intervals page....369
VC-4, page....367
viewing data....131
PFU....13
replacing....145
PFU Alarms and Status page....310
PFU1....13
PFU1 Configuration page....184
PFU2....13
PFU2 Configuration page....185
PFU3....13
PFU3 Configuration page....186
Plug-in units....8
adding....140
PM start time....131
PM view....131
Power Filter Unit, *See* PFU
PPP
interfaces, configuring....87
STM-1 interfaces, bandwidth....87
PPP and ML-PPP Counters page....291
PPP Configuration page....177
PPP Status page....290
Preferences page....267
Privileged Exec mode....100
Protected (1+1) Radio Terminal, configuring...50, 64, 66
Protection
1+1 SNCP....70
MSP....68
Proxy server, configuring Internet Explorer....33

R

Radio Terminal
configuration....62
initial setup....49
protected (1+0)....64, 66
unprotected (1+0)....63, 66
Radio Terminal Alarms and Status page....322
Radio Terminal Configuration page....158
RAU Alarms and Status page (MMU2)....328
RAU Configuration page....204
RAU IF Alarms and Status page (MMU2)....331
RAU IF Configuration page....203
Related documents....2
Replacing
ATU....152
Replacing (cont.)
lost passwords....136
LTU....140
MMU2....142
MMU2 B/C....143
NPU 8x2....147
NPU1 B....149
NPU2....151
PFU....145
SMU2
when used for co-siting....140
when used for protection....142
Report page....257
Reports
generating.... 111
Reset COnfiguration page....208
Restart page....278
Restore Configuration page....209
Restore NPU Configuration page....171
Revision information....2
RF
loop....127
RF Alarms and Status page (MMU2)....330
RF Configuration page....207
Router Configuration mode....101
Rx loop....127

S

Safety conventions....3
SBDF....91
Scheduled Activation page....272
Security
management....135
Security page....380
Select Option page....381
Setting loops....128
Settings page....263
Severity....117
SMU2....12
replacing
when used for co-siting....140
when used for protection....142
SMU2 Alarms and Status page....334
SMU2 Configuration page....198
SNCP, *See* 1+1 E1 SNCP protection
Software
baseline....19
installing on PC....18
uninstalling on PC....34

Software (cont.)
upgrade 91
baseline 91
modules 93
preferences 267
Software Baseline Description File, *See* SBDF
Software System Release 19
Software Upgrade – Installation Wizard page 161
Start Upgrade page 265
Starting LCT
for ATU 30
for NPU 8x2 26
Node/NPU Installation mode 28
Normal mode 29
for NPU2/NPU1 B 22
Static routes
configuring 110
creating 89
modifying or deleting 89
Static Routing Configuration page 179
Static Routing Status page 299
Status Bar 41
STM-1 interface 12, 86
Stub areas 88
CLI 107
Support 5
SWITCH Alarms and Status page (MMU2) 333
SWITCH Configuration page 210
Switch Multiplexer Unit, *See* SMU2
SWITCH Protection page 211
System
overview 7
requirements 17

T

Target group 2
TCP Status page 293
Technical support 5
Third party products 4
Traffic capacity
changing for Radio Terminal 153–154
changing for SMU2 (co-siting) 156
Traffic Routing List View page 234
Traffic Routing Matrix View page 232
Traffic routing of E1 79
creating
list view 80
matrix view 80
Traffic routing of E1 (cont.)
modifying or deleting
list view 82
matrix view 81
Traffic Routing Select Interfaces page 230
Troubleshooting 47
graphical layout problems in browser 47
MSM launch failure 47
Typical workflow 59
Typographic conventions 3

U

UDP Status page 295
Uninstalling
FTP server from PC 34
load modules from PC 34
MSM from PC 34
software from PC 34
USB driver from PC 34
Unit configuration 61
Unprotected (1+0) Radio Terminal
change to protected (1+1) 154–155
configuring 63, 66
Unsupported Unit Alarms and Status page 336
Upgrade of Baseline 91
Upgrade of Baseline page 260
Upgrade of Modules 93
Upgrade of Modules page 262
Upgrade Progress - Baseline page 269
Upgrade Progress - Modules page 271
USB
installing driver on PC 21
uninstalling driver from PC 34
USB Status page 289
USBLAN, *See* USB
User Input Alarms and Status page 347
User Input Configuration page 228
User interface
Confirm Button 42
Help 42
menus 36
naming principles 44
Navigation Tree 36
overview 35
reference 157
Status Bar 41
User names 135
FTP server default 21

User Output Alarms and Status page....348
User Output Configuration page....229
Using
EEM....35
help....42

V

VC-12
configuring a single interface on one unit....218
configuring all interfaces on one unit....220
VC-12 Alarms and Status page....346
VC-12 Configuration page....218
VC-12 Performance 15 Minute Intervals page....373
VC-12 Performance page....371
VC-4 Alarms and Status page....344
VC-4 Configuration page....216
VC-4 Performance 15 Minute Intervals page....369
VC-4 Performance page....367
View Report page....258
View Units page....266
view_user....135
Viewing
alarms....115
logged alarms and events....116
performance data....131

W

Warning, severity....117
Workflow....59

Ericsson AB
Transmission and Transport Networks
SE-431 84 Mölndal, Sweden
Telephone +46 31 747 00 00
Fax +46 31 27 72 25
www.ericsson.com

EN/LZT 712 0177 R2C/1