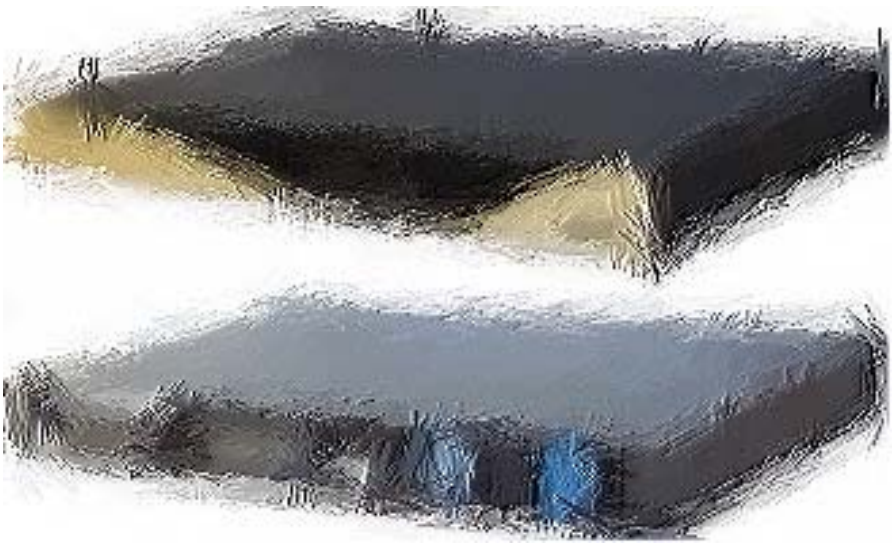
AXX155

Integrated
access device
for use
in fibreoptic networks

Product release 2

User guide

61001-05BA
Document version 2.0



Faster and more effective communication

Copyright

AXXESSIT ASA

Disclaimer

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

AXXESSIT ASA *makes no warranty of any kind with regard to this material, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose.*

AXXESSIT ASA shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance or use of this material. AXXESSIT ASA assumes no responsibility for the use or reliability of its software on equipment that is not furnished by AXXESSIT ASA.

Safety considerations

Prior to the installation and use of this product, review all safety markings and instructions.

WARNING indicates a hazard that can cause injury.

CAUTION indicates a hazard that can damage equipment or data.

Do not proceed beyond a WARNING or CAUTION notice until you have understood the hazard and have taken appropriate precautions.

Servicing

There are no user-serviceable parts inside the user-installable modules comprising the product. Only service-trained personnel must perform any servicing, adjustment, maintenance or repair.

© AXXESSIT ASA
Isebakkveien 25 • 1787 Berg i Østfold - Phone: + 47 69 17 38 00 • Telefax: + 47 69 17 39 00

1.1 Table of content

Chapter 2

2 About this guide

Objective

Audience

Document overview

Conventions

Glossary

References

2.1 Objective

The purpose of this User Guide is to describe the second release of AXX155, AXX155 R2.

After reading this User Guide, the user shall be able to install, configure and to put the AXX155 R2 into service. The AXX155 R2 Command Line Interface management solution is an integral part of this User Guide.

The higher-level management tool AXXMASTER is described in the separate AXXMASTER USER GUIDE.

Audience

A basic knowledge related to both SDH/TDM and TCP/IP is an advantage when reading this User Guide.

Document overview

The User Guide is split into ten chapters. User Guides are not automatically delivered together with the equipment they refer to. The number of User Guides per type to be supplied must be decided at contract level.

Warning

AXXESSIT ASA makes no warranty of any kind with regards to this manual, and specifically disclaims the implied warranties of merchantability and fitness for a particular purpose. AXXESSIT ASA will not be liable for errors contained herein or for damages, whether direct, indirect, consequential, incidental, or special, in connection with the furnishing, performance, or use of this material.

Notice

The product specification and/or performance levels contained in this document are for information purposes only and are subject to change without notice. They do not represent any obligation on the part of AXXESSIT ASA.

Copyright notification

Conventions

This User Guide describes the AXX155 R2 4x2 Mbit/s + Ethernet Bridge transmission system.

2.2 Glossary

6B/8B	Line code translated from 6 bit word to selected values of 8 bit words
ABER	Bit Error Rate switching threshold
AC	Alternate Current
ADM	Add Drop Multiplexer
AIS	Alarm Indication Signal (1111...)
APS	Automatic Protection Switching
AU	Administrative Unit
AUXP	Auxiliary Pattern (1010...)
B2B	Back-to-back
BAT	Battery
BER	Bit Error Ratio
BIDL	Bi-Directional Loopback Alarm
CLI	Command Line Interface
CLNP	Connection less Network Protocol
CO	Central Office
CRC-4	Method for detection of bit errors (ITU-T Rec. G.704)
DC	Direct Current
DCC	Data Communications Channel
DCE	Data Circuit-terminal Equipment
DCN	Data Communications Network
DL	Downlink (towards user)
DLAS	Degraded Laser
DQUI	Degraded Quality on User Interface
DTE	Data Terminal Equipment
ECT	Equipment Craft Terminal
EOW	Engineering Order Wire
EEPROM	Electrical Erase Programmable Read Only Memory
EMC	Electromagnetic Compatibility
EPROM	Erase Programmable Read Only Memory
ES	End System
ES	Errored Seconds

ET	Exchange Termination
ETSI	European Telecommunications Standards Institute
F1	Optical line interface
F2	Electrical 2 Mbit/s interface
FA	Frame Alignment
FC	Failure Condition
FC/PC	Optical Connector
FP	Fabry Perot
FPGA	Field Programmable Gate Array
FTP	File Transfer Protocol
GUI	Graphical User Interface
HBER	High Bit Error Rate
HDB3	High Density Binary Code
HDLC	High-level Data Link Control
HDSL	High bit rate Digital Subscriber Line
HW	Hardware
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
ICS	Item Change Status, AXXESSIT ASA version number
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IS	Intermediate System
ISDN	Integrated Services Digital Network
ITU-T	International Telecommunication Union Standardization Bureau
KLM	Numbering scheme for containers in SDH
LAP-D	Link Access Procedure on the D channel
LAN	Local Area network
LBER	Low Bit Error Rate
LCT	VT.100 compatible Local Craft Terminal
LD	Laser Diode
LED	Light Emitting Diode
LFA	Loss of Frame (BF) Alignment
LL2/LL3	Local Loop 2/3
LMF	Loss of Multiframe Alignment

LOS	Loss of Signal
LPS	Line Protection Switching
LTE	Line Termination Equipment
MAC	Medium Access
MD	Mediation Device
MF	Multiframe (G.704)
MIB	Management Information Base
MS	Multiplex Section
NC	Not Connected
NE	Network Element
NET	Network
NSAP	Network Service Access Point
NTE	Network Termination Equipment
NV	Non-Volatile
OC	Operating Center
OCT	Office Craft Terminal
ODF	Optical Distribution Frame
OFDLS	Optical Fibre Digital Line System (Associated LTE, NTE and fibre route)
OLOS	Optical LOS
OPOL	Optical Power out of Limit
ORX	Optical interface module RX
OSI	Open Systems Interconnection
OTX	Optical interface module TX
PABX	Private Automatic Branch Exchange
PC	Personal Computer
PCB	Printed Circuit Board
PDH	Plesiochronous Digital Hierarchy (ITU-T Rec. G.702)

2.3 References

ITU-T Recommendations

G.652	Single Mode Optical Fibre
G.701	Vocabulary of Transmission and Multiplexing, and Pulse Code Modulation (PCM) Terms.
G.702	Digital Hierarchy Bit Rates
G.703	Physical/Electrical Characteristics of Hierarchical Digital Interfaces
G.704	Synchronous Frame Structures at Primary and Secondary Hierarchical levels.
G.706	Frame Alignment and Cyclic Redundancy Check (CRC) Procedures Relating to Basic Frame Structures Defined in Recommendation G.704
G.707	Network node interface for the synchronous digital hierarchy (SDH)
G.783	Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks
G.823	The control of jitter and wander within digital networks that are based on the 2048 kbit/s hierarchy
G.825	The control of jitter and wander within digital networks that are based on the synchronous digital hierarchy (SDH)
G.832	Transport of SDH elements on PDH networks - Frame and multiplexing structures
G.957	Optical interfaces for equipments and systems relating to the synchronous digital hierarchy
G.958	Digital line systems based on the synchronous digital hierarchy for use on optical fibre cables
X.150	Principles of maintenance Testing for Public Data Network using Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) test Loops

ETSI Documents

EN 50082-2	Generic immunity standard Industrial environment
EN 55022	Specification for Limits and methods of Measurement of Radio Interference Characteristics of Information Technology Equipment
EN 55024	Electromagnetic Compatibility Requirements for Information Technology Equipment (Previously EN 55101)
EN 60825	Radiation Safety of Laser Products
EN 60950	Safety of Information Technology Equipment Including Electrical Business Equipment
ETS 300 011	Integrated Services Digital Network (ISDN); Primary rate user-network interface; Layer 1 specification and test principles
ETS 300 019	European Telecommunications Standard for Environment
ETS 300 233	Integrated Services Digital Network (ISDN); Access digital section for ISDN primary rate
ETS 300 246	Open Network Provision (ONP) Technical Requirements: 2048 kbit/s Digital Unstructured leased Line (2048 U) Interface Presentation
ETS 300 247	Open Network Provision (ONP) Technical Requirements: 2048 kbit/s Digital Unstructured Leased Line (D2048 U) Connection Characteristics
ETS 300418	Business Telecommunications (BTC); 2048 kbit/s Digital Unstructured and Structured Leased Lines Network Interface Presentation
ETS 300 419	Business TeleCommunications (BTC); 2048 kbit/s Digital Structured Leased Lines (D2048S) Connection Characteristics
ETS 300 461-1	Transmission and Multiplexing (TM) Flexible Multiplexer (FM) equipment; Part 1: Core functions 2048 kbit/s aggregate interface functions, tributary interface functions and special functions

IEC Documents

IEC 61000-4-2	Electromagnetic compatibility (EMC) - Part 4-2: Testing and measurement techniques - Electrostatic discharge immunity test
IEC 61000-4-3	Electromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques - Section 3: Radiated, radio-frequency, electromagnetic field immunity test
IEC 61000-4-4	Electromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques - Section 4: Electrical fast transient/burst immunity test. Basic EMC Publication
IEC 61000-4-6	Electromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques - Section 7: General guide on harmonics and interharmonics measurements and instrumentation, for power supply systems and equipment connected thereto

2.4 List of figures

2.5 List of tables

Chapter

3

3 Product overview

Functional overview

Features

Applications

Management

3.1 Functional overview

The AXX155 R2 is an Integrated Access Device for use in fibre optic networks. The AXX155 R2 combine IP- and TDM-traffic, by running IP-along with TDM-channels inside an SDH STM-1 frame structure that can be easily carried across the network. The bandwidth of the IP-channel is configurable up to 100 Mb/s true “wire-speed”. The IP part of the AXX155 R2 consists of a L2 switch.

Each tributary interface is mapped into a VC-12 container while the WAN traffic is mapped into a configurable number of VC-12 containers. Because the latter mapping is proprietary, the WAN connection can only be run with a pair of two AXX155 R2 s (communicating with each other over the aggregate ports).

The AXX155 R2 management solution is based on an embedded SNMP agent. An element manager application called AXXMASTER is provided for remote supervision of AXX155 R2 devices. AXX155 R2 also provides a simple VT100 command line interface (CLI) for direct communication with the embedded SNMP agent.

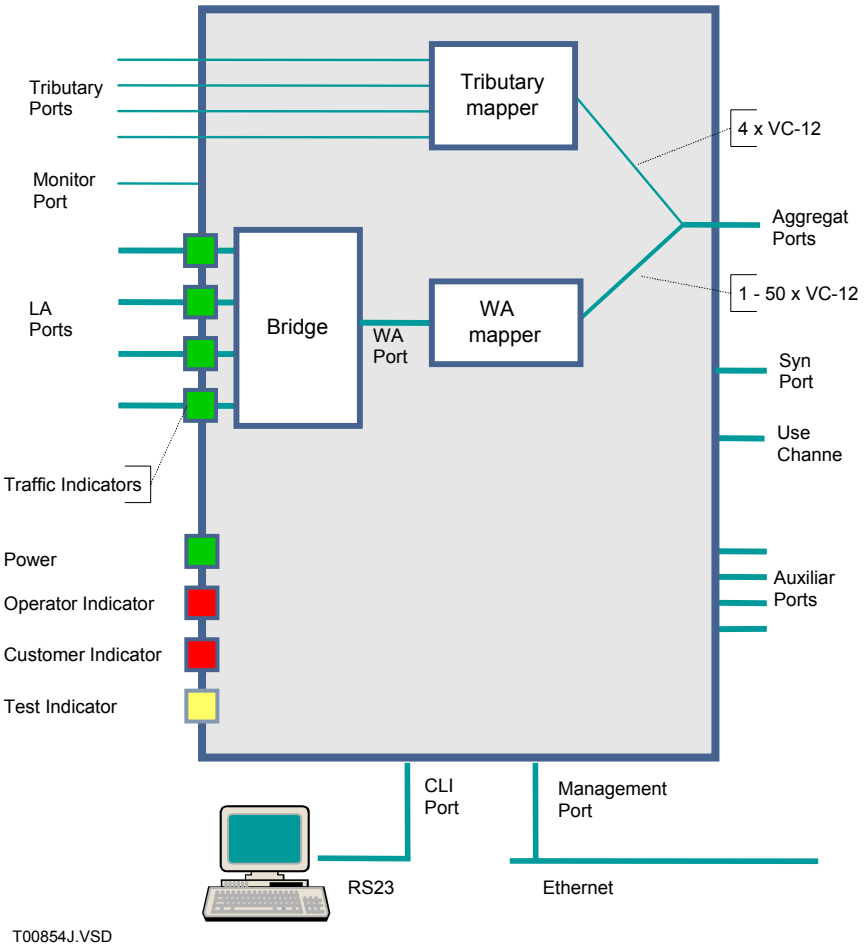


Figure 1. AXX155 R2 Overview

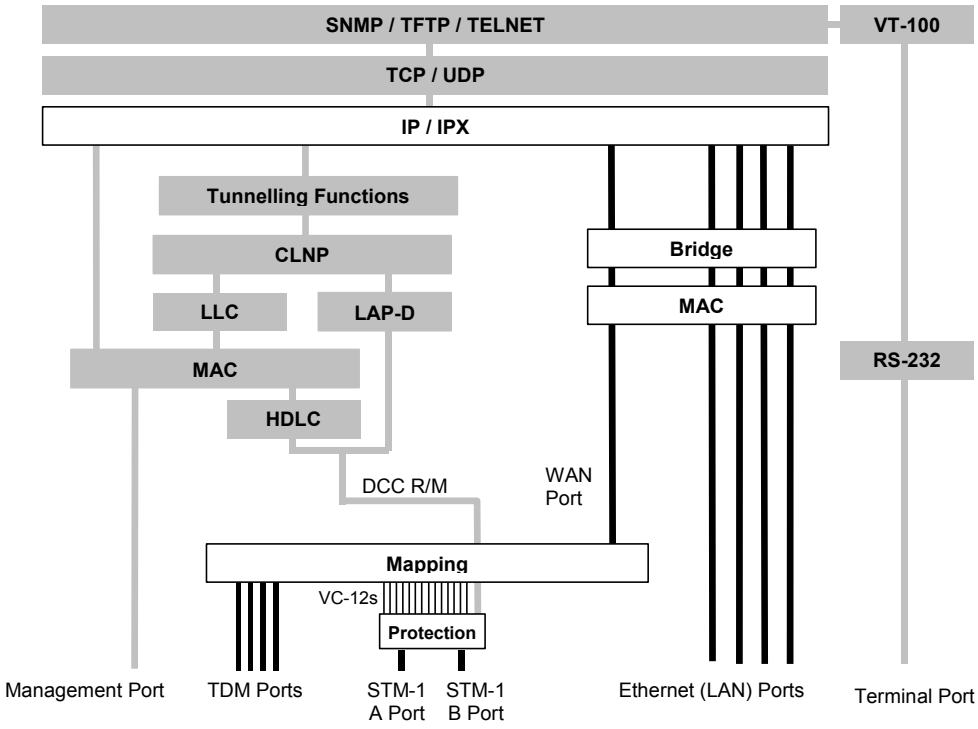


Figure 2. Functional Model for the AXX155 R2.

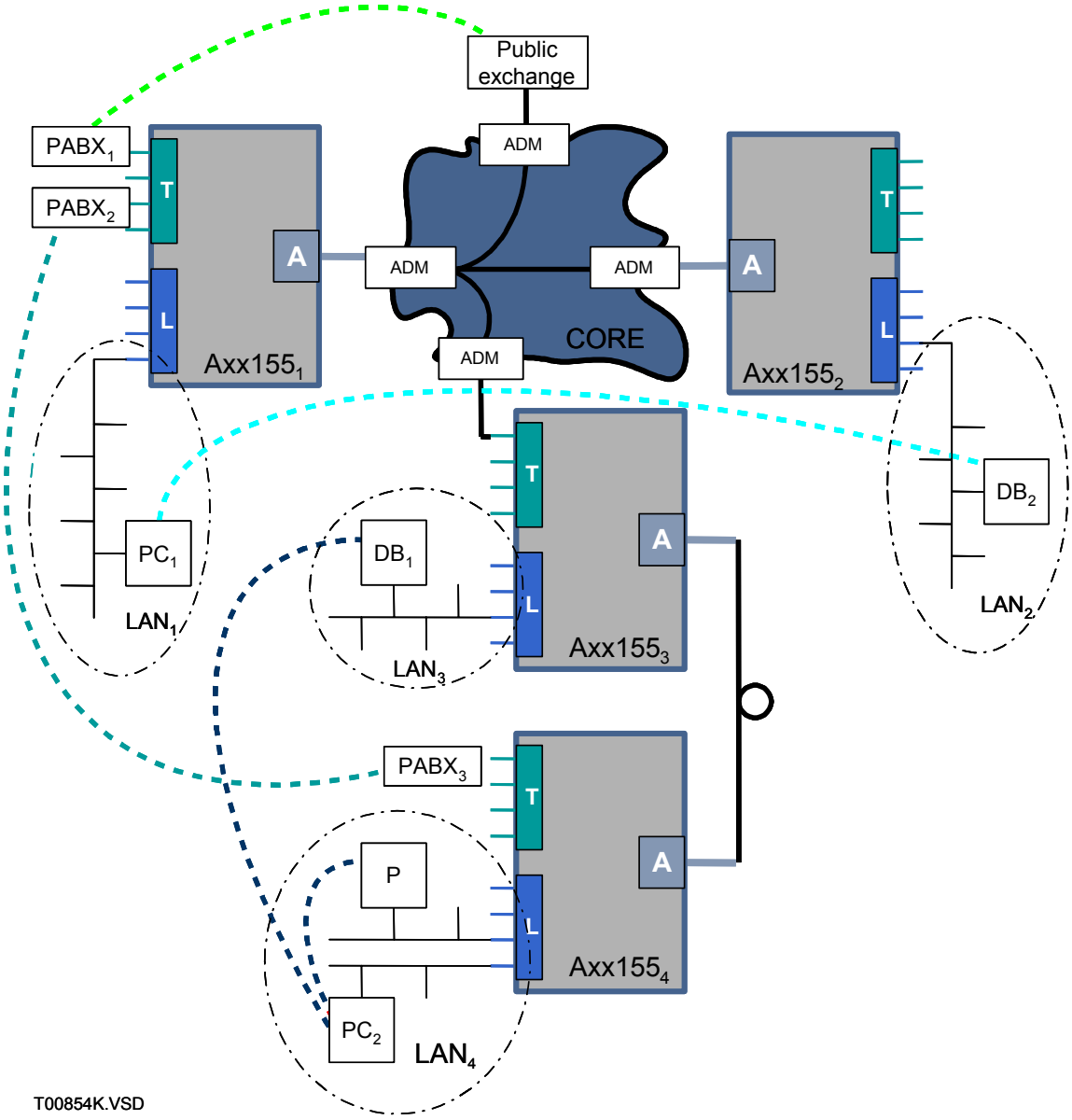


Figure 3. AXX155 R2 in a network

Figure 2 shows how AXX155 R2 typically fits into the access part of SDH network topologies. The figure shows two WANs. WAN_1 consists of LAN_1 and LAN_2, and the two LANs are connected using the core network. In this WAN the computer PC_1 has access to the database server DB_2.

WAN_2 consists of LAN_3 and LAN_4, and these LANs are connected locally using the optical ports of the AXX155 R2**.** As can be seen LAN_4 consists of two segments. In this WAN the computer PC_2 has access to the printer P using only the bridge functionality in AXX155 R2**.** PC_2 also has access to the database server DB_1 using the optical link between AXX155 R2 $_3$ and AXX155 R2 $_4$.,

3.2 Features

SDH multiplexing and mapping

AXX155 R2 has one STM-1 optical aggregate interface, i.e. no protection is provided. The aggregate interface only supports terminal multiplexer functions, and 63xVC-12 mapping. There is no support for VC-3 mapping.

Internal structure

The figure “Multiplexing and mapping in AXX155 R2” shows the internal structure of AXX155 R2**.** The bridge receives Ethernet frames on one of the ports and decides on which port to send it out. The Ethernet Mapper converts between Ethernet frames and VC-12s, while the Tributary Mapper converts between E1 signals and VC-12s. The SDH Multiplexer is responsible for the multiplexing of VC-12s into STM-1. The VC-12s are sent to - and received from - either the Tributary Mapper or the Ethernet Mapper.

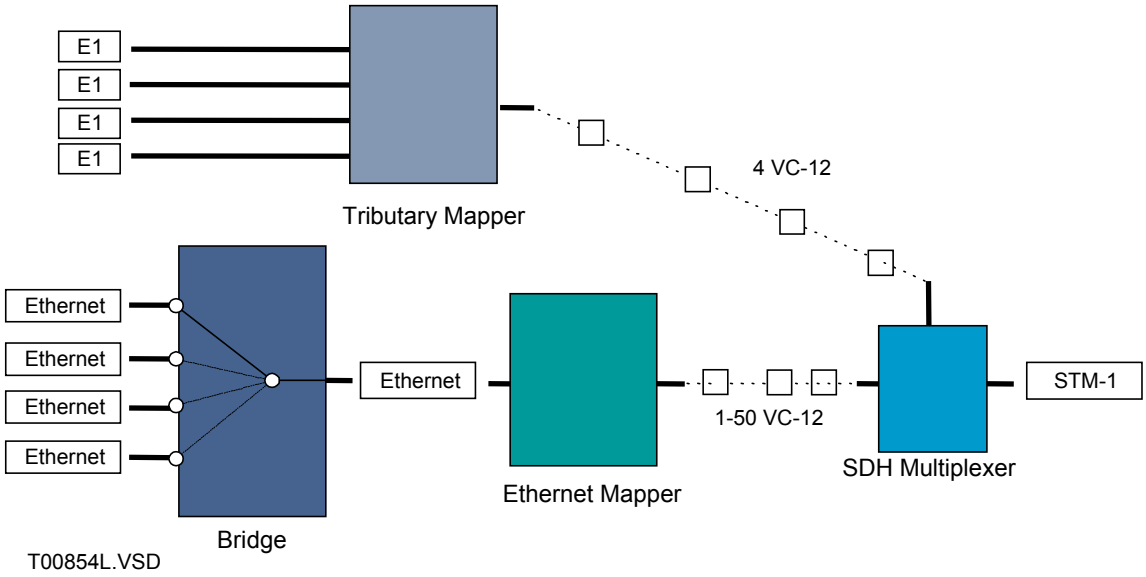
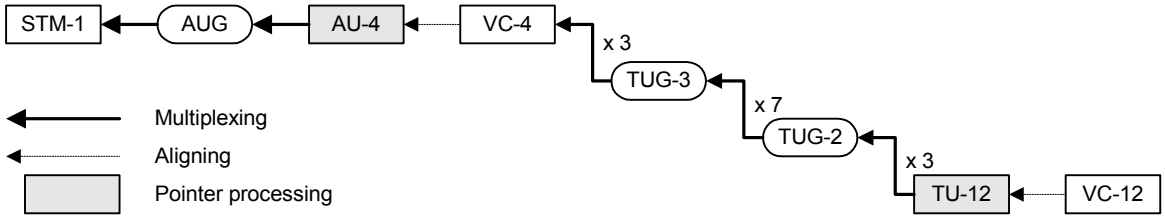


Figure 4. Multiplexing and mapping in AXX155 R2.

The WAN traffic is mapped into a number of VC-12 containers in a round-robin fashion with an inverse multiplexer function. The Ethernet traffic is mapped into one or a number of VC-12 containers. A proprietary mapping scheme is used to map the data into the VC-12 containers as shown below.



T00854N.VSD

Figure 5. Multiplexing structure in STM-1.

VC-12 (KLM)	Linked to
1.1.1	TRIBUTARY (1)
2.1.1	TRIBUTARY (2)
3.1.1	TRIBUTARY (3)
1.2.1	TRIBUTARY (4)
2.2.1	Unused
3.2.1	Unused
1.3.1	Unused
2.3.1	Unused
3.3.1	WAN-PORT
1.4.1	WAN-PORT
2.4.1	WAN-PORT
...and so forth until ...	
3.5.3	WAN-PORT
1.6.3	WAN-PORT
2.6.3	Unused
3.6.3	Unused
1.7.3	Unused
2.7.3	Unused
3.7.3	Unused

Table 1 VC-12 mapping scheme

Protection

The AXX155 R2 offers 1+1 linear Multiplex Section Protection (MSP). The protocol used for K1 and K2 (b1-b5) is defined in ITU-T G.841, clause 7.1.4.5.1.

The protocol used is 1+1 bi-directional switching compatible with 1:n bi-directional switching. The operation of the protection switch is configurable as described in the table below:

Parameters	Description
MSP Enabled	ENABLED or DISABLED
Switching type	UNIDRECTIONAL or BIDIRECTIONAL
Operation Type	REVERTIVE or NON_REVERTIVE
Wait-to-restore time (0:2147483647 seconds) Default: 300 seconds	Number of minutes to wait before switching back to the preferred link after it has been restored
Preferred Link	Identifier of the preferred working link (always LINK A for AXX155 R2)
Switching Commands	- Clear - Lockout of Protection - Forced switch to protection - Forced switch to working - Manual switch to protection - Manual switch to working - Exercise
Working Link	Identifier of the current working link
Local Request	Local request contained in K1 byte
Remote Request	Remote request contained in K1 byte

Table 2 **Protection switch parameters**

Performance monitoring

The AXX155 R2 offers full G.826 performance monitoring at the RS, MS, VC-4, and VC-12 levels in the SDH hierarchy. This includes B1 near end in RSOH section, B2 near and far end in MSOH section, B3 near and far end at VC-4 level and BIP-2 near and far end at VC-12 level.

The AXX155 R2 calculates excessive error and degrade signal defects assuming Poisson distribution of errors, according to ITU-T G.826.

The excessive error defect (dEXC) is detected if the equivalent BER exceeds a pre-set threshold of 10E-5, and be cleared if the equivalent BER is better than 10E-6, according to ITU-T G.806.

The degraded signal defect (dDEG) is detected if the equivalent BER exceeds a pre-set threshold of 10E-X, where x=6,7,8 or 9. The dDEG is cleared if the equivalent BER is better than 10E-(X+1), according to ITU-T G.806 .The threshold is individually configurable for the different levels in the SDH hierarchy, from 10E-6 to 10E-9.

Synchronisation

AXX155 R2 can synchronize to the following sources:

- An STM-1 interface (working link, backup link, or active link)
- The dedicated 2048 kHz sync input (Sync Port)
- A Tributary Port
- A local oscillator

Tributary synchronization is only relevant in certain configurations.

The synchronization source is a configurable parameter. If it is impossible to synchronize to the selected source, an alarm will be raised, and the system will automatically switch to free running, i.e. the local oscillator.

Switchback to the selected source is performed automatically whenever it becomes possible again. The alarm is cleared when the switchback is successful.

The default synchronization source is the local oscillator.

AXX155 also provides a 2048 kHz sync output for synchronization of external equipment.

3.3 IP Features

General

AXX155 R2 supports Layer 2 switching (bridge), with support for additional features in future software releases. Enabling of these features will require a specific license-key (see section; Feature Management in page 84).

Bridging

The bridge is a transparent multi-port remote Ethernet bridge as specified in IEEE 802.3. The Bridge consists of four LAN ports and one WAN port. Each port may have its own MAC address, but in most configurations one MAC address for the whole bridge is sufficient. The four LAN ports support 10/100BaseT Ethernet for UTP cables. Both 10Mbit/s and 100Mbit/s are supported with auto-negotiation. The LAN ports are compatible with IEEE 802.3.

The bridge supports the following features:

- MAC switching
- Self-learning MAC Addresses
- Automatic Ageing for MAC addresses
- MAC Multicast
- Transparent Bridging
- Port-based Virtual LANs (VLANs)
- Full IEEE 802.1Q VLAN tagging compliance
- Back pressure and flow control Handling
- Spanning Tree Protocol (STP) per device

The filtering rate of the bridge is able to operate at full wire speed. The forwarding rate is only limited by the forwarding interface speed, i.e. the selected WAN channel speed.

BootP

BootP is used to get one IP address for the AXX155 R2 under the installation process (see section;Device Replacement on page 84). This feature is typical a part of both variants.

Tributary ports

AXX155 R2 provides four 120 Ω 2.048 MHz Tributary Ports on the customer side. 75 Ωoperation is supported by adding an external balun.

Each Tributary Port can be individually configured to run in one of the following modes:

- G.703 Transparent (TRA)
- ISDN Primary Rate Access (PRA)

PRA is implemented according to ETS 300011 and ETS 300233. Note that AXX155 R2 can only implement the PRA NTE functions.

Transparent transmission mode.

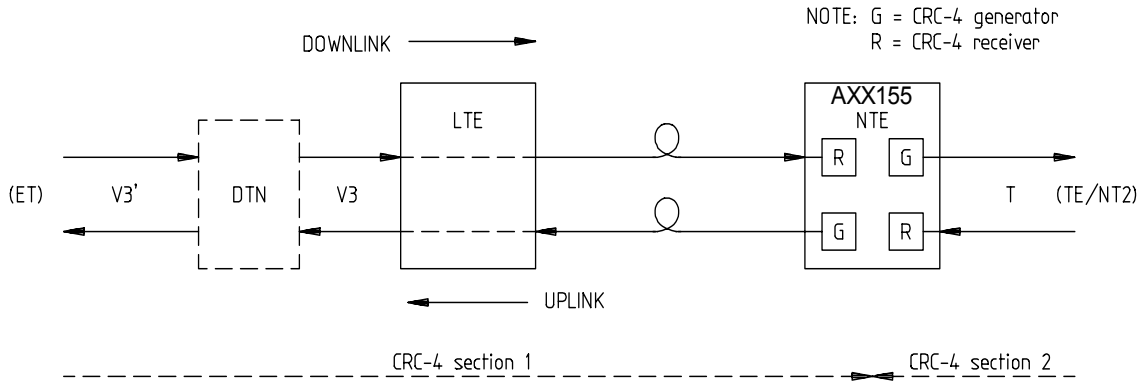
In this mode 2.048 Mbit/s plesiochronous data and timing are transferred independently of frame structure. The two directions of transmission are completely independent of each other.

Downstream AIS is generated on loss of signal or loss of optical frame alignment.

ISDN primary rate access (PRA) transmission mode.

The functional layout compliant to pr. ETS 300 233 is shown in Figure 5

DTN	Digital Network
V3' and V3	ISDN Reference Points, Exchange Termination Interface
T	ISDN Reference Point, Customer Interface
Downlink	Signal direction from Exchange Termination (ET)
Uplink	Signal direction to Exchange Termination (ET)



T00854O.VSD

Figure 6. AXX155 R2 ISDN PRA configuration

Downlink transfer

The LTE is transparent to the 2 Mbit/s signal. However, monitoring the G.704 multiframe format is performed for detection of loop-back 1 command from the Exchange Termination (TS 0 bit Sa6)

The NTE terminates CRC-4 section 1 by the Receiver (R) circuits, which pass the signal to the Generator (G) circuits with indication of basic frame start. The G circuits generate new TS 0 basic frame and multiframe to CRC-4 section 2, and pass transparently TS1 - TS31 and from TS 0 the RAI bit and the Sa-bits 4 to 8. AIS is generated to the TE on loss of signal and when R circuits have lost alignment to G.704 basic frames.

Uplink

The NTE terminates CRC-4 section 2 in the R circuits, which pass the signal to the G circuits with indication of basic frame start. The G circuits generate new TS 0 basic frame and multiframe to CRC-4 section 1 and pass transparently TS1- TS31 and from TS 0 the RAI bit and the Sa-bits 4,7 and 8.

The G circuits generate «substituted» frames to the ET on loss of signal or loss of alignment to basic G.704 frames from TE.

The LTE is transparent to the 2 Mbit/s signal.

On loss of optical line signal, the LTE generates an auxiliary pattern AUXP=1010.. to the ET.

Supervision by the exchange termination (ET)

The TS 0 bits Sa5 and Sa6 are used for supervision. Bit Sa5 being «0» downlink and «1» uplink, indicates the direction of transmission.

Four Sa6 bits aligned with the G.704 submultiframe are coded as follows:

ET generated downlink Sa6 codes:

Normal condition	Sa6 = 0000
Loop-back 1 command to LTE	Sa6 = 1111
Loop-back 2 command to NTE	Sa6 = 1010

NTE generated uplink Sa6 codes:

See table below.

Condition	Uplink report to Exchange Termination	Comments
Normal Operation	Sa6 = 00XX RAI = 0 Sa5 = 1	XX reports bit errors related to CRC-4 section 2
AIS Received at V3	Sa6 = 1111 RAI = 1 Sa5 = 1	RAI Generated by TE
Loss of Signal V3 (FV3) Loss of line signal or downlink FA (FC5)	Sa6 = 1110 RAI = 1 Sa5 = 1	RAI Generated by TE
Loss of Signal at T (FC4)	Sa6 = 1100 RAI = 0 Sa5 = 1	The NTE generates substituted frames with RAI=0. Reporting of other failure conditions has priority.
Power failure (NTE dying gasp)	Sa6 = 1000 RAI = X Sa5 = 1	Reporting of this failure condition has the highest priority.
Loss of Line Signal at LTE (FC1)	AUXP	Auxiliary alarm indication pattern (1010..) generated by the LTE.
Loop-back 1 activated by downlink Sa6=1111	Sa6 = 1111 RAI = 1 Sa5 = 0	The downlink signal is looped back fully transparently in the LTE.
Loop-back 2 activated by downlink Sa6=1010	Sa6 = 00XX RAI = 1 Sa5 = 0	The TS1-TS31 and the TS 0 bits RAI, Sa4,7 and 8 of the downlink signal are looped back by the NTE. Sa5 is changed to 0 by the NTE to indicate loop-back condition.

Table 3 **Time Slot 0 signalling in PRA mode**

Handling of CRC-4 errors

CRC-4 errors detected in R circuits downlink and uplink are inserted as E-bits to the ET and TE respectively.

If multiframe alignment is not obtained, the NTE reports all E-bits «0» (error).

Detected bit errors related to CRC-4 section 2 are reported to the ET by use of the two last bits of the Sa6 code in normal operational condition.

	Events	Sa6
a)	CRC-4 errors detected by the NTE:	“0010”
b)	CRC-4 errors reported as E-bits from the TE:	“0001”
	a)+b) or no MF alignment to signal received from the TE:	“0011”

Table 4 CRC-4 Section 2, bit-error reporting in the Sa6 code

ITU-T Rec.G.706, ANNEX B is applied to CRC-4 section 2 which means that the NTE stops «searching» for MF alignment after a given period of time without further actions. Continuous Sa6 = 0011 indicates to the ET that quality information is not available from CRC-4 section 2.

Test loops

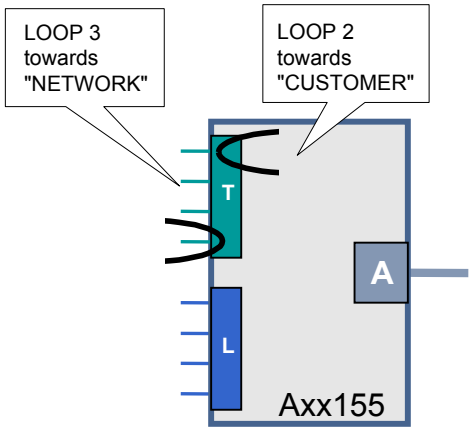
Two test loops are provided per Tributary Port, one in the customer direction (LL2) and one in the network direction (LL3), see figure “Test loops schematic view”. One Tributary Port can have only one loop activated at a time. The test loops can be activated, deactivated and monitored by the management system. The loop control logic depends on the tributary mode (TRA or PRA).

- In TRA mode the management system can operate the loops at any time.
- In PRA mode the loops are supposed to be controlled by some exchange termination equipment (ET) via inband channel 0 control bits. In this mode it is not possible to operate the loops from the AXX155 R2 management system.

It is possible to change the tributary mode regardless of the state of the loops. If the mode is changed, the loops will be cleared. The Test LED is ON if any tributary loop is activated, regardless of the tributary mode.

To change the tributary mode, the loop must be cleared.

A common monitor point is provided for monitoring of input and output signals for each of the tributary interfaces. The tributary monitored is configurable from the management system. Only one tributary can be monitored at a time.



T00854M.VSD

Figure 7. Test loops schematic view

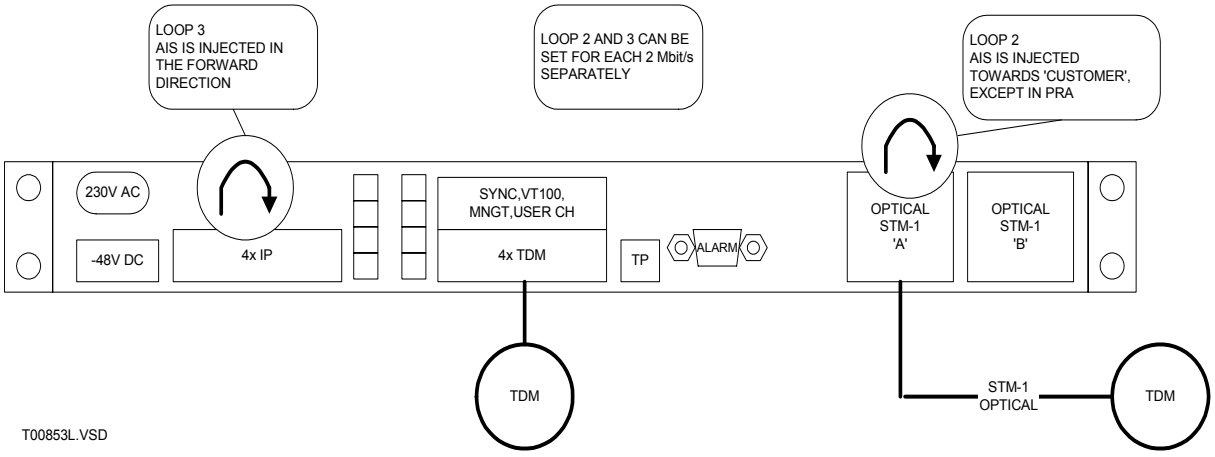


Figure 8. Test loops layout view

Alarm ports

The AXX155 provides facilities to report four auxiliary alarm inputs for associated equipment, e.g. power unit failure, battery condition, cabinet door etc. These alarms are activated by an external loop between a pair of contacts.

The polarity of the auxiliary alarm input ports is a configurable parameter, i.e. alarm can be defined either as a loop closed or a loop open condition.

The alarms are reported to the management system. Each alarm input port may have an individual configurable textual description associated with it.

The AXX155 provides also support for two alarm output ports (Alarm-out 1 and Alarm-out 2) used to signal equipment alarms and traffic related alarms. Alarm-out 1 and Alarm-out 2 reflect the status of the operator LED and the customer LED respectively .

LED indicators

The LED indicators are used to visualise the AXX155 R2 status:

Indicator	Colour	Function
Traffic Indicators	Green	LAN traffic indicator (one LED per LAN Port)
Customer Indicator	Red	Alarm on the AXX155 R2 customer side (including the Auxiliary Ports)
Operator Indicator	Red	Alarm on the AXX network side (Aggregate Port incl. VC12) or the device itself.
Test Indicator	Yellow	Test loop is present
Power Indicator	Green	Power OK

Table 5 LED indicators

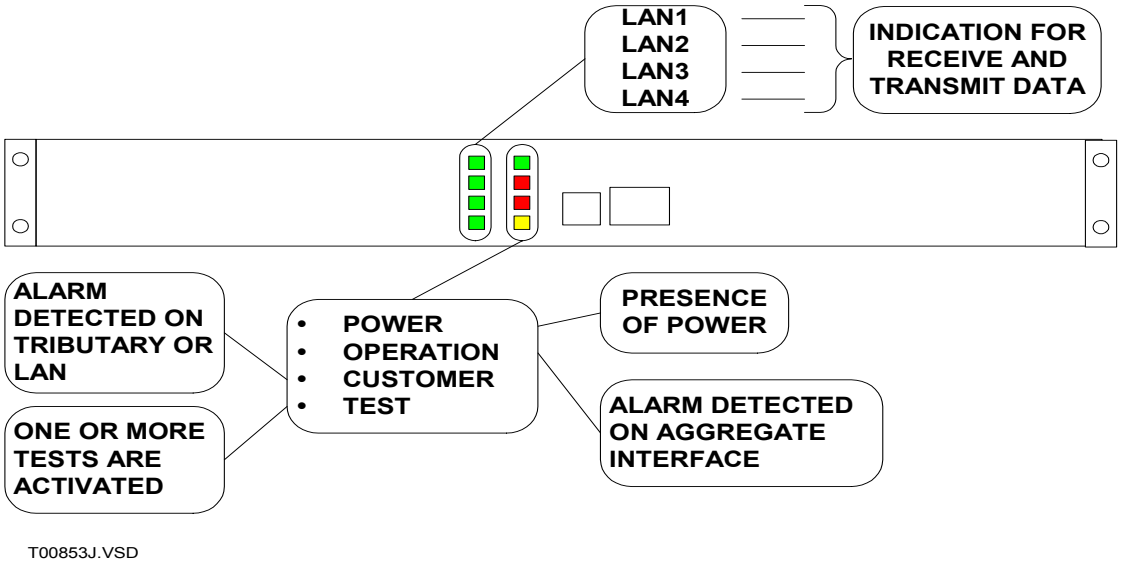


Figure 9. AXX155 R2 LEDs

User Channel

A transparent User Channel is provided (F1 byte in RSOH) for transportation of general data. The interface is balanced RS485 and supports synchronous 64 kbit/s or asynchronous 19.2 kbit/s by configuration.

Automatic System Clock setting

The AXX155 R2 supports a protocol for automatic date and time setting based on the Time Protocol (TP) described in RFC 868. To use this protocol, a TP-server must be available in the network. Because the Time Protocol provides only GMT time and does not take into account the day-light saving time (summer time), an additional parameter

(Time Zone – see page 72) allows the user to get the local time. The parameter must be adjusted twice a year to take into account the Day-Light Saving Time.

3.4 Applications

Back to back application

Normally the AXX155 R2 at the customer site is connected to an AXX155 R2 at the operator point of presence (PoP). A number of these systems can be connected in a star network and the IP traffic is groomed by an Ethernet switch before it is transmitted to the core network. Figure 1 shows the layout of a typical system with the AXX155 R2 incorporated. The network in this figure does not have a separate IP backbone network, but this could easily be supported.

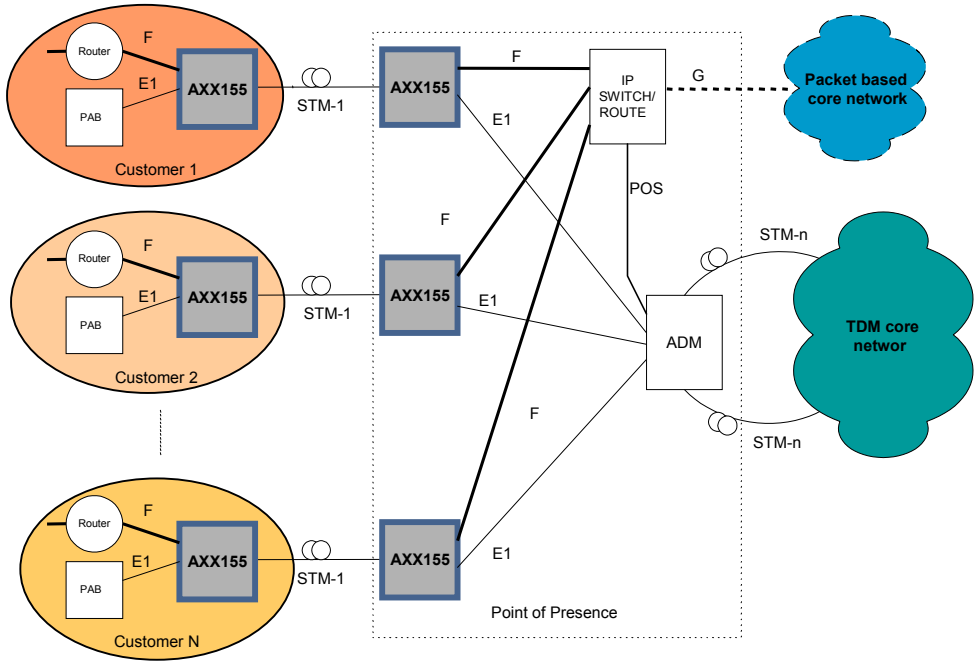


Figure 10. Back-to-back configuration across the access loop

Remote back to back application

The AXX155 R2 can also be directly connected to the SDH transport network if the operator wants to do IP grooming at a different site as shown in the figure below.

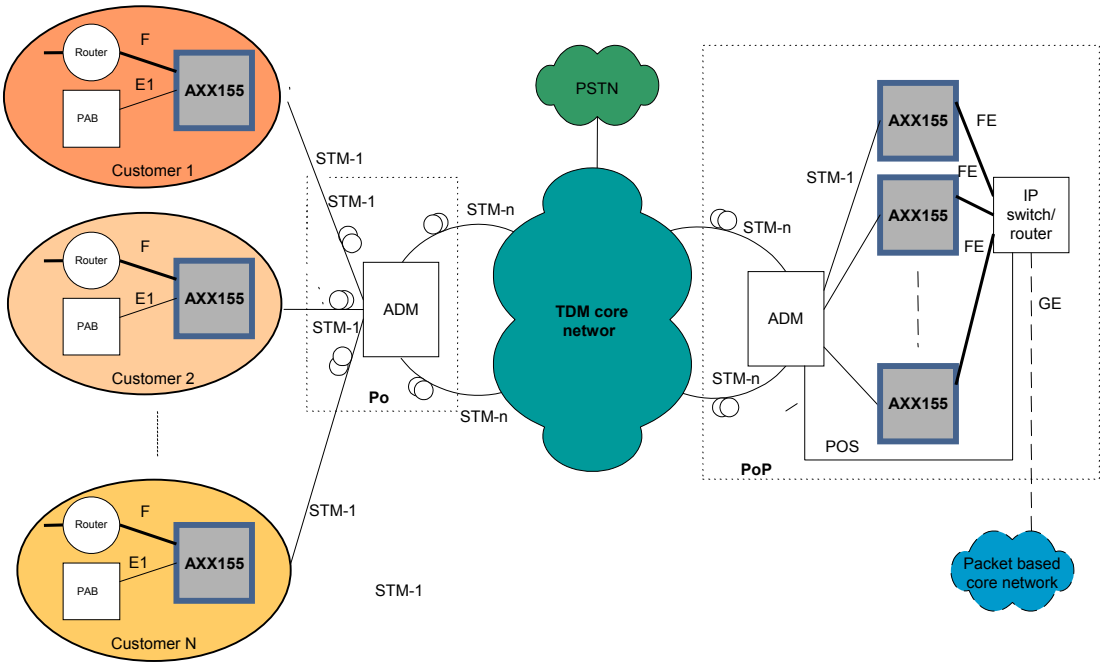


Figure 11. Typical system with no local grooming in the PoP

Point-To-Multipoint application used with AXX155E

The AXX155E product provides Point-To-Multipoint functionality with flexible and individual bandwidth configuration for each customer

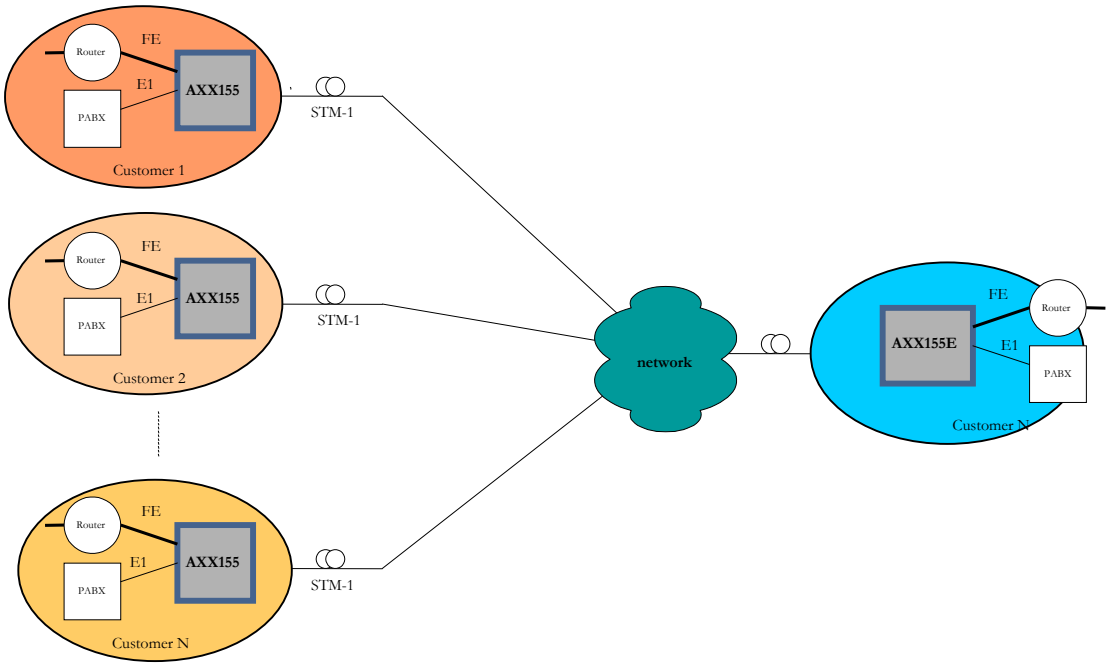


Figure 12. Typical system when connected to an AXX155E

Campus application

The AXX155 R2 can also be connected back to back without any connection to external networks. This is shown in the figure below.

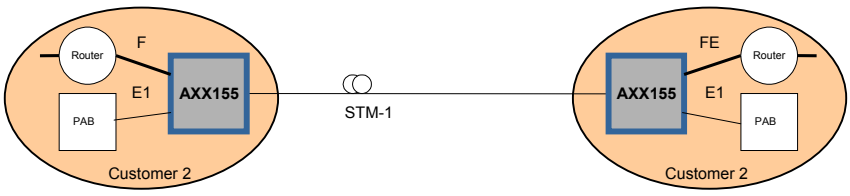


Figure 13. Typical network when used in a campus application

Connection to STM-1 leased line

STM-1 leased lines are typical sold as an electrical interface. The AXX155 R2 with an electrical interface can be directly connected to such an interface as shown in the figure below.

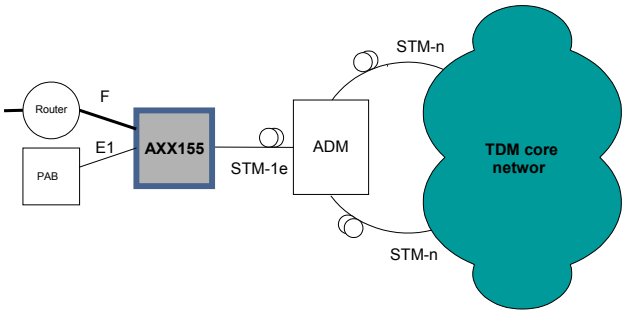


Figure 14. Typical system when connected to an STM-1 leased line

3.5 Management

The following main features are supported by the AXX155 R2 management system:

- Alarm Handling
- Configuration Management
- Performance Monitoring
- Test Support
- Backup/Restore
- Software Download
- Security

The AXX155 R2 management solution is based on an embedded SNMP agent, which can be accessed locally or from a remote management application.

The following standard MIBs are supported:

RFC no.	Title
1213	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
2674	Definitions of Managed Objects for Bridges (previously RFC 1493)
1573	Evolution of the Interfaces Group of MIB-II
1757	Remote Network Monitoring Management Information Base (RMON)
2495	Definitions of Managed Objects for the DS1, E1, DS2 and E2 Interface Types
2558	Definitions of Managed Objects for the SONET/SDH Interface Type
2665	Definitions of Managed Objects for the Ethernet-like Interface Types

Table 6 Standard MIBs

In addition, two enterprise specific MIBs are supported:

- ROS MIB (RADLAN)
- AXX155 R2 MIB (AXXESSIT ASA)

AXX155 R2 is managed by means of the AXXCLI Command Line Interface (CLI) and by means of the AXXMASTER element manager application. AXXCLI is an ASCII based VT-100 terminal interface, while AXXMASTER is a separate application that provides a graphical user interface providing an instant overview of the AXX155 R2**.** AXX155 R2 can be fully managed by means of the AXXCLI interface. Hence, AXXMASTER must be regarded as an optional product, which provides

more powerful and user-friendly element management. See the AXXMASTER User Guide for further info.

Various AXX155 R2 management access solutions

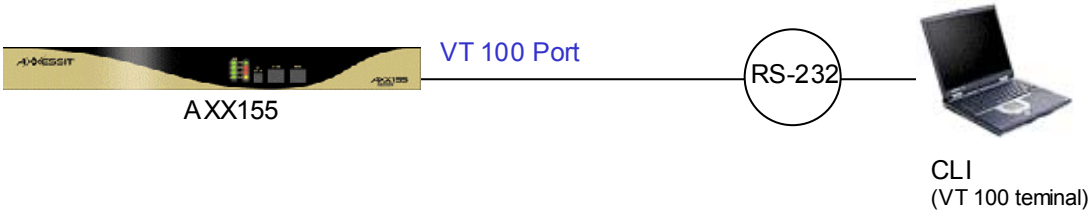


Figure 15. Local management with CLI

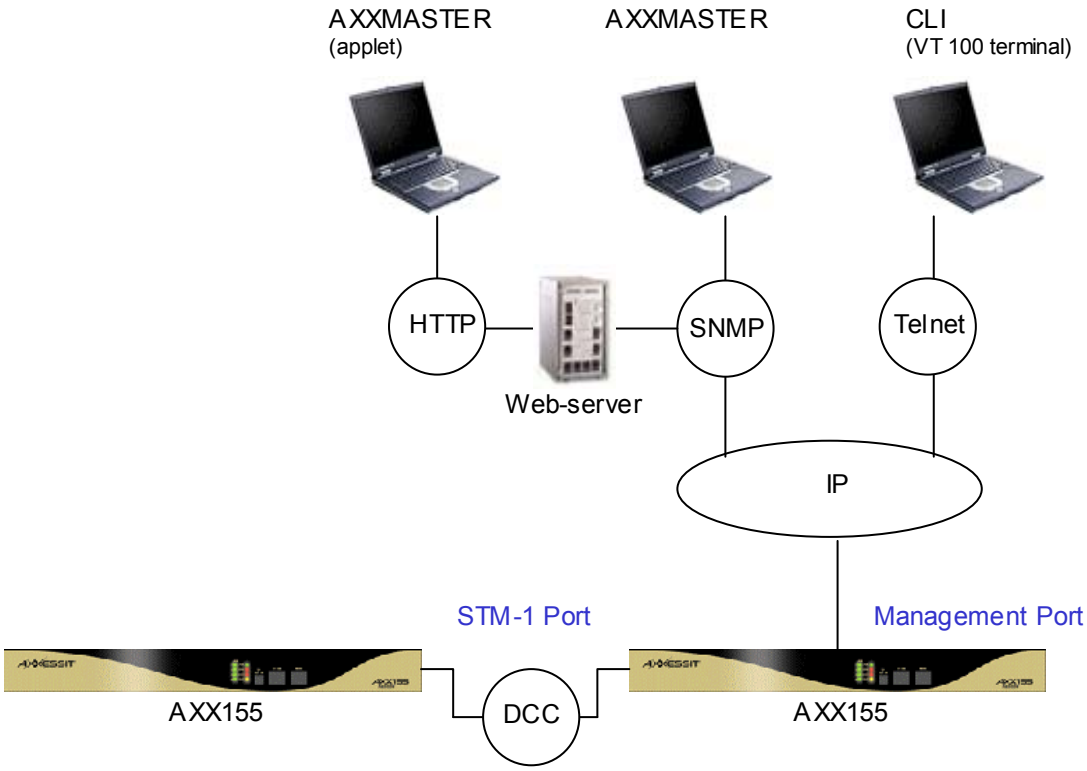
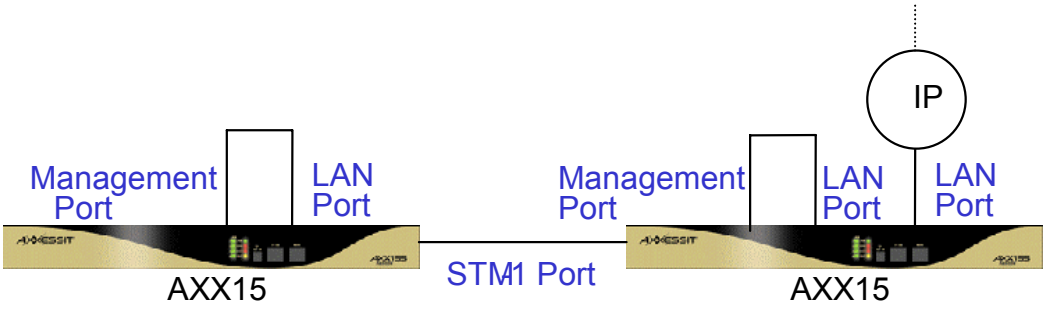


Figure 16. Local and remote management with CLI and



AXXMASTER.

Figure 17. Possible remote management via in-band traffic

(Looping remote LAN Port to Management Port. See Inband via one of the LAN-ports page 44 for restrictions).

Command line interface (CLI)

AXX155 R2 supports a serial RS-232 interface called CLI (Command line interface). CLI is a line-oriented ASCII-based management interface, which provides a simple local connection to any VT-100 compatible terminal. Each command provided by AXXMASTER in Zoom View has a CLI-equivalent, i.e. CLI provides a subset of the same functionality as the AXXMASTER. CLI is protected by a password.

AXX155 R2 also supports the connection of a remote CLI-terminal over Telnet/IP.

AXXMASTER

AXXMASTER is a Java application that can be run standalone on Sun or Microsoft Windows (95/98/NT). It can also be run as plug-in to e.g. HP Open View on either of these platforms. In addition, it can be run as a Web server application enabling user access through Web clients.

AXXMASTER provides a user-friendly Graphical User Interface (GUI), based on two views: The Main View and The Zoom View.

The Main view

The Main View provides management functions that are not related to one particular network element:

- System Configuration

  View and modify network element configuration files, SNMP/TFTP protocol parameters, device names connected to IP addresses etc.

- SNMP Trap Handling

  For each SNMP trap received by AXXMASTER a number of parameters are stored in the Traps Table (trap identifier, timestamp, IP address, event description etc.). The Traps Table is stored in a file. The traps can be read and deleted by the operator. By double clicking one particular trap, a Zoom View for the actual network element will be activated automatically.

The Main View is opened automatically with the AXXMASTER is started, and should remain open to make sure that no traps are lost.

The Zoom view

From the main view, it is possible to connect directly to one network element, i.e. one AXX155 R2**.** This view, called the Zoom View, provides a graphical representation of the current status of the AXX155 R2 device and its ports. Each port may have a user-friendly text field associated with it.

Once the operator has connected to one particular network element, all the facilities described in the AXXMASTER User Guide are available, assuming that the AXXMASTER has the right privileges. From the Zoom View it is possible to go directly to the "mate" AXX155 R2**,** i.e. the AXX155 R2 in the remote end, by means of one button.

Management connectivity

A local Ethernet interface, called the Management Port, is available for connecting to a management DCN. This port is compatible with IEEE 802.3 and supports 10/100BaseT Ethernet for UTP cables.

If an AXX155 R2 has no connectivity to the management DCN via the Management Port, mechanisms for transporting management information in the STM-1 DCC channel are provided.

The AXX155 R2 management system is based on SNMP and an IP-based DCN. However, if an IP-based DCN is not available, AXX155 R2 provides a mechanism for connecting to an OSI-based DCN by tunneling the IP-frames over CLNP.

Ways of connecting to the management DCN

AXX155 R2 can connect to the management DCN in four different ways:

Via the dedicated Ethernet connector, the Management Port, only

This solution assumes that both AXX155 R2 s in a pair have local IP- or OSI connectivity.

Via a proprietary HDLC-based protocol in the STM-1 DCC (DCC-R or DCC-M)

This solution assumes that one of the two AXX155 R2 s in a pair has IP connectivity via the Management Port and that the DCC channel is transparent between the two devices. In this mode, packets received via the Management Port are broadcasted over the DCC HDLC if the MAC address is within the range assigned to AXXESSIT ASA.

Via OSI-based DCN

In this case one of the two AXX155 R2 s is assumed to have OSI connectivity either via the core network (DCC) or via the Management Port. The transport between the two devices is in this case full OSI up to layer 3 (i.e. CLNP/LAPD) with ES-IS and IS-IS support. This variant is not supported in R1.

Inband via one of the LAN-ports

In this case the Management Port must be physically connected to one of the LAN-ports via an external HUB. The management traffic is carried over the Bridge WAN-port. If the AXX155 R2 device is not managed by the customer itself, the LAN-port used for management must belong to a separate VLAN, i.e. only three ports are left for customer access.

Every AXX155 R2 has one and only one IP address allocated to it in R1.

AXX155 R2 also keeps the IP address of its mate AXX155 R2**.** This simplifies the toggling between two AXX155 R2 s in a pair. In addition, the flexibility above implies the actual DCN strategy must be decided and configured per device (parameters like DCC enable/disable, NSAP address, IP/CLNP vs. IP/HDLC etc). This is further outlined in 3.10, page 59. If an OSI solution is used, an OSI/IP gateway is required between the DCN and the AXXMASTER. This gateway will terminate the CLNP tunnels towards a number of AXX155 R2 devices, and speak IP with the AXXMASTER management station. The gateway functionality is either implemented by a centralized PC, or by a number of AXX155 R2 devices.

All AXX155 R2 protocol stack options for implementing the above DCN strategies is illustrated below.

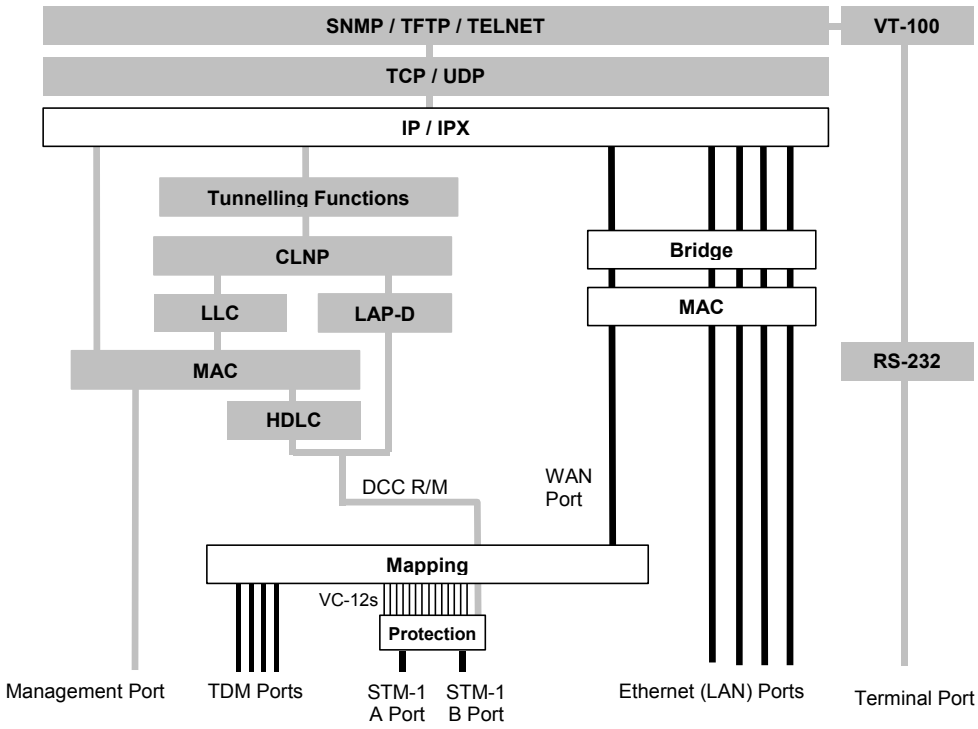


Figure 18. Management protocol stacks

3.6 DCN Features

General

The required DCN protocol support is shown below.

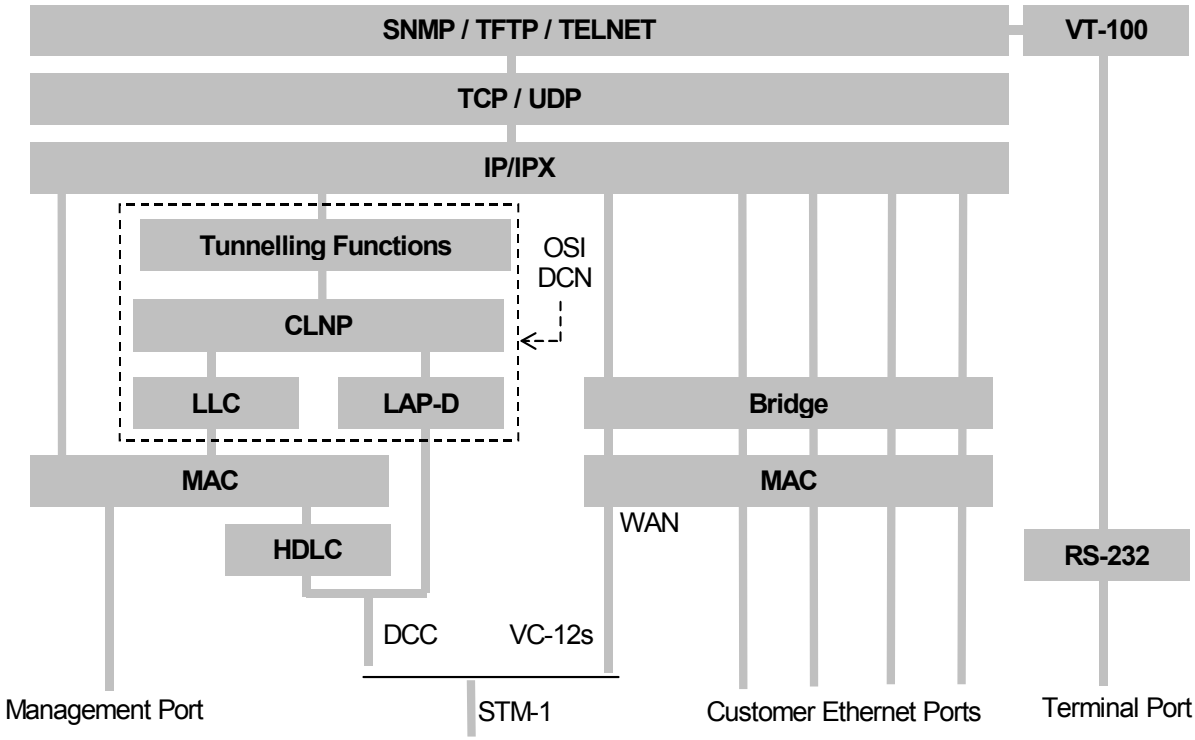


Figure 19. Management Protocol Stacks

The following standards apply:

Abbreviation	Standard
Bridge	IEEE 802.1d - Media Access Control Bridges, 1998 Edition Revision (incorporating IEEE 802.1p). The requirements in chapter 0 apply.
CLNP	CLNP, ES-IS, IS-IS, Static routing ISO 9542 - End System to Intermediate System Protocol (ES-IS) for Use in Conjunction with ISO 8473 ISO 10589 - Intermediate System to Intermediate System Protocol (IS to IS). ISO 8473 - Protocol for Providing the Connectionless-mode Networking Service (CLNS)
MAC / LLC	IEEE 802.x - Information Processing Systems - Local Area Networks
HDLC	ISO 4335 – High-level Data Link Control (HDLC) procedures
IP	RFC 791 - Internetwork Protocol
LAP-D	ITU-T Q.921 ISDN user-network interface -Data link layer specification
RS-232	EIA-232
TCP	RFC 793 - Transmission Control Protocol (TCP)
UDP	RFC 768 - User Datagram Protocol (UDP)

Table 7 Protocol Standards

It is possible to communicate with the management entities of the AXX155 via the customer Ethernet ports.

A local Ethernet port (10BaseT), called the Management Port, is available for connecting to a management DCN.

It is possible for the management traffic between the AXX155 R2 and a management station to be transported transparently through a multi-vendor SDH network. Although the AXX155 R2 management is based on SNMP and the IP protocol family, management communication on the SDH DCC channel is provided by encapsulation of the IP PDUs in the OSI-CLNP protocol (standardised network protocol for the SDH-DCC). The AXX155 R2 also provides functions for manager-side termination of the CLNP tunnel (here called a Gateway[1]).

Note

The Gateway function, i.e. the manager-side termination of the CLNP tunnel, should not be mixed up with the ITU-T G.784 Gateway Network Element (GNE) function which is the gateway between the CLNP network on SDH-DCC and another non-SDH based CLNP network

OSI encapsulation and Gateway functionality constitute a feature in AXX155 R2, called OSI encapsulation feature, which must be activated before it can be used (see section; Feature Management in page 84).

For subnets consisting of AXXESSIT devices only, a proprietary mechanism using HDLC framing of Ethernet packets on the DCC emulating a shared media is provided.

In addition, a VT-100 serial interface provides a local ASCII based terminal interface. The VT-100 functions are also available remotely via TELNET.

The DCN network configurations in section 3.7 , page 49 are supported.

SDH DCC channels

Both DCCR (Regenerator Section) and DCCM (Multiplexer Section) channels are supported independently. Note that both channels should not be active on the same port simultaneously, as this will result in looping of the traffic. Activation/deactivation of DCC channels are configurable on a per port basis.

DCN IP routing

The requirements to handling of the customer traffic (see , page 28) also apply to routing of the DCN traffic. The AXX155 R2 supports IP routing between the CLNP interface, the DCC interfaces and the management port.

CLNP routing

The AXX155 R2 supports ES-IS, IS-IS and static routing. The AXX155 R2 supports OSI routing between the DCC port and the management port.

Tunneling Functions

The tunneling functions provide the necessary functions to support the interworking between an IP-based DCN and an OSI-based DCN. These functions include encapsulation/decapsulation and address mapping functions. In addition, the manager side tunnel termination function (Gateway function) is available on the AXX155 R2.

The Gateway function is also available on a PC platform.

TELNET

TELNET sessions are possible via all paths of management traffic. Multiple TELNET sessions are not possible.

Security

It is possible to restrict management access to the AXX155 R2.

3.7 DCN Configurations supported

The configurations described in page 52 and 53, are applicable only if the routing feature is activated in the AXX155 R2 device.

DCN on management port

This configuration is applicable for users connecting an IP based DCN directly to the AXX155. For this type of connection, the management port is used.

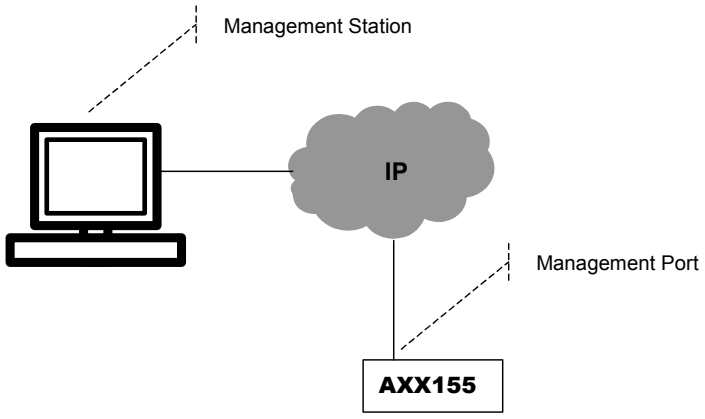


Figure 20. DCN on management port

Broadcasting over Management Port and HDLC- DCC

This configuration is applicable for a user having a subnet of AXX devices and an IP based DCN connected to the management port of the AXX155. AXXLINK is a product of the AXX™ broadband solutions by AXXESSIT offering support for SDH microwave radio.

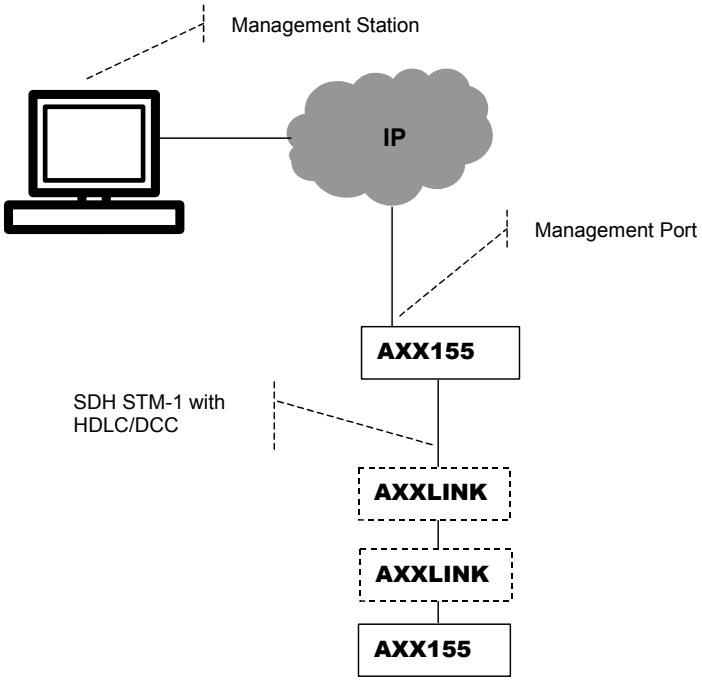


Figure 21. Broadcasting over Management Port and HDLC- DCC

In order not to saturate the DCC with unnecessary traffic, a filtering mechanism for MAC frames can be enabled. If the filter is enabled, MAC frames received via the management port are broadcasted over DCC only if their destination MAC address is within the range assigned to AXXESSIT ASA. If the filter is disabled, all MAC frames (regardless their destination MAC address) received via the management port are broadcasted over DCC.

An AXX155 configured to broadcast management traffic over the management port and DCC (as described above) can be used to provide IP DCN connectivity to a 3rd party network element via its Management Port, provided than the filter mechanism for MAC frames is disabled. A typical configuration is described below.

Note

To prevent indefinitely packet looping and/or packet proliferation, the following restrictions apply to the broadcast solution presented below:

- *Maximum one DCC per link (M- or R-).*
- *The broadcast solution can NOT be used in a (MSP) protection-configuration that involves one (or more) radio hop(s).*

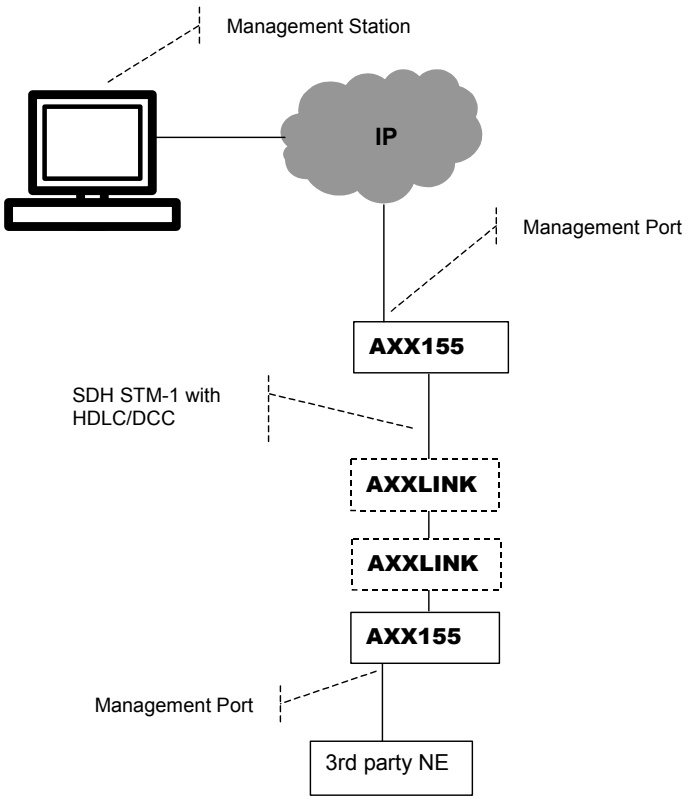


Figure 22. IP DCN connectivity to a 3rd party network element

Routing between Management Port and HDLC- DCC

This configuration is applicable for a user having a subnet of AXX devices and an IP based DCN connected to the management port of the AXX155 R2 (similar to the previous configuration). The difference with the previous configuration is that the management traffic is routed at the IP level between the Management port and the DCC port instead of being broadcasted at the MAC level. This provides the user with additional flexibility in terms of traffic control, but requires extra configuration.

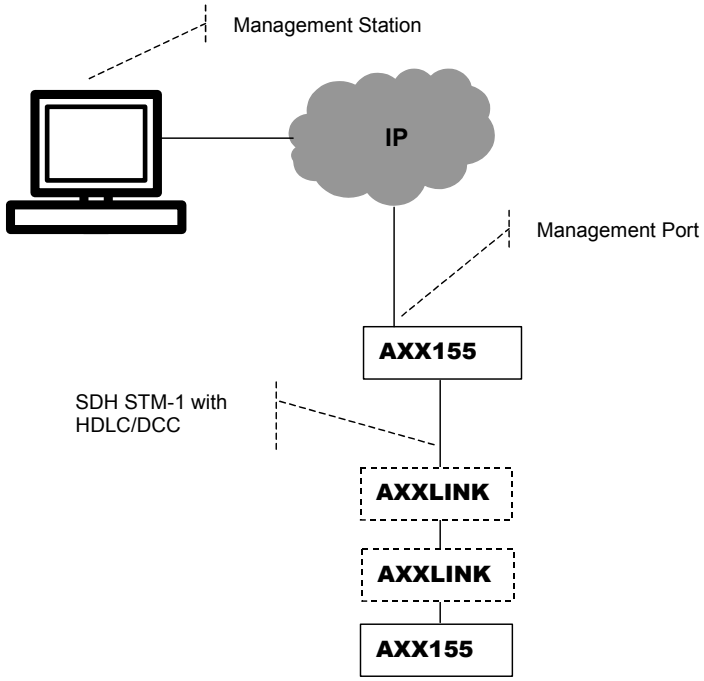


Figure 23. Routing between Management Port and HDLC- DCC

An AXX155 R2 configured to route management traffic between the management port and DCC (as described above) can be used to provide IP DCN connectivity to a 3rd party network element via its Management Port. A typical configuration is described in Figure 24. The only difference with the previous configuration using broadcasting (see Figure 22) is that the AXX155 R2 connected to the 3rd party NE acts as a router and isolates the 3rd party NE from the management traffic targeted to the AXXESSIT devices.

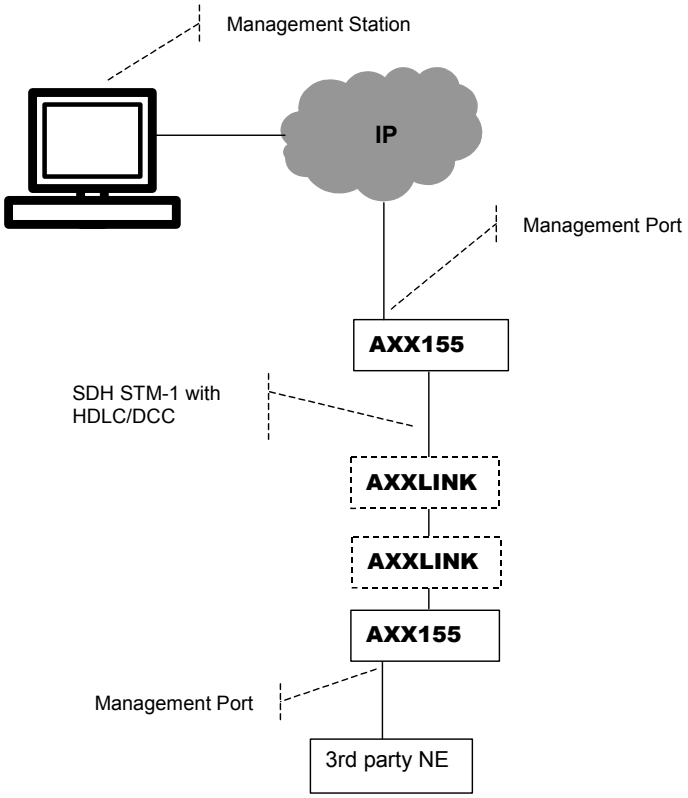


Figure 24. Example of network configuration

The AXXLINKs in Figure 24 above, do not require to be configured to route the management traffic between their DCC ports; they can be configured to broadcast the management traffic as described in section 49.

Tunneling on SDH-DCC (CLNP)

This configuration is applicable when an AXX155 R2 is managed remotely via a SDH network. The configuration is described in Broadcasting over Management Port and HDLC- DCC on page 49.

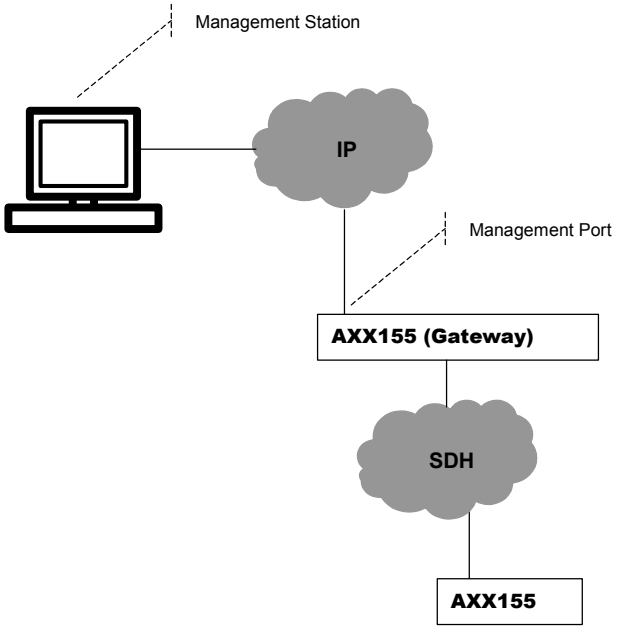


Figure 25. Tunneling on SDH-DCC (CLNP)

ITU-T G.784 Gateway Network Element

The CLNP router of the AXX155 R2 is able to act as a G.784 GNE (Gateway Network Element), i.e. routing between the SDH-DCC network and a CLNP-based LAN (IEEE 802.x LAN protocols). This configuration is applicable whenever a regular GNE function is needed in a SDH network.

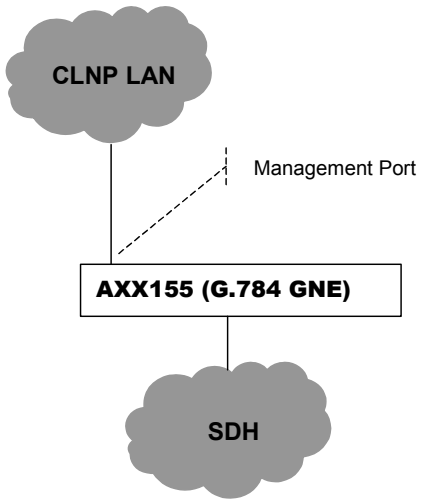


Figure 26. Gateway Network Element

3.8 AXX155 R2 Management

Managed objects

The description of the AXX155 R2 management system refers to manageable objects as listed below:

Object Name	#	Description
Device	1	The AXX155 R2 unit itself
Bridge Port	5	The four LAN Ports plus the WAN Port mapped into the STM-1
Tributary Port	4	The 2048 kHz tributary interfaces
Aggregate Port	1	The optical STM-1 link
Auxiliary Port	4	The general purpose auxiliary interfaces
Bridge	1	Common Bridge functionality, like VLAN and Spanning Tree

Table 8 Managed Objects

Alarm handling

General

The alarms are related to a managed object as defined in Table 8 above. The AXX155 R2 keeps a record of **current** and **historical** alarm events.

The list of **current** alarms contains the following parameters for each alarm:

- Timestamp
- Alarm Object (e.g. Tributary Port 1, Aggregate Port)
- Alarm Identifier
- KLM value if applicable
- Port Affected
- Alarm Description

Port alarms are suppressed if the port itself is disabled. In order to avoid alarm flooding, alarms at different levels are correlated. Lower order alarms are suppressed if a more important alarm at a higher level is active.

In addition to the alarms, the AXX155 R2 may generate a number of events. The events are not stored in the current alarm list, but they are appended to the historical alarm list in the same way as the alarms. The **historical** alarm list contains the same parameters per alarm as the current alarm list, and in addition the following parameter:

- Event Type (RAISED, CLEARED or EVENT)

Both the alarms and the events generate SNMP traps. The traps can be sent to a number of management stations. If they are sent to an AXXMASTER station, they can be viewed in the Main View as described in page 43.

It is possible to turn SNMP trap sending on/off on a per manager basis. This is the only alarm filtering mechanism provided by the AXX155 R2**.**

Alarm definition

The list below contains all the alarms that are defined for the AXX155 R2**.** For some of the Alarm IDs, the direction (RX or TX) is an integral part of the name. This terminology is used for the direction:

- **RX: Downlink (**From Network to Customer)
- **TX: Uplink (**From Customer to Network)

Device	HWFAIL	1	Hardware failure on the device itself
	LOSSY	1	Loss of external synchronisation (Sync Port)
Tributary Port	AISRX	4	Alarm indication signal received from network side.
	LFARX	4	Loss of frame alignment on network side.
	LFATX	4	Loss of frame alignment on customer side.
	LOSTX	4	Loss of signal on the tributary port.
Bridge Port	LOSLA	4	Loss of signal on the LAN ports of the Bridge (see Note 1)
Auxiliary Port	AUX	4	Alarm condition detected on an auxiliary port.
Aggregate Port	AUAIS	1	Alarm indication signal.
	AULOP	1	Loss of pointer on AU level.
	LOF	1	Loss of frame alignment on the STM-1 signal.
	LOM	1	Loss of multiframe alignment on the STM-1 signal.
	LOS	1	Loss of STM-1 signal (only valid for two-fibre operation)
	MSAIS	1	Alarm indication signal received in STM-1 Multiplex Section.
	MSDEG	1	Optical signal error rate exceeds a certain threshold (see Note 3)
	MSRDI	1	Remote defect indication on MS
	RSTIM	1	Trace identifier mismatch.
	TD	1	Transmit degrade on laser.
	TF	1	Transmit fail on laser.
Aggregate Port (VC12)	TUAIS	54	Alarm indication signal received from network for VC12.
	TULOP	54	Loss of pointer on VC12.
	LPDEG	54	VC12 error rate exceeds a certain threshold (see Note 3)
	LPRDI	54	Remote defect indication on VC12.
	LPTIM	54	Trace identifier mismatch on VC12
	LPUNEQ	54	Unequipped
	LPPLM	4	Payload mismatch on VC12 (see Note 2)

Table 9 AXX155 R2 alarms

Note 1

The Bridge Port LOSLA alarm is handled slightly different from the rest of the alarms: If a Bridge Port is unconnected or if it is forced “down” by the operator, it will cause a LOSLA event, which goes into the historical alarm list like other alarms. These alarms will, however, not cause a red LED to be lit, and they will not be stored in the current alarm list like the other alarms.

Note 2

The LPPLM alarm is only supported for the VC12 containers used by the Tributary Ports. It is not supported for the VC12(s) constituting the WAN port.

Note 3

The MSDEG and LPDEG alarms are based on the Near End BER counters over 20 seconds intervals.
The criterions for turning the alarms on and off are as follows:

Alarm	ON	OFF
MSDEG	$> 10^{-7}$	$< 10^{-8}$
LPDEG	$> 10^{-6}$	$< 10^{-7}$

3.9 Managed Objects

This chapter gives an overview of the parameters related to each managed object.

Managed Object	Description
Alarm	Auxiliary alarm input (for voltage-free switches).
AU-4	Administrative Unit level 4
AXX155 R2	AXX155 R2 device
Bridge	Bridging of Ethernet packets including Spanning Tree Protocol.
DCC / DCC-R / DCC-M	SDH Data Communication Channel as defined by ITU-T G.784
Ethernet	Physical (LAN + Mgmt Port) and logical (WAN) Ethernet interfaces
Ethernet/VC12 Mapping	Mapping of Ethernet traffic into a number of SDH VC12s
Feature	SW feature that can be enabled in the software.
Firmware	Firmware on a module.
LAN	Customer Ethernet interface mapped to a physical port.
LED	Customer LED indicator, and Operator LED indicator
Mgmt Port	Ethernet management port.
MS	SDH signal Multiplexer Section
OSI Stack	Forwarding and routing of CLNP traffic including routing protocols.
Port	Generalisation of all logical and physical interfaces.
Protection	SDH protection according to ITU.
RS	SDH signal Regenerator Section
RTC	Real-Time Clock
SDH	Optical or electrical SDH port
SNMP User	Registered SNMP user
Software	Software.
Trib.	PDH port (2Mbit/s).
TU-12	Tributary Unit level 12
Tunnel	Tunnel for encapsulation of IP packets in CLNP. This object covers both encapsulation/decapsulation and address mapping.
User Channel	Transparent serial communication channel.
User Traffic Ethernet	Ethernet interface for user traffic, i.e. LAN + WAN (specialisation the Ethernet managed object).
VC-12	SDH signal VC12 (virtual container)
VC-4	SDH signal VC4 (virtual container)
VLAN	Virtual LANs according to IEEE 802.1q
VT-100 User	Registered user of the VT100 interface
WAN	Ethernet interface not mapped to a physical port.

Table 10 Managed Objects

3.10 Managed Object Attributes

This chapter defines the managed object attributes, and their associated alarms. Note that all alarms are associated with a severity level, i.e. WARNING, MINOR, MAJOR, and CRITICAL. This is not shown in the tables.

Alarm

Attribute	Access	Type	Description
MODE	R/W	choice	ENABLED or DISABLED
TRIGGERED WHEN	R/W	choice	OPENS or CLOSES. Defines whether contact opening or contact closure is the alarm situation.
TRIGGERED	R	string	Indicates if an alarm situation is present on the port (YES or NO).
PERSISTENCY FILTER ALARM ON	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be on to be registered.
PERSISTENCY FILTER ALARM OFF	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be off to be registered.

Table 11 **Alarm attributes**

Alarm ID	Description
AUX	Alarm situation on alarm input port.

Table 12 **Alarm input port alarm**

AU-4

Attribute	Access	Type	Description
AIS FILTER	R/W	choice	ON/OFF filtering of AIS
PERSISTENCY FILTER ALARM ON	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be on to be registered.
PERSISTENCY FILTER ALARM OFF	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be off to be registered.
ALARM REPORTING	R/W	choice	ENABLED or DISABLED. Set the alarm reporting capability for this object. The alarms are listed below

Table 13 **AU-4 attributes**

Alarm ID	Description
AIS	Alarm indication signal
LOP	Loss of pointer

Table 14 **AU-4 alarms**

AXX155 R2

Attribute	Access	Type	Description
DESCRIPTION	R	String	Device type (always AXX155 R2)
NAME	R/W	Sting	User defined device name
LOCATION	R/W	String	User defined address
CONTACT	R/W	String	User defined responsible person(s)
TIME	R/W	hh:mm:ss	Current Device Time
DATE	R/W	dd/mm/yy	Current Device Date
SYSTEM UP-TIME	R	integer	Seconds since last restart
ADMINISTRATIVE SYNC SOURCE	R/W	choice	List of desired SDH synchronisation source in prioritised order. Legal values are EXTERNAL (sync port), LOCAL (free-running), ACTIVE PORT, any SDH port in the system, or any E1 interface configured in PRA mode.
OPERATIONAL SYNC SOURCE	R	string	Actual SDH synchronisation source. For legal values, see ADMINISTRATIVE SYNC SOURCE.
REMOTE DEVICE	R/W	IP address	IP address of the remote AXX155 R2.
ALARM REPORTING	R/W	choice	ENABLED or DISABLED. Set the alarm reporting capability for this object. The alarms are listed below.

Table 15 AXX155 R2attributes

Alarm ID	Description
HWFAIL	Hardware failure
LOSSY	Loss of external synchronisation (Sync port)

Table 16 AXX155 R2 alarms

Bridge

General Bridge Parameters

Attribute	Access	Type	Description
BRIDGE-ADDRESS	R	MAC	The device MAC address
BRIDGE-TYPE	R	text	Bridge Type, always “Transparent only” for AXX155 R2.

Table 17 General bridge attributes

General Spanning Tree Parameters

Attribute	Access	Type	Description
STATUS	R/W	choice	Enabling/disabling of the Spanning Tree Protocol. Legal values are TRUE/FALSE.
PROTOCOL	R	string	Always IEEE 802.1d
STP-TYPE	R	string	Always per Device (per VLAN is not supported).
BELONG-TO-VLAN	R/W	choice	Defines if STP shall be enabled on VLAN ports only or on all ports. Legal values are TRUE (VLAN only) or FALSE (all).
PRIORITY	R/W	integer	Bridge priority in the STP network (low numerical value makes it more likely to become the root) 0-65535
MAX-AGE	R/W	integer	The maximum age (in seconds) of STP-information learned from the network on any port before it is discarded
HELLO-TIME	R/W	integer	Time (in seconds) between transmission of config messages through a given port
FORWARD-DELAY	R/W	integer	As defined in IEEE 802.1d
STP-VERSION	R	integer	STP MIB version
ROOT-PORT	R	integer	Port number offering the lowest cost to the root node.
ROOT-ADDRESS	R	MAC	Current root node MAC address
ROOT-PRIORITY	R	integer	Current root node priority
ROOT-PATH-COST	R	integer	Cost from this bridge to the current root node (0 if this bridge is root)
TIME-SINCE-TOPOLOGY-CHANGE	R	integer	Time (in seconds) since last reconfiguration of STP-topology
TOPOLOGY-CHANGE-COUNT	R	integer	Number of STP reconfigurations since last restart
HOLD-TIME	R	integer	Minimum time (in seconds) between transmission of config messages through a given port (hard coded = 100).

Table 18 General STP attributes

The following attributes exist for each node or interface known to the bridge.

Attribute	Access	Type	Description
PORT	R/W	integer	Port through which the MAC has been learned.
MAC-ADDRESS	R	MAC	MAC address of the node.
VLAN-ID	R/W	integer	VLAN identifier (> 100 000)
STATUS	R	choice	Learned or manually configured addr. Possible values are LEARNED (the entry was automatically learned), SELF (the entry is a port on the device) or MGMT (the entry is a static set by the operator).
COUNT	R	integer	Current table size (per VLAN)

Table 19 STP node/interface attributes

The following attributes exists for each port of the bridge (port specific Spanning Tree Parameters):

Attribute	Access	Type	Description
PRIORITY	RW	integer	Port priority. 0-255
PORT-STATE	R	choice	STP state. Legal values are DISABLED, BLOCKING, LISTENING, LEARNING, FORWARDING.
PORT-ENABLE	R/W	choice	Defines whether the STP is enabled on a port or not. Legal values are ENABLED or DISABLED.
COST	R/W	integer	The cost added to the root path field. Used to determine the cost of the path to the root through this port. 0-65535.
DESIGNATED-ROOT	R	bridge identifier	Designated Bridge transmits a unique Bridge Identifier as the Root in the configuration messages (CMs) with priority and MAC address of the Designated Bridge being included.
DESIGNATED-COST	R	integer	The Designated Port path cost of network segments connected to this port. This value is compared to the Root Path Cost field in received configuration messages (CMs).
DESIGNATED-BRIDGE	R	bridge identifier	The Bridge Identifier, which this port considers to be the Designated Bridge for this port segment, with priority being included.
DESIGNATED-PORT	R	port Identifier	The Port Identifier on the Designated Bridge for this port LAN segment.
FORWARD-TRANSITIONS	R	integer	The number of times this port has transitioned from the Learning state to the Forwarding state.

Table 20 STP port attributes

DCC

There are two DCC objects per SDH port, one for DCC_R and one for DCC_M. Both have the following attributes.

Attribute	Access	Type	Description
ENABLED	R/W	choice	Defines whether this DCC is enabled. Legal values are TRUE/FALSE.
MODE	R/W	choice	Defines the use of the DCC. Legal values are: IP BROADCAST IP ROUTING OSI ENCAPSULATION
LAPD ROLE	R/W	choice	Defines the LAPD role on the DCC. Legal values are: NETWORK USER

Table 21 **DCC attributes**

Ethernet

Attribute	Access	Type	Description
CONNECTOR-TYPE	R	string	RJ45 or LC.
PORT-DESCRIPTOR	R	string	Always Ethernet in AXX155 R2
MAX-CAPACITY	R	string	Highest possible port speed.
MAC-ADDRESS	R	MAC	Port's MAC address
ASSIGN-PHYSICAL-ADDRESS	R/W	choice	Defines if the common bridge MAC address or a dedicated port address assigned by the system shall be used. Legal values are DEFAULT/RESERVE.
ADMINISTRATIVE-STATUS	R/W	choice	Enables/disables the port. Legal values are ON/OFF.
PORT-STATUS	R	string	Actual port status. UP or DOWN.
SPEED-ADMIN-MODE	R/W	choice	Desired port speed. Legal values are 0, 10, 100, and 1000. 0 means port speed not assigned 10 means force speed manually to 10 Mbit/s 100 means force speed manually to 100 Mbit/s 1000 means force speed manually to 1000 Mbit/s
AUTONEGOTIATION-MODE	R/W	choice	Defines whether speed and duplex mode shall be set manually or automatically. Legal values are ENABLE (automatic), DISABLE (manual).
PORT-SPEED	R	string	Current real speed on the port
DUPLEX-ADMIN-MODE	R/W	choice	Desired duplex mode. Legal values are NONE (mode not set), HALF or FULL.
DUPLEX-OPERATION-MODE	R	choice	Actual duplex mode (HALF or FULL).
BACK-PRESSURE-MODE	R/W	choice	ENABLE/DISABLLE
FLOW-CONTROL-MODE	R/W	choice	ON/OFF/AUTO

Table 22 Ethernet port attributes

Ethernet/VC12 Mapping

Attribute	Access	Type	Description
ADMINISTRATIVE-CAPACITY	R/W	integer	Bandwidth allocated by operator (0-100 in steps of 2 Mbps)
OPERATIONAL-CAPACITY	R	integer	Current real bandwidth (0-100)
KLM	R	string	Identification of the allocated SDH VC12 containers. Allocation of VC12s takes place according to the mapping scheme defined in section; SDH multiplexing and mapping, page 23
OPERATIONAL-STATUS	R	choice	Operational status per VC12 (UP or DOWN)
PATH-TRACE	R/W	choice	Enabling/disabling of path trace mechanism (for all allocated VC12s). Legal values are ENABLE/DISABLE.
EXPECTED-TI	R/W	string	Rx VC12 path trace pattern (15 char). Equal for all VC12s.
TRANSMIT-TI	R/W	string	TX VC12 path trace pattern (15 char). Equal for all VC12s.

Table 23 **Ethernet/VC-12 mapping attributes**

Feature

Attribute	Access	Type	Description
ENABLED FEATURES	R	list	List of enabled features on object. At least BRIDGING. Legal values are BRIDGING, ROUTING, OSI ENCAPSULATION.
FEATURE KEY	W	string	Software used to enable specific features.

Table 24 **Feature attributes**

Firmware

Attribute	Access	Type	Description
PRODUCT NUMBER	R	string	Product number
ICS	R	string	Item Change Status (revision)

Table 25 **Firmware attributes**

LED

Attribute	Access	Type	Description
SEVERITY THRESHOLD	R/W	choice	Defines which alarm severity shall turn on the LED. Legal values are: WARNING, MINOR, MAJOR, or CRITICAL.

Table 26 LED attributes

Mgmt Port

Attribute	Access	Type	Description
MODE	R/W	choice	Defines the use of the Management Port. Legal values are: IP MANAGEMENT PORT IP BROADCAST OSI ENCAPSULATION IP AND OSI ENCAPSULATION
MAC FRAME FILTER	R/W	choice	ENABLED or DISABLED. Defines whether the filtering mechanism for MAC frames coming from the Management Port shall be used or not. Valid only for IP BROADCAST mode.

Table 27 Mgmt Port attributes

MS

Attribute	Access	Type	Description
AIS FILTER	R/W	choice	ON/OFF filtering of AIS
RDI FILTER	R/W	choice	ON/OFF filtering of RDI
PERSISTENCY FILTER ALARM ON	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be on to be registered.
PERSISTENCY FILTER ALARM OFF	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be off to be registered.
SIGNAL DEGRADE TRESHOLD	R/W	integer	Threshold for signal degraded alarm, 10E-n where n is the threshold. Legal values are 6, 7, 8 and 9.
BBE	R	integer	Background Block Errors
ES	R	integer	Eroded Seconds
SES	R	integer	Severe Error Seconds
UAS	R	integer	Unavailable Seconds
ALARM REPORTING	R/W	choice	ENABLED or DISABLED. Set the alarm reporting capability for this object. The alarms are listed below.

Table 28 MS attributes

Alarm ID	Description
AIS	Alarm Indication signal.
EXC	Excessive error defect.
DEG	Degraded signal defect.
RDI	Remote Defect indication.
CSF	Communication subsystem failure, DCCM communication failure.

Table 29 MS alarms

OSI Stack

General

Attribute	Access	Type	Description
NSAP	R/W	list	List of up to 3 NSAP addresses for the device.
GATEWAY	R/W	choice	ENABLED or DISABLED. Defines whether the IP/OSI gateway functionality shall be used or not.
GATEWAY NSAP	R/W	NSAP address	Gateway NSAP address.
HELLO INTERVAL	R/W	integer	Frequency of the hello messages the device shall send to the gateway. Valid only if GATEWAY=DISABLED.
NE MAX AGE	R/W	integer	Timeout value for entries in Address Mapper Table (AMT). Valid only if GATEWAY=ENABLED.
AMT TIMER	R/W	integer	Frequency at which the gateway scans the AMT for removing out-dated entries. Valid only if GATEWAY=ENABLED.
IS MODE	R/W	choice	Operating mode of the IS-IS protocol. Legal values are NONE, IS, IS-LEVEL1 or IS-LEVEL2.
ORIGINATING LEVEL 1 BUFFER SIZE	R/W	integer	Maximum size of level 1 Link State PDUs (LSPs) and Sequence Numbers PDUs (SNPs) originated by the system.
ORIGINATING LEVEL 2 BUFFER SIZE	R/W	integer	Maximum size of level 2 Link State PDUs (LSPs) and Sequence Numbers PDUs (SNPs) originated by the system.

Table 30 General OSI stack attributes

OSI circuit attributes.

One record per circuit.

Attribute	Access	Type	Description
LAPD QoS	R/W	choice	AITS or UITS. Defines LAPD QoS mode.
ES-IS	R/W	choice	ENABLED or DISABLED. Defines whether the ES-IS protocol shall be used or not.
ES HOLD TIME	R/W	integer	Length of time (in sec) the system holds the information encapsulated in ES hello PDUs.
IS HOLD TIME	R/W	integer	Length of time (in sec) the system holds the information encapsulated in IS hello PDUs.
ES REPORT TIME	R/W	integer	ES local configuration timer indicating the frequency of ES Hello messages (in sec).
IS REPORT TIME	R/W	integer	IS local configuration timer indicating the frequency of IS Hello messages(in sec).
IS SUGG REPORT TIME	R/W	integer	Value (in sec) sent in IS Hello messages indicating the value that the IS would like the receiving ESs to use as their local configuration timer.
IS-IS	R/W	choice	ENABLED or DISABLED. Defines whether the IS-IS protocol shall be used or not.
L1 METRIC	R/W	integer	Sets the level 1 metric (indication of the cost and efficiency of using this circuit).
L2 METRIC	R/W	integer	Sets the level 2 metric (indication of the cost and efficiency of using this circuit).
MAX CLNP PDU LIFETIME	R/W	integer	Maximum lifetime of a CLNP PDU in seconds.
MAX CLNP REASSEMBLY TIME	R/W	integer	The maximum time (in sec) used by a system to reassemble a segmented message. Must be less than MAX CLNP PDU LIFETIME.
EXTERNAL DOMAIN	R/W	integer	Set to TRUE if the circuit goes outside the domain inhabited by the local system.
ISIS HELLO TIMER	R/W	integer	Sets the Hello Timer (in sec) employed by ISIS in the generation of ISIS Hello PDUs on this circuit.
L1 LAN DIS PRIORITY	R/W	integer	Sets the priority of the system for becoming the level 1 designated intermediate system (DIS). Valid only for a circuit running over the Management Port.
L2 LAN DIS PRIORITY	R/W	integer	Sets the priority of the system for becoming the level 1 designated intermediate system (DIS). Valid only for a circuit running over the Management Port.
DESIGNATED IS IIH TIMER	R/W	integer	Hello timer (in sec) to be used if the device is the LAN designated IS for a circuit. Valid only for a circuit running over the Management Port.

Table 31 OSI stack circuit attributes

Manual ES adjacencies.

One record per adjacency:

Attribute	Access	Type	Description
INTERFACE	R/W	integer	Interface number
NSAP	R/W	string	NSAP address of ES adjacency.
SNPA	R/W	string	Corresponding SNAP address from which the system ID will be found.

Table 32 Manual ES adjacency attributes

Reachable address prefix.

One record per reachable address (valid only for LEVEL 2 IS):

Attribute	Access	Type	Description
INTERFACE	R/W	integer	Interface number
REACHABLE ADDRESS PREFIX	R/W	string	Address prefix of an external routing domain.
SNPA	R/W	string	SNAP address of a system residing in the external routing domain.

Table 33 Reachable address attributes

Port

Common parameters for Ethernet, SDH, tributary, and alarm ports.

Attribute	Access	Type	Description
PORT NUMBER	R	integer	Port number on the module.
DESCRIPTION	R/W	string	User defined name of port

Table 34 Port attributes

Protection

The protection mode supported is 1 + 1 Multiplex Section Protection (MSP).

Attribute	Access	Type	Description
MSP Enabled	R/W	choice	ENABLED or DISABLED
Switching Type	R/W	choice	UNIDRECTIONAL or BIDIRECTIONAL
Operation Type	R/W	choice	REVERTIVE or NON-REVERTIVE
Wait-to-restore time	R/W	integer	Number of minutes to wait before switching back to the preferred link after it has been restored (default = 300 secs).
Preferred Link	R	string	Identifier of the preferred working link (always LINK A for AXX155 R2).
Commands	R/W	choice	CLEAR, LOCKOUT-OF-PROTECTION, FORCED-SWITCHED-TO-PROTECTION, FORCED-SWITCHED-TO-WORKING, MANUAL-SWITCHED-TO-PROTECTION, MANUAL-SWITCHED-TO-WORKING, or EXERCISE
Working Link	R	string	Identifier of the current working link
Local Request	R	integer	Local request contained in K1 byte
Remote Request	R	integer	Remote request contained in K1 byte
PERSISTENCY FILTER ALARM ON	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be on to be registered.
PERSISTENCY FILTER ALARM OFF	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be off to be registered.
ALARM REPORTING	R/W	choice	ENABLED or DISABLED. Set the alarm reporting capability for this object. The alarms are listed below.

Table 35 Protection attributes

Alarm ID	Description
MSP	Problem with MSP signalling with another NE across K1/K2 bytes.

Table 36 Protection alarm

RS

Attribute	Access	Type	Description
PERSISTENCY FILTER ALARM ON	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be on to be registered.
PERSISTENCY FILTER ALARM OFF	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be off to be registered.
SIGNAL DEGRADE TRESHOLD	R/W	integer	Threshold for signal degraded alarm, 10E-n where n is the threshold. Legal values are 6, 7, 8 and 9.
BBE	R	integer	Background Block Errors
ES	R	integer	Eroded Seconds
SES	R	integer	Severe Error Seconds
UAS	R	integer	Unavailable Seconds
RS TRACE	R/W	choice	Enabling/disabling of trace mechanism. Legal values are ENABLE/DISABLE.
RS TRACE RECEIVED	R	string	Actual Received Regenerator Section Trace Identifier, string (15 octets).
RS TRACE EXPECTED	R/W	string	Expected Regenerator Section Trace Identifier, string (15 octets).
RS TRACE TRANSMITTED	R/W	string	Actual Transmitted Regenerator Section Trace Identifier, string (15 octets).
ALARM REPORTING	R/W	choice	ENABLED or DISABLED. Set the alarm reporting capability for this object. The alarms are listed below.

Table 37 RS attributes

Alarm ID	Description
EXC	Excessive error defect.
DEG	Degraded signal defect.
CSF	Communication subsystem failure, DCCR communication failure.
TIM	Trace Identifier mismatch.

Table 38 RS alarms

RTC

Attribute	Access	Type	Description
TIME SERVER IP ADDRESS	R/W	IP address	IP address of a host acting as a server for the Time Protocol (RFC 868)
TIME SYNC INTERVAL	R/W	integer	Frequency at which the date/time on the AXX155 R2 should be synchronised with the date/time on the server. Setting this parameter to 0 means use manual setting time.
TIME ZONE	R/W	integer	Used to adjust the GMT time received from the server to the local time, and to possibly take into account the Day-Light Saving Time.

Table 39 RTC attributes

SDH

Attribute	Access	Type	Description
ADMINISTRATIVE STATUS	R/W	choice	Desired operational status. ENABLED or DISABLED.
OPERATIONAL STATUS	R	string	Actual status on interface. UP or DOWN
RX Level	R	integer	Received optical signal level in dBm (Not applicable with electrical interface).
CONNECTED TO	R/W	list of 100 integers	This attribute is added in order to enable network level management applications to discover the physical network topology. Use of the list entries is user defined and may be variable according to type of network element connected in the other end. Typically the first entry defines which type of NE this port is connected to. The next entries may contain e.g. rack, subrack, IP address, NSAP, module, port.
PERSISTENCY FILTER ALARM ON	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be on to be registered.
PERSISTENCY FILTER ALARM OFF	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be off to be registered.
ALARM REPORTING	R/W	choice	ENABLED or DISABLED. Set the alarm reporting capability for this object. The alarms are listed below.

Table 40 SDH attributes

Alarm ID	Description
LOS	Loss of STM-1 signal
LOF	Loss of frame alignment on the STM-1 signal.
TD	Transmit Degrade on laser (Not applicable with electrical interface).
TF	Transmit fail on laser (Not applicable with electrical interface).

Table 41 SDH alarms

SNMP User

The SNMP User object contains a table of SNMP users. Each entry of the table contains the following parameters.

Attribute	Access	Type	Description
IP ADDRESS	R/W	IP address	IP address of authorised manager
TRAPS ENABLE	R/W	choice	Defines if traps shall be sent to this manager. Legal values are YES and NO.
ACCESS RIGHT	R/W	choice	Defines the access rights of the user. Legal values are SUPER, READ-WRITE and READ-ONLY.
PASSWORD	R/W	string	Password use to access the NE (SNMP community string).

Table 42 SNMP user attributes

Software

Attribute	Access	Type	Description
PRODUCT NUMBER	R	string	Product number
ICS	R	string	Item Change Status (revision)

Table 43 Software attributes

Tributary port

Attribute	Access	Type	Description
ADMINISTRATIVE STATUS	R/W	choice	Defines if port is ENABLED or DISABLED
OPERATIONAL STATUS	R	choice	Actual port status UP or DOWN
PERSISTENCY FILTER ALARM ON	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be on to be registered.
PERSISTENCY FILTER ALARM OFF	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be off to be registered.
TRIBUTARY MODE	R/W	choice	Tributary port mode, TRA (G.703 Transparent mode) or PRA (ISDN Primary Rate Access)
LOOP MODE	R/W	choice	Loop mode, possible values are: NONE, No loop activated on this trib LL2, Local Loop 2 is active LL3, Local Loop 3 is active
PATH TRACE	R/W	choice	Enabled or disabled
RECEIVED TI	R	string	Actual Received Path Trace Identifier, string (15 octets).
EXPECTED TI	R/W	string	Expected Path Trace Identifier, string (15 octets).
TRANSMIT TI	R/W	string	Actual Transmitted Path Trace Identifier, string (15 octets).
ALARM REPORTING	R/W	choice	ENABLED or DISABLED. Set the alarm reporting capability for this object. The alarms are listed below.

Table 44 Tributary port attributes

Alarm ID	Description
LOSTX	Loss of signal
AISRX	Alarm indication signal network side
LFARX	Loss of frame alignment customer side
LFATX	Loss of frame alignment customer side

Table 45 Tributary port alarms

TU-12

Attribute	Access	Type	Description
AIS FILTER	R/W	choice	ON/OFF filtering of AIS
PERSISTENCY FILTER ALARM ON	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be on to be registered.
PERSISTENCY FILTER ALARM OFF	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be off to be registered.
ALARM REPORTING	R/W	choice	ENABLED or DISABLED. Set the alarm reporting capability for this object. The alarms are listed below.

Table 46 TU-12 attributes

Alarm ID	Description
AIS	Alarm indication signal
LOP	Loss of pointer

Table 47 TU-12 alarms

Tunnel

Attribute	Access	Type	Description
OSI MODE	R/W	choice	GATEWAY or NE. Defines whether the AXX155 R2 device is acting as a gateway or a NE.
NSAP ADDRESS	R/W	string	NSAP address of the device. Entered as Area Address, System ID, and NSEL. (NB: Up to 3 area addresses can be defined for one system).
GATEWAY NSAP	R/W	string	NSAP address of the Gateway. Applicable if OSI MODE=NE only. Entered as Area Address, System ID, and NSEL.
HELLO INTERVAL	R/W	integer	Number of seconds between each hello message issued from the NE to the Gateway. Applicable if OSI MODE=NE only.
NE MAX AGE	R/W	integer	Defines how long a NE entry is kept in the Gateway address-mapping table before it is discarded. Applicable if OSI MODE=GATEWAY only.
AMT TIMER	R/W	integer	Address Mapping Table timer. Defines how often the Gateway scans the address-mapping table.

Table 48 Tunnel attributes

User Channel

Attribute	**Access**	**Type**	**Description**
ADMINISTRATIVE STATUS	R/W	choice	Defines if user channel is ENABLED or DISABLED.
AGGREGATE PORT	R/W	choice	Identify the aggregate port used to carry user channel data. Legal values are A, B, or ACTIVE PORT.
DESCRIPTION	R/W	string	User defined name.
MODE	R/W	choice	Speed. Legal values are 64 kbit/s and 19.2 kbit/s

Table 49 User Channel attributes

User Traffic Ethernet

See Ethernet.

VC12

Attribute	Access	Type	Description
AIS FILTER	R/W	choice	ON/OFF filtering of AIS
RDI FILTER	R/W	choice	ON/OFF filtering of RDI
PERSISTENCY FILTER ALARM ON	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be on to be registered.
PERSISTENCY FILTER ALARM OFF	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be off to be registered.
SIGNAL DEGRADE TRESHOLD	R/W	integer	Threshold for signal degraded alarm, 10E-n where n is the threshold. Legal values are 6, 7, 8 and 9.
BBE	R	integer	Background Block Errors
ES	R	integer	Eroded Seconds
SES	R	integer	Severe Error Seconds
UAS	R	integer	Unavailable Seconds
ALARM REPORTING	R/W	choice	ENABLED or DISABLED. Set the alarm reporting capability for this object. The alarms are listed below.

Table 50 VC-12 attributes

Alarm ID	Description
UNEQ	Unequipped
TIM	Trace identifier mismatch
PLM	Payload mismatch
EXC	Excessive error defect.
DEG	Degraded signal defect.
RDI	Remote defect indication

Table 51 VC-12 alarms

VC4

Attribute	Access	Type	Description
RDI FILTER	R/W	choice	ON/OFF filtering of RDI
PERSISTENCY FILTER ALARM ON	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be on to be registered.
PERSISTENCY FILTER ALARM OFF	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be off to be registered.
SIGNAL DEGRADE TRESHOLD	R/W	integer	Threshold for signal degraded alarm, 10E-n where n is the threshold. Legal values are 6, 7, 8 and 9.
BBE	R	integer	Background Block Errors
ES	R	integer	Eroded Seconds
SES	R	integer	Severe Error Seconds
UAS	R	integer	Unavailable Seconds
PATH TRACE	R/W	choice	Enabled or disabled
RECEIVED TI	R	string	Actual Received Path Trace Identifier, string (15 octets).
EXPECTED TI	R/W	string	Expected Path Trace Identifier, string (15 octets).
TRANSMIT TI	R/W	string	Actual Transmitted Path Trace Identifier, string (15 octets).
ALARM REPORTING	R/W	choice	ENABLED or DISABLED. Set the alarm reporting capability for this object. The alarms are listed below.

Table 52 VC-4 attributes

Alarm ID	Description
LOM	Loss of multiframe alignment
UNEQ	Unequipped
TIM	Trace identifier mismatch
PLM	Payload mismatch
EXC	Excessive error defect
DEG	Degraded signal defect
RDI	Remote defect indication

Table 53 Table 1 VC-4 alarms

VLAN

Attribute	Access	Type	Description
NAME	R/W	string	User defined VLAN name.
MAC-ADDRESS	R	MAC	Permanent VLAN MAC address, permanently assigned.
ADDRESS-TYPE	R/W	choice	DEFAULT or RESERVE.
TAG	R/W	integer	VLAN tag for encapsulation of traffic in a remote bridge. Legal values are 0-4000.

Table 54 VLAN attributes

The following attributes exist for each port being member of a VLAN.

Attribute	Access	Type	Description
VLAN PORT NUMBER	R/W	integer	Defines an Ethernet port on the device.
VLAN PORT TYPE	R	choice	
TAGGING	R/W	choice	Defines whether tagging shall be enabled on this port. Legal values are ENABLE/DISABLE.

Table 55 VLAN port attributes

VT100 User

The VT100 User object contains the password for the VT100 port and for TELNET access.

Attribute	Access	Type	Description
VT100 PASSWORD	R/W	string	Password
TELNET PASSWORD	R/W	string	Password

Table 56 VT100 user attributes

WAN

See Ethernet.

3.11 Fault Management

Alarm Definitions

The different alarms together with their relations to the managed objects are defined in the chapter Managed Object Attributes, starting on page 59.

Alarm Parameters

The table below defines the parameters associated with an alarm.

Parameter	Description
Timestamp	Date/Time of alarm event
Alarm Object	Object subject to alarm situation. Should contain both object type (class) and identification (instance).
Alarm Identifier	Short form alarm description, e.g. “LOS”
Alarm Description	Alarm description, e.g. “Loss of signal”
Alarm Severity	According to ITU-T X.733
Event Type	Raised, Cleared or Event. Applicable for alarm log only. Event means alarm with no duration.

Table 57 Alarm Parameters

The Alarm Severity is configurable per alarm object. Default values are assigned automatically.

Alarm Severity

The Alarm Severity is configurable per alarm object. Default values are assigned automatically as shown below

Alarm		Default Alarm Severity
Object-Id	**Alarm-Id**	
AXX155 R2	HWFAIL	critical
	LOSSY	minor
ALARM	AUX	warning
SDH	LOS	critical
	LOF	critical
	TD	minor
	TF	critical
RS	TIM	critical
	CSF	minor
	EXC	major
	DEG	minor
MS	AIS	minor
	CSF	minor
	RDI	minor
	EXC	major
	DEG	minor
MSP	MSP	minor
AU4	LOP	critical
	AIS	minor
VC4	UNEQ	minor
	TIM	critical
	EXC	major
	DEG	minor
	RDI	minor
	PLM	critical
	LOM	critical
TU12	LOP	critical
	AIS	minor
VC12	UNEQ	minor
	TIM	critical
	EXC	major
	DEG	minor
	RDI	minor
	PLM	critical
Tributary	LOSTX	critical
	AISRX	warning
	LFARX	major
	LFATX	major

Table 58 **Default Alarm Severity Table**

Alarm Suppression

Alarms are suppressed if the object subject to alarm is disabled. It is possible to inhibit alarm reporting for a specific managed object. It is possible to inhibit all alarms from one AXX155 R2.All SDH and PDH objects have two configurable persistency filters:

- Persistency filter alarm ON: alarms must have been on for a certain amount of time before being reported.
- Persistency filter alarm OFF: alarms must have been off for a certain amount of time before being cleared.

In addition, the STM-1 interfaces follow the alarm suppression scheme below.

Alarm		Suppress the following alarms
Object-Id	**Alarm-Id**	
SDH	LOS	yes
	LOF	yes
RS	TIM	yes
	CSF	no
	EXC	no
	DEG	no
MS	AIS	yes
	CSF	no
	RDI	no
	EXC	no
	DEG	no
MSP	MSP	no
AU4	LOP	yes
	AIS	yes
VC4	UNEQ	yes
	TIM	yes
	EXC	no
	DEG	no
	RDI	no
	PLM	yes
	LOM	yes
TU12	LOP	yes
	AIS	yes
VC12	UNEQ	yes
	TIM	yes
	EXC	no
	DEG	no
	RDI	no
	PLM	yes
Tributary	AISRX	yes
	LFARX	yes

Table 59 **Alarm Suppression table**

Alarm		Suppress the following alarms
Object-Id	**Alarm-Id**	
Tributary	LOSTX	yes
LFATX	LFATX	yes

Table 60 **Alarm Suppression table for Tributary Tx-Alarms**

Alarm		Suppress the following alarms
Object-Id	**Alarm-Id**	
VC4	EXC	yes
	DEG	no

Table 61 **VC4 Alarm Suppression table for EXC/DEG**

Alarm		Suppress the following alarms
Object-Id	Alarm-Id	
RS	EXC	yes
	DEG	no

Table 62 **Alarm Suppression table for EXC/DEG**

Alarm		Suppress the following alarms
Object-Id	Alarm-Id	
MS	EXC	yes
	DEG	no

Table 63 **MS Alarm Suppression table for EXC/DEG**

Alarm		Suppress the following alarms
Object -Id	Alarm-Id	
VC12	EXC	yes
	DEG	no

Table 64 **VC12 Alarm Suppression table for EXC/DEG**

Alarm Collection

It is possible to view the alarms of all AXX155 R2 devices present in the network, e.g. currently reachable from the management system. The AXX155 R2 device stores a list of all current alarms and a log of alarm events. The size of the log of alarm events is 1000 entries.

Alarm Classification

It is possible for the operator to change the assignment of alarm severity for each pair of Object Type / Alarm ID. The possible severity levels are WARNING, MINOR, MAJOR, and CRITICAL.

Alarm Indication

The Customer LED on indicates that one or more Tributary alarms are on.

The Operator LED on indicates any alarm on, other than AUX-alarms and Tributary-alarms.

It is possible to define an alarm severity threshold for each LED defining which alarm severity shall turn on the corresponding LED.

3.12 Configuration Management

Backup and Restoration of Configuration Data

It is possible to back-up the configuration data of an AXX155 R2 device. It is possible to reload the configuration from the back-up. The back-up media must be a central repository.

Software Download

It is possible to download a new software version to the AXX155 R2 device. The download process does not influence traffic processing. The new software is used when booting after the next restart. The previous

software version is saved in the device. If booting with the new software fails, the AXX155 R2 reboots with the old software, and an alarm is raised.

See also page 91 and 114.

Device Reset

It is possible to reset (reboot) the device with or without resetting the current configuration. Reboot does not affect the TDM traffic.

Device Replacement

It is possible to replace an AXX155 R2 device with a new one with an identical physical configuration.

No manual configuration on the device is required. The AXX155 R2 is assigned one IP address automatically from a BootP server[2]. In addition, the BootP reply contains a reference to a configuration file, and the IP address of the FTP/TFTP server from where this file can be downloaded (see Backup and Restoration of Configuration Data on page 83). Once the configuration has been received, the AXX155 R2 must be rebooted.

Feature Management

The embedded software in the AXX155 R2 is capable of supporting all features (licensed or not licensed) finalised at the time of the release. To activate a specific feature, the device checks whether it has the corresponding licensed right to do it. Licenses are based on a software key bound to the serial number of each AXX155 R2 device, and they are stored internally in each AXX155 R2. The features supported by AXX155 R2 are bridging (always activated), routing, and OSI encapsulation.

Managed Object Attributes

All attributes defined in section 3.9 Managed Objects (page 58) are available for read or read/write access by the management applications specified in page 42.

[2] Automatic IP address assignment presupposes that the BootP database has been updated with the mapping between the IP address and the hardware address of the new AXX155 device.

3.13 Performance monitoring

The performance monitoring functions specified under Aggregate port below and Bridge port, page 87 are available in both AXXMASTER and AXXCLI. The section " AXXMASTER services "in page 89, specifies additional functions available by AXXMASTER only.

Aggregate port

The table below defines the mapping between the dialogue parameters and MIB variables for the Aggr Port Statistics submenu.

Parameter	MIB variable(s)	Comment
Aggregate Port		Choice between A or B
Path/Section		Choice between RS, MS, VC4, or VC12
VC12 (KLM)	axx155TribPortMapPort ifStackLowerLayer (rfc1573) axx155SdhVc12MoTable axx155WanVc12Klm	Only valid if Path/Section choice is VC12. ifIndex of tributary. ifIndex of VC12 connected to tributary. K.L.M value of VC12 connected to tributary. K.L.M value of VC12s connected to WAN.
Date/Time	rndManagedTime (RADLAN) rndManagedDate (RADLAN)	
Current Interval Time Elapsed	sonetMediumTimeElapsed (rfc2558)	
Current ES	sonetSectionCurrentESs (rfc2558) sonetLineCurrentESs (rfc2558) sonetPathCurrentESs (rfc2558) sonetVTCurrentESs (rfc2558)	Regenerator Section. Multiplex Section. VC4. VC12.
Current Far End ES	sonetFarEndLineCurrentESs (rfc2558) sonetFarEndPathCurrentESs (rfc2558) sonetFarEndVTCurrentESs (rfc2558)	Multiplex Section. VC4. VC12.
Current SES	sonetSectionCurrentSESs (rfc2558) sonetLineCurrentSESs (rfc2558) sonetPathCurrentSESs (rfc2558) sonetVTCurrentSESs (rfc2558)	Regenerator Section. Multiplex Section. VC4. VC12.
Current Far End SES	sonetFarEndLineCurrentSESs (rfc2558) sonetFarEndPathCurrentSESs (rfc2558) sonetFarEndVTCurrentSESs (rfc2558)	Multiplex Section. VC4. VC12.

Current BBE	sonetSectionCurrentBBEs sonetLineCurrentBBEs sonetPathCurrentBBEs sonetVTCurrentBBEs	Regenerator Section. Multiplex Section. VC4. VC12.
Current Far End BBE	sonetFarEndLineCurrentBBEs sonetFarEndPathCurrentBBEs sonetFarEndVTCurrentBBEs	Multiplex Section. VC4. VC12.
Current UAS	sonetSectionCurrentUASs sonetLineCurrentUASs (rfc2558) sonetPathCurrentUASs (rfc2558) sonetVTCurrentUASs (rfc2558)	Regenerator Section. Multiplex Section. VC4. VC12.
Current Far End UAS	sonetFarEndLineCurrentUASs (rfc2558) sonetFarEndPathCurrentUASs (rfc2558) sonetFarEndVTCurrentUASs (rfc2558)	Multiplex Section. VC4. VC12.
Index	sonetLineIntervalNumber (rfc2558) sonetPathIntervalNumber (rfc2558) sonetVTIntervalNumber (rfc2558)	Multiplex Section. VC4. VC12.
Timestamp	rndManagedTime (RADLAN) rndManagedDate (RADLAN) sonetMediumTimeElapsed (rfc2558) sonetLIneIntervalNumber (rfc2558) sonetPathIntervalNumber ((rfc2558) sonetVTIntervalNumber ((rfc2558)	Timestamp must be calculated from these values and index. Multiplex Section. VC4. VC12.
ES	sonetSectionIntervalESs (rfc2558) sonetLineIntervalESs (rfc2558) sonetPathIntervalESs (rfc2558) sonetVTIntervalESs (rfc2558)	Regenerator Section. Multiplex Section. VC4. VC12.
Far End ES	sonetFarEndLineIntervalESs (rfc2558) sonetFarEndPathIntervalESs (rfc2558) sonetFarEndVTIntervalESs (rfc2558)	Multiplex Section. VC4. VC12.
SES	sonetSectionIntervalSESs (rfc2558) sonetLineIntervalSESs (rfc2558) sonetPathIntervalSESs (rfc2558) sonetVTIntervalSESs (rfc2558)	Regenerator Section. Multiplex Section. VC4. VC12.
Far End SES	sonetFarEndLineIntervalSESs (rfc2558) sonetFarEndPathIntervalSESs (rfc2558) sonetFarEndVTIntervalSESs (rfc2558)	Multiplex Section. VC4. VC12.
BBE	sonetSectionIntervalBBEs sonetLineIntervalBBEs sonetPathIntervalBBEs sonetVTIntervalBBEs	Regenerator Section. Multiplex Section. VC4. VC12.
Far End BBE	sonetFarEndLineIntervalBBEs sonetFarEndPathIntervalBBEs sonetFarEndVTIntervalBBEs	Multiplex Section. VC4. VC12.

UAS	sonetSectionIntervalUASs sonetLineIntervalUASs (rfc2558) sonetPathIntervalUASs (rfc2558) sonetVTIntervalUASs (rfc2558)	Regenerator Section. Multiplex Section. VC4. VC12.
Far End UAS	sonetFarEndLineIntervalUASs (rfc2558) sonetFarEndPathIntervalUASs (rfc2558) sonetFarEndVTIntervalUASs (rfc2558)	Multiplex Section. VC4. VC12.

Table 65 Aggr Port Statistics parameter mappings

Bridge port

Performance counters for the Bridge ports (including the WAN port) are available for the manager via the following variables in the RMON MIB:

- etherStatsDropEvents
- etherStatsOctets
- etherStatsPkts
- etherStatsBroadcastPkts
- etherStatsMulticastPkts
- etherStatsCRCAlignErrors
- etherStatsUndersizePkts
- etherStatsOversizePkts
- etherStatsFragments
- etherStatsJabbers
- etherStatsCollisions
- etherStatsPkts64Octets
- etherStatsPkts65to127Octets
- etherStatsPkts128to255Octets
- etherStatsPkts256to511Octets
- etherStatsPkts512to1023Octets
- etherStatsPkts1024to1518Octets

As opposed to the Aggregate port counters, the Bridge port counters must be started and stopped by the operator.

AXX155 R2 keeps no history records for the Bridge port counters. In AXXMASTER this is partly compensated by means of the element statistics feature described in “Graphs “in page 89.

AXXMASTER services

In addition to the port specific counters specified in the previous sections Aggregate port and Bridge port, which are also supported by AXXCLI, AXXMASTER provides some special services related to performance. These services are described in this section.

Device counters

AXX155 R2 provides counters for the IP-traffic terminating in the device itself via the Management Port and/or the DCC channel (MIB-II counters, IP counters, SNMP counters etc.). These counters, called Optional Counters, are not available for the AXXCLI operator, but they can be monitored from AXXMASTER.

Thresholds

All counters, except the Aggregate Port performance counters, may have a rising and falling threshold assigned to it in AXXMASTER. The alarm criterions assigned to such counters are defined in the **Statistics Alarm Table**. When the threshold is crossed, an alarm event (raised/cleared) is generated. For each such alarm, it may also be defined whether the alarm should be logged in the **Log Table** or if it should be sent as an SNMP Trap.

The AXXMASTER feature described in this section, implements an additional alarm facility on top of the Alarm Handling facilities described in section Bridge port in page 87. An overview of all logs related to alarms and errors is provided in the section describing Management logs in page 93.

Graphs

AXXMASTER provides an element statistics feature based on periodic polling of the Bridge and Device performance counters. The user defines the polling interval. The counter reading in each interval is visualised by means graphs.

Ping

An IP ping service is provided by AXXMASTER. With this service ping series with different parameters to a number of different devices can be started. The result of each sequence is displayed in the Ping Table.

3.14 Back-up and restore

It is possible to up/download the AXX155 R2 configuration to/from a TFTP server, that is :

- to save the AXX155 R2 configuration in a file onto an TFTP server,
- to download a configuration file from a TFTP server onto the AXX155 R2 .

The operator determines the file names. It is possible to modify the configuration file off-line.

The following read-write parameters shall be available to control the backup/restore facility:

Parameters	Description
File Name	Device Configuration File to be backed-up/restore
TFTP Server IP Address	IP address of TFTP server where the SW file is located.

Table 66 Backup/restore Parameters

Note

The backup/restore facility is supported by AXXMASTER only.

3.15 Software download

Local

It is possible to load a new software version by means of a PC directly attached to the CLI Port. This service requires local operator presence at the AXX155 R2 .

The file is loaded by means of the X-Modem protocol, and the transfer is at 115.200 kbit/s.

Booting the system triggers local software download. Hence, the traffic is lost during the loading.

Remote

It is possible to download new AXX155 R2 software from a remote server (i.e. AXXMASTER via Management Port) by means of the TFTP protocol. In R1 this service can be activated by AXXMASTER only.

The AXX155 R2 supports two banks, one for the active (current) file and one for the new file. The AXX155 R2 traffic is not being affected.

At the end of the remote software download, AXXMASTER will automatically invoke a restart. AXX155 R2 detects whether the FPGA files (that is; HW) has changed. If there are no FPGA changes, the restart does not affect the traffic. Otherwise the system will be down for some seconds.

Remote software download is controlled by one single read-write parameter:

Parameters	Description
File Name	Software File to be downloaded

Table 67 SW download parameters

3.16 Security

The management access to the AXX155 R2 is controlled by parameters in a "Community Table". This table can only be modified by users with SUPER access rights. The parameters in the Community table are only visible for SUPER users.

For each defined user, the following parameters must be provided:

- IP address
- Community string
- Access Right (READ-ONLY, READ-WRITE, SUPER)
- Traps (Enable/Disable)

One management station (i.e. IP address) may have several users with different access rights. These users are identified by means of the community string.

The CLI access is controlled by means of a password, one for the local access and one for the Telnet access. A management station SUPER user can modify the CLI password.

The CLI user has SUPER access rights.

3.17 Management logs

This sub-section summarises the various logs used for alarms, errors and statistics. As visualised in figure the figure “Management logs”, all logs except the Trap Log are located inside the AXX155 R2 .

In addition to the logs described below, the system provides logs for troubleshooting, containing detailed debug information. These logs are not available for normal users, and they are not specified in this document.

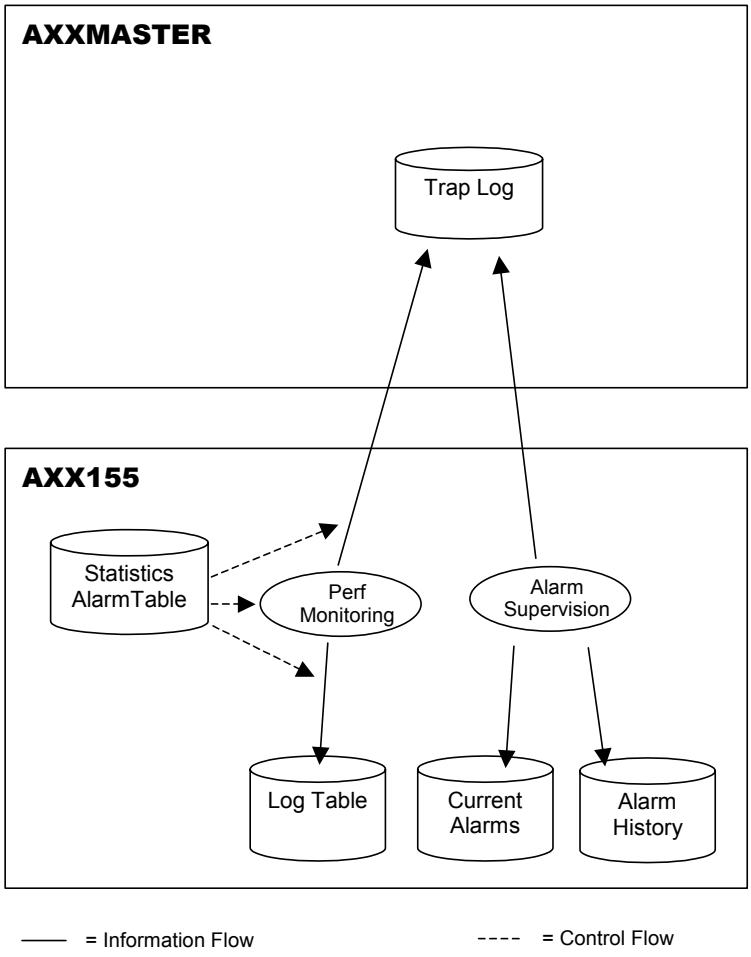


Figure 27. Management logs

Name	Location	Description
Trap Log	AXXMASTER	Contains all events reported by the AXX155 R2 , including the alarm and performance traps.
Statistics Alarm Table	AXX155 R2	Controls the monitoring of bridge and LAN port performance. It contains definition of threshold alarms and also decides if performance alarms shall be logged locally in Log Table, or sent as trap to the manager or both. This table corresponds to the RMON alarm Table.
Log Table	AXX155 R2	This table contains the logged performance alarms controlled by the Statistics Alarm Table. This table corresponds to the RMON log Table.
Current Alarms	AXX155 R2	This table contains all alarms currently on.
Alarm History	AXX155 R2	This table contains a log of all events, including alarm events. The latest 1000 events are stored.

Table 68 Management logs

3.18 Physical description

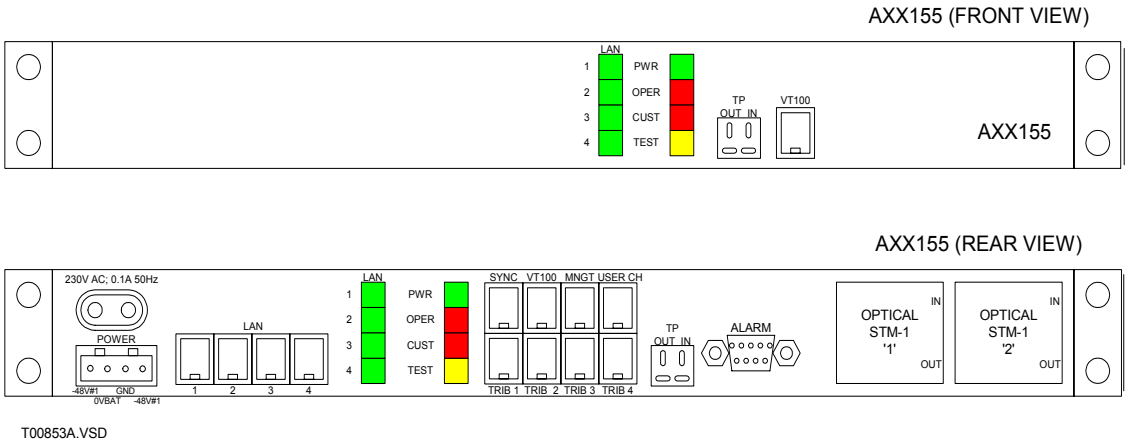


Figure 28. AXX155 R2 front and rear view

Form of construction

The equipment is provided as a sub-rack suitable for mounting within a 19-inch equipment cabinet. The height of the unit 1U (44.45 mm).

The AXX155 R2 dimensions are:

Height: 43 mm

Width: 430 mm

Depth: 240 mm

The weight of the unit is 4 kg.

The thermal design of the unit meets the requirements of EN 60950.

This chapter describes the different types of physical interfaces in AXX155 R2 .

The table below gives the relationship between the type of interface and the logical names used in this document.

Interface	No. of interfaces	Logical name
Optical/Electrical	2	Aggregate Port
Tributary	4	Tributary Port
Ethernet	5	LAN Ports and Management Port
Alarm	6	4 alarm input and 2 alarm out
Synchronisation	1	Sync Port
Monitor point	2	Monitor Port
RS232	1	CLI Port
Power supply	2	230 V AC & -48 V DC
Indicators	8	4 Traffic Indicators, Power Indicator, Operator Indicator, Customer Indicator, Test Indicator

Table 69 AXX155 R2 interfaces

Note

The aggregate ports are both optical or both electrical.

AXX155 R2 light emitting diodes (LEDs)

		State		
Identity	**Colour**	**On**	**Flashing**	**Off**
POWER	Green	Presence of power	Not applicable	Power failure
OPERATION	Red	Alarm detected on aggregate interface	Not Applicable	No alarm detected on aggregate interface
CUSTOMER	Red	Alarm detected on tributary or LAN interface	Not applicable	No alarm detected on tributary or LAN interface
TEST	Yellow		One or more tests are activated.	
LANn (n=1,2,3,4)	Green	Ethernet traffic in operation	Not applicable	No Ethernet traffic in operation

Table 70 AXX155 R2 LEDs

Optical

For AXX155 R2 the transmission over the optical interface is bi-directional on one fibre or uni-directional on two fibres. The wavelength used is the same in both directions of transmission. The two-fibre interface is a standard S-1.1 interface. The single fibre interface is a proprietary interface with respect to optical parameters.

The second optical interface is used for protection purposes (see page 71, Protection.

Electrical and optical connections

A separate power plug is delivered with the AXX155 R2 for this use.

Connect the 48V battery wires to the plug and connect it to the AXX155 R2 Power Socket, see figure below.

The 230 V mains supply input on the AXX155 R2 is provided via a standard connector according to EN60320.

The –48V DC supply input on the AXX155 R2 is provided via a 4 pin power connector.

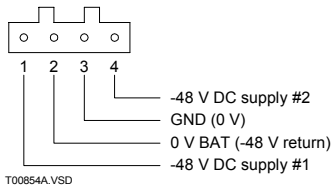


Figure 29. Power socket

GND

Connection of the AXX155 R2 to protective earth is recommended if the various tributary equipment may have different earth potentials.

Optical F1 interface

The receptacle(s), for termination of the optical fibre cords, are accessed on the right at the rear panel, see figure " AXX155 R2 front and rear view " in page 95 . The optical F1 interface has FC/PC receptacles. Other types on request.

The receptacles can then be of the following types:

- FC/PC (default)
- SC/PC
- E-2000

Alarm interfaces

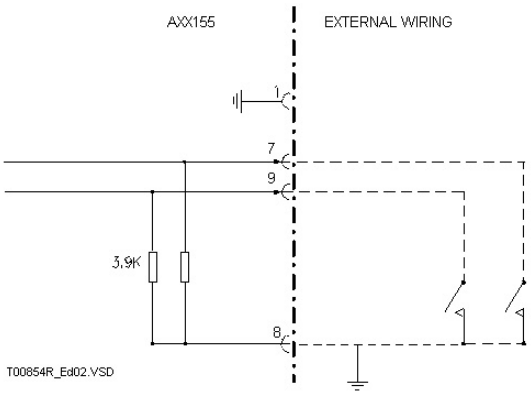


Figure 30. AXX155 R2 alarm in-/out-puts

Alarm status can be read via CLI or AXXMASTER.

Pin	Signal
1	Gnd
2	Alarm input 1 (aux 1)
3	Alarm input 2 (aux 2)
4	Alarm input 3 (aux 3)
5	Alarm input 4 (aux 4)
6	Alarm input return
7	Alarm output 1
8	Alarm output return
9	Alarm output 2

Table 2 Pin-out alarm interface

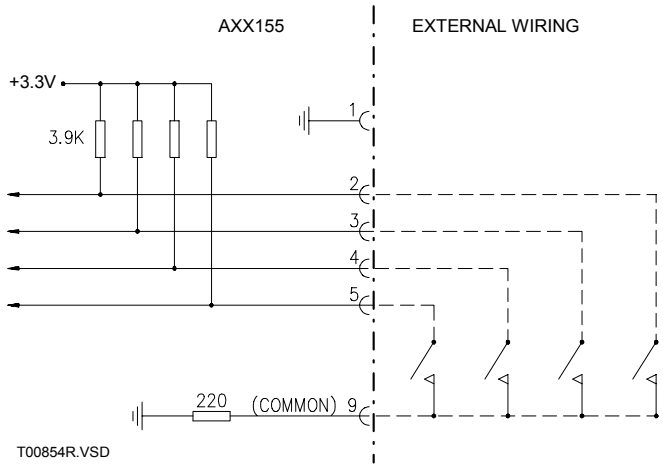


Figure 31. Auxiliary alarm inputs

Activated alarm: Selectable, closed or open contact. If used, the Alarm Inputs shall be connected in parallel to the alarm source.

LAN interface

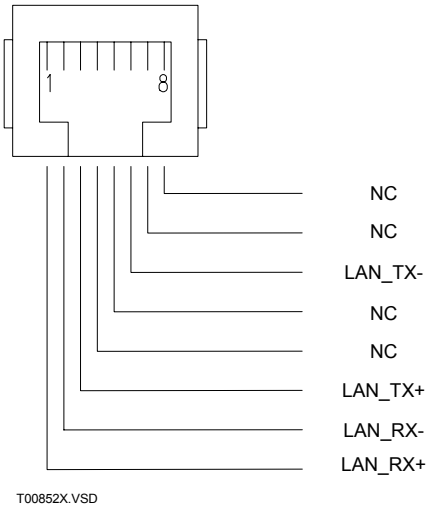


Figure 32. LAN interface connector

Pin	Signal
1	TxD+
2	TxD--
3	RxD+
4	NC
5	NC
6	RxD--
7	NC
8	NC

Tributary interfaces

This is an ISDN PRA connector with pin-out according to ISO/IEC 10173.

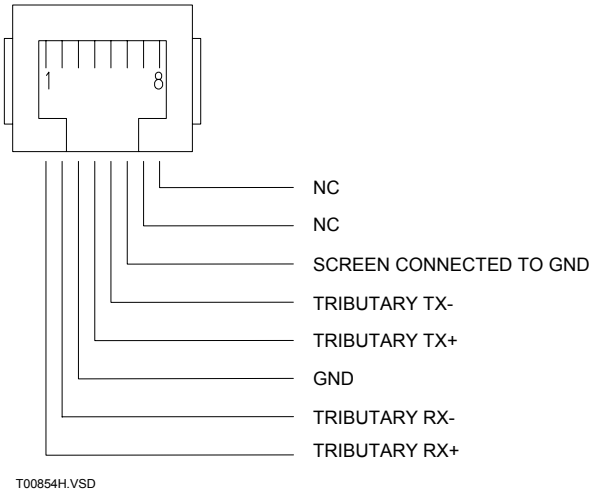


Figure 33. Tributary 120 Ω interface connector.

Synchronisation

AXX155 R2 has one 2048 kHz synchronisation output port and input. Both input and output is provided on 8 pin RJ-45 connector, with the following pin-out:

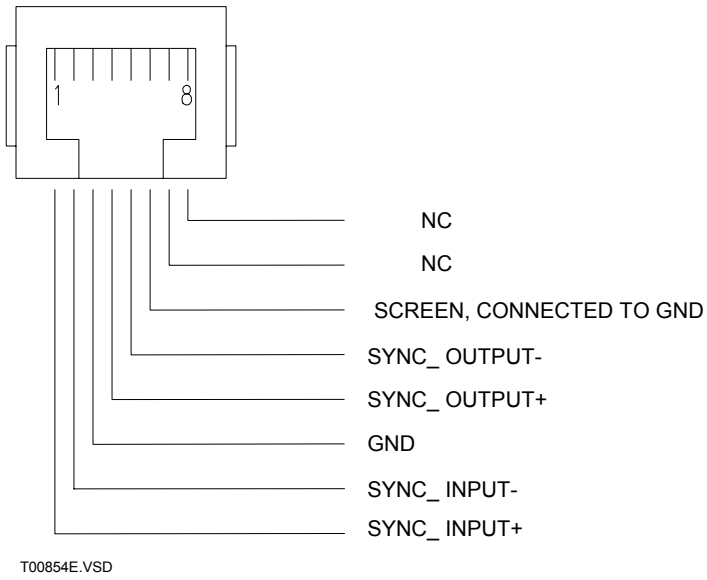


Figure 34. Synchronisation input/output connector

Monitor point

The monitor point interface for AXX155 R2 is provided using a DIN41616 connector, with the following pin-out:

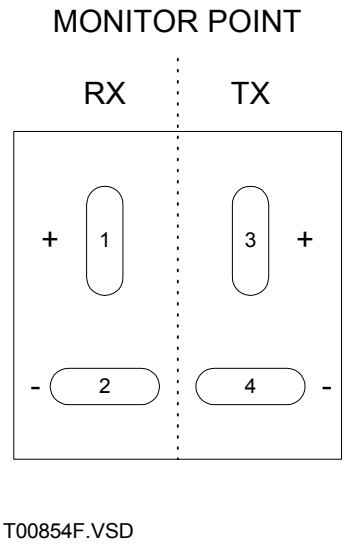


Figure 35. Monitor point connector

CLI port

The CLI Port is accessible from both the front and rear side of the unit by means of two parallel connectors.

The RS232 interface for AXX155 R2 is provided using a RJ-45 connector, with the following pin-out:

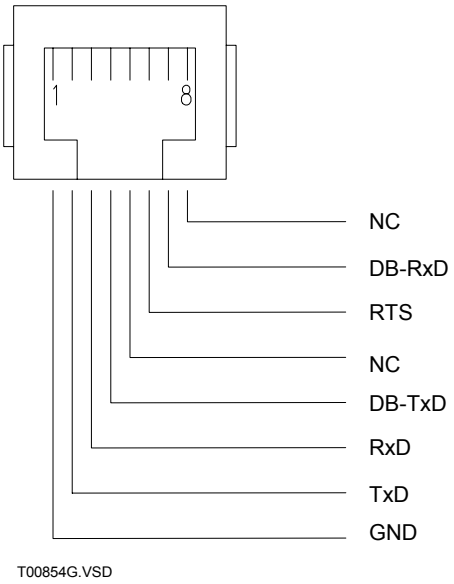


Figure 36. CLI port connector

NOTE

Pin 4 and 7 are only used for debug purposes.

Balun 120 -> 75 Ω

An additional balun has to be used to provide access for TDM tributaries with 75 Ω interfaces. The AXXESSIT ASA balun is recommended since it is carefully designed with the following capabilities:

- Fully shielded
- For EMC reasons, the incoming 2 Mbit/s cable screen is separated from GND, and is AC-grounded inside the AXX155 R2 .

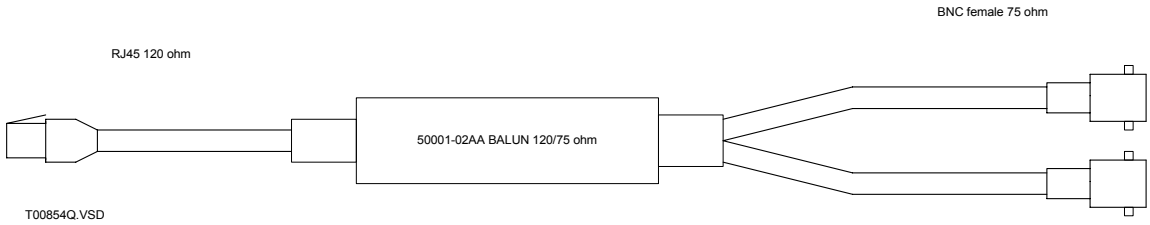


Figure 37. 120/75 ohm balun

User Channel

A user channel is provided for transportation of general data. The port is balanced V.11 and support synchronous 64kbit/s or asynchronous 19.2kbit/s by configuration.

Connector

The user channel interface for AXX155 is provided using a RJ-45 connector, with the following pin-out:

Pin	Signal
1	TxD+
2	TxD-
3	RxD+
4	TxCLK-
5	TxCLK+
6	RxD-
7	RxCLK+
8	RxCLK-

Table 71 Pin-out user channel connector

Compliance

Standard	Comment
ITU-T V.11	

Table 72 User channel interface conformance

AXX155 R2 equipment list

Name	**Brief Description**	AXXESSIT ASA **code no.**
AXX155 R2 2-fibre unprotected	Integrated Access Device, combining IP- and TDM-traffic, for use in the fibre optic networks 2 fibre operation, 1310 nm.	50001-01AA
AXX155 R2 2-fibre, line protected	Integrated Access Device, combining IP- and TDM-traffic, for use in the fibre optic networks Protected 2-fibre operation, 1310 nm.	50001-01CA
AXX155 R2 2-fibre long haul unprotected	Integrated Access Device, combining IP- and TDM-traffic, for use in the fibre optic networks 2 fibre operation, 1310 nm. Long haul. Optical connector FC/PC.	50001-01EA
AXX155 R2 2-fibre long haul protected	Integrated Access Device, combining IP- and TDM-traffic, for use in the fibre optic networks Protected 2-fibre operation, 1310 nm. Long haul. Optical connector FC/PC.	50001-01HA
AXX155 R2 Different connector options	Other optical connector possible as E2000, SC and LC	Not applicable
AXX155 R2 1-fibre unprotected	Integrated Access Device, combining IP- and TDM-traffic, for use in the fibre optic networks Bi-directional 1 fibre operation, 1310 nm.	50001-01BA
AXX155 R2 1-fibre, line protected	Integrated Access Device, combining IP- and TDM-traffic, for use in the fibre optic networks Protected bi-directional 1-fibre operation, 1310 nm.	50001-01DA
Balun	120 – 75 Ω adapter	50001 – 02AA
Rack mount kit 19”	Brackets for mounting of AXX155 R2 in a 19” rack.	50001 – 04AA
Rack mount kit ETSI	Brackets for mounting of AXX155 R2 in a ETSI rack.	50001 – 04AB
AXX155 R2 User Guide	User Guide. Covering installation and operation of the AXX155 R2 equipment	61001 – 05BA
AXXMASTER User Guide	User Guide. Covering operation and management via AXXMASTER SW	50001 – 10AA

Table 73 List of AXX155 R2 related equipment

Chapter

4

4 Installation

Safety recommendations

Site requirements

Unpacking the AXX155 R2

Rack mounting

Cabling

Basic software configuration

4.1 Safety recommendations

SAFETY RULES

The whole installation must be executed without powering the equipment.

Power Supply connection must be the last to be executed.

SAFETY RULES

Due to possible very high currents in case of short-circuit at the battery power input, it is essential that the battery power distribution line shall be provided with a short circuit back-up protection with adequate breaking capacity.

4.2 Site requirements

In-door, temperature controlled environment is required.

4.3 Unpacking the AXX155 R2

General

The following procedures have been issued and must be observed when unpacking the equipment. The reciprocal operation must be done for repacking. In such case it is recommended to use the original packing material.

The following sturdy outer packing material is utilized in order to protect the equipment against mechanical and climatic stresses to which they are subjected:

- **wooden crates**
  for transport by ship, air, on road for periods longer than 60 days
- **ply-wood crates**
  for transport by ship, air, on road for periods of 30 to 60 days
- **cardboard boxes**
  for transport by air or on road for periods of less than 30 days

Preliminary checks

The following information should be printed on the outer crate:

- International symbols


side up :


keep dry


fragile

- trade mark/address of the manufacturing company;
- labels (or template marks) indicating information on the contract and destination site of the product;
- an envelope holding among others the packing list

Upon receipt check:

- that the final destination of the crates is that indicated on the label;
- that no damage was made to the cases

Report any shipping damages to the Company's representative or the Shipping Agent.

Unpacking

When having to unpack proceed as follows:

- make sure that the packing has been properly positioned, refer to the  symbol
- open the case;
- remove the shockproof material;
- remove the goods from the case;
- remove pre packing, the polyethylene bag and any other protection;
- remove the plastic bags cello taped to the rack and containing accessories;
- remove the dehydrating bags;
- ascertain that the goods are not damaged and that they correspond to those indicated on the packing list enclosed in the envelope. Conversely, contact the agency's representative.

Note

When unpacking it is advisable to handle the packing material with care; it might be reused for packing again if it must be reshipped.

Warehousing

If having to store the packed material, the following requirements must be met:

- the cardboard boxes must be placed indoors in a room with ventilation.
- the wooden or plywood cases can be placed outdoors, provided they are protected against rain and direct sunlight.

4.4 Rack mounting

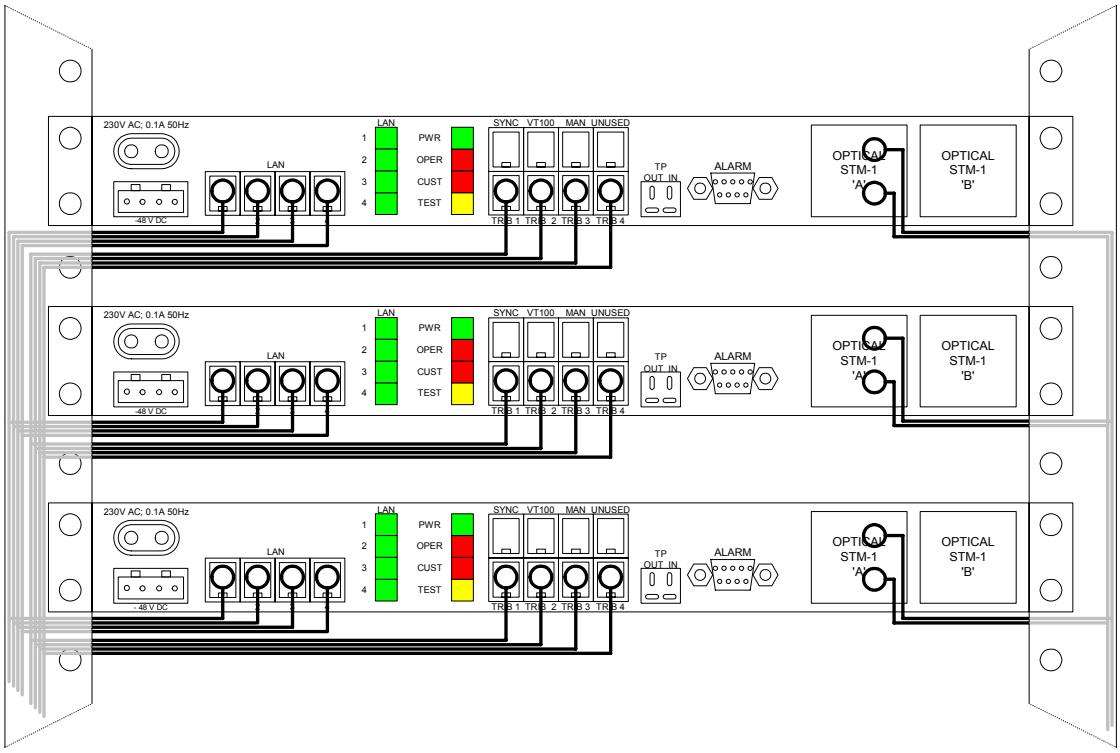
AXX155 R2 is housed in a 19”/1U steel cabinet. The cabinet can be delivered with brackets for mounting in either 19” or 600 mm ETSI racks. The brackets can be mounted on either side of the cabinet. Either the front or rear side can face outwards dependent on whether rear or front cabling in the rack is to be used. The man-machine-interfaces (LEDs and CLI connectors) are available on both sides of AXX155 R2 .

4.5 Cabling

For 100 Mbit/s LAN connections, UTP CAT5 cables are required. For the other electrical connections, shielded twisted pair cables are recommended for EMC/RFI reasons.

When installing the AXX155 R2 in a rack, it is recommended to separate guiding of electrical and optical cables. Viewed from the rear side of the AXX155 R2 , the cable duct on the left side of the rack will then guide electrical cables, and the cable duct on the right side will guide the optical cables.

When using the 120/75 Ω balun, it is normally fixed along the cable duct using tie-wraps.



T00856A.VSD

Figure 38. Cabling principle

Port name	#	Recommended cable type:
LAN	4	UTP Cat 5 for 100 Mbit/s Ethernet
Management	1	UTP Cat 5
Tributary	4	STP
Aggregate	1	MM fibre according to ITU-T G.651 or SM fibre according to ITU-T G.652
VT.100 (‘CLI)	1	UTP Cat 1
ALARM	1	UTP
SYNC	1	UTP

Table 74 Recommended cable types

Straight-through vs. cross-over LAN cable

A straight through cable shall be used to connect two ports when one of the ports is designated with an X.

A cross-over cable shall be used to connect two ports when both ports are designated with an X, or when both ports do not have an X.

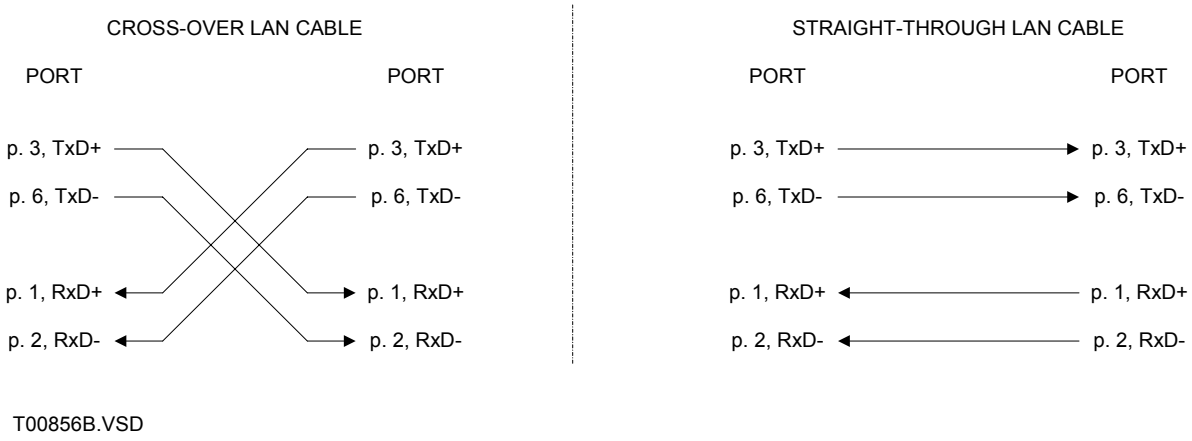


Figure 39. Straight-through vs. cross-over LAN cable

4.6 Basic software configuration

While there are a lot of parameters that can be adjusted and tweaked to optimise the AXX155 R2 for work in your network, the following part describes a general setting that will get you started working. These and the other commands are described further in the chapters concerning Management and the Command Line Interface.

Connect your workstation to the VT100 port on the AXX155 using the provided serial cable. Use the following communication settings: 19200,8,N,1, no flow control. Type AXXCLI at the prompt, and supply the factory set password “AXXCLI” when prompted.

To set the A155 up to work as a basic bridge some parameters must be set:

Create a basic VLAN:

```
AXXCLI>Device\VLAN\VLAN-Table\Add Name=Test
```

This should result in the following output (except the specific MAC-address):

```
VLAN-NUMBER:    100000
NAME:           Test
MAC-ADDRESS:    00047AFFF400
ADDRESS-TYPE:   default
TAG:            1
PORTS:          <none>
```

Include all Ethernet ports in the VLAN.

```
AXXCLI>Device\VLAN\VLAN-Port-Table\Add VLAN=100000
Ethernet-Ports=1,2,3,4,5
```

A table describing the relation between Ethernet ports and VLAN will be displayed:

```
VLAN-NUMBER:  100000

-----------------------------------------
VLAN-PORT-NUMBER  VLAN-PORT-TYPE TAGGING
-----------------------------------------
1                 static         disable
2                 static         disable
3                 static         disable
4                 static         disable
5                 static         disable
```

```
AXXCLI>Device\VLAN\VLAN-Port-Table\
```

The bridge is now ready to forward traffic on all Ethernet ports.

Set the Management Interface parameters

To be able to log in using Telnet, or to manage the device using AXXMASTER, the Management Interface parameters must be set:

```
AXXCLI>Device\Management-Configuration\Management-Mode
MODE=ipManagementPort

Change management configuration, are you sure? (y/n)? y
```

and

AXXCLI>Device\Management-Configuration\IP-Management-Port\IP-Configuration IP=<IP address> Subnet=<IP address> Default-Gateway=<IP address>

Be sure you are using valid IP addresses to avoid conflict with other equipment on your LAN. When these parameters are set you should be able to connect the AXX155 management port to your LAN.

Entry in the Community Table

Additionally, to get access, using AXXMASTER, an entry in the Community Table is necessary:

```
AXXCLI>Security\Community-table\Add Manager MANAGER=<IP
address> COMMUNITY=public ACCESS=super TRAPS=enable
```

Here the IP address is referring to the workstation running AXXMASTER.

4.7 SW download through local VT100 interface

It is possible to load a new software version by means of a PC directly attached to the VT100 Port. This service requires local operator presence at the AXX155 R2. The file is loaded by means of the X-Modem protocol. Booting the system triggers local software download. Hence, the Ethernet-traffic is always lost during the loading new software. Traffic on 2 Mbit tributaries can be affected, please read release notes for details.

Please follow the steps below for a successful download operation:

Step 1

Make sure that you are connected and the cursor AXXCLI>DEVICE\> is visible.

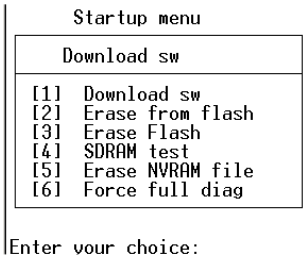
Step 2

Write the command "reset" and push the enter-button. Press "Y" to confirm command.

You have now triggered a software restart, and the boot-process will be started immediately.

Step 3

When you see a window containing the following:



Enter "1" immediately.

Note

*If you are to slow entering "*1*" the device will continue the boot process and you will have to reboot again.*

Step 4

When finished step 3 you will immediately be prompted to choose a baud-rate for the X-Modem. Recommended 115 200 kbit/s.

Choose the number for your selection

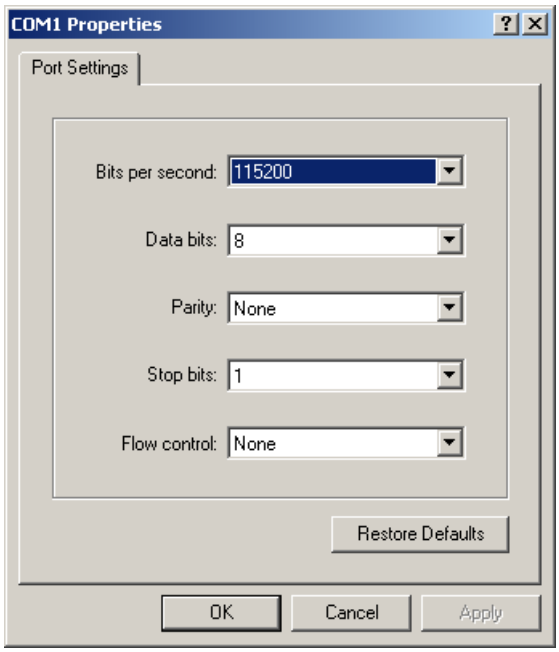
An example is shown below.

```
Choose 0 - 4 to change baud rate
0 for 9600   Bits Per Second
1 for 19200  Bits Per Second
2 for 38400  Bits Per Second
3 for 57600  Bits Per Second
4 for 115200 Bits Per Second
Any other key to continue:   4
```

Step 5:

When finished step 4 you will be requested to set up your terminal according to chosen baud-rate. Example shown below:

Disconnect and set terminal speed to 115200, connect and press Enter to continue.



Step 6:

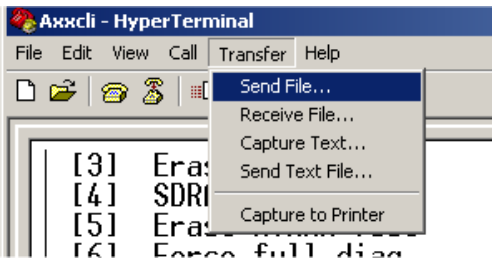
When setup is correct the following message will appear in terminal window:

Please download program using XMODEM.
$$$$

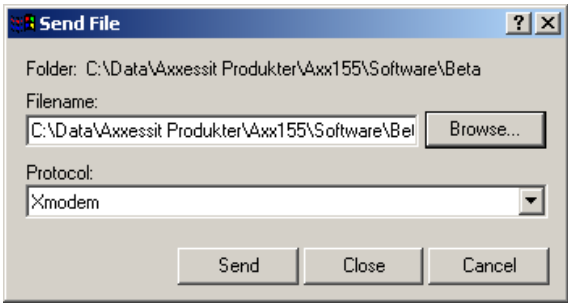
The device is now ready to receive the new software (firmware).

If you perform this by using HyperTerminal (Windows) please perform the steps shown in the following screenshots:

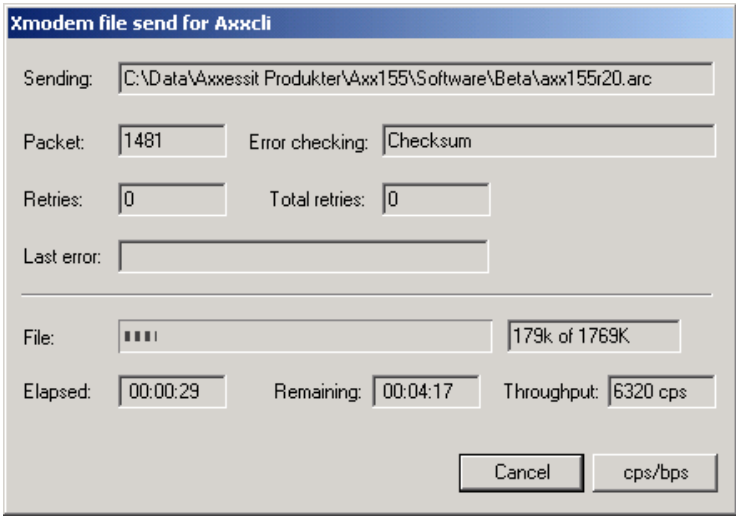
Select "Send File".



Select directory containing the software
Choose Xmodem
Press "Send"



The download is now started and you can attend the process in the field "Remaining"



When the download has finished the device will immediately start to write to flash and update its registry and automatically reboot. The total time for download operation is approximately 10 minutes.

To make sure that the download operation was successful you can see the inventory list by using the following string:

```
AXXCLI>Device\Inventory
```

If the Software upgrade contains new features e.g. OSI-routing functionality for management-connectivity, a specific license-key is needed for each device. The key can be ordered and sent per e-mail, or other ways desirable by the customer.

Chapter

5

5 Command line interface

Accessing CLI

Syntax rules

Basic command syntax

Command hierarchy

5.1 Introduction

AXXCLI is a line-oriented ASCII-based management interface to AXX155 R2 , by means of which simple commands – possibly with parameters - may be issued to access or modify the AXX155 R2 configuration.

The functionality provided by the CLI closely parallels that of AXXMASTER, and the command hierarchy offered by the CLI closely reflects the menu hierarchy provided by AXXMASTER.

Accessing CLI

The CLI is accessed via a serial port or via an IP connection (Telnet). The serial connection communications parameters are fixed: 19200 bit/s, no parity, 8 bits, 1 stop bit, and no hardware flow control. VT100 terminal codes are used.

Invoke a CLI session

A CLI session is invoked by typing **AXXCLI** at the CLI terminal.
User authentication (password, 8-12 ASCII characters) is required, as the following session start-up sequence shows:

```
AXX155 R2 Command Line Interface
Password:  *********
\>
```

Incorrect password

Each password characters is echoed as '*'. An incorrect password is rejected with the message:

```
invalid password
```

and the password prompt is re-issued.

Exit

The **Exit** command is used to terminate a CLI session. The CLI session will be automatically terminated after a period of 10 minutes of inactivity. CLI does not accept simultaneous sessions.

An authorised CLI user obtains full access rights to the available management information.

Syntax rules

A CLI command line begins with a prompt (issued by CLI), which serves to indicate the current position in the command hierarchy.

A CLI command is issued by typing the command followed by ENTER. Optionally, and only at the lowest level in the command hierarchy, one or more parameters may also be supplied. These are identified by keywords. The command name, parameter keywords and parameter values are delimited by one or more spaces.

It is only necessary to type sufficient leading characters of the command name to avoid ambiguity – the same applies to keywords. BACKSPACE or DELETE may be used to edit the command line. Commands and keywords are NOT case-sensitive, although for clarity they are written in this document using both upper- and lowercase letters. A list of valid commands that have been issued in the current session is maintained in a command history.

Universal commands

There are a number of universal commands:

`..`	return to previous command level
\	go to top command level
?	issue a list of commands valid at the current level, or show the command usage
↑	recall previous command in command history
↓	recall next command in command history
Status	present current device and port status
Exit	exit AXXCLI

Some commands (in particular **Show**) may potentially produce many lines of output. After a predetermined number of lines of output in response to a single command, the user is prompted to enter y(es) or n(o) to continue the output. The line number limit is defined with the **`DISPLAY-LINES`** parameter to the **`Command-Line-Interface`** command.

Command lines may be edited by using the ← and → keys to position along the line, and by using BACKSPACE or DELETE to remove characters. All other (graphical) characters are inserted at the current position in the line.

5.2 Basic command syntax

A basic command has the following syntax:

```
<basic command>      ::= [<path>]<command> [<parameter>]… <CR>
<path>               ::= [\]<command\>[<command>\]…
<command>            ::= <command name> | ..
<parameter>          ::= <spaces> <keyword>=<value> | ?
<value>              ::= <integer> |
                         <choice> |
                         <IP address> |
                         <string> |
                         <MAC address> |
                         <NSAP address> |
                         <time> |
                         <date> |
                         <KLM> |
                         <portList> |
                         <port>

<NSAP address>      ::= <area address>:<system id>:<selector>
<portList>          ::= <port>[,<port>]..
<areaAddressList>   ::= <area address>[,<area address>]...

where:

<spaces>                 is a string of one or more ASCII
                         spaces;

<integer>                is a decimal integer in the range
                         [m:n], where the values m and n are
                         context-dependent;

<choice>                 is a literal string, whose
                         permissable values and their
                         significance are context-dependent
                         and may be obtained by using the help
                         (“?”) parameter;

<IP address>             is an IP address of the form
                         ddd.ddd.ddd.ddd, where d is a
                         decimal digit. Leading zeroes in each
                         ddd may be omitted;

<string>                 is a string of graphical ASCII
                         characters, excluding quotation
                         marks (“). If the string contains one
                         or more spaces, then it MUST be
                         enclosed in quotation marks. The
                         maximum length of the string is
                         context-dependent;

<MAC address>            is exactly 12 hexadecimal digits;

<time>                   is a time-of-day of the form
                         hh:mm:ss, where h, m and s are
                         decimal digits;

<date>                   is a date of the form dd/mm/yy, where
                         d, m and y are decimal digits;
<KLM>                    is a string of the form k.l.m, where
                         k is a decimal digit in the range
                         [1:3], l is a decimal digit in the
                         range [1:7], and m is a decimal
                         digit in the range [1:3].
<port>                   is a decimal integer;
<area address>           is a hexadecimal string;
<system id>              is a hexadecimal string;
<selector>               is a hexadecimal string;
```

The complete AXXCLI command hiearchy is shown below. Each basic command is shaded, and is marked by a number that refers to the appropriate line in the following parameter description table. The complete names of both commands and parameter keywords are shown.

Optional parameters are enclosed in square brackets. For clarity, parameter command keywords are written in capital letters, for example *[TFTP-SERVER <IP>]*. and lengthy commands are shown on several lines.

The order of parameters (keyword/value pairs) is not significant. The help command "*?*" will display all available commands at the current level, each with a short description.

.

The help command

The help command "**?**" will display all available commands at the current level, each with a short description. E.g. typing "?" at the root level will list the commands which are available at this level:

```
AXXCLI>?

*** valid commands:
Device:     Device configuration
Ports:      Port properties
Bridge:     Bridge/Spanning Tree Protocol settings
Security:   Security settings
Statistics: Performance monitoring and statistics
Services:   Utility functions
Alarms:     Current alarms and alarm history
Status:     Device status
Exit:       Exit from AXXCLI

AXXCLI>
```

Command hierarchy

In the command hierarchy, the lowest level is represented by a basic command with one or more parameters.

For example, selecting the

```
\Device\Management-Configuration\IP-Management-Port\
IP-Configuration IP ADDRESS=193.69.136.104
```

modifies only the IP address. For most commands, if no parameters are supplied then all the current parameter values are displayed, so that the command

```
 \Device\Management-Configuration\IP-Management-Port\
IP-Configuration
```

displays the current management interface information in the following manner:

```
IP-ADDRESS:     193.69.136.104
SUBNET-MASK:     255.255.255.0
DEFAULT-GATEWAY: 193.69.136.54
```

If the help parameter "**?**" is supplied (excluding the quotation marks), then any other parameters are ignored and the basic command usage is displayed.

Table entries are accessed by introducing an additional command level giving access to the entire table. At this lowest level, the command **Add** (with the index and required table entries as parameters) may be used to add an element to the table and **Edit** to replace an existing element in the table – if these operations are permitted on the table. Similarly the command **Remove** (with the entry index as parameter) may be used to remove an existing element from the table, if this is permitted. The command **Show** with an entry index value, as parameter will display the specified table

entry. If no parameter is supplied with the **Show** command, the current contents of the entire table will be displayed.

AXXCLI menu structure

The complete AXXCLI command hiearchy for AXX155 R2 is found in page 158.

Chapter

6

6 Troubleshooting

Introduction

Problem solving

Identifying start-up problems

6.1 Introduction

AXX155 R2 s are tested extensively and burned-in before leaving the factory. However, if your system appears to have problems starting up, use the information in this chapter to help isolate the cause.

When the initial system boot is complete, verify the following:

- Power is being supplied to the system.
- System software boots successfully.

If the start-up sequence fails before these conditions are met, use the procedures in this chapter to isolate and, if possible, resolve the problem.

If you are unable to easily solve the problem, contact a customer service representative for assistance and further instructions. Before you call, have the following information ready to help your service provider assist you as quickly as possible:

- Date you received the equipment
- Chassis serial number
- Type of software and release number
- Brief description of the problem you are having
- Brief explanation of the steps you have already taken to isolate and resolve the problem
- Maintenance agreement or warranty information

6.2 Problem solving

The key to problem solving the system is to try to isolate the problem to a specific subsystem. The first step in solving start-up problems is to compare what the system **is doing** to what it **should be doing**. Since a start-up problem can usually be attributed to a single component, it is more efficient to first isolate the problem to a subsystem rather than troubleshoot each separate component in the system.

The AXX155 R2 consists of the following subsystems.

- Main Card
- Electrical/Optical transceiver card

6.3 Identifying start-up problems

LEDs indicate all system states in the start-up sequence. By checking the state of the LEDs, you can determine when and where the system failed in the start-up sequence.

When you plug in the power supply to start the system, the following should occur:

- The 'POWER' LED turns green when you plug in the switch.
- The 'OPERATION', 'CUSTOMER' and 'TEST' LEDs operate as follows during equipment start-up:

  All LEDs are lit simultaneously for a few seconds with an interval of ~1 minute during start-up. The start-up procedure takes approximately 3 minutes.

  Any LAN LED is only lit when the actual LAN port is carrying traffic.

Chapter

7

7 Technical data

Optical power budget

Optical power budget – Long Haul

Electrical environment

Climatic and mechanical environment

Mechanical characteristics

Reliability

Health and safety

7.1 Optical power budget

The definitions of optical parameters and reference points S and R refer to ITU-T G.957, and exceed the requirements of STM-1/S.1.1 power budget. Reference point S means transmit side while R is the receive side of the fibre link.

The connector can be one of the following:

- FC/PC
- SC/PC (on request only)
- E-2000 (on request only)

Optical budget AXX155 Two-fibre version

Parameter	Value
Type of fibre	SM 10/125 um MM 50/125um, MM 62.5/125 um
Modulation rate on optical line	155 520 kbit/s, STM-1
Wavelength range	1270 – 1335 nm
Transmitter at reference point S	
Source type	MLM
Spectral characteristics (max. RMS width)	3.0nm
Mean launched power (max.)	-8 dBm
Mean launched power (min.)	-12 dBm
Min. extinction ratio	8.2 dB
Optical path between S and R	
Attenuation range	0 – 17 dB
Max. tolerable dispersion	280 ps/nm
Min. optical return loss	30 dB
Max. discrete reflectance between S and R	NA
Receiver at reference point R	
Min. sensitivity (BER < 1 in 10^{10})	-30 dBm
Min. Overload	0 dBm
Max. optical path penalty	1 db
Max. reflectance at R	NA

Table 75 Optical power budget AXX155 R2 Two – fibre version

Factory testing to Power Budget :
Mean launched power: Adjusted to -10 dBm at S point.
Receiver sensitivity test:
Maximum signal level -32 dBm at R point at BER < 1 in 10^{-10}.
Initial equipment margin: > 3 dB

Cable planning

Cable Loss, according to ITU-T G.957, Appendix 1	Single Mode fibre Acc. to ITU-T G.652	Multi Mode fibre Acc. to ITU-T G.651
Fibre Cable Attenuation Cable Margin (Mc) Loss in Optical Distribution Frame Loss Limited Span	0.5 dB/km *) Incl. in *) 1 dB 34 km	1.0 dB/km 3 dB 1 dB 13 km
Cable Dispersion:		
Maximum Chromatic Dispersion Coefficient Modal bandwidth Overall bandwidth (Requirement >80 MHz) Dispersion Limited Span	4.5 ps/nm*km - - 41 km	6 ps/nm*km 800 MHz*km 84 MHz (9km) 9 km
Overall Link Span	34 km	9 km

Table 76 Cable planning

Optical budget single-fibre

Parameter	Value
Modulation rate on optical line	155 520 kbit/s
Wavelength range	1260 - 1360 nm
Transmitter at reference point S	
Source type	MLM
Spectral characteristics (max. RMS width)	7.7nm
Mean launched power (max.)	-6 dBm
Mean launched power (min.)	-8 dBm
Min. extinction ratio	8.2 dB
Optical path between S and R	
Attenuation range	0 – 13 dB
Max. tolerable dispersion	96 ps/nm
Min. optical return loss	30 dB
Max. discrete reflectance between S and R	NA
Receiver at reference point R	
Min. sensitivity (BER < 1 in 10^{10})	-21 dBm
Min. overload	-6 dBm
Max. optical path penalty	1 db

Table 77 Optical budget single fibre parameters

Optical budget two-fibre

Parameter	Value
Modulation rate on optical line	155 520 kbit/s
Wavelength range	1261 – 1360 nm
Transmitter at reference point S	
Source type	MLM
Spectral characteristics (max. RMS width)	7.7 nm
Mean launched power (max.)	-8 dBm
Mean launched power (min.)	-15 dBm
Min. extinction ratio	8.2 dB
Optical path between S and R	
Attenuation range	0 – 12 dB
Max. tolerable dispersion	96 ps/nm
Min. optical return loss	NA
Max. discrete reflectance between S and R	NA
Receiver at reference point R	
Min. sensitivity (BER < 1 in 10^{10})	-28 dBm
Min. overload	-8 dBm
Max. optical path penalty	1 db
Max. reflectance at R	NA

Table 78 **Optical budget two-fibre parameters**

7.2 Optical power budget – Long Haul

This section applies for the AXX155-OPL , Long Haul – Single Mode 1310 nm.

Optical Power Budget

Parameter	Value
Nominal Bit Rate	155520 kbit/s
Minimum Optical output power (S)	0.0 dB
Maximum Optical output power (S)	3.0 dB
Receiver sensitivity (R) (BER= 10-10)	- 30.0 dB
Dispersion margin (dB)	1.0 dB
Net power budgte (S/R)	**29.0 dB**
Equipment Margin (Me)(dB) (included)	3.0 dB

Table 79 **Optical power budget – Long Haul**

Dispersion budget

Parameter	Value
Optical Wavelength	1280-1335 nm
Maximum Tolerable Dispersion	280 ps/nm
Laser Spectralwidth	3 nm

Table 80 **Dispersion budget – Long Haul**

Cable planning

Parameter	Value
Fibre attenuation	0.50 dB/km
Loss limit	58 km
Maximum Chromatic Dispersion Coefficient	3.5 ps/nm*km
Dispersion Limited Span	80km
Overall Link Span	**58 km**

Table 81 **Example of cable planning according to ITU-T Rec G.957**

7.3 Electrical interface specifications

Electrical

It is possible to equip the Axx155 with an electrical STM-1e aggregate interface. The interface is bi-directional and running on a coaxial cable at 155Mbit/s,CMI encoded.

The second electrical STM-1e interface is used for protection purposes (see section Protection, page 71.

Connector type

The connector shall be a coaxial connector type Siemens 1.0/2.3. The screen is always DC connected to ground on the transmit side and AC coupled to ground on the receiver side.

Output jitter

Filter bandwidth	Jitter limit
500 Hz - 1.3 MHz	0.50 Uipp
65 kHz - 1.3 MHz	0.10 Uipp

Table 82 Electrical output jitter parameters

Input jitter

Frequency range	Jitter limit
500 Hz - 6.5 kHz	1.5 Uipp
6.5 kHz - 65 kHz	Decaying, slope equal to 20 dB/decade
65 kHz - 1.3 MHz	0.15 Uipp

Table 83 Electrical input jitter parameters

Compliance

Standard	Comment
ITU-T G.703	Cable attenuation Input reflection loss Input port immunity against reflection Output pulse mask
ITU-T G.707	Line signal
ITU-T G.783	RX pull-in and hold range
ITU-T G.813	Output jitter
ITU-T G.825	Input jitter

Table 84 Electrical interface compliance

Tributary interfaces

Tributary input jitter

Frequency range	
20 Hz - 2.4 kHz	1.5 Uipp
2.4 kHz - 18 kHz	Decaying, slope equal to 20 dB/decade
18 kHz - 100 kHz	0.2 Uipp

Table 85 **Tributary input jitter**

Tributary input reflection loss

	Reflection loss
51 kHz - 102 kHz	12 dB
102 kHz - 2048 kHz	18 dB
2048 kHz - 3072 kHz	14 dB

Table 86 **Tributary input reflection loss**

Tributary output jitter

Filter bandwidth	Jitter output (p-p)	
	Output jitter in the absence of input jitter and pointer movements	Output jitter in the absence of input jitter, but with pointer movements
20 Hz - 100 kHz	< 0.25 UI	< 0.4 UI
700 Hz - 100 kHz	< 0.075 UI	< 0.075 UI

Table 87 **Tributary output jitter**

Tributary compliance reference list

Standard	
ETS 300 246	Connector
ETS 300 247	Connector
ETS 300 011	Impedance towards ground Tolerable longitudinal voltage
ETS 300 126	Output signal balance
ITU-T G.703	Cable attenuation Input reflection loss Input port immunity against reflection Output pulse mask
ITU-T G.783	Output jitter in the absence of input jitter (Chapter 10.2.3.1 in the specification) Output combined jitter (Chapter 10.2.3.3 in the specification)
ITU-T G.823	Max. tolerable input jitter

Table 88 **Tributary compliance reference list**

LAN ports and Management Port

Standard	Comment
ISO/IEC8877	MAU MDI connector
IEEE 802.3	Section 14 and 24, physical medium.
ANSI X3T12 TP-PMD	Physical medium 100BASE-T

Table 89 **LAN and Management port compliance list**

Synchronisation

AXX155 R2 has one 2048 kHz synchronisation output port and input.

Synchronisation input jitter

Frequency range	Jitter limit
20 Hz - 2.4 kHz	1.5 Uipp
2.4 kHz - 18 kHz	Decaying, slope equal to 20 dB/decade
18 kHz - 100 kHz	0.2 Uipp

Table 90 **Synchronisation input jitter**

Synchronisation input reflection loss

	Reflection loss
2048 kHz	15 dB

Table 91 **Synchronisation input reflection loss**

Synchronisation output jitter

Filter bandwidth	
20 Hz - 100 kHz	< 0.05UI

Table 92 **Synchronisation output jitter**

Synchronisation compliance reference list

Standard	Comment
ETS 300 246	Connector
ETS 300 247	Connector
ITU-T G.703	Cable attenuation Output pulse mask

Table 93 **Synchronisation compliance reference list**

Alarm inputs

Parameter	Value
Nom. Closed contact current	1 mA
Max. closed contact resistance	0.8 kΩ
Nom. Open contact voltage	3 V
Min. open contact resistance	10 kΩ

Table 94 **Alarm Inputs**

Alarm outputs

Parameter	Value
Maximum load bias referred to common return	+/- 75 V
Maximum load current	50 mA
Common return to AXX155 R2 earth (maximum)	+/- 250 V
Maximum contact resistance	50 Ω

Table 95 **Alarm Outputs**

Power supply

AXX155 R2 supports two different power supplies:

- Single phase 230 V 50 Hz AC mains supply
- -48 V DC supply

The 220V mains supply input on the AXX155 R2 is provided via a standard connector according to EN60320.

Parameter	Limit
Power dissipation	< 15W
Fuse	0.5A
Battery voltage range	-36 to –72V DC *
Mains voltage	-230V AC +/- 10%

*** Restrictions when applying voltage larger than 60 volt on the -48V DC supply**

The maximum voltage for the DC supply is in the range from -36 to -60 Volt. If the supply voltage is in the range from -60 to -72 Volt, the placement of the equipment has to be in a Restricted Access Location (RAL) as defined in IEC 950 1.2.7.3.

Table 96 Power supply

CLI port

The CLI Port is accessible from both the front and rear side of the unit by means of two parallel connectors.

The interface has a physical interface according to EIA RS-232, and is running at a data rate of 19.200 baud.

Monitor point

Tributary test point connector type: IEC 130-12.

The monitor point interface for AXX155 R2 is provided using a DIN41616 connector.

The monitor output signal shall be a 20dB attenuated exact replica of the monitored signal.

7.4 Electrical environment

Electromagnetic compatibility (EMC)

The equipment conforms to the requirements of EN 55022 Class B for radiated and conducted emissions.

The equipment conforms to the requirements of EN 50082-1 for radiated and conducted susceptibility.

The equipment is also compliant with these standards:

- IEC 61000-4-6 Conducted Immunity.
  150 kHz - 80 kHz, Test level 2 (3V emf), 80%
  Amplitude Modulated at 1 kHz,
  'Performance Criterion A'

- IEC 61000-4-3 Radiated Immunity.
  80 MHz - 1000 MHz, Test Level 2 (3V/M), 80%
  Amplitude Modulated at 1 kHz,
  'Performance Criterion A'. A'

- IEC 61000-4-4 Fast Transients.
  Test Level 2 (Power ports 1kV, I/O ports 0.5kV),
  'Performance Criterion B'

- IEC 61000-4-2 Electrostatic Discharge (ESD).
  Test Level 2 (4kV contact, 8kV air),
  'Performance Criterion B'

In order to apply the 'CE' mark to the equipment, is not only compliant with EN50082-2 and EN55022, but also with any other European Standards applicable to the equipment under consideration, i.e. electrical safety EN60950, and the Low Voltage Directive.

7.5 Climatic and mechanical environment

	ETSI Specification
Operation	ETS 300 019-2-3 Class 3.2
Transportation	ETS 300 019-2-2 Class 2.2
Storage	ETS 300 019-2-1 Class 1.1

Table 97 **Specification of Climatic and Mechanical Environment**

7.6 Mechanical characteristics

Equipment	Size (mm)	
AXX155 R2	43 x 240 x 1U	1.60

1U = 44.45mm

Table 98 **Mechanical characteristics**

7.7 Reliability

The overall error ratio of a tributary channel is better than 10E-10.

According to MIL-HDBK-217F with a correction factor adjustment related to the following conditions:

- Ground benign
- +35^{o}C ambient temperature
- Stress value 0.5.

Equipment	MTBF [Years]
AXX155 R2 non-redundant optics	40
AXX155 R2 redundant optics (NA for AXX155 R1.0)	47

MBTF : Mean Time Before Failure

Table 99 **Reliability**

7.8 Health and safety

The equipment meets the requirements in EN60950 and EN60825.

Chapter

8

Index

Entries

Chapter

9

9 BOOTP Application Note

Introduction

Bootstrap Protocol (BOOTP)

BOOTP Structure and Configuration

BOOTP and TFTP process in Radlan Devices

9.1 Introduction

This section is identical to this document made by RADLAN:

Document Version	Change Reason	Change Date	Change Responsibility
1.0	First Release by Naftali Tanin	24/12/01	
1.1	Revision	2/01/02	

The information is reproduced after written consent of RADLAN.

Copyright

Introduction

The section describes how to manage the configuration process of a device booted with no configuration file. It includes a short description of the BOOTP protocol, configuration process and Radlan proprietary options of BOOTP responses.

Background

A device is configured through *Bootstrap Protocol (BOOTP)* and a *Trivial File Transfer Protocol (TFTP)* server. The order in which they are used and the specifics of the processes must be understood to be able to determine how to manage the process.

9.2 Bootstrap Protocol (BOOTP)

A TCP/IP protocol is used by the device (booted with no IP configuration) to obtain its IP address and other network information, such as IP address, server name and its IP address, default gateway, IP address of a default router, etc.Upon startup, the device sends out a BOOTP request in a UDP packet to the BOOTP server. The BOOTP server that receives the request looks up the configuration information.

Two options are possible at this point:

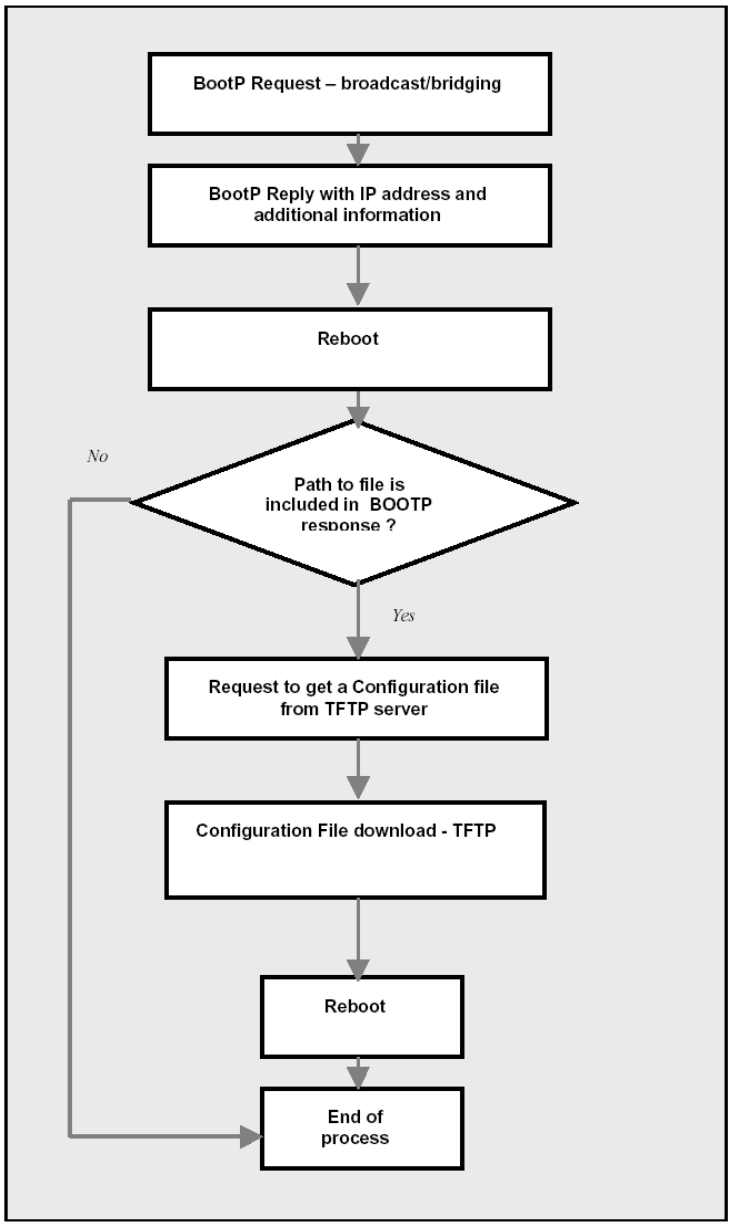
1. The BOOTP server can look in its table and map MAC addresses into

IP addresses; or

2. The BOOTP server allocates an IP address from its pool of addresses.

The BOOTP server places the IP address information in a single BOOTP reply message, and returns the reply to the requesting device.

Configuration Process



Configuring a device is an automatic process. Once the physical connections are correctly made, and all the required files are correctly installed, the process can be started. Fig.1 illustrates the configuration process. A BOOTP process is initialized on a non-configured device (that is a device with no IP configured on it [3]) by sending broadcasts "requesting" an IP address. In this process, after boot-up, the device waits approximately one minute before sending BOOTP requests. If no response is received, a request is repeated every two seconds. This continues for approximately 10 minutes. After this period, requests are sent every minute. Be aware of the fact that entering information or commands through the ASCII terminal stops the BOOTP process.

[3] Although a device configured with a VLAN only sends BOOTP requests and reboots after receiving BOOTP responses, IP configuration may be problematic if the port is an *untagged* one.

Each device has a defined *Media Access Control (MAC)* address that is included in the BOOTP request. The BOOTP server maintains a pool of IP addresses that are allocated at request and may have a table that maps MAC addresses to IP addresses. After receiving a request from a device, the BOOTP server sends a reply with the specific IP address from the MAC-IP table or the

BOOTP server allocates an IP address from a pool of available IP addresses. The device gets its IP address and reboots. After rebooting, the device has its IP address and can receive a configuration file through an available TPTP server that can run jointly with the BOOTP server (under the condition that the configuration file is correct and installed properly, and the path, file name and TFTP Server IP address were specified in the TFTP response sent by the BOOTP server).

The format of a TFTP request is as follows:

```
TFTP – IP address – get – configuration file location
```

The TFTP server fetches the configuration file and sends it to the device. If the configuration file is not available, the device sends an error messages (see below) and the configuration process ends. If the configuration file is available and correct, the device automatically configures itself and reboots.

Note

If the Radlan Network Management System (NMS) is available, the Configuration file can be downloaded with the application. The menu selection is File > Configuration > Get Configuration File.

9.3 BOOTP Structure and Configuration

The BOOTP structure is defined in RFC 951 and updated in 1542. The Options field was added and formatted in accordance with RFC 2132.The following figure illustrates the BOOTP message format.

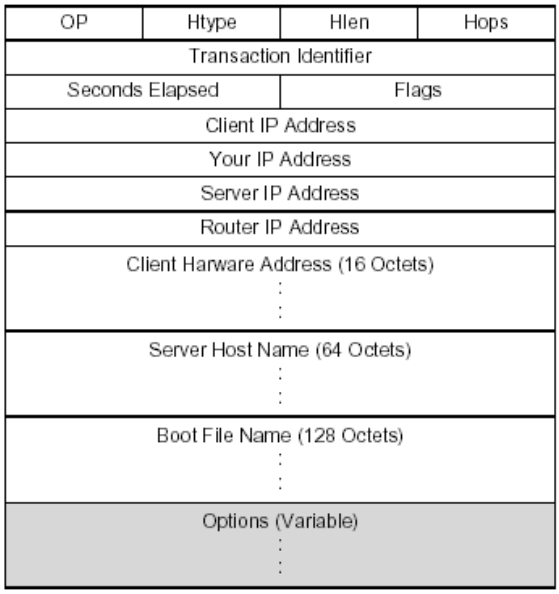


Figure 40. BOOTP Message structure

The Options field format is:

`Option ID – Option Length – Option Info`

The following is an example of Radlan proprietary Options field:

#define BTPCP_tag_community_CNS 128

#define BTPCP_tag_ip_nms_CNS 129

#define BTPCP_tag_root_CNS 130

#define BTPCP_tag_rip_type_CNS 131

The following table describes the fields to be completed.

Tag No.	Field Name	Value
128*	BTPCP_tag_community_CNS	A string specifying a community.
129**	BTPCP_tag_ip_nms_CNS	Always 4 bytes and defines the NMS Server IP address which is TFTP server address as well (must be on the same network as the initial configuration given to the device).
130	Not in use	
131	BTPCP_tag_rip_type_CNS	One byte defining the RIP version. The options are as follows: • RIP disabled - 0 • RIP version 1 - 1 • RIP version 2 - 2

Table 100 BOOTP Fields

* Enter *public* in the community field

** IP NMS should not be 0.0.0.0 – an error message is displayed.

9.4 BOOTP and TFTP process in Radlan Devices

In order to achieve a successful and complete BOOTP and TFTP process in Radlan devices, the following fields of the BOOTP response (from the BOOTP Server) must be configured:

1. BOOTP configuration file name and path

2. NMS IP address (Vendor's option 129)

3. Community string – Public (Vendor's option 128)

If a user failed to specify correctly one of the above parameters, error messages are as follows:

- If file name was config(ured) must config(ure) ip nms in boot.
- Length of the file name too long in bootp msg.
- An error message has been received:

  1 < File not found. >

  Explanation: this is a TFTP message displayed when the path to the configuration file (in a BOOTP reply) is wrong or no such file exists.

Chapter

10

10 AXXCLI command hiearchy

10.1 Introduction

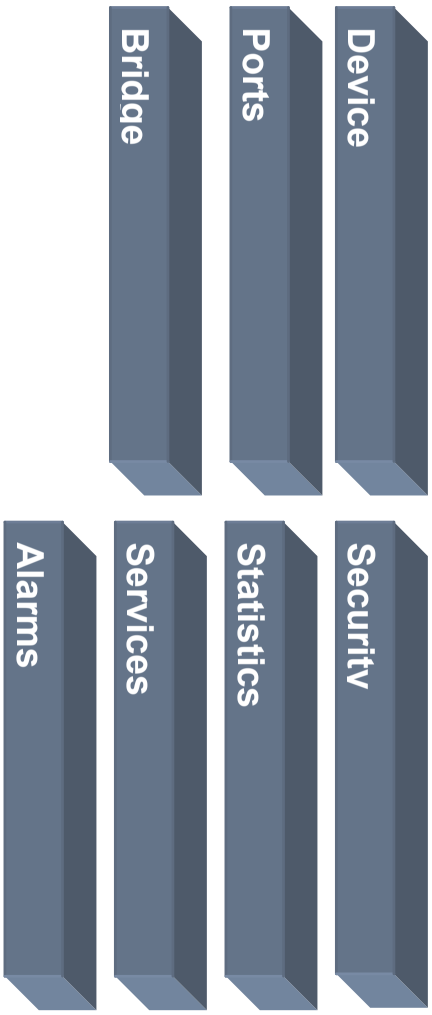
The complete AXXCLI command hiearchy for AXX155 R2 is shown on the following pages . Each basic command is shaded, and is marked by a number that refers to the appropriate line in the following parameter description table.

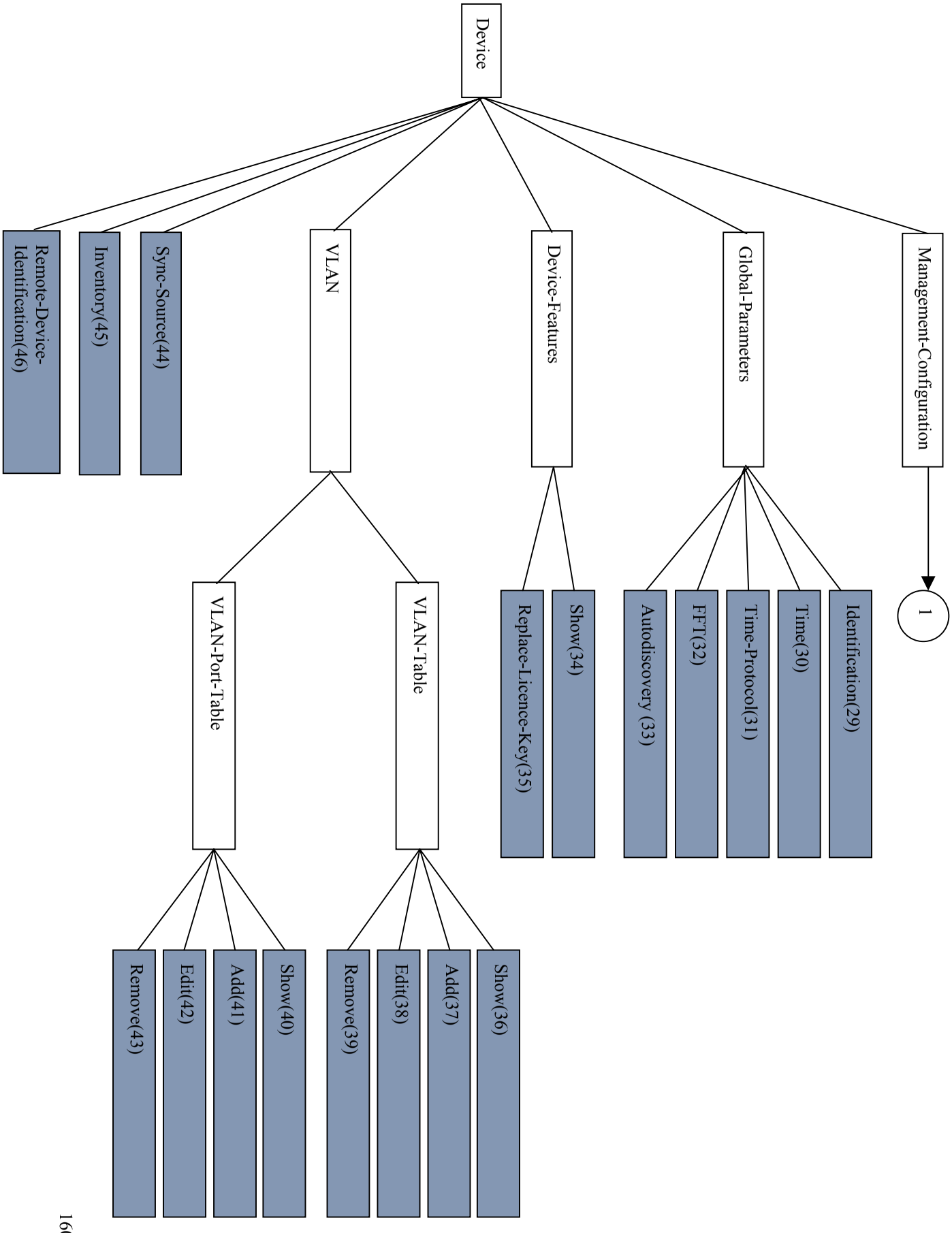
Note

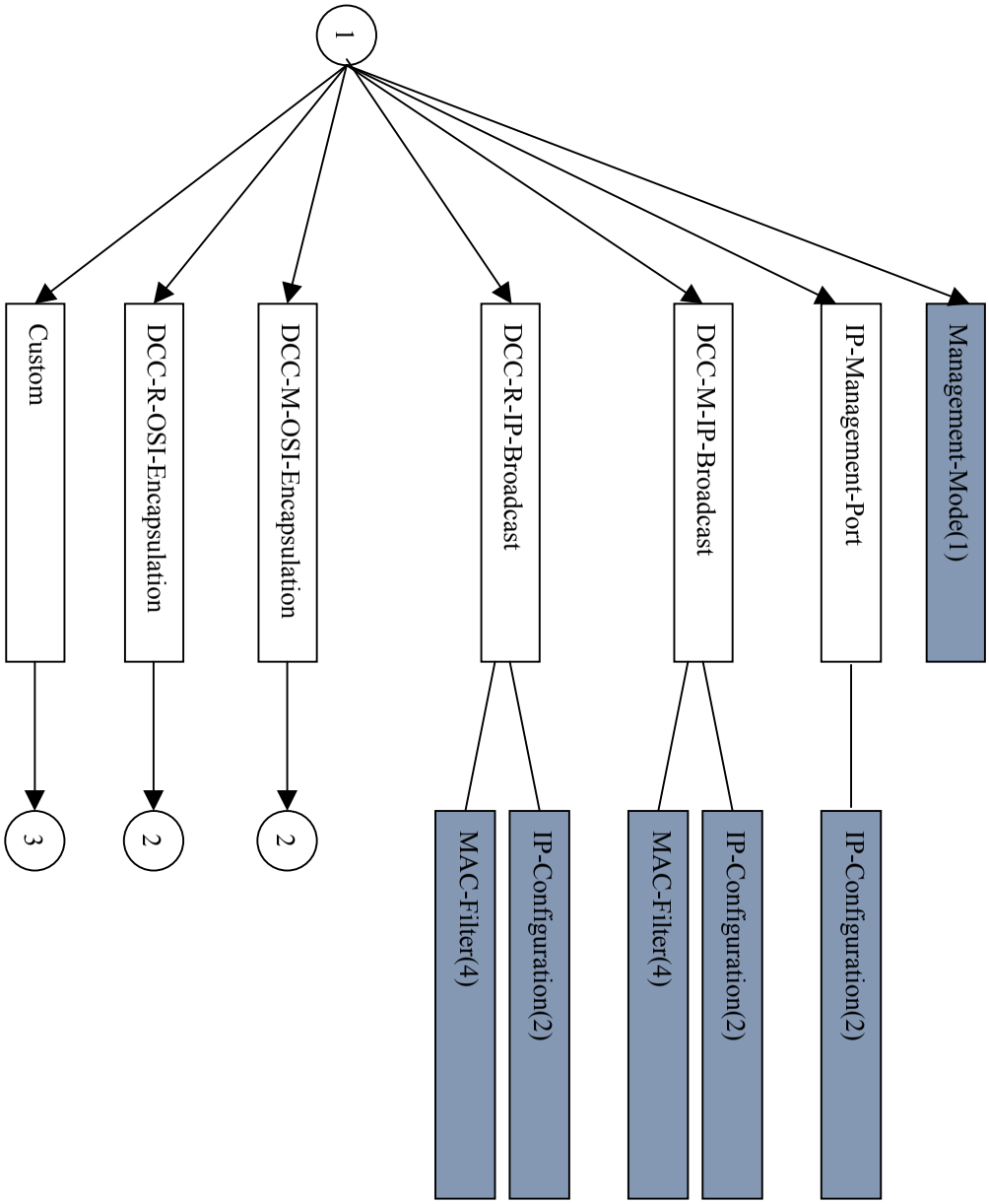
Blank columns in the parameter description table are reserved for future commands with their parameters.

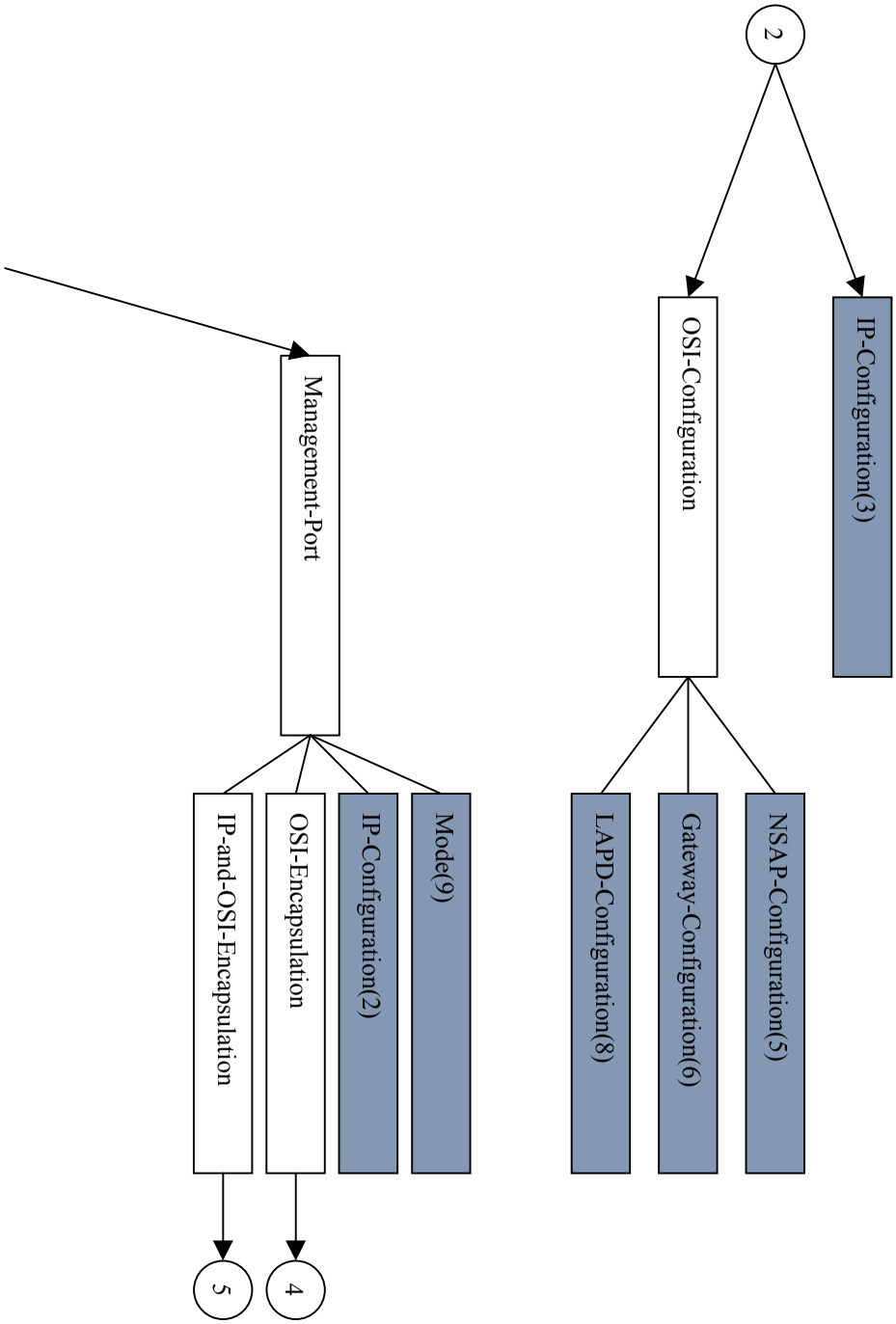
The complete names of both commands and parameter keywords are shown. Optional parameters are enclosed in square brackets. For clarity, parameter command keywords are written in capital letters, and lengthy commands are shown on several lines.

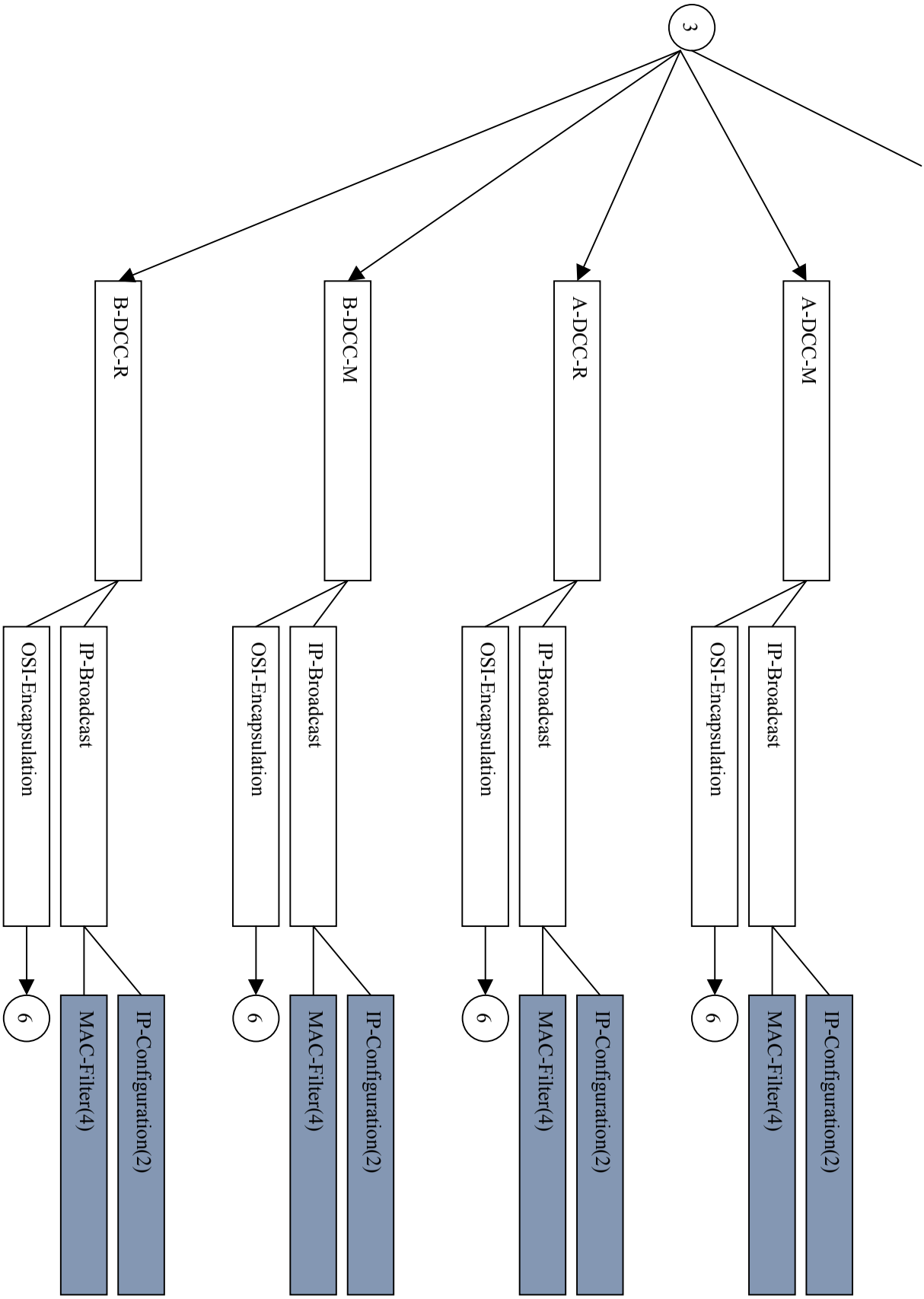
The order of parameters (keyword/value pairs) is not significant. The help command "?" will display all available commands at the current level, each with a short description.

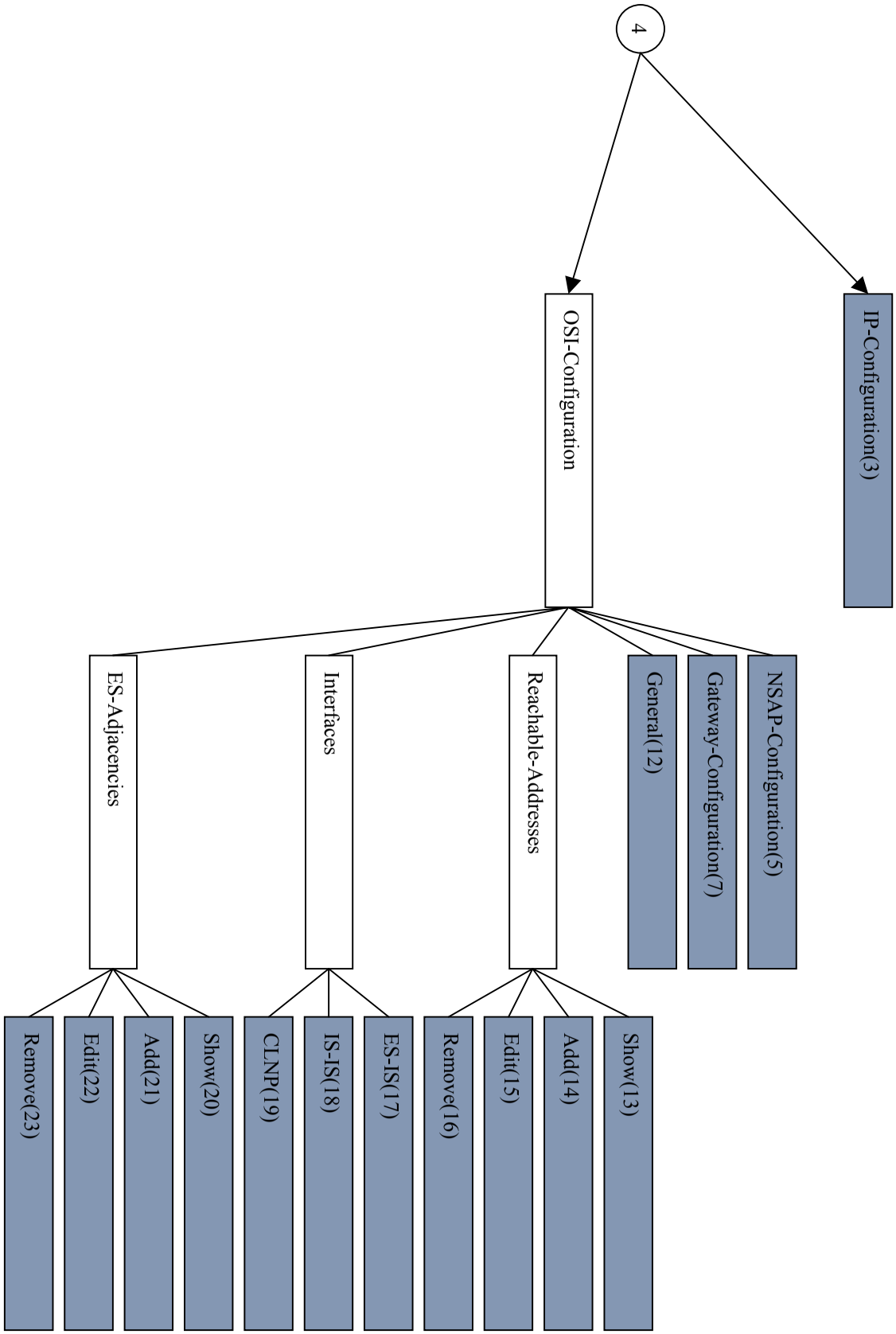

Device
Ports
Bridge
Security
Statistics
Services
Alarms

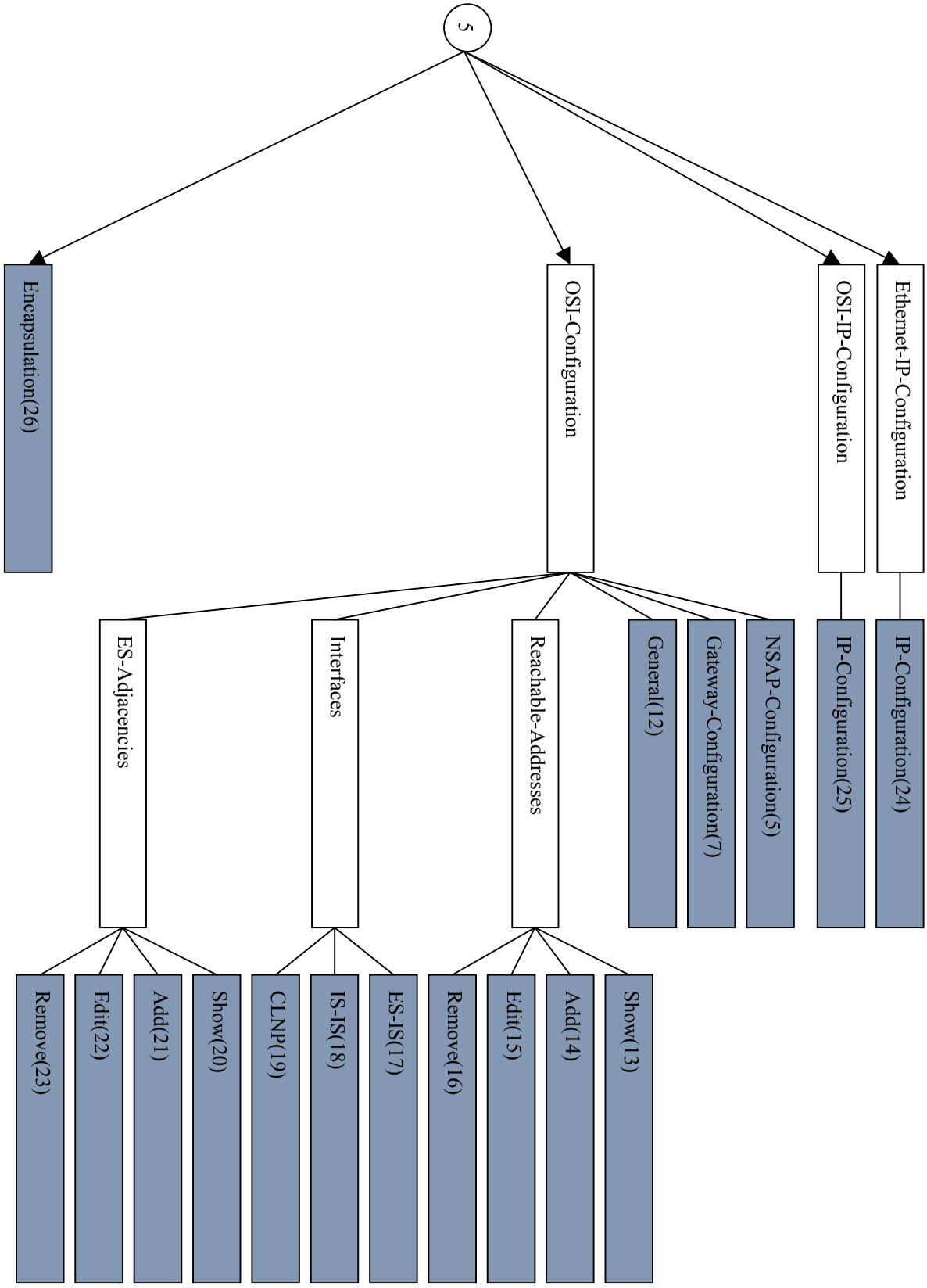

Device
Management-Configuration
Global-Parameters
Device-Features
VLAN
Sync-Source(44)
Inventory(45)
Remote-Device-Identification(46)
1
Identification(29)
Time(30)
Time-Protocol(31)
FFT(32)
Autodiscovery (33)
Show(34)
Replace-Licence-Key(35)
VLAN-Table
VLAN-Port-Table
Show(36)
Add(37)
Edit(38)
Remove(39)
Show(40)
Add(41)
Edit(42)
Remove(43)

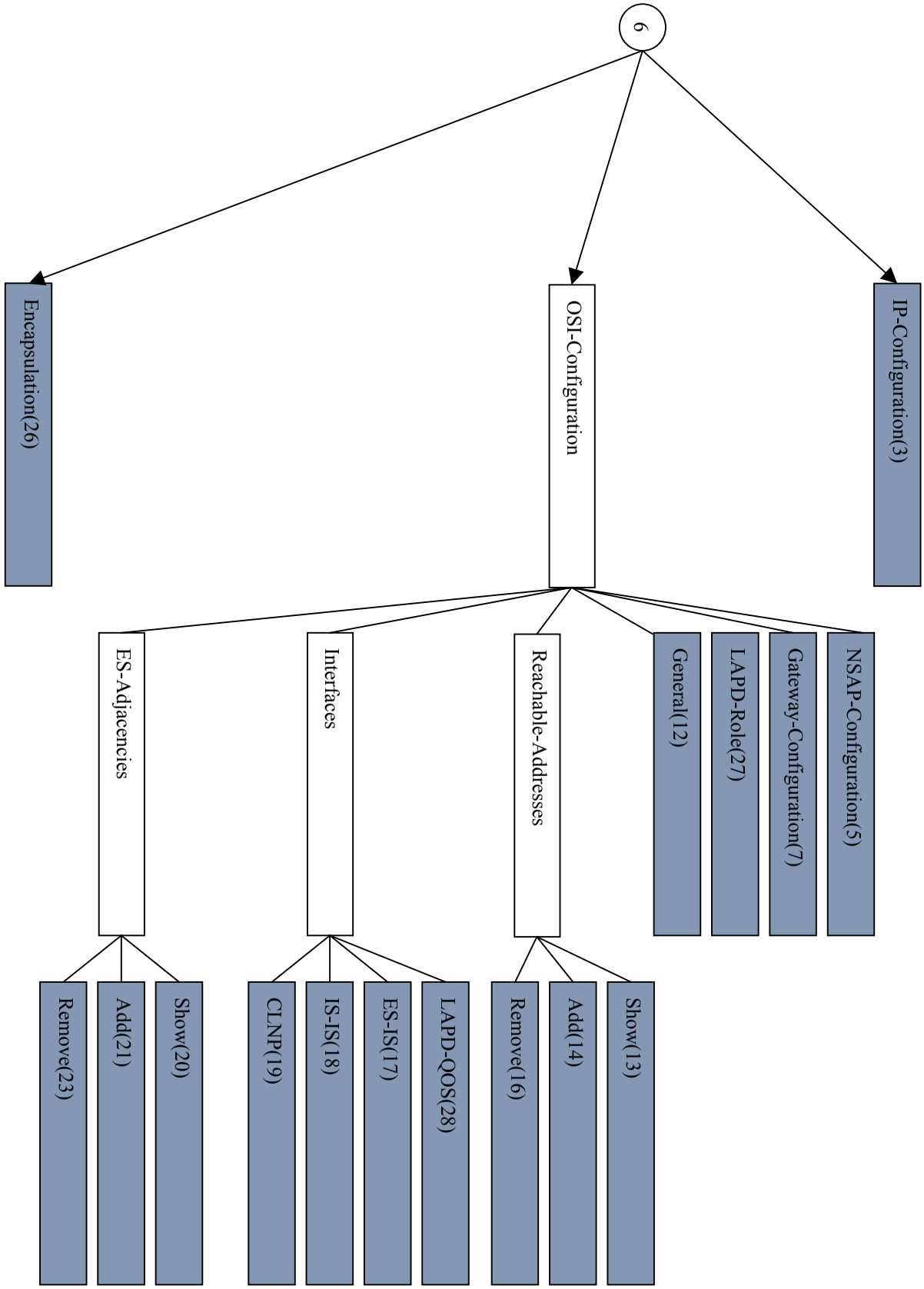

1
Management-Mode(1)
IP-Management-Port
IP-Configuration(2)
DCC-M-IP-Broadcast
MAC-Filter(4)
IP-Configuration(2)
DCC-R-IP-Broadcast
MAC-Filter(4)
IP-Configuration(2)
DCC-M-OSI-Encapsulation
2
DCC-R-OSI-Encapsulation
2
Custom
3

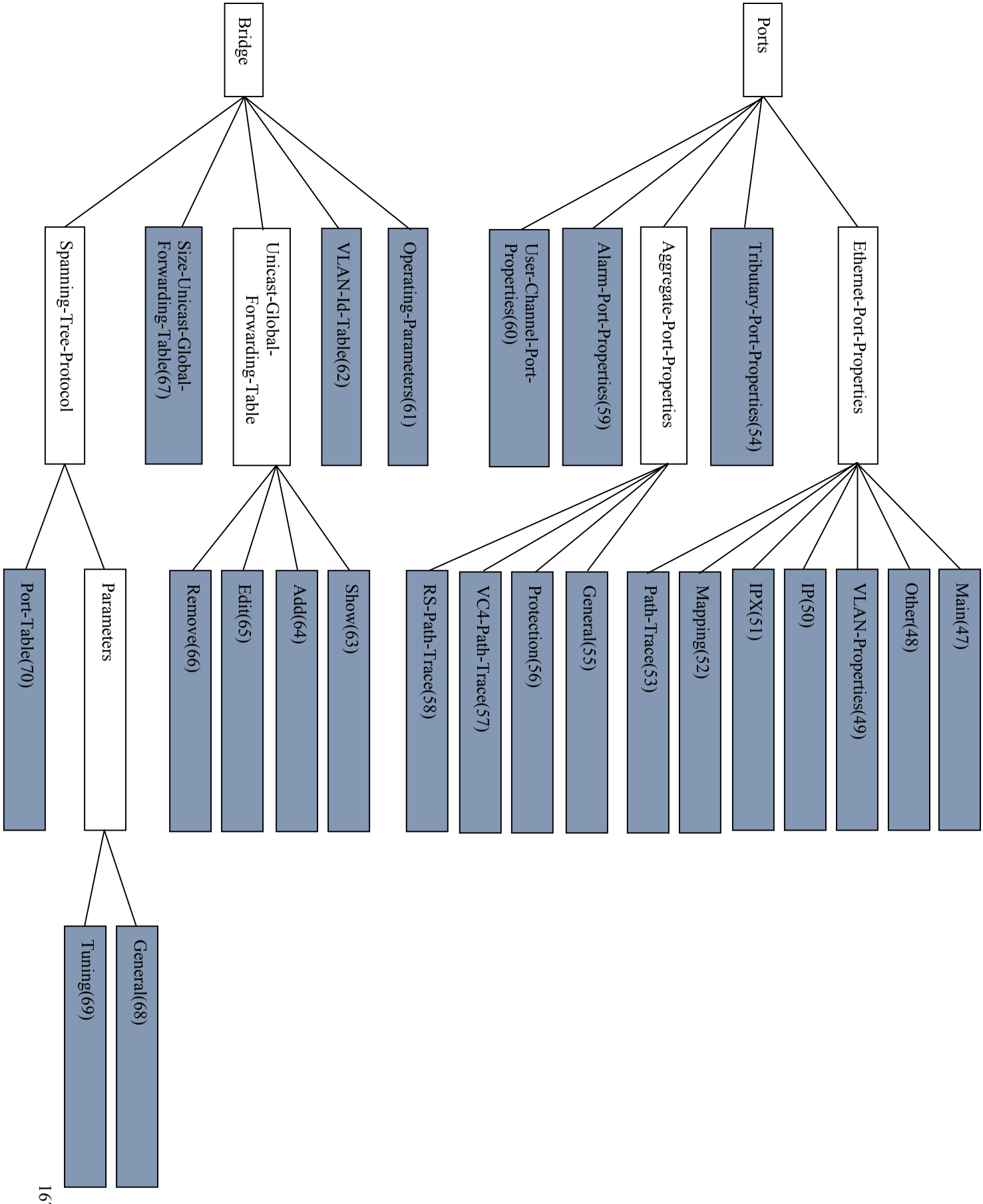

2
OSI-Configuration
IP-Configuration(3)
Management-Port
LAPD-Configuration(8)
Gateway-Configuration(6)
NSAP-Configuration(5)
IP-and-OSI-Encapsulation
OSI-Encapsulation
IP-Configuration(2)
Mode(9)
5
4

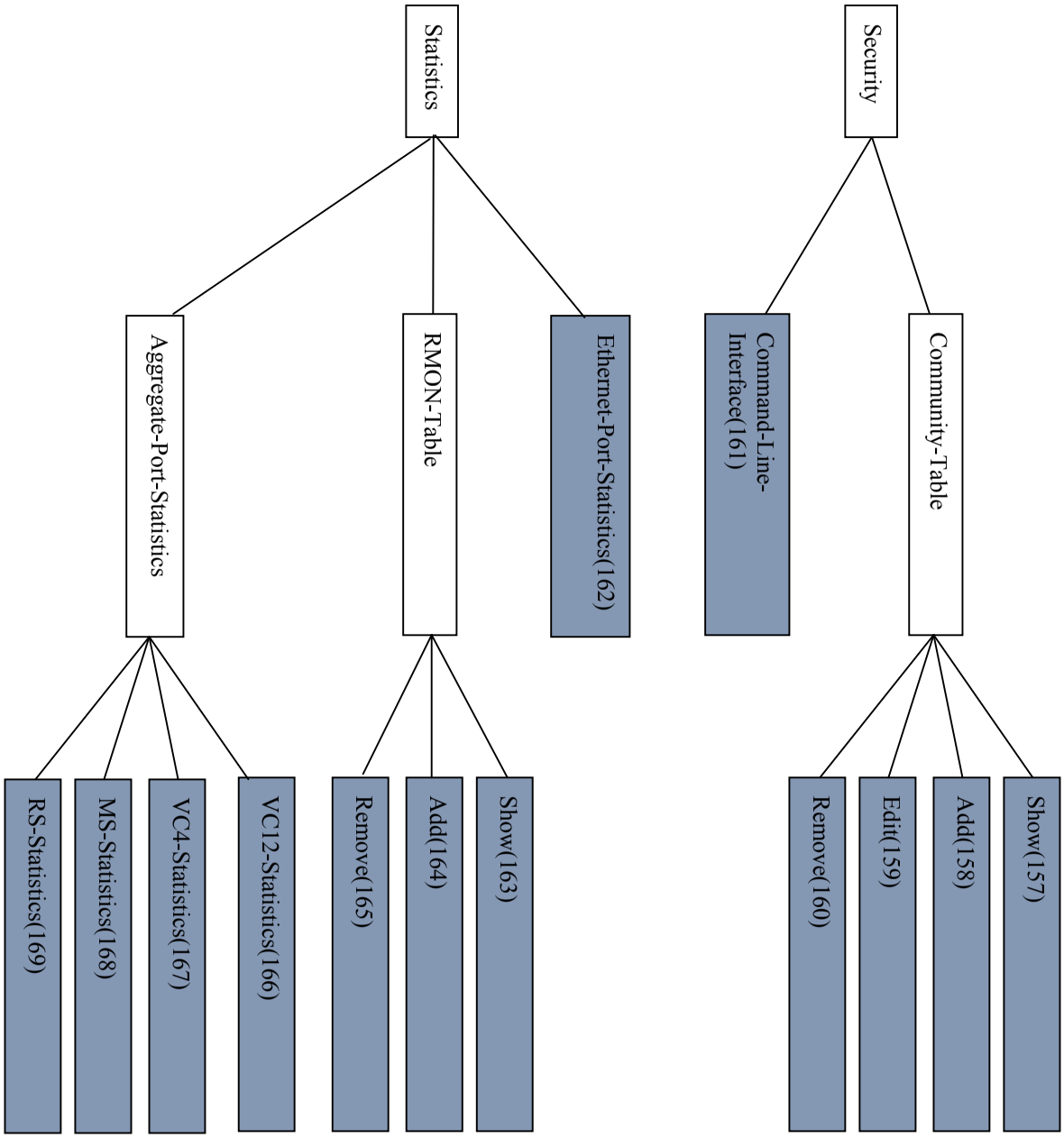

3
A-DCC-M
A-DCC-R
B-DCC-M
B-DCC-R
IP-Broadcast
OSI-Encapsulation
IP-Configuration(2)
MAC-Filter(4)
6

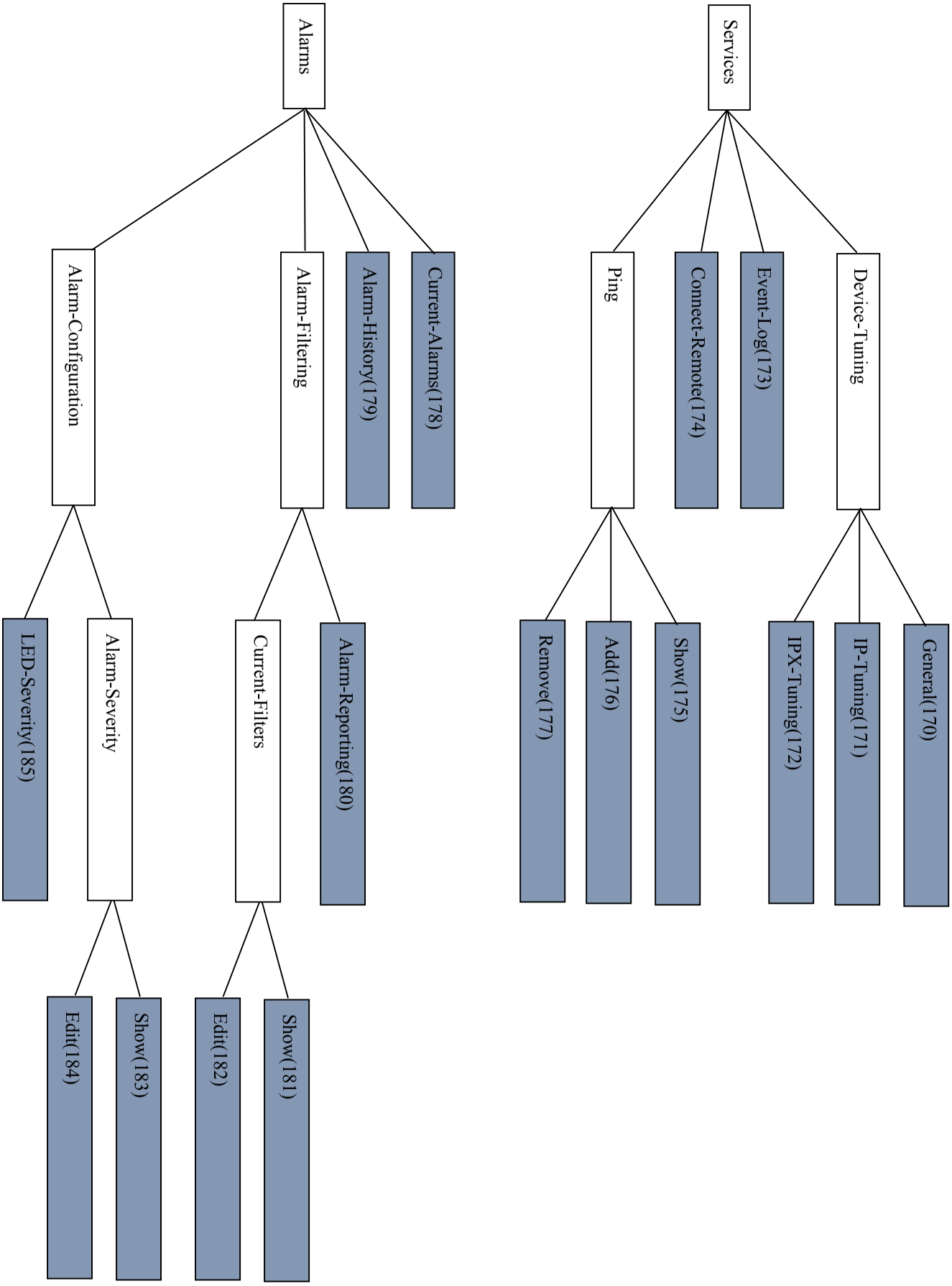

4
IP-Configuration(3)
OSI-Configuration
NSAP-Configuration(5)
Gateway-Configuration(7)
General(12)
Reachable-Addresses
Interfaces
ES-Adjacencies
Show(13)
Add(14)
Edit(15)
Remove(16)
ES-IS(17)
IS-IS(18)
CLNP(19)
Show(20)
Add(21)
Edit(22)
Remove(23)


5
Encapsulation(26)
OSI-Configuration
OSI-IP-Configuration
Ethernet-IP-Configuration
ES-Adjacencies
Interfaces
Reachable-Addresses
General(12)
Gateway-Configuration(7)
NSAP-Configuration(5)
IP-Configuration(25)
IP-Configuration(24)
Remove(23)
Edit(22)
Add(21)
Show(20)
CLNP(19)
IS-IS(18)
ES-IS(17)
Remove(16)
Edit(15)
Add(14)
Show(13)


6
Encapsulation(26)
OSI-Configuration
IP-Configuration(3)
ES-Adjacencies
Interfaces
Reachable-Addresses
General(12)
LAPD-Role(27)
Gateway-Configuration(7)
NSAP-Configuration(5)
Remove(23)
Add(21)
Show(20)
CLNP(19)
IS-IS(18)
ES-IS(17)
LAPD-QOS(28)
Remove(16)
Add(14)
Show(13)


Ports
Ethernet-Port-Properties
Main(47)
Other(48)
VLAN-Properties(49)
IP(50)
IPX(51)
Mapping(52)
Path-Trace(53)
Tributary-Port-Properties(54)
Aggregate-Port-Properties
General(55)
Protection(56)
VC4-Path-Trace(57)
RS-Path-Trace(58)
Alarm-Port-Properties(59)
User-Channel-Port-Properties(60)
Bridge
Operating-Parameters(61)
VLAN-Id-Table(62)
Unicast-Global-Forwarding-Table
Show(63)
Add(64)
Edit(65)
Remove(66)
Size-Unicast-Global-Forwarding-Table(67)
Spanning-Tree-Protocol
Parameters
General(68)
Tuning(69)
Port-Table(70)


Statistics
Aggregate-Port-Statistics
RMON-Table
Ethernet-Port-Statistics(162)
RS-Statistics(169)
MS-Statistics(168)
VC4-Statistics(167)
VC12-Statistics(166)
Remove(165)
Add(164)
Show(163)
Security
Command-Line-Interface(161)
Community-Table
Remove(160)
Edit(159)
Add(158)
Show(157)


Services
Ping
Connect-Remote(174)
Event-Log(173)
Device-Tuning
Remove(177)
Add(176)
Show(175)
IPX-Tuning(172)
IP-Tuning(171)
General(170)
Alarms
Alarm-Configuration
Alarm-Filtering
Alarm-History(179)
Current-Alarms(178)
LED-Severity(185)
Alarm-Severity
Current-Filters
Alarm-Reporting(180)
Edit(184)
Show(183)
Edit(182)
Show(181)

Command	Parameters
1. Management-Mode	[MODE=< ipManagementPort | ipBroadcastDccR | ipBroadcastDccM | osiEncapsulationDccR | osiEncapsulationDccM | customise >]
2. IP-Configuration	[IP-ADDRESS=<IP address>][SUBNET-MASK=<IP address>] [DEFAULT-GATEWAY=<IP address>]
3. IP-Configuration	[OSI-IP-ADDRESS=<IP address>][OSI-SUBNET-MASK=<IP address>] [OSI-DEFAULT-GATEWAY=<IP address>]
4. MAC-Filter	[MAC-FILTER-SWITCH=<enabled | disabled>]
5. NSAP-Configuration	[AREA-ADDRESS-LIST=<areaAddressList>] [SYSTEM-ID=<system id>] [NSEL=<selector>]
6. Gateway-Configuration	[NSAP=<NSAP address>]
7. Gateway-Configuration	[NSAP=<NSAP address>] [STATUS=<enabled | disabled>]
8. LAPD-Configuration	[PORT-A-LAPD-ROLE=<network | user>] [PORT-B-LAPD-ROLE=<network | user>]
9. Mode	[MODE=<notUsed | ip | clnp |ipAndClnp>]
10.	
11.	
12. General	[L1-LSP=<integer>] [L2-LSP=<integer>] [IS-MODE=<disable|is|l1Is|l2Is>]
13. Show	
14. Add	PREFIX=<Area address> [SNPA=<mac address>]
15. Edit	PREFIX=<Area address> [SNPA=<mac address>]
16. Remove	PREFIX=<Area address>
17. ES-IS	[STATUS=<enabled | disabled>] [ES-HOLD-TIMER=<integer>] [ES-REPORT-TIMER=<integer>] [IS-HOLD-TIMER=<integer>] [IS-REPORT-TIMER=<integer>] [SUGGESTED-TIMER=<integer>]
18. IS-IS	[STATUS=<enabled | disabled>] [L1-METRIC=<integer>] [L2-METRIC=<integer>] [CIRCUIT-OUTSIDE-DOMAIN=< true | false>] [IS-IS-HELLO-TIMER=<integer>] [L1-DIS-PRIORITY=<integer>] [L2-DIS-PRIORITY=<integer>] [ES-IIH-TIMER=<integer>]
19. CLNP	[MAXIMUM-CLNP-PDU-LIFETIME=<integer>] [MAXIMUM-CLNP-REASSEMBLY-TIME=<integer>]
20. Show	
21. Add	NSAP=<NSAP address> [SNPA=<mac address>]
22. Edit	NSAP=<NSAP address> [SNPA=<mac address>]
23. Remove	NSAP=<NSAP address>
24. IP-Configuration	[IP-ADDRESS=<IP address>][SUBNET-MASK=<IP address>]
25. IP-Configuration	[OSI-IP-ADDRESS=<IP address>][OSI-SUBNET-MASK=<IP address>]
26. Encapsulation	[NE-MAX-AGE=<integer>] [AMT-TIMER=<integer>] *or* [HELLO-INTERVAL=<integer>] [1]
27. LAPD-Role	[ROLE=<network | user>]

Command	Parameters
28. LAPD-QOS	[QOS=<aits | uits>]
29. Identification	[NAME=<string>] [LOCATION=<string>] [CONTACT=<string>]
30. Time	[TIME=<time>] [DATE=<date>]
31. Time-Protocol	[SERVER-IP-ADDRESS=<ip-address>] [SYNC-INTERVAL=<integer>] [UTC-DELTA=<integer>]
32. FFT	[IP-FASTFORWARDING=<enable|disable>] [IPX-FASTFORWARDING=<enable|disable>]
33. Autodiscovery	[STATUS=<enabled|disabled>] [TRAP-FREQUENCY=<integer>]
34. Show	<none>
35. Replace-Licence-Key	LICENCE-KEY=<string>
36. Show	[VLAN-NUMBER=<integer>]
37. Add	NAME=<string> [ADDRESS-TYPE=<default|reserve>] [TAG=<integer>]
38. Edit	VLAN-NUMBER=<integer> [NAME=<string>] [ADDRESS-TYPE=<default|reserve>] [TAG=<integer>]
39. Remove	VLAN-NUMBER=<integer>
40. Show	[VLAN-NUMBER=<integer>]
41. Add	VLAN-NUMBER=<integer> ETHERNET-PORTS=<portList> [TAGGING=<enable|disable>]
42. Edit	VLAN-NUMBER=<integer> ETHERNET-PORTS =<portList> TAGGING=<enable|disable>
43. Remove	VLAN-NUMBER=<integer> ETHERNET-PORTS =<portList>
44. Sync-Source	[ADMINISTRATIVE-SOURCE=<local|trib1|trib2|trib3|trib4|aggr1| external| aggr2|activeAggr>]
45. Inventory	<none>
46. Remote-Device-Identification	[REMOTE-DEVICE=<IP address>]
47. Main	[ETHERNET-PORT=<port>] [SPEED-ADMIN-MODE=<10M|100M>] [ADMINISTRATIVE-STATUS=<on|off>] [DESCRIPTION=<string>] [DUPLEX-ADMIN-MODE=<none|half|full>] [PHYSICAL-ADDRESS-ASSIGNMENT=<default|reserve>] [AUTONEGOTIATION-MODE=<enabled|disabled>]
48. Other	[ETHERNET-PORT=<port>] [BACK-PRESSURE-MODE=<enable|disable>] [FLOW-CONTROL-MODE=<on|off|autoNegotiation>]
49. VLAN-Properties	[ETHERNET-PORT=<port>]
50. IP-Properties	[ETHERNET-PORT=<port>]
51. IPX-Properties	[ETHERNET-PORT=<port>]
52. Mapping	[ADMINISTRATIVE-CAPACITY=<integer>]
53. Path-Trace	[PATH-TRACE=<enabled|disabled>] [EXPECTED-TI=<string>] [TRANSMIT-TI=<string>]

Command	Parameters
54. Tributary-Port-Properties	[TRIBUTARY-PORT=<port>] [DESCRIPTION=<string>] [ADMINISTRATIVE-STATUS=<enable|disable>] [MODE=<TRA|PRA>] [LOOP-MODE=<NONE|LL2|LL3>] [PATH-TRACE=<enabled|disabled>] [EXPECTED-TI=<string>] [TRANSMIT-TI=<string>] [MONITORING-STATUS=<ENABLED|DISABLED>]
55. General	AGGREGATE-PORT=<port> [ADMINISTRATIVE-STATUS=<enable|disable>] [DESCRIPTION=<string>] [CONNECTED-TO=<string>]
56. Protection	[MSP-STATUS=<enabled|disabled>] [PROTECTION-TYPE=<unidirectional|bidirectional>] [REVERTING-STATUS=<enabled|disabled>] [WAIT-TO-RESTORE-TIME=<integer>] [SWITCHING-COMMAND=<clear|exercise|manualSwitchToProtecting|manualSwitchToWorking| forcedSwitchToProtecting|forcedSwitchToWorking|lockoutProtection>]
57. VC4-Path-Trace	[STATUS=<choice>] [EXPECTED-TI=<string>] [TRANSMIT-TI=<string>]
58. RS-Path-Trace	AGGREGATE-PORT=<port> [STATUS=<choice>] [EXPECTED-TI=<string>] [TRANSMIT-TI=<string>]
59. Alarm-Port-Properties	[ALARM-PORT=<port>] [MODE=<enabled|disabled>] [DESCRIPTION=<string>] [TRIGGERED-WHEN=<yes|no>]
60. User-Channel-Port-Properties	[DESCRIPTION=<string>] [AGGREGATE-PORT=<integer>] [DATA-RATE=<sync64000|async19200>]
61. Operating-Parameters	<none>
62. VLAN-Id-Table	ETHERNET-PORT=<port>
63. Show	<none>
64. Add	VLAN-ID=<integer> MAC-ADDRESS=<MAC address> ETHERNET-PORT=<port> [STATUS=<permanent|deleteOnReset>]
65. Edit	VLAN-ID=<integer> MAC-ADDRESS=<MAC address> ETHERNET-PORT=<port> [STATUS=<permanent|deleteOnReset>]
66. Remove	VLAN-ID=<integer> MAC-ADDRESS=<MAC address> ETHERNET-PORT=<port>
67. Size-Unicast-Global-Forwarding-Table	<none>
68. General	[STATUS=<true|false>] [BELONG-TO-VLAN=<true|false>] [PRIORITY=<integer>] [MAX-AGE=<integer>] [HELLO-TIME=<integer>] [FORWARD-DELAY=<integer>]
69. Tuning	<none>
70. Port-Table	[ETHERNET-PORT=<port>] [PRIORITY=<integer>] [ENABLE=<enabled|disabled>] [PATH-COST=<integer>]
71.	
72.	
73. Show	[IP-ADDRESS=<IP address>]
74.	
75.	

Command	Parameters
76.	
77.	
78.	
79.	
80.	
81.	
82.	
83.	
84.	
85.	
86.	
87.	
88.	
89.	
90.	
91.	
92.	
93.	
94.	
95.	
96.	
97.	
98.	
99.	
100.	
101.	
102.	
103.	
104.	
105.	
106.	
107.	
108.	

Command	Parameters
109.	
110.	
111.	
112.	
113.	
114.	
115.	
116.	
117.	
118.	
119.	
120.	
121.	
122.	
123.	
124.	
125.	
126.	
127.	
128.	
129.	
130.	
131.	
132.	
133.	
134.	
135.	
136.	
137.	
138.	
139.	
140.	
141.	

Command	Parameters
142.	
143.	
144.	
145.	
146.	
147.	
148.	
149.	
150.	
151.	
152.	
153.	
154.	
155.	
156.	
157. Show	[MANAGER=<IP address>]
158. Add	MANAGER=<IP address> COMMUNITY=<string> ACCESS=<readOnly|readWrite|super> TRAPS=<enable|disable>
159. Edit	MANAGER=<IP address> COMMUNITY=<string> [ACCESS=<readOnly|readWrite|super>] [TRAPS=<enable|disable>]
160. Remove	MANAGER=<IP address> COMMUNITY=<string>
161. Command-Line-Interface	[AXXCLI-PASSWORD=<string>] [TELNET-PASSWORD=<string>] [DISPLAY-LINES=<integer>] [ALLOW-MESSAGES=<YES|NO>]
162. Ethernet-Port-Statistics	ETHERNET-PORT=<port>
163. Show	<none>
164. Add	ETHERNET-PORT=<port>
165. Remove	ETHERNET-PORT=<port>
166. VC12-Statistics	KLM=<KLM>
167. VC4-Statistics	<none>
168. MS-Statistics	AGGREGATE-PORT=<port>
169. RS-Statistics	AGGREGATE-PORT=<port>
170. General	[BRIDGE-MAX-ENTRIES-AFTER-RESET=<integer>] [RMON-MAX-ENTRIES-AFTER-RESET=<integer>]

175

Command	Parameters
171. IP-Tuning	[IP-RIP-MAX-ENTRIES-AFTER-RESET=<integer>] [ARP-FORWARDING-MAX-ENTRIES-AFTER-RESET=<integer>] [IP-FFT-MAX-ENTRIES-AFTER-RESET=<integer>] [DHCP-MAX-CONNECTION-AFTER-RESET=<integer>] [IP-FFT-UPPER-LIMIT=<integer>] [IP-FFT-LOWER-LIMIT=<integer>]
172. IPX-Tuning	[IPX-RIP-MAX-ENTRIES-AFTER-RESET=<integer>] [IPX-SAP-MAX-ENTRIES-AFTER-RESET=<integer>] [IPX-FFT-MAX-ENTRIES-AFTER-RESET=<integer>] [IPX-FFT-UPPER-LIMIT=<integer>] [IPX-FFT-LOWER-LIMIT=<integer>]
173. Event-Log	<none>
174. Connect-Remote	<none>
175. Show	[IP-ADDRESS=<IP address>]
176. Add	IP-ADDRESS=<IP address> [COUNT=<integer>] [SIZE=<integer>] [TIMEOUT=<integer>] [DELAY=<integer>]
177. Remove	IP-ADDRESS=<IP address>
178. Current-Alarms	<none>
179. Alarm-History	<none>
180. Alarm-Reporting	[ALARM-REPORTING=<enabled|disabled>]
181. Show	[OBJECT-TYPE=<DEVICE|ALARM|TRIB|SPI|RST|MST|MSP|VC-4|AU-4|TU-12|VC-12>]
182. Edit	OBJECT-TYPE=<DEVICE|ALARM|TRIB|SPI|RST|MST|MSP|VC-4|AU-4|TU-12|VC-12> [PORT=<port>] [ALARM-REPORTING=<enabled|disabled>] [PERSISTENCY-ON=<integer>] [PERSISTENCY-OFF=<integer>] [SD-THRESHOLD=<integer>] [AIS=<enabled|disabled>] [RDI=<enabled|disabled>]
183. Show	[ALARM-ID=<alarmId>]
184. Edit	ALARM-ID=<alarmId> ALARM-POINT=<unknownAlarmPoint|device|sdhPhysical|rst|mst|msp|au4|vc4|tu12|vc12|trib|aux|ethernet> [SEVERITY=< critical|major|minor|warning>] [DESCRIPTION=<string>]
185. LED-Severity	[CUSTOMER-LED-MIN-SEVERITY=<critical|major|minor|warning>] [OPERATOR-LED-MIN-SEVERITY=<critical|major|minor|warning>]

[1] Depending upon whether the device is a gateway or not.