AXX155E R3.0

Technical Reference

61009-01CA

AXXESSIT

Notification List

AXXTMN

Desktop

Management Tree

AXXCRAFT

Alarms

Events

DCC

Layer 3

OSI

IP

Layer 2

Download

Configuration

Slot

PDH

Ports

SDH

LAN

MSP

Synchronization

Cross Connections

WAN

Troubleshooting

VLAN

FAQ

Link Aggregation

IPX

IPM

Performance

Credits
This technical reference could not have been created without the help from people involved in developing the AXX155E.

V.Sebjørnsen
Technical author

Copyright

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 merchant ability 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.

Occurrence of **blank pages** are intentionally,
to accommodate double-sided printing.

AXXESSIT

Notification List
AXXTMN
Desktop
Management Tree
AXXCRAFT
Alarms
Events
DCC
Layer 3
OSI
IP
Layer 2
Download
Configuration
Slot PDH
Ports
SDH LAN
MSP
Synchronization
Cross Connections
WAN
Troubleshooting
VLAN FAQ
Link Aggregation
IPX
IPM
Performance

INSTALLATION OF AXX155E 1-1

MANAGED OBJECTS 6-1

GLOSSARY 9-1

Installation of AXX155E

System Overview

Features

Physical Interfaces

Mechanics & other Characteristics

Managed Objects

BOOTP Application Note

AXXCLI Command Hierarchy

Glossary

Installation of AXX155E

System Overview

Features

Physical Interfaces

Mechanics & other Characteristics

Managed Objects

BOOTP Application Note

AXXCLI Command Hierarchy

Glossary

1

INSTALLATION OF AXX155E

AXX155E

1.1 ABOUT THIS DOCUMENT

1.1.1 Objective

The purpose of this Technical Reference is to describe the integrated access device AXX155E.

After reading this Technical Reference, the user shall be able to install, configure and to put the AXX155E into service.

The AXX155E Command Line Interface management solution is an integral part of this Technical Reference.

Operation and management of AXX155E utilising the GUI based configuration tool AXXCRAFT and the higher-level management systems within the AXXTMN portofolio is described in their respective User Guides.

Audience

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

Document overview

The latest edition of this Technical Reference is delivered on a CD for each shipped unit, but since this document is frequently updated we recommend to check the Support WEB to make sure you have the latest release at all times.

Recommended reading

There are a number of documents, which can be useful to read to fully understand the functionality and operation of the AXX155E.

The Ethernet Engineering Guideline for AXX155E and the AXXCRAFT/AXXINSITE User Guides can be considered as supplements to this manual. These documents can be downloaded from our support web (www.axxessit.no).

Conventions

This Technical Reference describes the AXX155E 12x2 Mbit/s + Ethernet Bridge transmission system.

In SDH terminology the AXX155E is a terminal multiplexer.

1.2 PRE-INSTALLATION PROCEDURES

This chapter provides pre-installation procedures for the AXX155E.

1.2.1 Shipment verification

When the AXX155E equipment is received, please verify that the shipment is according to order.

NOTE! *Ship equipment from one site to another in the original packing including the antistatic bags.*

NOTE! *Keep the AXX155E system equipment in the original shipping containers if storage is required. Storage more than 12 months is not recommended. The equipment should be stored in a ventilated and static-safe location.*

1.2.2 Preliminary inventory check

Verify that the packing list information is equal to the information provided on the shipping labels. Please notify contact resource if any discrepancies must be reported.

1.2.3 Reporting damage

Damage to shipped articles must be reported to contact resource. See “Repair and return procedure” on page 1-22.

1.3 SITE PREPARATION

1.3.1 Safety recommendations

The whole installation must be executed without powering the equipment.

Power supply connection must be the last to be executed.

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.

1.3.2 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.

1.3.3 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.

1.3.4 Site requirements

In-door, temperature controlled environment is required.

1.4 UNPACKING

1.4.1 General

Before unpacking the AXX155E, inspect the package and report any evidence of damage immediately.

1.4.2 Unpacking Procedure

1. Place the container on a clean flat surface and cut all straps securing the container.
2. Open the container or remove the container top.
3. Carefully remove the unit from the container and place it on a secure and clean surface.
4. Remove all packing material.
5. Inspect the product for damage. Report any damage immediately.

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.*

1.5 RACK MOUNTING

AXX155E 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 AXXCLI connectors) are available on both sides of AXX155E.

1.5.1 Mounting Procedure

1. Put on an ESD wrist strap and attach the ESD clip to a metal surface to act as ground.
2. Place the AXX155E device on a flat and stable surface.
3. Place the supplied rack-mounting bracket on one side of the AXX155E ensuring the mounting holes on the AXX155E line up to the mounting holes on the rack-mounting bracket. The following figure illustrates the mounting holes lined up.
4. Insert the supplied screws into the rack mounting holes and tighten with a Phillips screwdriver.
5. Repeat the process for the rack-mounting bracket on the other side of the AXX155E device.
6. Insert the unit into the 19-inch rack and secure the unit to the rack with the supplied rack screws. When securing, fasten the lower pair (1) of screws before the upper pair (2) of screws. This ensures that the weight of the unit

is evenly distributed during installation. Ensure that the ventilation holes are not obstructed.

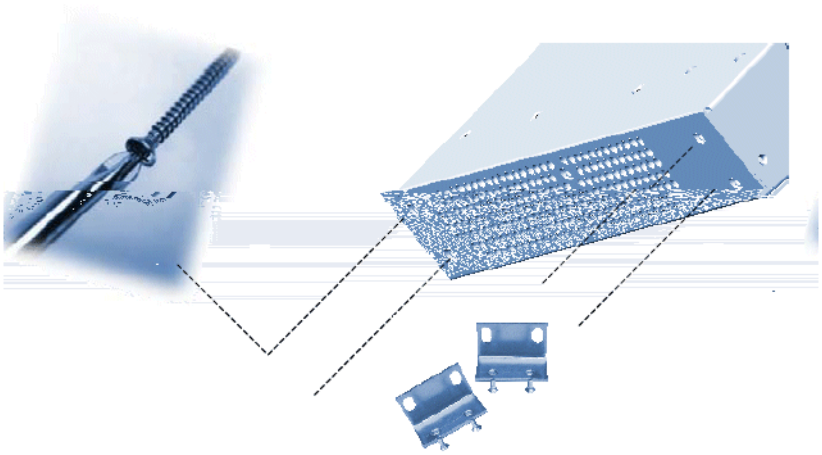


Figure 1-1. Rack-mounting brackets

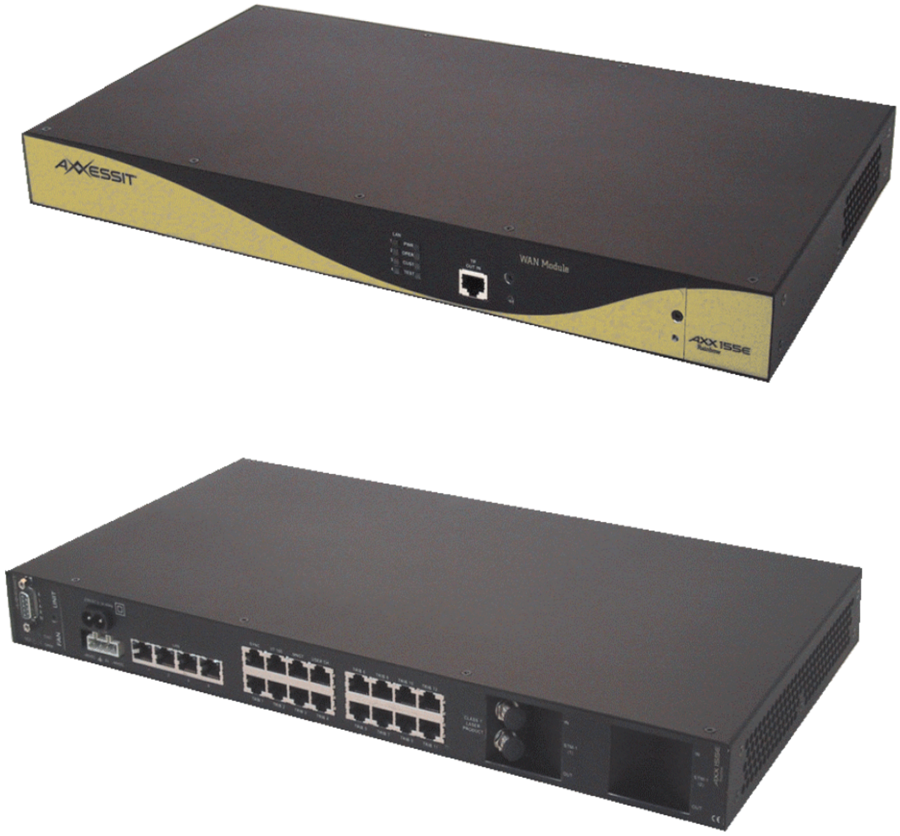


Figure 1-2. AXX155E- front and connector side

1.5.2 Installation in Restricted Access Location (RAL)

The AXX155E can be installed in a restricted access location (RAL) or outside of an RAL.

After installation in a RAL, such as in a telecommunication center, the AXX155E must be properly installed in a rack with brackets or in other ways properly connected to a safety ground.

The AXX155E 48V DC must not be powered from a source external to the RAL. All communication interfaces used must be limited to SELV. E1 interface used should be limited to SELV.

Installation outside of a Restricted Access Location

After installation, the AXX155E 48V power and all communication ports used must be connected to SELV circuits, for example a port on a personal computer or 10/100 Mbit Ethernet hub/router or other Information Technology (IT) equipment.

The 48V DC power must not exceed 60 VDC and must be powered from an certified external power supply unit (PSU) or a battery unit (no connection to -48 V telecom voltage).

The optical ports (if present) has no limitations regarding safety recommendations.

Definitions

Restricted Access Location (RAL)

A location for equipment where both of the following paragraphs apply:

- access can only be gained by service persons or by users who have been instructed about the reasons for the restrictions applied to the location and about any precautions that must be taken; and
- access is through the use of a Tool or lock and key, or other means of security, and is controlled by the authority responsible for the location.

SELV Circuits

SELV Circuits are ports that have maximum DC working voltage level less than 60Volt (42.4 VAC). In addition, the ports must not be connected to telecommunication networks in the EN 60950 meaning of the term (CEI/ IEC 60950-1 2001-10 standard clause 1.2.13.8).

In practice, the electrical cables must not exit the building. In addition, the electrical cables shall connect to equipment that either:

- are installed in RAL or
- shall not have electrical cables that exits the building unless those ports are TNV circuits or
- shall have a written consent or in other ways evident that its connecting port towards the SELV circuit port is not a telecommunication network.

Telecommunication Network

A metallically terminated transmission medium intended for communication between equipment that may be located in separate buildings, excluding:

- the mains system for supply, transmission and distribution of electrical power, if used as a telecommunication transmission medium;
- Cable Distribution System;
- SELV Circuits connecting units of information technology equipment.

TNV Circuit

A circuit which is in the equipment and to which the accessible area of contact is limited and that is so designed and protected that, under normal operating conditions and single fault conditions (CEI/IEC 60950-1 2001-10 standard clause 1.4.14), the voltages do not exceed specified limit values.

1.6 POWER SOURCE PROTECTION

The AXX155E have 2xDC- and 1xAC inputs enabling up to three power sources to be connected simultaneously. Two independent DC supplies can be connected using a single, common cable. Then the 0V inlet can be split and shared and the two -48V inlets should connected to separate DC sources. In case of both AC and DC connected the AXX155 will backup & switch the AC/DC inputs by the following rules: - when DC is less than -52V the AC is the operational source - when DC is between -52 to -60V the load will be shared on AC and DC - when DC is between -60 to -72V the active source is DC.

There are no indications in higher-level management or AXXCLI to see active power source. In case of loosing the active power source, traffic should normally not be disturbed if the removal/loss of supply is controlled and definite. In a worst-case scenario bit-errors may be introduced at the optical aggregate.

1.7 WAN-MODULE INSERTION/ EJECTION

1.7.1 WAN module insertion

1. To prevent electrostatic discharge, put on an ESD wrist strap and attach the ESD clip to a metal surface to act as ground.
2. Power-down the AXX155E device.
3. Unscrew the front panel securing screws and remove it. Store the front panel in a secure location for future use.
4. Make sure that the target slot is clear.
5. Remove the module from its packaging.
6. Using the guide rails, gently slide the switch module into the slot until the back connector is firmly inserted in the slot connectors and the module front panel touches the enclosure frame. Power-up the AXX155E device.

CAUTION! *Ensure the module is correctly lined up with the guide rails before inserting the module into the enclosure.*

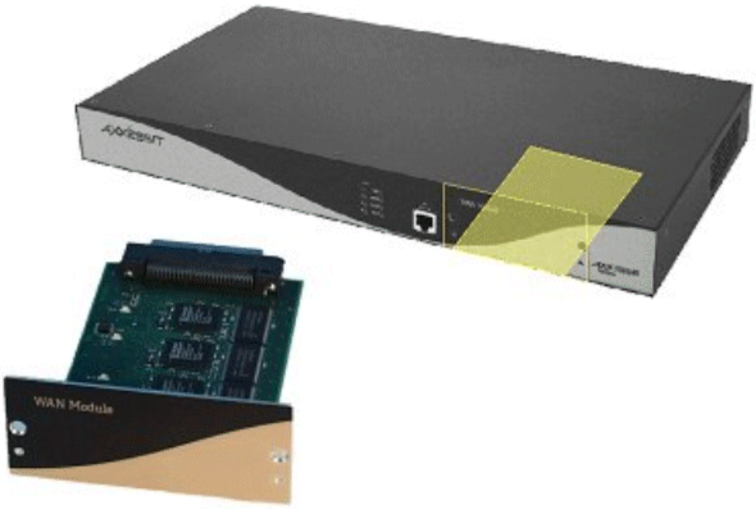


Figure 1-3. WAN module insertion

7. Fasten the two fastening screws on the module front panel, upper holes. To tighten the WAN module firmly, you have to use the two screws to help the insertion of the module the last couple of millimeters

1.7.2 Ejecting the WAN module

1. To prevent electrostatic discharge, put on an ESD wrist strap and attach the ESD clip to a metal surface to act as ground.
2. Power-down the AXX155E device. Unscrew the two fastening screws on the WAN module front panel.
3. Fasten the two fastening screws on the WAN module front panel, but now use the bottom holes. Tighten the screws gently on each side, until the WAN module loosens.
4. Gently pull out the WAN module. Power-up the AXX155E device.

1.8 AXX155E - 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 AXX155E in a rack, it is recommended to separate guiding of electrical and optical cables. Viewed from the rear side of the AXX155E , 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 W balun, it is normally fixed along the cable duct using tie-wraps.

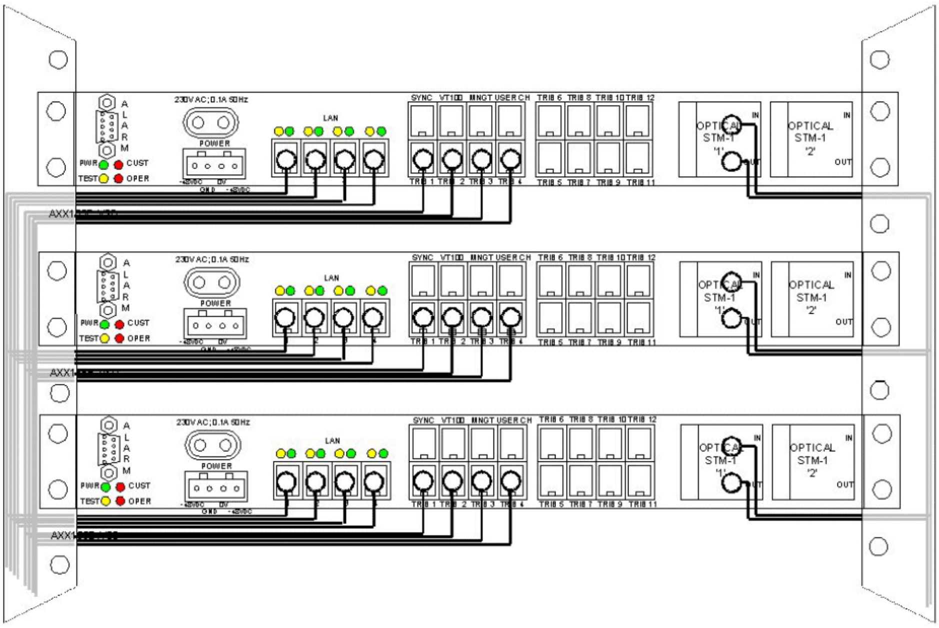


Figure 1-4. Cabling principle

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 orSM fibre according to ITU-T G.652
VT.100 ('AXXCLI)	1	UTP Cat 1
ALARM	1	UTP
SYNC	1	UTP

Table 1.1. Recommended cable types

1.9 INITIAL CONFIGURATION

By following the guides below you should be able to do the most important configurations of AXX155E.

Factory pre-configuration

Since the AXX155E is a flexible product with a lot of possible network applications the factory pre-configuration is limited when delivered. The Ethernet-ports 1-5 are members of VLAN 1, the aggregate (STM-1) is enabled and one VC-12 container is allocated to the Ethernet WAN-port number 5. In addition an entry in the SNMP community-table is pre-configured so that when an IP-address is assigned, the AXX155E it is possible to take advantage of AXXCRAFT. This configuration persists, regardless of whether the WAN-module is inserted or not.

The factory settings can also be restored by use of the AXXCLI command:

```
AXXCLI>Device\Factory-Reset
```

This command will only restore the factory settings properly if the configuration is cleared before the command is given. To make sure reset configuration is done, following line appears on the system terminal when Factory-Reset command is given:

```
Are device configuration) erased (y/n)?
```

Follow the next steps in this chapter to perform initial configuration of AXX155E:

- System-Mode
- Assign IP address
- Define SNMPv1 community
- Erase a community string

Assign an IP-address to the AXX155E

The AXX155E supports remote management solutions by the means of Telnet and SNMP .The possibilities as regards connectivity can be rather advanced for the AXX155E so the only explained solution in this document is when directly connected the management-port (MNGT). For more information please refer the Technical Reference.

To achieve one of the above mentioned management solutions it is necessary to assign an IP-address, subnet-mask and if required a default-gateway address must be defined.

System Mode

From Axx155ER3.0 on, an additional management mode, system mode is added. System mode has two options ip and ipunnumbered.

```
AXXCLI>...\Management-Configuration\sys ?


Usage:
   System-Mode
[SYSTEM-MODE=<ip|ipunnumbered>]
```

System Mode - IP

```
AXXCLI>...\Management-Configuration\sys sys=ip
Change management configuration, are you sure? (y/n)?
```

Assign an IP-address:

If system mode is ip the command for IP configuration is:

```
AXXCLI>Device\Management-Configuration\Management-Port\IP-
Configuration IP-ADDRESS=193.69.136.104, SUBNET-
MASK=255.255.255.0.
```

System Mode - IP Unnumbered

```
AXXCLI>...\Management-Configuration\sys sys=ipunnum
Change management configuration, are you sure? (y/n)?
```

Assign an IP-address:

If system mode is ipunnumbered the command for IP configuration is:

```
AXXCLI>Device\Management-Configuration\IP-Configuration IP-
ADDRESS=193.69.136.104, SUBNET-MASK=255.255.255.0.
```

For most commands, if no parameters are supplied then all the current parameter values are displayed, so that the command

```
AXXCLI>Device\Management-Configuration\IP-Configuration
```

or

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

depending on the system mode, 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 no router licence>
```

Command:

```
AXXCLI>Device\Management-Configuration\Custom\Management-
Port\IP-Configuration ip-address=10.0.0.1 subnet-
mask=255.255.255.0 default-gateway=10.0.0.254         "Enter"


IP-ADDRESS:       10.0.0.1
SUBNET-MASK:      255.255.255.0
DEFAULT-GATEWAY:  10.0.0.254
```

NOTE *The availability of assigning a default gateway IP-address depends on whether you have loaded a L3-license or not. If L3-routing is enabled on the device, all routes is managed in the routing-table.*

Define SNMPv1 Community

Factory pre-configured community:

```
Manager: 0.0.0.0
Community:public
Access:Super
Traps:Disabled
```

This is an insecure community, which enables all managers regardless of the IP-address for the SNMP manager to access the device with the community string "public".

To add your own community string please use the following command:

```
AXXCLI>Security\Community-Table\add manager=10.0.0.20
community=admin access=super traps=enable "Enter"
```

Erase a Community string

To remove a community string the following command can be used:

```
AXXCLI>Security\Community-Table\remove manager=0.0.0.0
community=public"Enter"
```

1.10 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 AXX155E. 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.

1.10.1 Steps 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.

```
AXXCLI>DEVICE\>reset
```

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 the Startup menu :

Enter "**1**" immediately.

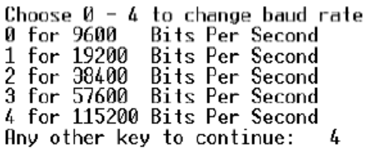
NOTE! *If you are to slow entering "1" the device will continue the boot process and you will have to reboot again.*

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.



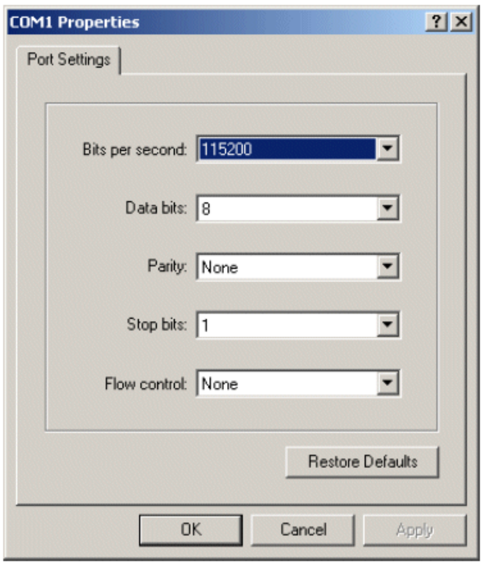
```
Choose 0 - 4 to change baud rate
0 for 9600   Bits Per Second
1 for 19200  Bits Per Second
2 for 38400  Bits Per Second
3 for 57600  Bits Per Second
4 for 115200 Bits Per Second
Any other key to continue:   4
```

Figure 1-5. X-Modem- example

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.



COM1 Properties

Port Settings

Bits per second: 115200

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

Figure 1-6. COM Properties

Step 6

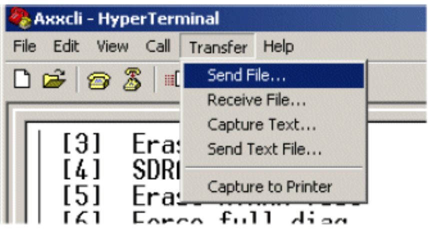
When setup is correct the following message will appear in terminal window:

```
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**.



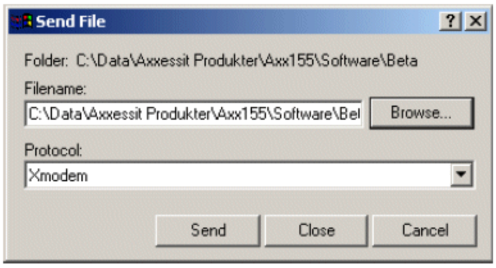
```
[3] Eras
[4] SDRI
[5] Eras
[6] Force full diag
```

Figure 1-7. AXXCLI Transfer menu

Select **directory** containing the software

Choose **Xmodem**

Press **Send**


Send File

Folder: C:\Data\Axxessit Produkter\Axx155\Software\Beta

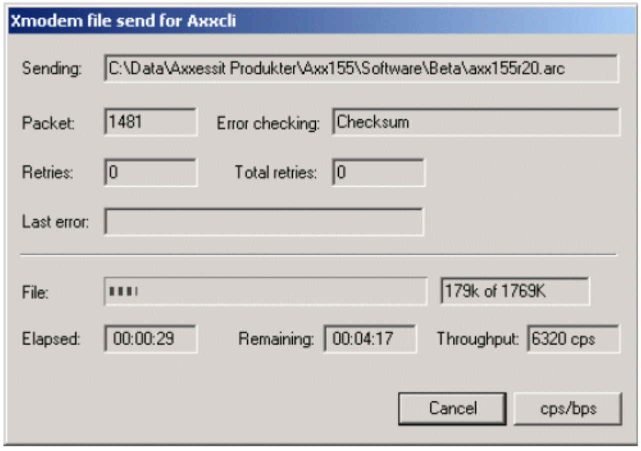
Filename: C:\Data\Axxessit Produkter\Axx155\Software\Bet

Protocol: Xmodem

Figure 1-8. AXXCLI send file - example

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

field "Remaining"



Xmodem file send for Axxcli

Sending: C:\Data\Axxessit Produkter\Axx155\Software\Beta\axx155r20.arc

Packet: 1481 Error checking: Checksum

Retries: 0 Total retries: 0

Last error:

File: 179k of 1769K

Elapsed: 00:00:29 Remaining: 00:04:17 Throughput: 6320 cps

Figure 1-9. X- modem file send for AXXCLI - example

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 a specific license-key may be required for each device. The key can be ordered and sent per e-mail.

1.11 REPAIR AND RETURN PROCEDURE

1.11.1 General

All our equipment and parts are warranted against defects in material and workmanship for a period as agreed in the order or general agreement.

All faulty parts (equipment, units, modules, boards etc.) returned must have the AXX - Service & Repair Form enclosed in printed format or sent by e-mail. Latest edition of the form can be downloaded from our web site. This required that login for support web is provided.

The intension for this procedure is to inform and explain how Repair & Return should be handled from both yours and ours side. We assume that all general terms for repair in general agreements are already well known. Typically price information for repair and contact information to your Customer Service Manager will be stated there. Following this procedure will benefit quality of response and handling by AXXESSIT.

NOTE! *The instructions above are significant to customers of AXXESSIT ASA. Other readers of this document are recommended to follow the guidelines as agreed in the order or general agreement with the supplier of the equipment.*

1.11.2 Repair & Return Process

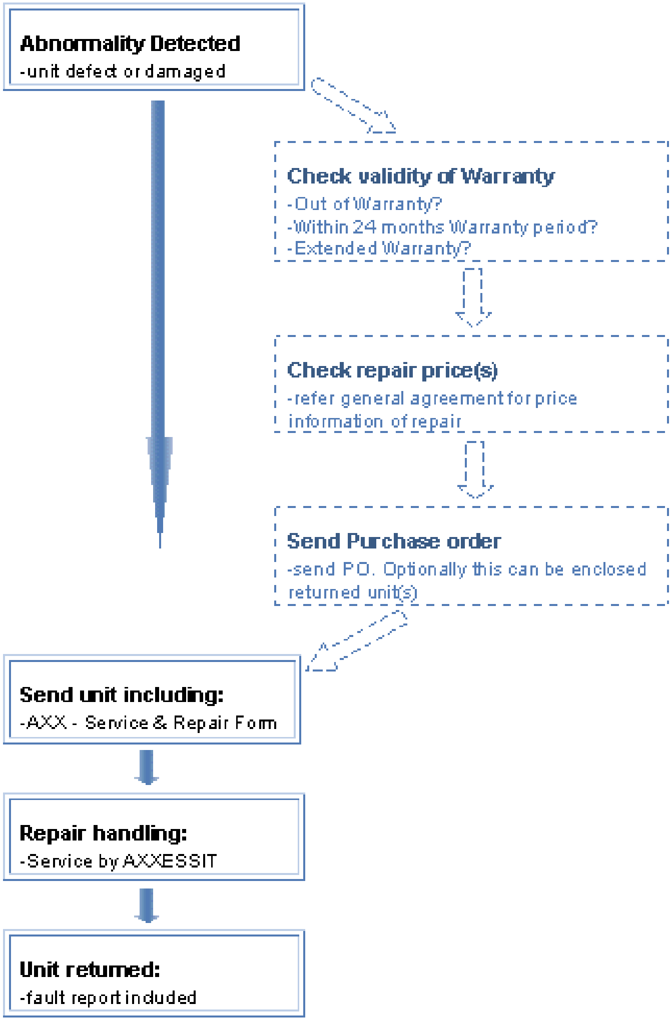


Figure 1-10. Repair & Return Process

1.11.3 Purchase order for out of warranty repair

After receiving modules, with AXX - Service & Repair Form, the unit will be registered and validity of warranty will be verified. If out of warranty we will send a quotation for the repair cost if purchase order for repair not received in advance.

No repairs will be commenced by AXXESSIT until a purchase order for the amount quoted for repair is received through the normal ordering mechanisms outlined in general agreement, which states all contact information for your Customer Service Manager in AXXESSIT.

Items received by AXXESSIT, without a completed AXX - Service & Repair Form, may be placed on hold and no repair actions will be commenced until all the above documentation is completed.

1.11.4 Packaging

When packaging the item please use anti-static bags especially when using foam chips as packing material. Please ensure that the packaging is sufficient to protect the equipment from damage during shipment. Ideally, equipment should be returned in the same packaging it was supplied in.

Any items that are received in a damaged condition, that appears to have arisen from inadequate packing, will be placed on hold until a new quote has been provided to you to cover repair of the additional damage and a purchase order is received by AXXESSIT.

1.12 AXXCLI COMMAND LINE INTERFACE

1.12.1 Introduction

AXXCLI is a line-oriented ASCII-based management interface to AXX155E, by means of which simple commands - possibly with parameters - may be issued to access or modify the AXX155E configuration.

The configuration functionality provided by the AXXCLI closely parallels what can be performed in AXXCRAFT or higher-level management tools e.g. AXXINSITE. Except for lack of sophisticated backup & restore facility the most common operations can be executed from AXXCLI.

Accessing AXXCLI

General

The AXXCLI is accessed via a serial port (VT100) or via an IP connection (Telnet).

Default passwords

Telnet password = **telnet**

Terminal password = **axxcli**

NOTE!

When using Telnet to access the device it is important to know both passwords. The operator can change both the Telnet password and the terminal password from management.

Password recovery

If you for some reason have forgotten or lost the passwords to access the AXX155E through VT100 or Telnet please contact your level 1 support centre. A master password can be generated based on the serial number of the device.

To ensure rapid service make sure to provide the serial number at first inquiry.

COM-port settings

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 AXXCLI session

An AXXCLI session is invoked by typing AXXCLI at the AXXCLI terminal. User authentication (password, 6-12 ASCII characters) is required, as the following session start-up sequence shows:

```
AXX155E Command Line Interface
Password:  ********* (axxcli by default)
\>
```

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 an AXXCLI session. After using the local terminal you have to wait 30 seconds to be able to use Telnet, but ONLY if you Exit AXXCLI in the local terminal. If not the time-out is 30 minutes.

The AXXCLI session will be automatically terminated in case of 30 minutes in "idle state".

AXXCLI does not accept simultaneous sessions.

An authorized AXXCLI user obtains full access rights to the available management information.

Syntax rules

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

An AXXCLI 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, which can be reached from all menus in AXXCLI:

Command	**Description**
..	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
Free	Shows VC-12 containers not yet utilized
Used	Lists VC-12 container in use
Status	Present current device and port status
Exit	Exit AXXCLI

Table 1.2. AXXCLI - Universal commands

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.

1.12.2 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 hierarchy** is shown “AXXCLI Command Hierarchy” starting in page page 8-2. 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:

NOTE!

The menu-choices available in the AXXCLI are dependent of licenses loaded to the AXX155E. E.g. the top-level option "Router" is only available when L3-license is loaded.

```
AXXCLI>?

*** current menu path:
<root>

*** valid commands:
Device:     Device configuration
Ports:      Port properties
Bridge:     Bridge/Spanning Tree Protocol settings
Router:     Router configuration
Security:   Security settings
Statistics: Performance monitoring and statistics
Services:   Utility functions
Alarms:     Current alarms and alarm history
Free:       List of free VC12
Used:       List of used VC12
Exit:       Exit from 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 hierarchy for AXX155E is found in "AXXCLI Command Hierarchy"

NOTE! *Available menus and commands are dependent of installed licenses.*

1.13 TROUBLESHOOTING

1.13.1 Introduction

AXX155E 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:

1.13.2 Making enquiries to AXXTAC

When making enquiries to AXXTAC proper information is mandatory to provide the expected support. Dependent of type of assistance needed from AXXTAC the following scenarios apply:

HW REQUESTS OR IF SUSPECTING FAILURE (WRITTEN FORMAT APPRECIATED):

- Product/Application
- Inventory data reported from management. Optionally part no. and serial no. from labels on HW unit
- Contact person
- Details about when error occurred / was discovered
- Short explanation of the problem.

EMBEDDED SW REQUESTS OR IF SUSPECTING FAILURE (WRITTEN FORMAT APPRECIATED):

- Product/Application
- Inventory data reported from management. Optionally part no. and serial no. from labels on HW unit
- Activated features (licenses)
- Contact person
- Details about when error occurred / was discovered
- Remote login information to system
- Reports from management system
- Short explanation of the problem

.

1.13.3 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 AXX155E consists of the following subsystems.

- Main Card
- FAN-module
- Electrical/Optical transceiver card
- WAN-module (optional)

1.13.4 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.

SYSTEM OVERVIEW

2

AXX155E

2.1 GENERAL

The main R2 to R3 enhancement is the introduction of GFP/LCAS, which is a Ethernet framing standard to transport Ethernet packets in virtual containers through a SDH network. Additionally this edition introduces a new option for management connectivity, which will simplify design and configuration of a network supplied by AXXESSIT. All features in this release is aligned with new releases of AXX155A and AXXEDGE.

The AXX155E is an Integrated Access Device mainly intended for use in fibre optic networks, but can also be suppied as a HW option with support for electrical STM-1. The AXX155E 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 AXX155E R3 consists of a L2/L3 switch.

Each tributary interface (E1) is mapped into a VC-12 container while the WAN traffic can be transported via either nxVC-3 or nxVC12.

The AXX155E have room for a plug-in module, which adds more WAN-ports to achieve multiple connections with differentiated bandwidth per customer and/or service.

The AXX155E management solution is based on an embedded SNMP agent. Several management options can be provided for supervision and maintenance of AXX155E devices. The AXXTMN product portofolio cover any operators' need and a SNMP Craft utility (AXXCRAFT) is supplied with the deliveries of AXX155E. Minimum required to operate and configure the AXX155E isa simple VT100 command line interface (CLI) for direct communication with the embedded SNMP agent.

2.1.1 Functional overview

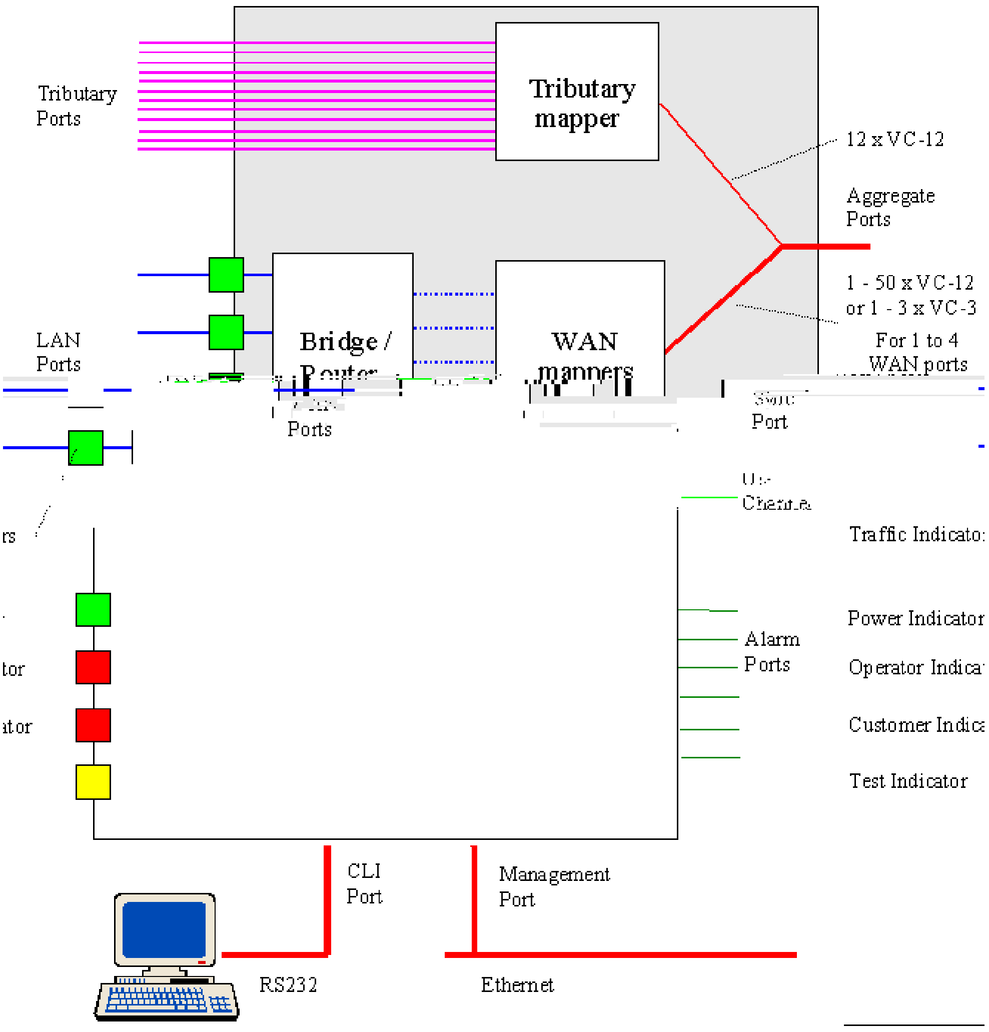


Figure 2-1. AXX155E overview

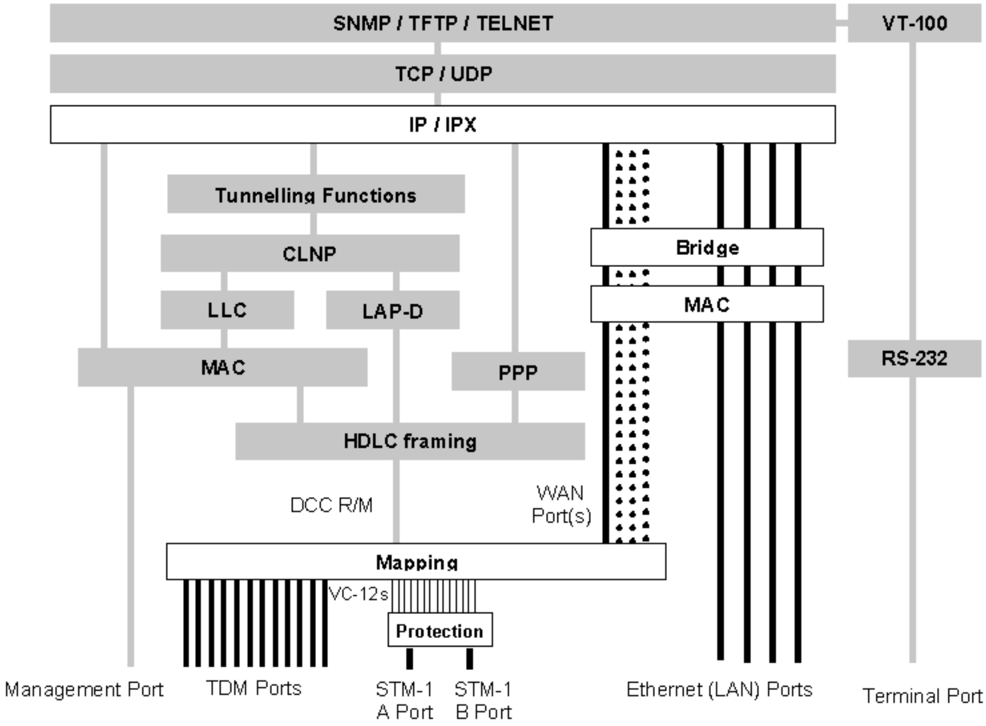


Figure 2-2. Functional model for the AXX155E.

From an element management perspective, the AXX155E is a multi-protocol machine with several types of interfaces as shown in the figure above.

2.2 APPLICATIONS OF THE AXX155E

2.2.1 Back to back application

Normally the AXX155 or AXX155E at the customer site is connected to an AXX155 or AXX155E 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 AXX155E incorporated. The network in this figure does not have a separate IP backbone network, but this could easily be supported.

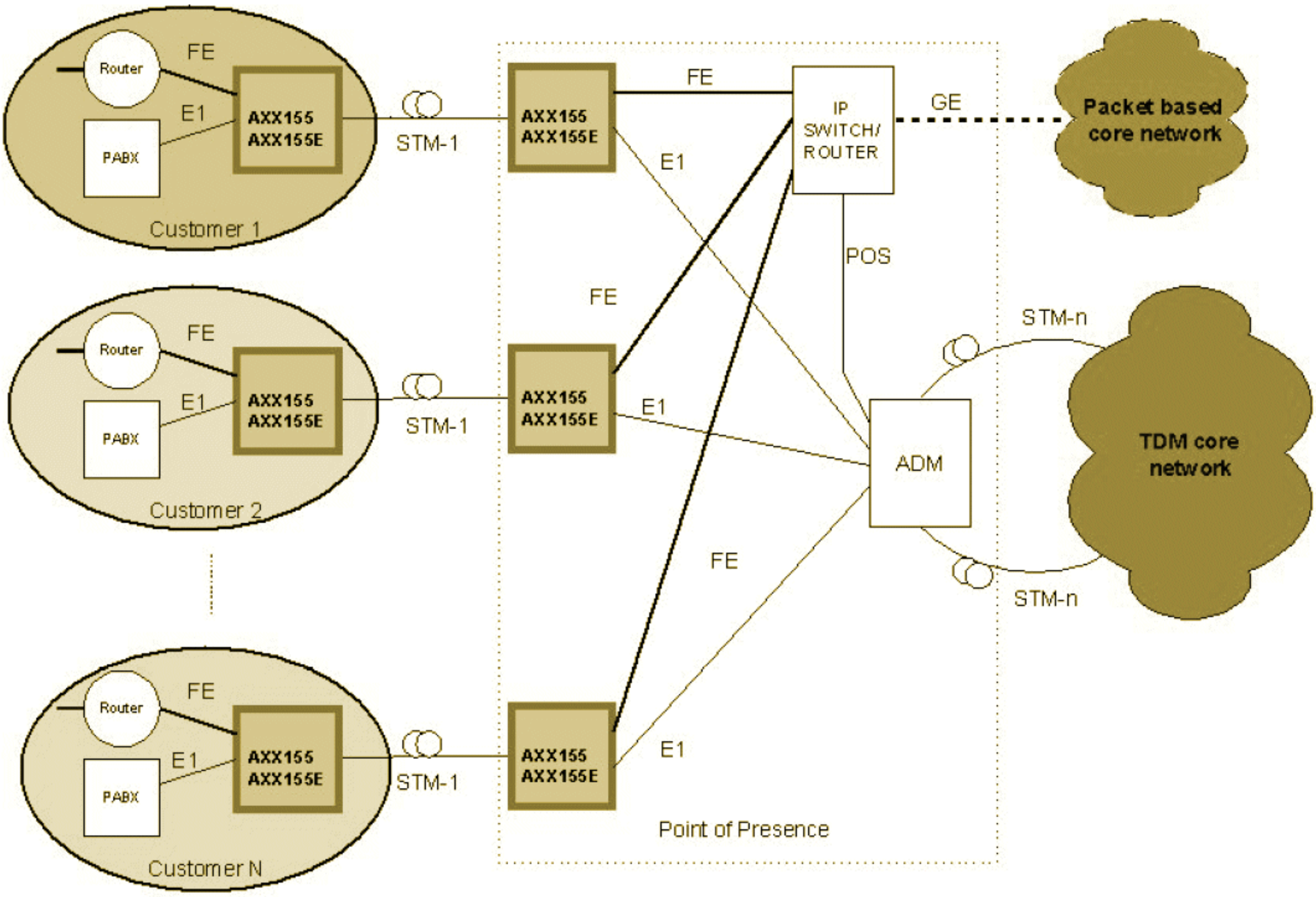


Figure 2-3. Back-to-back configuration across the access loop

2.2.2 Remote back to back application

The AXX155E 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.

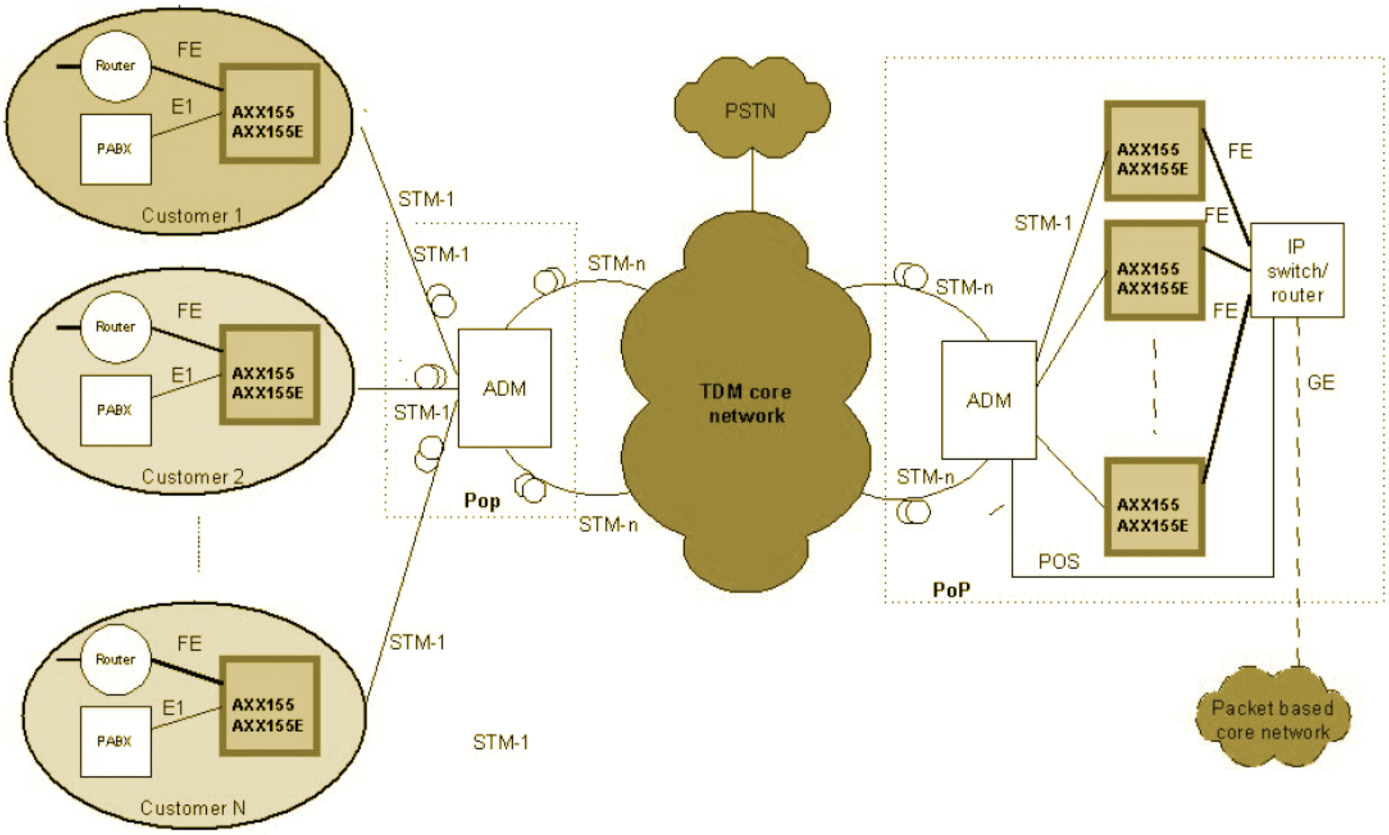


Figure 2-4. Typical system with no local grooming in the PoP

2.2.3 Headquarter office to branch office

The main IP enhancement of the AXX155E from release 2 of AXX155 is the addition of up to four WAN channels. This means that the AXX155E can be connected to four different AXX155 or AXX155E units without any additional IP switch. This is shown in the figure below.

A WAN module must be inserted in AXX155E to be able to do this.

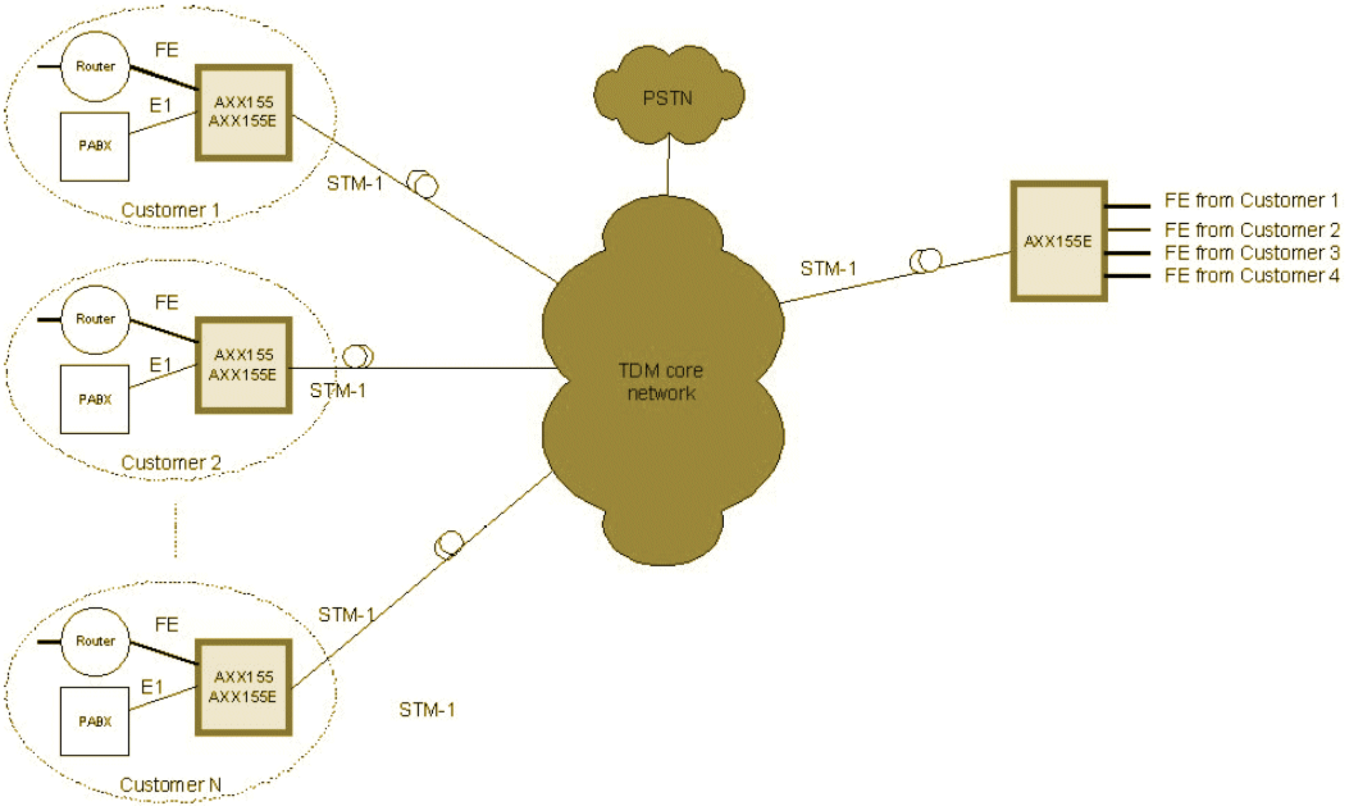


Figure 2-5. Typical system when connected to an AXX155E

2.2.4 Single ended used together with AXXEDGE

The AXXEDGE product can replace the ADM in the single-ended application. This is shown in the figure below. The AXXEDGE integrates the functionality of the ADM, IP switch/router and the number of AXX155/AXX155E in the PoP.

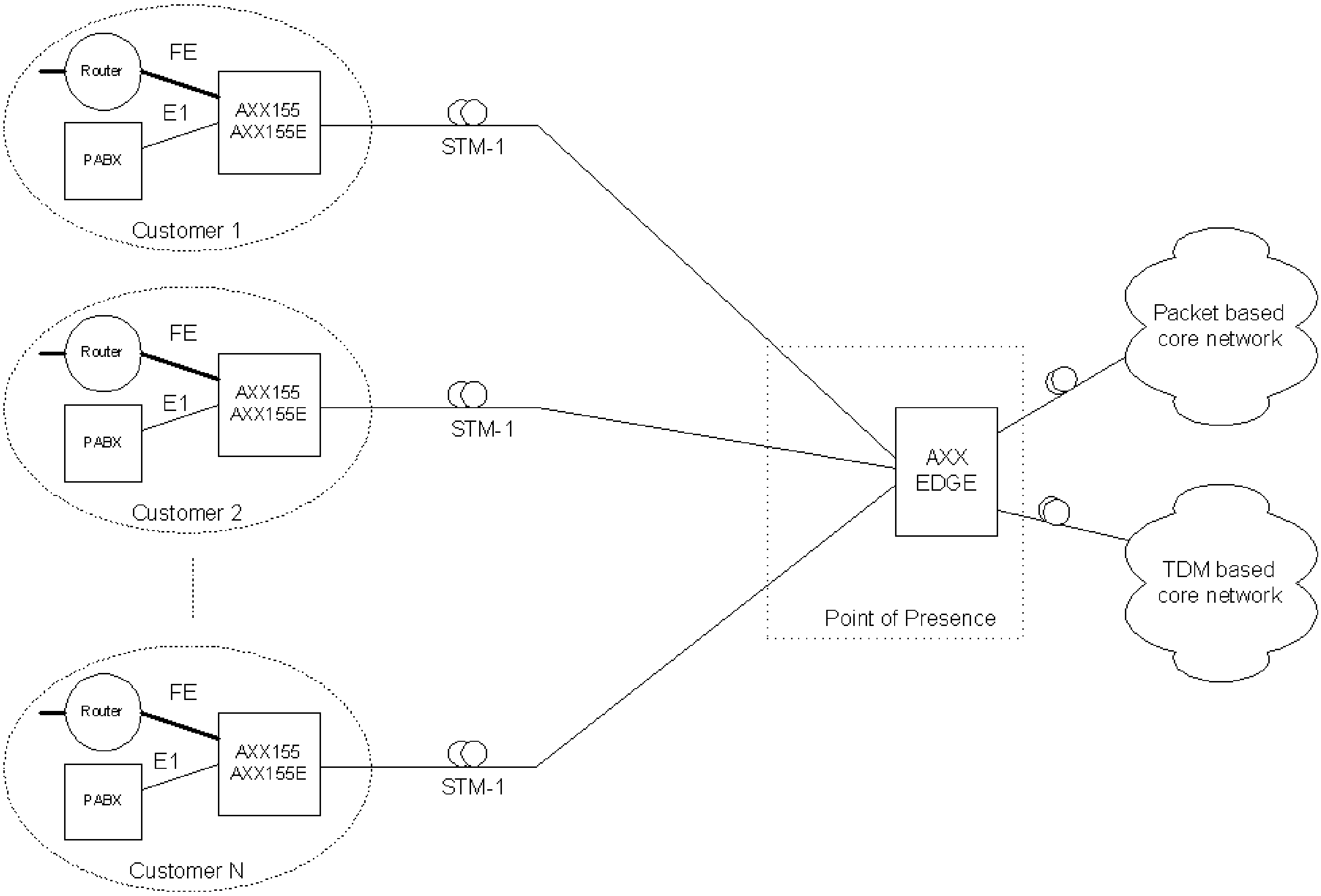


Figure 2-6. Typical system when connected to an AXXEDGE

2.2.5 Campus application

The AXX155E can also be connected back to back without any connection to external networks. This is shown in the figure below.

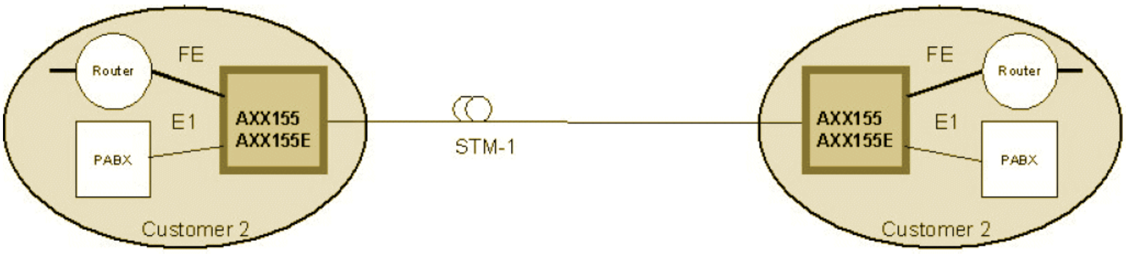


Figure 2-7.   Typical network when used in a campus application

2.2.6 Connection to STM-1 leased line

STM-1 leased lines are typical sold as an electrical interface. The AXX155E with an electrical interface can be directly connected to such an interface as shown in the figure below.

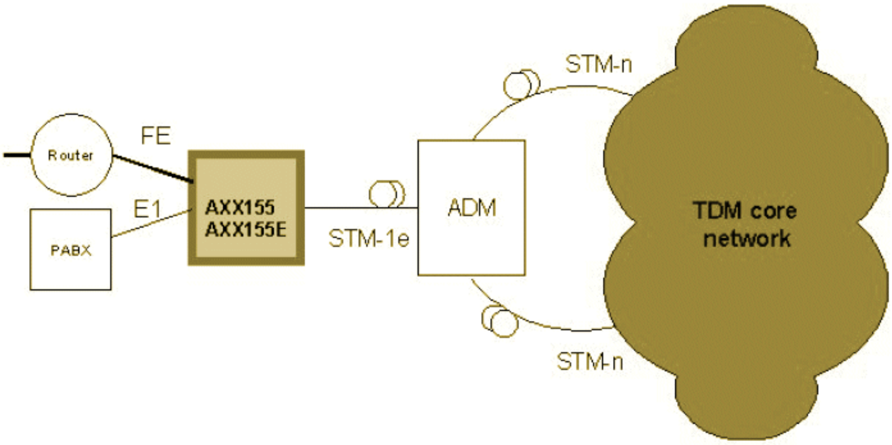


Figure 2-8. Typical system when connected to an STM-1 leased line

3

FEATURES

AXX155E

3.1 SDH FEATURES

3.1.1 Multiplexing structure and mapping modes

The aggregate interface supports only terminal multiplexer functions, with a mixture of terminated VC-12 and/or VC-3 container as indicated in Figure 3-2.

The internal structure of AXX155E is depicted in Figure 3-1. The bridge/router receives an Ethernet frame/IP datagram on one of the ports and decides on which port to send it out. The Ethernet Mapper mapps the Ethernet frames into VC-12/VC-3 containers while the Tributary Mapper converts between E1 signals and VC-12s. The SDH Multiplexer is responsible for the multiplexing of VC-12/VC-3 containers into STM-1. The VC-12/VC-3 containers are sent to - and received from - either the Tributary Mapper or the Ethernet Mapper.

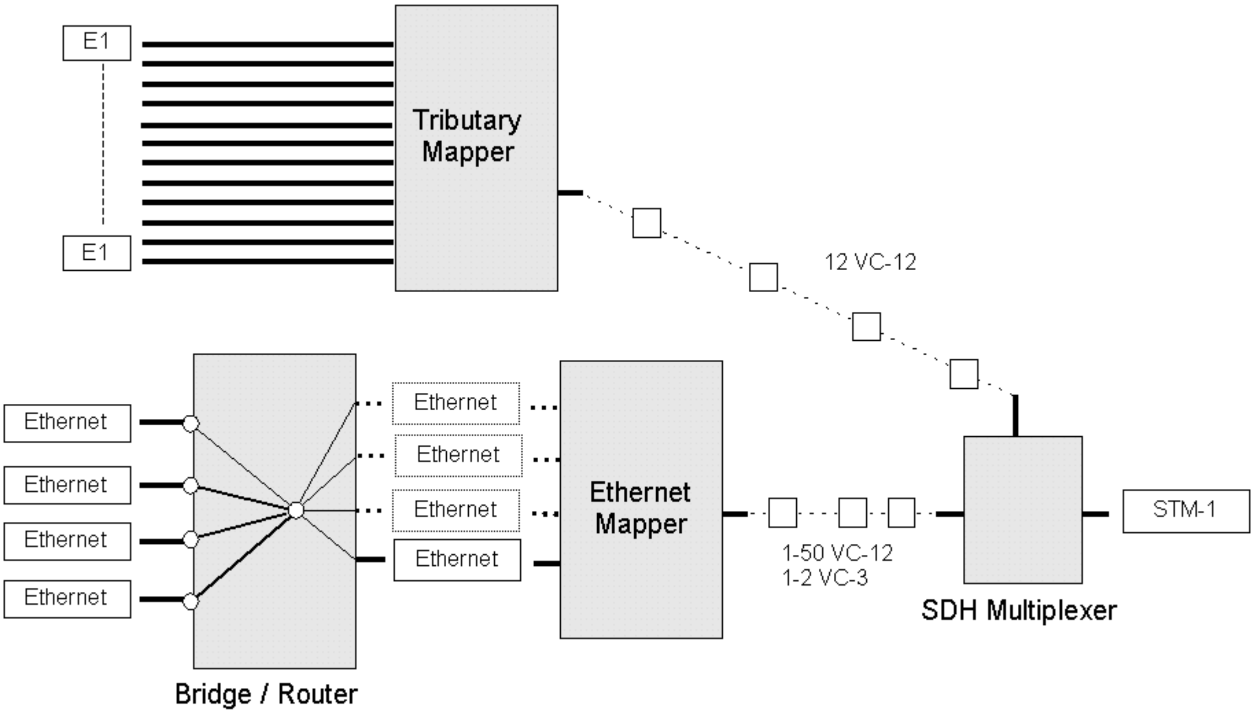


Figure 3-1. Multiplexing and mapping in AXX155E.

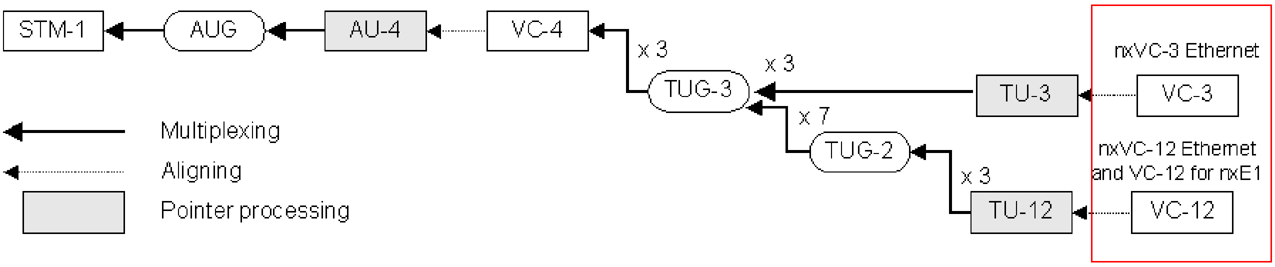


Figure 3-2. Multiplexing structure in STM-1.

3.1.2 Protection

The AXX155E R3 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 3.1.

Attribute	Access	Type	Description
MSP Enabled	R/W	choice	ENABLED or DISABLED
Switching Type	R/W	choice	UNIDIRECTIONAL or BIDIRECTIONAL
Operation Type	R/W	choice	REVERTIVE or NON-REVERTIVE
Wait-to-restore time	R/W	integer	Number of seconds to wait before switching back to the preferred link after it has been restored (0,1, ...,12 minutes, default 5 min)
Preferred Link	R	string	Identifier of the preferred working link (always LINK A for AXX155E R3).
Commands	R/W	choice	CLEAR, LOCKOUT-OF-PROTECTION, FORCED-SWITCHED-TO-PROTECTION, FORCED-SWITCHED-TO-WORKING, MANUAL-SWITCHED-TO-PROTECTION, MANUAL-SWITCHED-TO-WORKING EXERCISE, or NO-COMMAND
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 3.1. Protection switch parameters

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

Table 3.2. Protection alarm

3.1.3 Performance monitoring

The AXX155E R3 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 AXX155E 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.

3.1.4 Synchronisation

AXX155E R3 can synchronize to the following sources:

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

Tributary synchronization is only relevant in certain configurations (ISDN PRA).

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 AXX155E operates in three different modes:

- Locked
- Holdover
- Free running

The default synchronization source is the local oscillator. The tolerance for this oscillator is +/- 10 ppm.

AXX155E also provides a 2048 kHz sync output for synchronization of external equipment.

NOTE! *AXX155E R3 does not support SSM signaling in the S1 byte, default transmitted value is "do not use".*

NOTE *SSM signalling in S1 byte support in the AXX155E is not relevant since the network element does only support the configuration of one single sync-source at the time. In case of a protected device, i.e. an HW variant of AXX155E with two aggregate interfaces configured in 1+1 MSP protection, the configuration of synchronisation source should be set to sync-source=**active**.*

3.2 ETHERNET OVER SDH MAPPING

3.2.1 Mapping modes

The AXX155E supports two different modes of Ethernet over SDH (EOS) mapping

- AXXESSIT proprietary mapping combined with inverse multiplexing at VC-12 level
- GFP-F mapping, combined with VCAT ,at VC-12 and VC-3 level, and LCAS

NOTE!

The support of the different EOS modes are dependent on the WAN module inserted. WAN module with ICS 01 supports mode 1, WAN module with ICS 02 supports mode one and mode two on a pr. port basis.

3.2.2 AXXESSIT proprietary mapping

The AXX155E provides a proprietary mapping scheme for mapping of Ethernet traffic into a number of VC-12 containers.

The HDLC encapsulated Ethernet frames are mapped into a number of VC-12 containers in a round-robin fashion with an inverse multiplexer function. The mapping process is described in “Multiplexing structure and mapping modes” on page 3-2.

A total differential delay of up to 8ms is supported.

The total bandwidth for one WAN channel is 100 Mbps or 50xVC-12 containers. AXXESSIT Proprietary VC-12 mapping scheme for Ethernet take advantage of 2,16 Mbps in each VC-12, which means that 47xVC-12 are sufficient to transport 100MbpsEhernet.

The VC-12 k.l.m reference assignment for the Ethernet WAN port is fully flexible, and controlled in the same way as a VC-12 cross connect.

The sequence number attached to each VC-12 is used for alarm indication only in case of a sequence mismatch, the sequence number is not used for reordering of the incoming VC-12's. The order of VC's carrying Ethernet traffic between two WAN-ports therefore needs to be obtained.

In case of a failure on one of the VC-12's, the effected VC-12 is removed from the channel, allowing the traffic to flow on the remaining VC-12 connections. RDI is used to indicate a failure to the remote side.

3.2.3 Standardised mapping

The AXX155E R3 supports standardised ways of mapping Ethernet over SDH. The mapping schemes includes mapping protocol, concatenation scheme and control protocols.

GFP

AXX155E supports framed mapped GFP (GFP-F) according to ITU-T 7041.The GFP implementation supports the following functions:

- The implementation only supports GFP null extension header
- Client data frames are supported
- Client management frames are supported
- For control frames, the implementation only supports GFP idle frames insertion and processing, other unspecified control frames are dropped
- Standard GFP scrambling is supported, with the polynomial $1+x^{43}$
- The implementation supports the optional data FCS insertion and checking via the PFI bit
- The implementation supports frame sizes from 9 bytes up to 64kbytes (only sizes from 64 bytes to 9k bytes are applicable for this implementation)

GFP Alarm and Event Conditions

The GFP implementation supports the following alarm and event conditions:

- GFP Frame Delineation Loss Event, LFD
- Payload Mismatch, PLM

Alarm based on detection of PTI field value in ITU-T G.7041

- User Payload Mismatch, UPM

  • Alarm based on detection of UPI field value in ITU-T G.7041

- Payload FCS Mismatch, PFM.

  - Alarm based on detection of PFI field value in ITU-T G.7041
- Extension Header Mismatch, EXM
  - Alarm based on detection of EXI field value in ITU-T G.7041

GFP Performance Monitoring

The GFP implementation collects the following performance parameters:

- Total number GFP frames transmitted and received
- Total number Client management frames transmitted and received
- Number of bad GFP frames received, based upon payload CRC calculation
- Number of cHEC correted errors
- Number of cHEC uncorrected errors
- Number of tHEC correted errors
- Number of tHEC uncorrectee errors
- Number of Dropped GFP frames Downstream

A degrade alarm is available for the following performance parameters:

- Number of bad GFP frames received, based upon payload CRC calculation, degFCS
- Number of tHEC corrected and uncorrected errors, degtHEC

The deg alarms are handled in a similar way as the SDH degrade alarms.

Virtual Concatenation (VCAT) and LCAS

AXX155E supports virtual concatenation according to ITU-T 707. The VCAT implementation supports the following functions:

- VC-12-nV, where n=1..50
- VC-3-nV, where n=1..3

The VC-x level is individually configurable pr. mapper port, a mix of different VC-x levels in one VCG group is not allowed.

A total differential delay of up to 62ms is supported for the different VCG groups.

AXX155E supports the LCAS protocol in conjunction with VCAT as defined in ITU-T 7042. The LCAS protocol implemented covers the following functions:

- Automatically temporary removal of a faulty VCAT member
- Automatically insertion of a temporary removed VCAT member when the fault is repaired
- Hitless increase of the VCG capacity by adding a VCG new member
- Hitless decrease of the VCG capacity by removing a current VCG member
- Inter-working with equipment supporting VCAT but not supporting LCAS

VCAT and LCAS configuration modes

The AXX155E offers two different operation modes for the VCAT and LCAS functionality, the two modes are:

1.VCAT with LCAS enabled

2.VCAT without LCAS enabled

Mode 1

VCAT with LCAS enabled is always uni-directional, which enables the possibility to have different capacity in each direction, but requires a separate cross connect/capacity setup in each direction.

Mode 2

When VCAT is used without LCAS, there is no mechanism for removing of a faulty VC container in a VCG group. To solve this problem the AXX155E implements, in addition to the standard mode, a proprietary mode.

The following configuration is available in mode 2:

- Default mode, unidirectional connections with the possibility of configuring symmetric capacity as explained in mode 1. Same features as in mode 1 but without LCAS
- SoftLCASBidirectional mode

If SoftLCASBidirectional mode is enabled, the cross connections are uni-directional, but bi-directional. In addition RDI signalling are enabled. A faulty container in a VCG group isremoved based upon the VC alarm condition or based upon RDI signalling (similar to AXXESSIT proprietary mapping). This will allow a VCG group to continue operation even if the VCG has a failed member. This configuration mode is proprietary.

VCAT and LCAS Alarm and Event Conditions

The following alarms related to the VCAT and LCAS are reported by default:

LOM	Vcat, loss of multiframe
SQM	Vcat sequence indicator mismatch
LOA	Lcas loss of alignement for channels with traffic
GIDERR	Lcas Group Id different for active channels
LCASCRC	Lcas CRC error detected
NONLCAS	Lcas non-Lcas source detected
PLCR	Lcas partial loss of capacity receive
TLCR	Lcas total loss of capacity receive
PLCT	Lcas partial loss of capacity transmit
TLCT	Lcas total loss of capacity transmit
FOPR	Lcas failiure of protocol
SQNC	Inconsistent SQ numbers

Table 3.3. Default alarms - VCAT and LCAS

In addition to the above default alarms, the following alarms are available if enabled from the management system:

acMstTimeout -- Lcas acMst timeout	
rsAckTimeout	Lcas RS-ack timeout
eosMultiple	Lcas two or more channels have EOS
eosMissing	Lcas one channel has EOS
sqNonCont	Lcas missing SQ detected in set of channels
sqMultiple	Lcas equal SQ for two or more channels
sqOor	Lcas SQ outside of range
mnd	Lcas member not deskewable
ctrlOor	Lcas undefined Ctrl-word for one or more channels

Table 3.4. Optional alarms - VCAT and LCAS

3.3 IP FEATURES

3.3.1 General

AXX155E R3 supports both bridging and routing. It is possible to sell the product in two different variants:

- Bridging (basic)
- Routing

The variants are described in the next sections. The embedded software in AXX155E is capable of supporting both variants. To upgrade an AXX155E from the basic variant (bridging) to the routing variant, the routing feature must be activated. This requires a specific key (see “Feature Management” on page 3-51).

3.3.2 L2Bridging

The bridge is a transparent multi-port remote Ethernet bridge as specified in IEEE 802.3. The Bridge consists of four LAN ports and up to four WAN ports. 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 10 Mbit/s and 100Mbit/s are supported with auto-negotiation. The LAN ports are compatible with IEEE 802.3.

In addition to standard bridging functionality support, the AXX155E also support provider bridge functionality.

The bridge supports the following features:

- MAC switching
- Static MAC entries
- Support of up to 32k MAC addresses
- Automatic Learning & Ageing for MAC addresses
- Auto negotiation (speed/duplex)
- Fixed Ethernet Port settings i.e. 10/100 half/full duplex
- MAC Multicast
- Transparent Bridging
- Port-based Virtual LANs (VLANs)

- VLAN by Port and VLAN by Port and Protocol
- IEEE 802.1Q VLAN tagging compliance (VLAN id. 1-4000)
- Head of Line Blocking prevention
- Back pressure and flow control Handling
- IGMP snooping
- Mirroring Port
- IEEE 802.1p priorities (Strict Policy, 4 queues)
- GARP VLAN registration protocol (GVRP)
- MTU Size 6144 bytes
- Rapid Spanning Tree Protocol per device (RSTP)

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 port speed.

The AXX155E R3.0 also support a LAN-WAN port correlation function used in architectures requiring Ethernet protection. The port correlation function, if enabled on a LAN port, reflects the status of the corresponding WAN port on the actual LAN port. This means that if the operational capacity of the WAN port is 0, due to a network error, the corresponding LAN port is disabled, allowing external equipment to very rapidly detect the network error and thereby switch to the other path.

Rapid Spanning Tree Protocol per device (RSTP)

Previous versions of the product supported common STP acc. to IEEE 802.1D 1998. This version supports Rapid Spanning Tree Protocol (RSTP) acc. to 802.1D 2004, which is compatible with STP. By default (when enabled) the device is setup to run RSTP, but when inserted in a topology which runs STP, the algorithm will adapt to run this version instead.

3.3.3 L2 Provider bridging functionality

In addition to the standard L2 functionality the following Provider Bridge functionality is supported:

- Tag insertion/removal for Provider bridging/ VLAN tunnelling support
- Protocol tunnelling, offering transparency of the following MAC addresses/protocols:

- All MAC addresses in the range from 0180C2000000 to 0180C20000FF,except ...01, is transported transparently, including the following protocols: RSTP.MSTP.STP,GVRP,GMRP,LACP and 802.1x

The offering of Provider bridging /VLAN tunnelling and protocol tunnelling enables the user to offer transparent Ethernet services in a L2 network with guaranteed security, also called L2 VPN's. The functionality is enabled at the ingress and egress ports in the network.

The Ethertype used for the Tag insertion is 0xFFFF, interoperability with other systems using 0x8100 is obtained by enabling Ethertype swapping on the WAN ports. This functionality is only supported on the new WAN module.

Protocol Tunnelling

The parameter "FilterBPDU" in the RSTP port table control whether BPDUs are forwarded or filtered when RSTP is disabled. As this is configurable per port, the setting is checked against the RSTP setting of the individual ports (enable/disable) and not the general RSTP setting for the device.

The configuration of FilterBPDU is not available while RSTP is enabled on the port in question.

After disabling RSTP on the port. FilterBPDU can be set to "filter" or "forward". The default value is "filter".

Selecting the option "forward" disables BPDU filtering on the specific port, and forwards all frames normally filtered by the switch as regular multicast frames (i.e. they are forwarded to all ports that are members of the same VLAN as the ingress ports).

To achieve a totally transparent Ethernet service (i.e. no filtering) BPDU filtering must be disabled on all ports involved (both LAN and WAN ports).

The parameter "ProtocolTunneling" under the "ProviderVlan" menu for the WANX ports control whether the reserved MAC addresses for BPDUs are swapped with a regular multicast address (in the AXXESSIT range [this info might not be good for OEM User Guides]) or not.

Replacing the MAC addresses allows the BPDUs to be forwarded through intermediate nodes in the network (i.e. to be tunnelled) before they are swapped back at the destination node. This implies that the destination node must also support this tunneling feature.

Protocol Tunneling is only possible when BPDU filtering is disabled (filterBPDU=forward).

Example

How to use AXXEDGE and AXX155E to tunnel traffic between two 3rd. party devices.

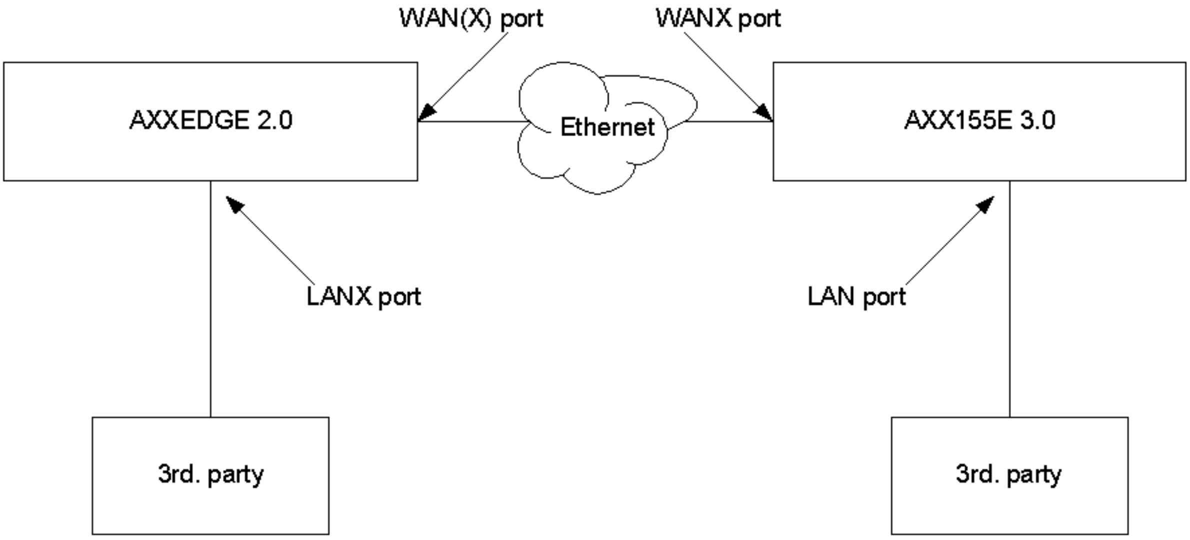


Figure 3-3. Protocoll Tunneling - Example

AXXEDGE

Prerequisites:

- AXXEDGE must be running sw 2.0 or later, and the port facing the 3rd. party equipment must be a LANX port (i.e. a port on the 8xFE+MAP or 2xGE+MAP modules).
- Provisioning of VLAN, speed/duplex settings/ EoS mapping to achieve the desired connectivity.

Configuration:

LANX port:

- Disable RSTP on the particular port (RSTP port table) if RSTP is enabled on the device.
- Enable Protocol Tunneling on the port.

Limitations:

The LANX port with Protocol Tunnelling enabled will not be able to participate in any protocols being tunneled. This includes all protocols (e.g. RSTP and GVRP) depending on the use of destination MAC addresses in the range 01:80:C2:00:00:00 to 01:80:C2:00:00:FF
(With the exception of :01, PAUSE frames which are not forwarded under any circumstance).

The tunnelling is a proprietary solution that require an AXXEDGE or AXX155E as opposite party to do the detunneling.

AXX155E

Prerequisites:

AXX155E must be running sw 3.0 ICS05 or later, and must be equipped with a WAN-GFP module.

Provisioning of VLAN, speed/duplex settings/ EoS mapping to achieve the desired connectivity.

Configuration:

- Disable RSTP on both the LAN and WANX port that will be used for tunnelling by setting "portEnable" to "disable" (RSTP port table), regardless of whether RSTP is enabled on the device.
- Disable BPDU filtering on both the LAN and WANX port that will be used for tunnelling by setting "filterBPDU" to "forward" (RSTP port table).
- Enable Protocol Tunneling on the WANX port (ProviderVlan menu on the WANX port).

Limitations:

·The ports with Protocol Tunnelling enabled will not be able to participate in any protocols being tunneled. This includes all protocols (e.g. RSTP and GVRP) depending on the use of destination MAC addresses in the range 01:80:C2:00:00:00 to 01:80:C2:00:00:FF (With the exception of :01, PAUSE frames which are not forwarded under any circumstance)

·The tunnelling is a proprietary solution that require an AXXEDGE or AXX155E as opposite party to do the detunneling.

3.3.4 Routing

The AXX155E R3 can be configured as a multi-port router. The router is able to route both IPv4 and IPX traffic.

Parts of the IP-routing functionality in AXX155E are supported even if there is no routing license downloaded to the device. In this case the routing will be performed by CPU and mainly intended for management purpose.

The router supports the following IP features:

- IP Routing *
- IP Redundancy Protocol (Proprietary)
- Address Resolution Protocol (ARP) *
- ARP proxy *
- Internet control message protocol (ICMP) Messages *
- Static IP routes *
- Routing information protocol (RIP) versions I and II *
- RIP subnet filtering *
- Open shortest path first (OSPF) version 2 *
- User datagram protocol (UDP) Relay *
- IP Multicast Routing - PIM Dense Mode
- Internet group management protocol (IGMPv2) support

* This feature is included both for SW and HW based routing.

The router has the following IPX features:

- IPX route and socket filters
- RIP and IPX Server Advertisement Protocol (SAP) filters
- Variable RIP and SAP timers
- IPX Get Nearest Server (GNS)
- Novell NetBIOS type 20 propagation support

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

3.3.5 DHCP

DHCP is used to provide IP addresses to end nodes. This feature is typical a part of the router variant.

It is able to support up to 2679 clients.

The router also provides DHCP relay functions.

3.3.6 BootP client

BootP client is used to get one IP address for the AXX155E R3 under the installation process (see “Device Replacement” on page 3-51). This feature is typical a part of both variants.

The router is also able to provide BootP relay functions.

3.4 TDM FEATURES

AXX155E R3 provides twelve 120-ohm 2.048 MHz Tributary ports on the customer side. 75-ohm operation 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 AXX155E can only implement the PRA NTE functions.

Two test loops are provided per Tributary Port, one in the customer direction (LL3) and one in the network direction (LL2), see Figure 3-4.

A 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 as long as the port is enabled.
- 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 be possible to operate the loops from the AXX155E management system.

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

The Test Indicator LED is ON if any tributary loop is closed, regardless of the tributary mode.

AXX155E does not support any monitor points (as oposed to AXX155).

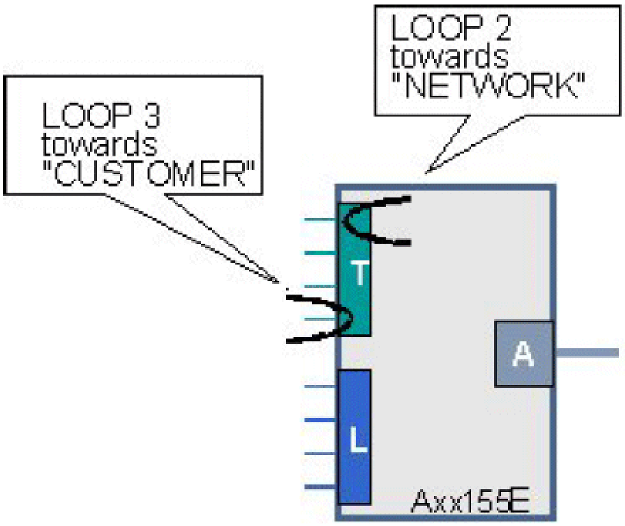


Figure 3-4. Test loops

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 below.

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)

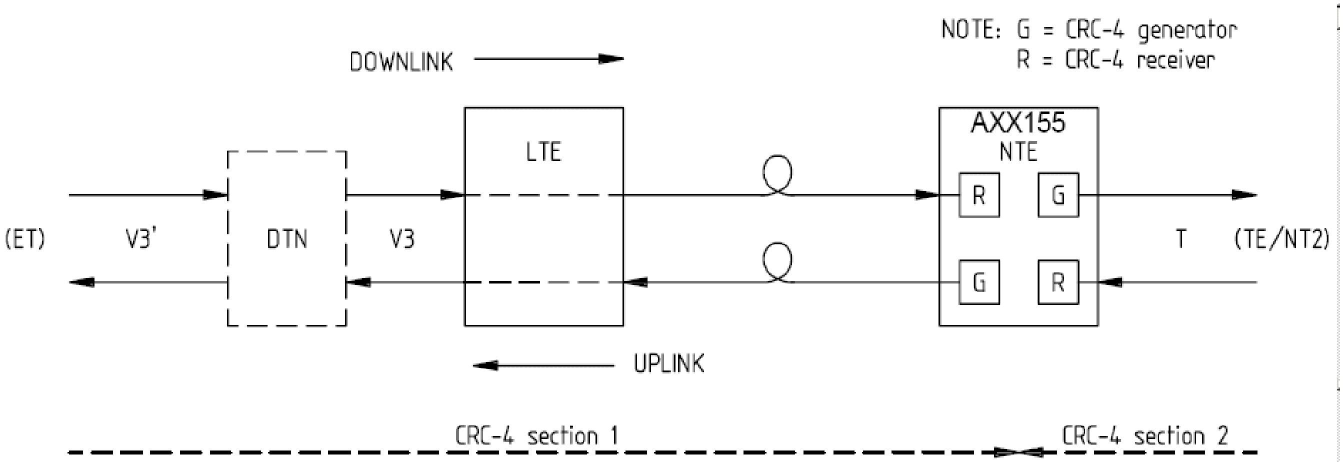


Figure 3-5. AXX155E ISDN PRA configuration

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:

Table 3.5.

Condition	Uplink report to ExchangeTermination	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 SignalV3 (FV3)Loss of line signalor 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.

Condition	Uplink report to ExchangeTermination	Comments
Loss of Line Signal at LTE **(FC1)**	AUXP	Auxiliary alarm indication pattern(1010..) generated by the LTE.

Loop-back 1activated bydownlink
Sa6=1111
	Sa6 = 1111
	RAI = 1
	Sa5 = 0
		The downlink signal is looped back fully transparently in the LTE.

Loop-back 2activated bydownlink
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 3.6. 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 3.7. 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.

3.4.1 Alarm Ports

The AXX155E 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 AXX155E provides also support for two alarm output ports used to signal equipment alarms and traffic related alarms.

3.4.2 LED Indicators

The LED Indicators are used to visualize the AXX155E status:

Indicator	Colour	Function
Traffic Indicators	Green	LAN traffic indicator (one LED per LAN Port)
Customer Indicator	Red	Alarm on the AXX155E customer side, i.e. Tributary 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 3.8. LED Indicators

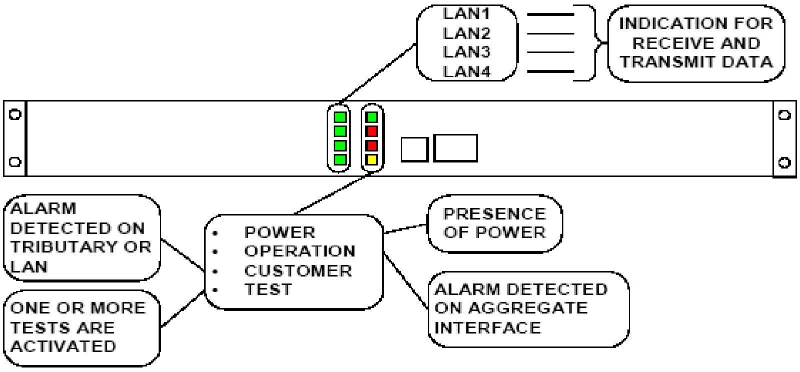

LAN1
LAN2
LAN3
LAN4
INDICATION FOR RECEIVE AND TRANSMIT DATA
ALARM DETECTED ON TRIBUTARY OR LAN
ONE OR MORE TESTS ARE ACTIVATED
• POWER
• OPERATION
• CUSTOMER
• TEST
PRESENCE OF POWER
ALARM DETECTED ON AGGREGATE INTERFACE

Figure 3-6. LED Indicators

3.4.3 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.

The user channel interface can only be used when the AXX155E is using only one WAN port or when it is connected to the AXX155E.

3.4.4 Automatic System Clock setting

The AXX155E R3 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 Table 6.77.) 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.

AXXCLI

Current Device Time

Should be adjusted during first time installation. In case of periods with lacks of power the Time settings will be kept in memory for a period of 48 hours

TIME (SYSTEM)	**R/W**	**hh:mm:ss**

Current Device Date

Should be adjusted during first time installation. In case of periods with lacks of power the Date settings will be kept in memory for a period of 48 hours.

DATE	**R/W**	**yyyy-mm-dd**

UTC Delta

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.

Default setting : 0

This parameter is not recommended or required to configure when using the AXXCRAFT/AXXINSITE as configuration tool since this calculation is best maintained by the management system.

```
UTC-DELTA              R/W      integer[-720:720min]
```

3.5 DCN FEATURES

3.5.1 Introduction

In this context the term "DCN" (Data Communication Network) is used to denote the network that transports management information between a management station and the NE. This definition of DCN is sometimes referred to as MCN (Management Communication Network). The DCN is usually physically or logically separated from the customer network.

The AXX155E management solution is based on SNMP over IP. The main purpose of the DCN implementation is to provide connectivity to the SNMP Agent inside the AXX155E via different DCN topologies. The DCN implementation also support transport of management traffic between other AXXESSIT or third party nodes.

Allthough the management application is IP-based, the DCN solution also support OSI-only and mixed IP/OSI-networks at layer 2 and 3. The various options and features related to different DCN topologies are specified throughout this section.

In general, the term "OSI" in this document is used to denote a CLNP-routed network, ie. it is only used for L3. Higher level OSI-protocols are not considered. At L2 different protocols are supported, including LAP-D. The AXX155E OSI-implementation supports CLNP, IS-IS Level 1 and Level 2 and ES-IS.

For the "IP In-band" L2 topology the management traffic is switched/routed between LAN/WAN ports. When IP-addressing a VLAN IF (id 100000-104000) the management connectivity is obtained at wire-speed along with the user traffic or on a separate WAN-port dedicated for management.

For all other cases, the following applies: The DCN traffic is always routed (IP or OSI) between the management interfaces. Two different router modes are available for management connectivity. One operates for "Numbered mode" and the second operates in "Un-numbered mode". Both routers are not accessible for DCN purpose simultaneously, and a system mode is introduced to enable desired router.

SW based DCN routing does not require a routing licence.

Most topologies in the following sections assume standard numbered IP interfaces, ie. every interface connected to the router takes an IP address and a subnet. However, from R3.0 on, a new feature called "IP Unnumbered Interfaces" is supported. With this feature the device will need only one IP address .

3.5.2 Management Interfaces

The following interfaces may be used to carry management traffic:

Management port

The AXX155E has a dedicated Ethernet port for management, called the "Management Port". This port can be used for local management, e.g. connecting a craft terminal. It can also be used for connecting to a separate external management network. The management port can be turned off to avoid unauthorised local access. The management port cannot be member of a VLAN.

LAN ports

The LAN ports are FE Ethernet ports used for connecting customer IP traffic to the AXX155E. LAN-ports in AXX155E are connected to the switch and can be used to carry management traffic.

WAN ports

The WAN ports are device internal FE Ethernet ports that can be mapped into one or more virtual containers of an SDH STM-n signal. From a DCN perspective, there are no functional differences between LAN and WAN ports in AXX155E.

DCC channels

The SDH architecture defines data communication channels (DCC) for transport of management traffic in the regenerator section (DCCR - 192 kbit/s) and in the multiplexer section (DCCM - 576 kbit/s).

The two SDH-links in AXX155E may terminate up to 4 DCC channels (2 DCCR and/or 4 DCCM). All DCC channels may be active simultaneously, but this depends on the selected mode. Activation/ deactivation of DCC channels is configurable on a per port basis.

Local VT-100 serial port

Also this RS-232 interface is regarded as a management interface, allthough it does not relate to the various DCN topologies described throughout the rest of this section. In AXX155E full management capability is provided over the CLI..

3.5.3 External DCN

"External DCN" means that the management station connects to the AXX155E via a separate DCN. The physical connection to the AXX155E is the Management Port.

Both IP/Ethernet and CLNP/802.x is supported. The AXX155E can run both stacks on the Management Port simultaneously.

The AXX155E may also serve as a gateway from an External DCN to other AXXESSIT-nodes in the SDH network, ie. the External DCN topology may be combined with other topologies described in the next subsections. If External DCN (in OSI mode) is combined with OSI/DCC, the AXX155E implements a Gateway Network Element (GNE) as defined in ITU-T G.784.

The direct connection of a craft terminal to the Management Port may be regarded as a special case of the External DCN topology.

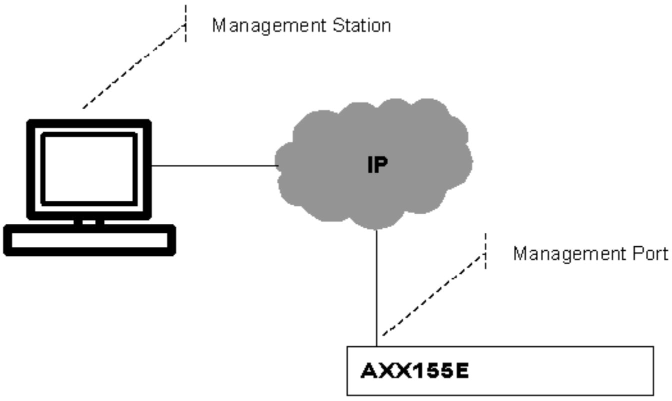


Figure 3-7. External DCN

3.5.4 IP In-band DCN

"IP-Inband" means that LAN and WAN ports are carrying management traffic together with customer traffic. This is useful in topologies where (parts of) the SDH-network is owned by a different operator which does not allow a third party to use the DCC capacity.

With IP in-band it is possible to build tunnels between "islands" that have other DCN solutions.

In AXX155E all LAN- and WAN-ports are connected to the switch. Any LAN- or WAN-port may be used to carry in-band management traffic, assuming an IP-address is assigned to it, or to the VLAN it belongs to.

The L1 IP In-band options as used in other AXXESSIT products is not supported by AXX155E. Between LAN/WAN ports the switching is always at wire-speed. If a routing licence is provided, also routing between LAN/WAN is at wire-speed. Between LAN/WAN and other management interfaces the traffic is always routed by the CPU. It is possible to split management traffic from user traffic by assigning dedicated LAN/WAN ports to management traffic.

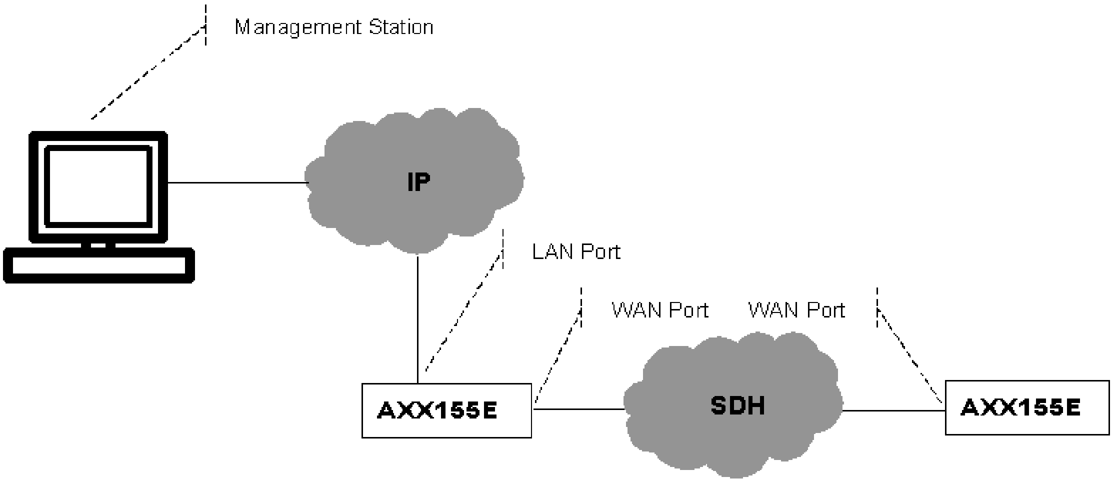


Figure 3-8. IP Inband DCN

3.5.5 OSI/DCC (IP over OSI) DCN

This option is useful if the AXX155E is connected to an OSI-based DCN. The AXX155E IP-based management traffic will be transported through the DCC-channels of a general (multi-vendor) SDH network by means of standard OSI-protocols at layer L2 and L3.

L3 protocols supported are CLNP, IS-IS Level 1 and Level 2 and ES-IS. The L2-protocol in the DCC-channels in OSI-mode is LAP-D.

All the interfaces that have the OSI option enabled will be connected to the internal CLNP router. This implies that also third-party DCC-traffic can be routed across the AXX155E CLNP router.

A CLNP tunnelling mechanism is provided for transport of IP datagrams between the management station and the AXX155E SNMP Agent over an OSI-based network. One AXXESSIT node (AXX155E or other) must be configured to act as a gateway (GW) to an IP-based network for a number of NEs. The NEs must know the NSAP address of its GW. Both ends will encapsulate the IP datatgrams in CLNP-frames and transmit them across the OSI network. The encapsulation methods used are mostly in accordance with RFC 3147 Generic Routing Encapsulation over CLNS Networks and RFC 2784 Generic Routing Encapsulation.

The DCC channels connects to CLNP individually, and CLNP is connected to the IP router via one router port. In OSI/DCC mode the AXX155E must have both an NSAP address and (at least) one IP address. From an IP perspective the GW is a router between OSI and the Management port.

The GW maintains an Address Mapping Table between the NEs' IP and NSAP addresses by means of a proprietary protocol.

All NEs associated with a GW are on the same IP subnet.

Note: The GW functionality described above, 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 network.

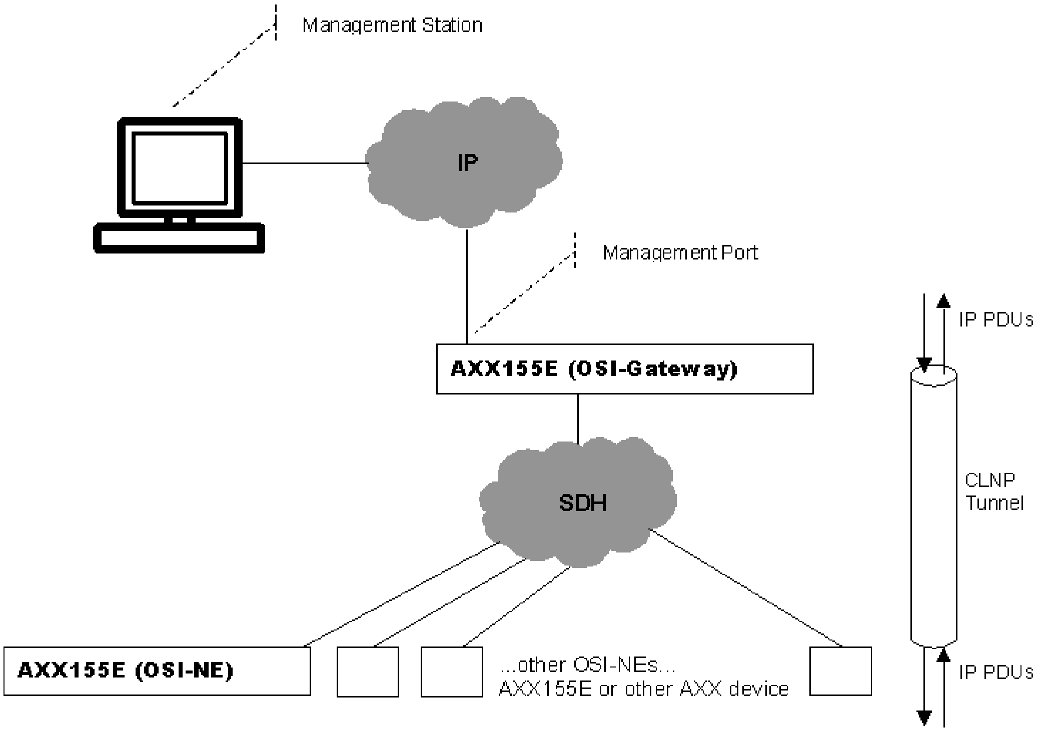


Figure 3-9. OSI/DCC DCN

Limitations

- Max number of NEs per GW: 32
- Max number of entries in the IS-IS L1/L2 routing-table: 200

3.5.6 PPP/DCC DCN

PPP/DCC means that the management IP-traffic is carried in PPP over the SDH DCC channels according to NSIF-DN-0101-001. The PPP implementation supports RFC1661 (PPP), RFC1662 (PPP in HDLC-like framing) and RFC1332 (IPCP).

Each PPP/DCC channel connects to the IP router individually. Normally this would take one IP subnet per DCC-link, and this is how previous versions of AXX155E would behave.

However, from AXX155E R3.0 on a more comprehensive PPP/DCC strategy is supported. This strategy is based on the feature called "IP Unnumbered Interfaces", and the rest of this section assumes this option.

The IP Unnumbered concept allows the system to provide IP processing on a serial interface or in general a point-to-point without assigning it an explicit IP address. The IP unnumbered interface borrows the IP address of another interface already configured on the system/router (ie. the Management Port), thereby conserving network and address space, and making the system easier to configure, manage and maintain.

With IP Unnumbered, all nodes connected via PPP-links may be on the same IP subnet. An essential part of the implementation is the DCN ARP Proxy Agent, which makes sure that connectivity between the nodes is obtained without having to provision static routes. The Proxy Agent builds entries for all the DCN IP destinations, and will reply to ARP requests on behalf of them.

"IP Unnumbered" is regarded as a main mode, and can not be combined with other modes that require numbered interfaces. This implies that this PPP/DCC option can not be combined with IP Inband or OSI.

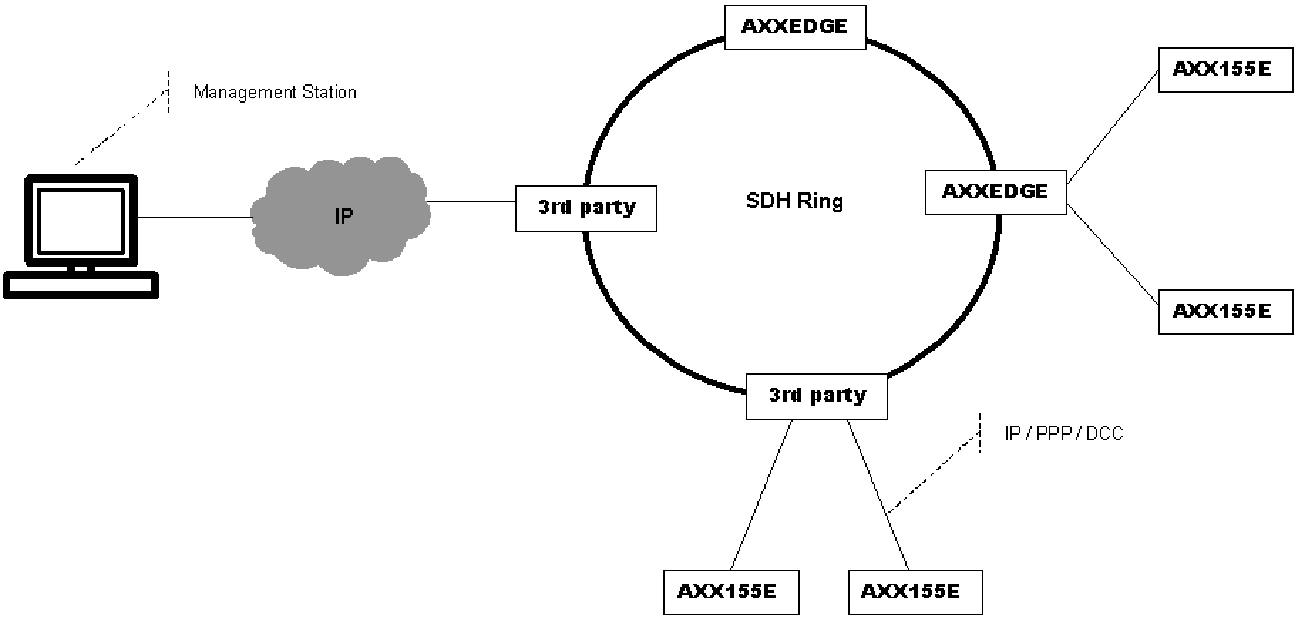


Figure 3-10. PPP/DCC DCN

Compatibility issues

AXX155E R3.0 is able to provide DCN connectivity with all types of AXXESSIT devices already deployed, including the installed base of AXX155E devices with an earlier SW revision. Hence, two additional DCN options, are supported: PPP/DCC for numbered interfaces and prorietary IP/DCC communication.

PPP/DCC (IP over PPP)

AXX155E supports PPP/DCC also on numbered interfaces. This option can not co-exist with the IP unnumbered version of PPP/DCC as described in 2.9.6. However, the numbered variant of PPP/DCC has the advantage that it can be used in combination with all other DCN modes.

Note that in the previous AXX155E release (R2.0), PPP was only supported over DCC-r. R3.0 will support both DCC-m and DCC-r.

IP/DCC (IP over HDLC)

IP/DCC is a non-standard IP broadcast mechanism used for conveying management information on the SDH DCC channels in a network of AXXESSIT devices only. The IP datagrams are encapsulated in HDLC frames before they are sent out on the SDH DCC. Broadcast in this context means that the AXXESSIT devices emulate a shared medium on the SDH DCC channels at the MAC layer. Packets with destination MAC different from the device's MAC are forwarded transparently to the active DCC Tx channel(s).

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. If the filter is disabled, all MAC frames (regardless their destination MAC address) received via the management port are broadcasted over DCC. With this MAC filter disabled it is possible to provide IP DCN connectivity to a remote 3rd party network element, connected to the far end AXX155E's Management Port.

The IP/DCC configuration is applicable for a user having a subnet of AXXESSIT devices and an IP based DCN connected to one AXX155E. The configuration is illustrated by Figure 3-11.

The IP/DCC option has two special restrictions, imposed by the proprietary pseudo-broadcast mechanism:

- Maximum one DCC per link (M or R)
- The broadcast solution cannot be used in a MSP protection configuration, which involves one, or more radio hops.

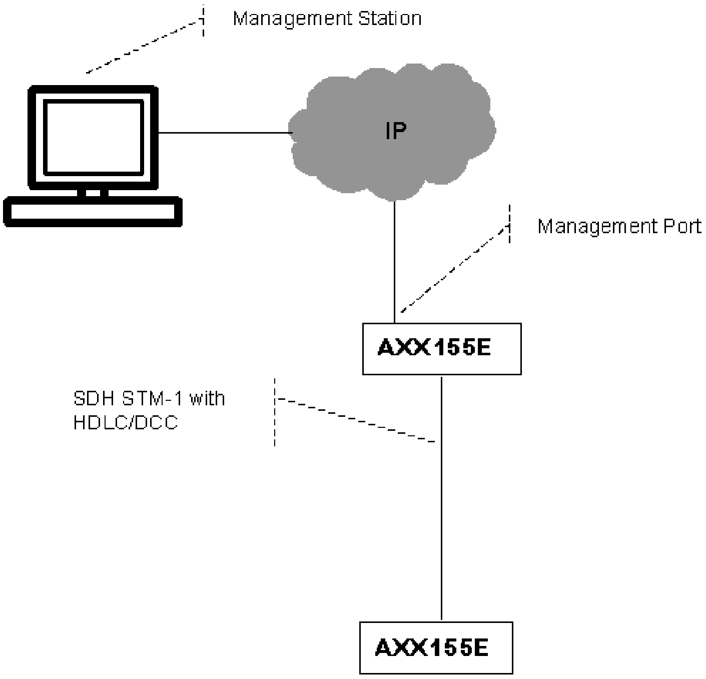


Figure 3-11. IP/DCC DCN

3.5.7 Protection

The two SDH-links in AXX155E are protected by means of MSP (1+1 link protection)

For MSP protected links, the DCN behavior depends on the DCN mode:

§If the mode is PPP/DCC (numbered or unnumbered) or IP/DCC (broadcast), the management traffic over DCC follows the user traffic, i.e. traffic is sent over both links (working and protecting), but received only from the active link.

§In all other modes, the two DCC channels will be individual interfaces to the router (CLNP and/or IP), and switch-over will be handled at routing level.

3.5.8 Security

In order to prevent unauthorized access to the SNMP Agent, the following security and traffic control features are supported

Management Port on/off

The Management Port can be turned on and off, thereby preventing unauthorized local access to the management network.

SNMPv1 Community

The SNMPv1 packet contains a password (called community string) that must be known by both the manager and the agent. Different community names can be defined for read and read/write access. The community string is, however, transferred unencrypted.

SNMP Manager Identity

This is an enhancement of the SNMPv1 Community feature. Here, the SNMP manager's IP address must be configured in the AXXESSIT device subject to management. Only legal combinations of community name and source IP address in SNMP requests are accepted.

SNMP read/write control

The access rights of the registered management systems can be set to read/write or read only.

VLAN (802.1Q)

This security mechanism relates to the IP in-band option only: By configuring a separate VLAN for the management traffic and assigning an IP address to it, the end-users will not be able to access the device or generate traffic into the management VLAN.

CLI AccessControl

CLI is protected by user name and password. CLI is by default a superuser and can block all remote SNMP users by changing the access rights and passwords. Remote CLI access via Telnet must in addition have a Telnet password.

3.6 MANAGEMENT

The following main features are supported by the AXX155E management system:

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

The AXX155E management solution is based on an embedded SNMP agent, which can be accessed locally or from a remote management application.

Supported MIB's

Two enterprise specific MIBs are supported:

- ROS MIB (RADLAN)
- AXX155E MIB (AXXESSIT ASA)

In addition to the enterprise specific MIBs, the standard MIBs in the below Table 3.9. , are partly supported. By "partly supported" is meant that relevant parts of the listed MIBs are implemented and used to manage the associated features in the NEs (Network Elements). Not all parts of the MIBs are used, and there are other features in the NEs not managed through standard MIBs (because covering standard MIBs for the latter features do not exist).

RFC #	Mnemonic	Title
1213	MIB-II	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
1724	RIP2-MIB	RIP Version 2 MIB Extensions
1471	PPP-LCP-MIB	The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol
1473	PPP-IP-NCP-MIB	The Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol
1493	BRIDGE-MIB	Definitions of Managed Objects for Bridges
1757	RMON-MIB	Remote Monitoring (RMON) Management Information Base
1850	OSPF-MIB	OSPF Version 2 Management Information Base
2096	IP-FORWARD-MIB	IP Forwarding Table MIB
2233	IF-MIB	The Interfaces Group MIB using SMIv2
2495	DS1-MIB	Definitions of Managed Objects for the DS1, E1, DS2 and E2 Interface Types
2558	SONET-MIB	Definitions of Managed Objects for the SONET/SDH Interface Type
2665	EtherLike-MIB	Definitions of Managed Objects for the Ethernet-like Interface Types.
2674	P-BRIDGE-MIBQ-BRIDGE-MIB	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions
2932	IPMROUTE-STD-MIB	IPv4 Multicast Routing MIB
2933	IGMP-STD-MIB	Internet Group Management Protocol MIB
2934	PIM-MIB	Protocol Independent Multicast MIB for IPv4

Table 3.9. MIB’s of AXX155E

AXX155E can be managed and supervised by means of the AXXCLI Command Line Interface (AXXCLI) or by a SNMP supporting management systems. AXXCLI is an ASCII based VT-100 terminal interface, but if desirable to monitor and maintain multiple AXX155E devices, a more complete management solution is recommended/required, e.g. AXXINSITE.

AXX155E can be fully managed by means of the AXXCLI interface. Hence, e.g. AXXINSITE must be regarded as an optional product, which provides more powerful and user-friendly element management. Refer AXXINSITE User Guide for more information.

3.7 MANAGEMENT CONNECTIVITY

The management traffic pertinent to AXXESSIT devices is IP carrying SNMP, TELNET and FTP application protocols. In order to support connectivity in any possible topology and application, the AXXESSIT products support management traffic on a mix of interfaces:

- Dedicated management port (Ethernet)
- LAN ports (Dependent on product and configuration)
- WAN ports (Dependent on product and configuration)
- SDH ports (DCC)
- Local VT-100 serial port

The support of these interfaces is dependent on type of product and configuration. The subsequent paragraphs describe the above mentioned interfaces in further detail. The purpose of the VT-100 serial port is to access a local command line interface (AXXCLI) by utilising terminal emulating software and is not discussed in further detail. Most AXXESSIT products support remote access to the AXXCLI via TELNET.

3.7.1 Dedicated Management Port (MNGT port)

AXXESSIT devices equipped with a dedicated Ethernet port for management, called the "MNGT Port", can be connected directly to a computer with a network interface card (NIC) for local management, e.g. with the AXXCRAFT toolkit. The MNGT port can also be used for connecting an AXXESSIT device to an external management network, and it may serve as the gateway to several AXXESSIT devices remote in the network. In addition it can provide connectivity for other needs i.e. remote control of switches etc. The MNGT port can be disabled, e.g. in order to avoid unauthorized access.

The management port is for security reasons isolated from the VLAN membership possibility. If desirable, the management can be reached through a VLAN by connecting this port to an external VLAN aware switch or to a LAN port on an AXXESSIT device.

3.7.2 Ethernet ports

Dependent on the inserted modules, the AXXESSIT multiplexers contain, a L2/L3 switch. This switch is mainly intended for customer connections, but the switch can also be used for MCN purposes. The Ethernet ports can be defined as LAN ports and WAN ports.

LAN ports

The LAN ports are Ethernet ports used for connecting end-user IP traffic to the AXXESSIT device. This can typically be ISP/ASP access or LAN interconnect etc. A LAN port can potentially be a router port, member of one or more VLANs, or a combination of both (the VLAN gets an IP address). The LAN port can be utilized for MCN purposes and in combination with WAN ports the configurations can be quite sophisticated.

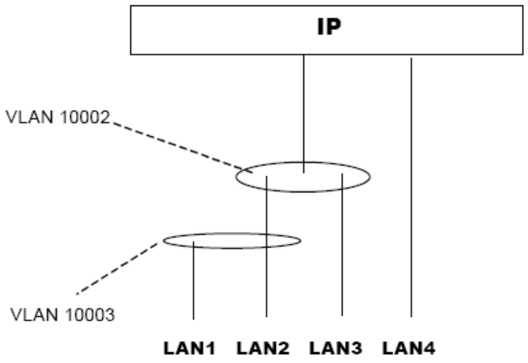


Figure 3-12.   LAN port MCN example

WAN ports

The WAN ports are the logical Ethernet ports that can be mapped into one or more VC-12s in a VC-4 container (STM-n signal). Apart from this, a WAN port has the same characteristics as a LAN port as described above.

3.7.3 SDH ports

The SDH architecture defines data communication channels (DCC) for transport of management traffic in the regenerator section (DCC_R - 192 kbit/s - D1-D3 in RSOH) and in the multiplexer section (DCC_M - 512 kbit/s - D4-D12 in MSOH). The AXXESSIT products can utilize the SDH-DCC channel using several different methods:

3.7.4 Feature Support

This section gives an overview of the communications and security features supported by the AXXESSIT product types.

Feature	AXX155E
Communication	
IP/DCC-Broadcasted DCCR	X
IP/DCC & Broadcasted DCCM	X
IP/DCC & Routed	X
IP/PPP DCCR	X
IP/PPP DCCM	X
IP unnumbered	X
IP-Forwarding	X
IP-Routing Numbered mode (RIP ver. 1.2 and OSPF)	X (a)
IP-Riuting Unnumbered mode (OSPF)	X
CLNP Routing	X (b)
IP/OSI (OSI-NE) DCCR	X (b)
IP/OSI (OSI-NE) DCCM	X (b)
IP/OSI (OSI-Gateway)	X (b)
In-band	X
Security & Traffic Control	
Management Port on/off	X
SNMPv1 Community	X
SNMP Manager Identity	X
SNMP read/write control	X
VLAN (802.1Q)	X

Table 3.10. Feature support

Legend

X	**= Supported**
NA	**= Not applicable**
(a)	= Software based routing if no license loaded.
(b)	= OSI license required.
(c)	= Dependent of equipped module(s)
(d)	= Indirectly by using a crossed cable between MNGT port and a LAN port. A separate VLAN must be configured to take care of management traffic

3.8 AXX155E MANAGEMENT

3.8.1 Managed objects

The description of the AXX155E management system refers to manageable objects as listed below. See “Managed Objects of AXX155E” on page 6-2 for further details.

Object Name	#	Description
Device	1	The AXX155E 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(2)	The STM-1 aggregate. Optical or Electrical. Dual ports for MSP (1+1) or single fiber operation.
Auxiliary Port	4	The general purpose auxiliary interfaces
Bridge	1	Common Bridge functionality, like VLAN and Spanning Tree

Table 3.11. Managed Objects

3.9 FAULT MANAGEMENT

The different alarms together with their relations to the managed objects are defined in “Managed Objects” starting in page 6-2.

3.9.1 Alarm handling

General

The alarms are related to a managed object as defined in Table 3.11.

The AXX155E keeps a record of current and historical alarm events. The list of current alarms contains the following parameters for each 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 3.12. Alarm Parameters

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 AXX155E 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. 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 AXX155E.

NOTE!

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!

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!

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

3.9.2 Alarms

The Alarm Severity is configurable per alarm object. Default values are assigned automatically as shown in Table 3.13. See the AXXCRAFT User Guide for details on VCAT/LCAS alarm.

Alarm		Description	Default Severity
Object-Id	**Alarm-Id**		
AXX155E	HWFAIL	Hardware failure.	Critical
	LOSSY	Loss of external sync.	Minor
	SyncHoldOver	Loss of configured synchronisation source	Major
	TEMP	Too high temperature in the unit i.e. above +45o	Critical
	FAN	FAN failure.	Major
ALARM	AUX	Dry contact alarm.	Warning
SDH (STM-1)	LOS	Loss of STM-1 signal.	Critical
	LOF	Loss of frame alignment on the STM-1 signal.	Critical
	TD	Transmit Degrade on laser (Not applicable for electrical interface).	Minor
	TF	Transmit fail on laser (Not applicable for electrical interface).	Critical
RS	TIM	Trace Identifier mismatch (J0-byte).	Critical
	CSF	Communication subsystem failure, DCCR communication failure. (Just applicable for OSI-routing)	Minor
	EXC	Excessive error defect. BER > E-5	Major
	DEG	Degraded signal defect. BER > E-6 - E-9 (default E-6)	Minor
MS	AIS	Alarm Indication signal.	Minor
	EXC	Excessive error defect.	Major
	DEG	Degraded signal defect.	Minor
	RDI	Remote Defect indication.	Minor
	CSF	Communication subsystem failure, DCCM communication failure. (Just applicable for OSI-routing)	Minor
MSP	MSP	Problem with MSP (1+1 protection) signalling with another NE across K1/K2 bytes.	Minor
AU4	LOP	Loss of pointer	Critical
	AIS	Alarm indication signal	Minor
VC4	LOM	Loss of multi-frame alignment	Critical
	UNEQ	Unequipped.	Minor
	TIM	Trace identifier mismatch (J1-byte) .	Critical

Alarm		Description	Default Severity
	PLM	Payload mismatch.	Critical
	EXC	Excessive error defect. BER > E-5	Major
	DEG	Degraded signal defect. BER > E-6 - E-9 (default E-6)	Minor
	RDI	Remote defect indication.	Minor
TU12	AIS	Alarm indication signal.	Minor
	LOP	Loss of pointer.	Critical
VC12	UNEQ	Unequipped.	Minor
	TIM	Trace identifier mismatch (J2-byte).	Critical
	PLM	Payload mismatch.	Critical
	EXC	Excessive error defect. BER > E-5	Major
	DEG	Degraded signal defect. BER > E-6 - E-9 (default E-6)	Minor
	RDI	Remote defect indication.	Minor
Tributary (E1)	LOSTX	Loss of signal.	Critical
	AISRX	Alarm indication signal network side.	Warning
	LFARX	Loss of frame alignment customer side.	Major
	LFATX	Loss of frame alignment customer side.	Major
	UNASS	Tributary (E1) activated but not mapped to an available VC-12.	Critical
Ethernet WAN-port Proprietary	WANDELAY	Differential VC-12 delay for the WAN port is greater than +/-6,5ms	Critical
	seqFail	Seq wrong channel number p2p, i.e. wrong order of VC-12 allocated to a WAN-port....orone or more VC-12 containers not carrying Ethernet traffic terminated on the WAN-port.	Critical

Table 3.13. Default Alarm Severity Table

3.9.3 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 AXX155E.

All SDH and PDH objects have a configurable two 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

Alarm		**Suppress the following alarms**
VC12	UNEQ	yes
	TIM	yes
	EXC	no
	DEG	no
	RDI	no
	PLM	yes
Tributary	AISRX	yes
	LFARX	yes

Table 3.14. Alarm Suppression table

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

Table 3.15. Alarm Suppression table for Tributary Tx-Alarms

Alarm		**Suppress the following alarms**
Object-Id	**Alarm-Id**	
VC4	EXC	Yes
	DEG	No

Table 3.16. VC4 Alarm Suppression table for EXC/DEG

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

Table 3.17. RS Alarm Suppression table for EXC/DEG

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

Table 3.18. MS Alarm Suppression table for EXC/DEG

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

Table 3.19. VC12 Alarm Suppression table for EXC/DEG

3.9.4 Alarm Collection

It is possible to view the alarms of all AXX155E devices present in the network, e.g. currently reachable from the management system. The AXX155E device stores a list of all current alarms and a log of alarm events. The size of the log of alarm events is 1000.

3.9.5 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.

3.9.6 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.

3.10 CONFIGURATION MANAGEMENT

3.10.1 Backup and Restoration of Configuration Data

It is possible to back-up the configuration data of an AXX155E device. It is possible to reload the configuration from the back-up. The back-up media must be a central repository. Any management software supplied by AXXESSIT can maintain this repository.

3.10.2 Software Download

It is possible to download a new software version to the AXX155E device. The download process does not influence traffic processing of TDM traffic (E1s) unless the update/upgrade includes FPGA changes. Ethernet traffic will always influence the Ethernet traffic running via LAN/WAN - ports and remote management connectivity will not be maintained during the reset period. 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 AXX155E reboots with the old software, and an alarm is raised.

The software can be downloaded locally via the management interface or remotely via the DCC channels.

3.10.3 Device Reset

It is possible to reset (reboot) the device with or without resetting the current configuration. Reboot have minimal impact on traffic processing. The following situations will affect Ethernet/IP traffic and require a Device reset to become operative:

- after configuration and changes of OSI(CLNP) related parameters (Ethernet/IP traffic affecting)
- when decreasing/increasing entries in tunable tables e.g. maxARP, maxIP-forwarding, maxVLAN's, maxDHCP, maxBridge, etc.
- software upgrade without FPGA fix (Ethernet/IP traffic affecting)
- software upgrade with FPGA fix (All traffic affected)

3.10.4 Device Replacement

It is possible to replace an AXX155E device with a new one with an identical physical configuration.

No manual configuration on the device is required. The AXX155E is assigned one IP address automatically from a BootP server[1] . 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 3-50). Once the configuration has been received, the AXX155E must be rebooted.

3.10.5 Feature Management

The embedded software in the AXX155E is capable of supporting all features (licensed or not licensed) finalized 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 AXX155E device, and they are stored internally in each AXX155E. The features supported by AXX155E are bridging (always activated), routing, and OSI encapsulation.

3.10.6 Managed Object Attributes

All attributes defined in the “Managed Objects of AXX155E” on page 6-2 are available for read or read/write access by the management applications specified in “Management Connectivity” on page 3-39.

[1] 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.

3.11 PERFORMANCE MONITORING

The performance monitoring functions specified below, “Aggregate port” on page 3-52, and in “Bridge port” on page 3-54, are available in both AXXCRAFT, AXXINSITE and AXXCLI.

Higher-level management systems supplied by AXXESSIT may have database-oriented storage of performance data. Contact your sales representative within AXXESSIT for more information.

3.11.1 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.

Parameter	MIB variable(s)	Comment
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.

Parameter	MIB variable(s)	Comment
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 3.20. Aggr Port Statistics parameter mappings

3.11.2 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
- etherStatsPkts1024to1536Octets

As opposed to the Aggregate port counters, the Bridge port counters must be started and stopped by the operator. AXX155E keeps no history records for the Bridge port counters.

Ping

An IP ping service is available in the AXX155E.

This service is available in all management solutions. In AXXCLI this option can be found under the Service menu options. 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. The ping session supports different packet sizes as well as number of "ping's" generated for reply.

3.12 BACK-UP AND RESTORE

It is possible to up-/ download the AXX155E configuration to/ from a TFTP server, that is :

- To save the AXX155E configuration in a file onto an TFTP server,
- To download a configuration file from a TFTP server onto the AXX155E.

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

The following read-write parameters are 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 3.21. Backup/restore Parameters

NOTE!

The backup/restore facility is supported by any AXXESSIT SNMP management solutions. Please refer relevant user guides for more information

3.13 SOFTWARE DOWNLOAD

3.13.1 Local

It is possible to load a new software version by means of a PC directly attached to the AXXCLI Port. This service requires local operator presence at the AXX155E .

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.

3.13.2 Remote

It is possible to download new AXX155E software from a remote server (i.e. via Management Port) by means of the TFTP protocol. In R1 this service can be activated by AXXMASTER only.

The AXX155E supports two banks, one for the active (current) file and one for the new file. The AXX155E traffic is not being affected.

At the end of the remote software download, will automatically invoke a restart. AXX155E 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 3.22. SW download parameters

3.14 SECURITY

The management access to the AXX155E 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 AXXCLI 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 AXXCLI password.

The AXXCLI user has SUPER access rights.

3.15 MANAGEMENT LOGS

This section summarizes the various logs used for alarms, errors and statistics. As visualized in the figure "Management logs", all logs except the Trap Log are located inside the AXX155E .

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

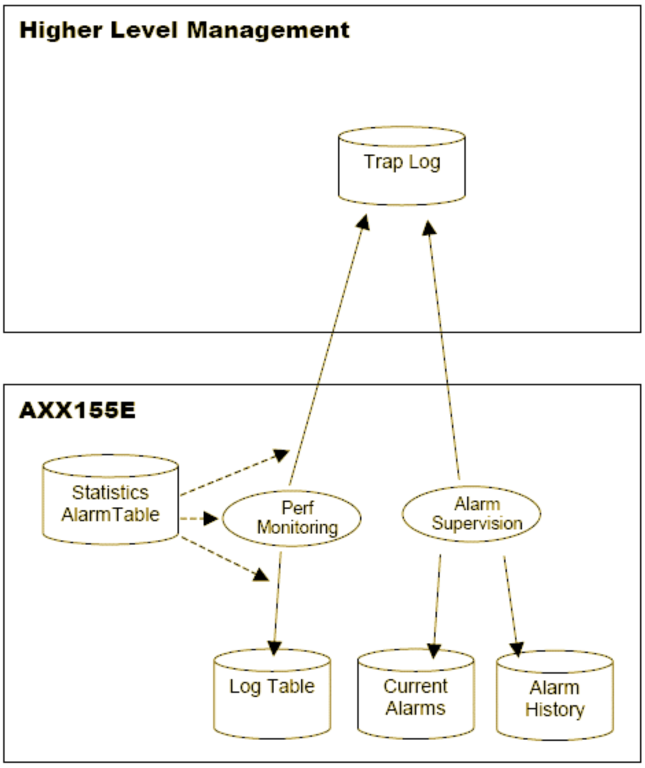


Figure 3-13. Management logs

Name	Location	Description
Trap Log	Higher Level Management	Contains all events reported by the AXX155E , including the alarm and performance traps.
Statistics Alarm Table	AXX155E	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	AXX155E	This table contains the logged performance alarms controlled by the Statistics Alarm Table. This table corresponds to the RMON log Table.
Current Alarms	AXX155E	This table contains all alarms currently on.
Alarm History	AXX155E	This table contains a log of all events, including alarm events. The latest 1000 events are stored.

Table 3.23. Management logs

4

PHYSICAL INTERFACES

AXX155E

4.1 FRONT AND REAR VIEW

This chapter describes the different types of physical interfaces in AXX155E.

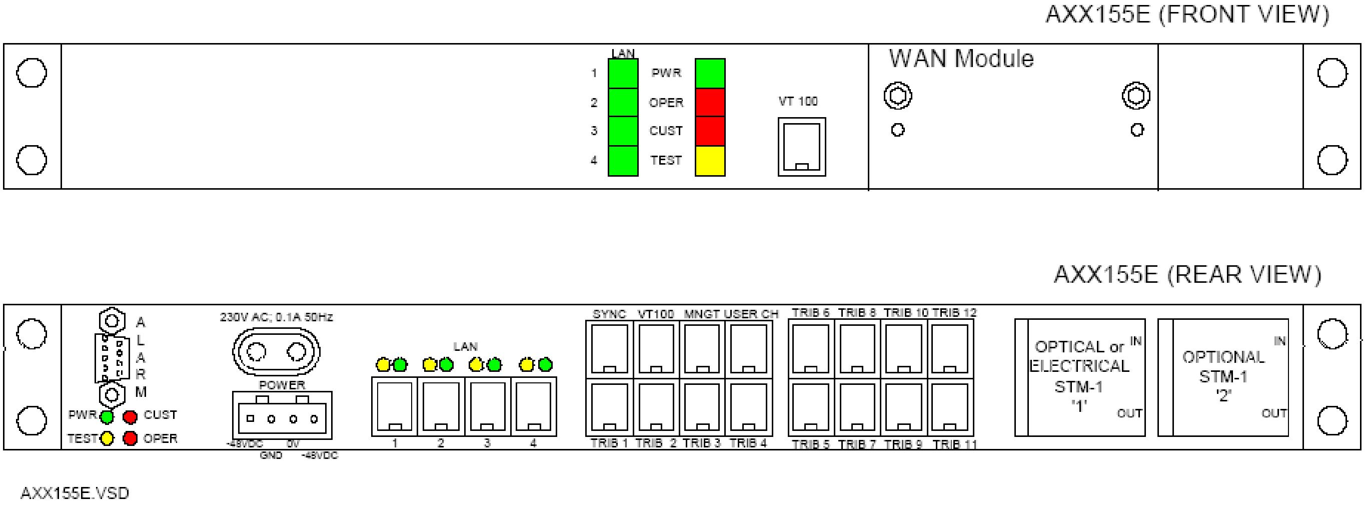


Figure 4-1. AXX155E front and rear view

4.1.1 Form of construction

The equipment is provided as a sub-rack suitable for mounting within a 19-inch equipment cabinet.

Height (mm)	Width (mm)	Depth (mm)
44	445	240

Table 4.1. Mechanical characteristics

The weight of the unit is:

- 3,8 kg with WAN modul.
- 3,7 kg without WAN modul.

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

4.2 INTERFACES

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

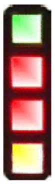
Interface	No. of interfaces	Logical name
Optical/Electrical	1 or 2	Aggregate Port
Tributary	12	Tributary Port
Ethernet	5	LAN Ports
Ethernet	1	Management Port
Ethernet	1 (+3)	WAN port(s). Total of 4 ports applies when WAN-module inserted.
Alarm	6	4 alarm input and 2 alarm out
Synchronisation	1	Sync Port
RS232	1	AXXCLI Port
Power supply	2	-48V DC and 220V AC
User Channel	1	User Channel Port
Indicators	8	4 Traffic Indicators, Power , Operator, Customer, Test

Table 4.2. AXX155E interfaces

NOTE!

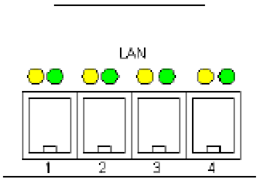
The aggregate ports can be delivered as either optical- or electrical-variants, single- or dual- fiber operation, and finally but not least one- or two ports when protection (1+1) needed in setup. Refer pricelist or contact your sales representative within AXXESSIT.

4.3 LIGHT EMITTING DIODES (LEDS)



		State		
Identity	**Color**	**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.	

Table 4.3. LEDs - Operational status

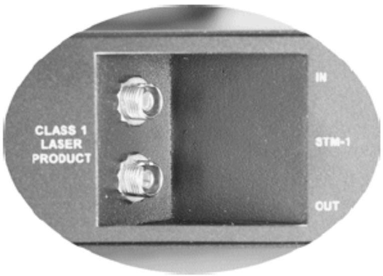


		State			
Identity	**Color**	**On**	**Flashing**	**Off**	**Identity**
LANn 100 Mb (n=1,2,3,4)	Green	Left	100 Mb	NA	NA
LANn 100 Mb (n=1,2,3,4)	Green	Right	Link OK	Ethernet traffic in operation	Link down
LANn 10 Mb (n=1,2,3,4)	Yellow	Left	10 Mb	NA	NA
LANn 10 Mb (n=1,2,3,4)	Green	Right	Link OK	Ethernet traffic in operation	Link down

Table 4.4. LEDs - LAN Ports

4.4 OPTICAL AGGREGATE LINE INTERFACE

The AXX155E aggregate line interface is bi-directional with a transmit (Tx) and a receive (Rx) direction. There are variants of AXX155E with Tx and Rx transmission on separate fibres as well as on a single fibre.



The two-fibre variants are a Short-Haul (SH), ITU-T Rec. G.957 S-1.1 compliant variant and a Long-Haul (LH) variant. The transmission cable can be either Single Mode (SM) or Multi Mode fibre (MM) type.

The single fibre version has a SM-fibre interface and the optical wavelength is the same in both directions

AXX155E is also available as protected variants with duplicated optical interfaces and protection switching logic to maintain traffic in case of fibre faults.

The optical interfaces are located at the rear panel and there are several choices of optical connector types:

FC/PC, SC/PC, E-2000, E2000/APC8, LC

Other types are available on request.

4.4.1 Parameters

The definitions of optical parameters and reference points S and R refer to ITU-T G.957. Reference point S means transmit direction while R is the receive direction of the fibre.

4.4.2 Optical power budget AXX155E SH and LH, two-fibre

Parameter		**Short-Haul**	**Long-Haul**	
Type of fibre:	ITU-T Rec. G.652	10/125		µm
	ITU-T Rec. G.651	50/125		
	IEC 739-2	62.5/125		
Modulation rate on optical line		155 520		kbit/s
Wavelength range		1270 - 1335		nm
Transmitter at reference point S				
Source type		MLM		
Spectral characteristics (max. RMS width)		3		nm
Mean launched power (max.)		-8	3	dBm
Mean launched power (min.)		-12	0	dBm
Min. extinction ratio		8.2		dB
Optical path between S and R				
Attenuation range		0 - 17	0-29	dB
Max. tolerable dispersion		280		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 1010)		-30		dBm
Min. overload		0		dBm
Max. optical path penalty		1	1	dB
Max. reflectance at R		NA		

Table 4.5. Optical power budget AXX155E SH and LH

Factory testing to Power Budget: Mean Launched Power adjusted to -10dBm (SH) and +0.5dB (LH). Receiver sensitivity test: Max. signal level -32 dBm at R point at BER < 1 in 10-^{10}. Initial equipment margin: >3dB.

4.4.3 Optical power budget AXX155E single fibre

Bi-directional transmission on a single fibre is possible using either an integrated fibre directional coupler version of AXX155E or by using an external coupler with the AXX155E two-fibre versions.

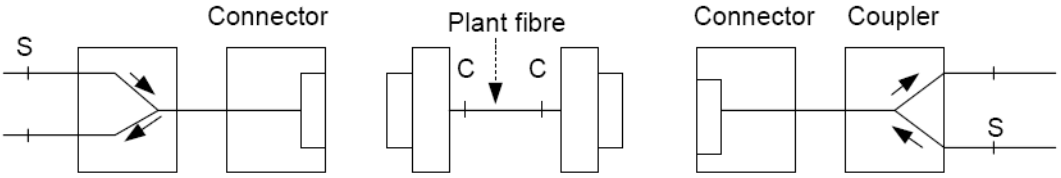


Figure 4-2. Bidirectional single fibre line

AXX155E single fibre has the same specification on the S and R interfaces as the two fibre SH version. With a directional coupler as in the table below:

Directional Coupler Properties	Short-Haul	Long-Haul	
Directivity	40		dB
Maximum insertion loss in coupler	4		dB

Table 4.6. Directional Coupler Properties

4.4.4 The optical power budget below applies:

Parameter	Value
Type of fibre: ITU-T Rec. G.652	10/125 µm
Modulation rate on optical line	155 520 kbit/s
Wavelength range	1270 - 1330 nm
Transmitter at reference point S	
Source type	MLM
Spectral characteristics (max. RMS width)	3nm
Mean launched power (max.)	-11 dBm
Mean launched power (min.)	-16 dBm
Min. extinction ratio	8.2 dB
Optical path between C and remote C	
Attenuation range	0 - 10 dB
Max. tolerable dispersion	280 ps/nm
Min. optical return loss of cable plant at C	30 dB
Max. discrete reflectance between C points	-36 dB
Receiver at reference point R	
Min. sensitivity (BER < 1 in 1010)	-26 dBm
Min. overload	0 dBm
Max. optical path penalty	0 db

Table 4.7. Optical budget single fibre parameters

NOTE! *The AXX155E power monitoring of mean Rx power is measured on the R interface.*

4.4.5 Example of Cable planning for AXX155E

Cable Loss, according to ITU-T Rec. G.957	Single Mode fibre Acc. to ITU-T G.652	Multi Mode fibre Acc. to ITU-T G.651
Fibre Cable Attenuation	0.5 dB/km *)	1.0 dB/km
Cable Margin (Mc)	Inc.. in *)	3 dB
Loss in Optical Distribution Frame	Inc.. in *)	1 dB
Cable Dispersion:		
Maximum Chromatic Dispersion Coefficient	3.5 ps/nm*km	6 ps/nm*km
Modal bandwidth	-	800 MHz*km
Overall bandwidth (Requirement >80 MHz)	-	84 MHz (9km)

Table 4.8. Typical Cable Parameters

AXX155E version/ type of fibre		Loss Limited Span	Dispersion Limited Span	Overall Link Span
Short-Haul	SM	34 km	80 km	34 km
	MM	13 km	9 km	9 km
Long-Haul	SM	58 km	80 km	58 km
	MM	25 km	9km	9 km
Single fibre	SM	20 km	80 km	20 km

Table 4.9. Typical Link Spans for AXX155E

4.4.6 Optical Output Jitter

Jitter on the Tx optical output signal is lower than the values specified in ITU-T Rec. G.813.

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

Table 4.10. Optical output jitter requirements as given in ITU-T Rec. G.813.

4.4.7 Maximum Tolerable Input jitter

The input aggregate port tolerates the input litter and wander specified in ITU-T Rec. G.825. This applies in the whole operating optical range of the receiver.

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

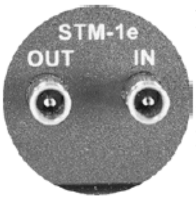
Table 4.11. Maximum Tolerable Input Jitter on the Optical Rx interface.

4.4.8 Compliance

Standard	Comment
ITU-T G.652	Single Mode Fibre specification 10/125
ITU-T G.651	Multi Mode Fibre specification 50/125 µm
IEC 793-2	Multi Mode Fibre specification 62.5/125 µm
ITU-T G.707	Optical line signal
ITU-T G.783	RX pull-in and hold range
ITU-T G.813	Optical output jitter
ITU-T G.825	Optical input jitter
ITU-T G.957	Optical spectrum, Optical output power, Optical eye diagram, Optical extinction ratio.

Table 4.12. Optical interface compliance

4.5 ELECTRICAL



It is possible to equip the AXX155E 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 “Protection” on page 3-3.

4.5.1 Connector type

The connector is 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 4.13. 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 4.14. Electrical input jitter parameters

Compliance

Standard	Comment
ITU-T G.703	Cable attenuationInput reflection lossInput port immunity against reflectionOutput 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 4.15. Electrical interface compliance

4.6 TRIBUTARY PORTS

4.6.1 Connectors

The connectors are RJ-45 connectors, with the following pin-out:

Pin	Signal
1	P120OUT
2	N120OUT
3	GND
4	P120IN
5	N120IN
6	SHIELD
7	NC
8	NC

Table 4.16. Pin-out tributary interface

NOTE! *The outer screen is always connected to ground.*

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

4.6.2 Balun 120 -> 75 W

An additional balun has to be used to provide access for TDM tributaries with 75 W 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 AXX155E .

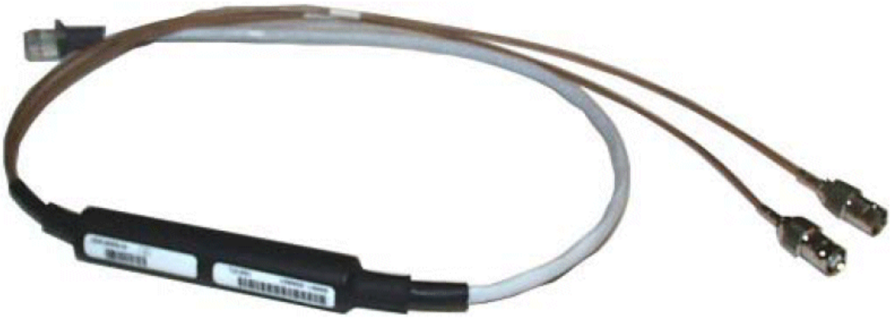


Figure 4-3.   120/75 ohm balun

4.6.3 Parameters

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 4.17. Tributary input jitter parameters

Input reflection loss

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

Table 4.18. Tributary input reflection loss

Output jitter

The requirements for output jitter in the absence of input jitter and pointer movements are:

Filter bandwidth	Jitter output (p-p)
20 Hz - 100 kHz	< 0.25 UI
700 Hz - 100 kHz	< 0.075 UI

Table 4.19. Tributary output jitter without pointer movements

The requirements for output jitter in the absence of input jitter but with pointer movements are:

Filter bandwidth	Jitter output (p-p)
20 Hz - 100 kHz	< 0.4 UI
700 Hz - 100 kHz	< 0.075 UI

Table 4.20. Tributary output jitter with pointer movements

Compliance

Standard	Comment
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
ITU-T G.823	Max. tolerable input jitter

Table 4.21. Tributary interface conformance

4.7 LAN PORTS AND MANAGEMENT PORT

4.7.1 Connectors

The connectors are RJ-45 connectors, with the following pin-out:

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

Table 4.22. Pin-out Ethernet ports

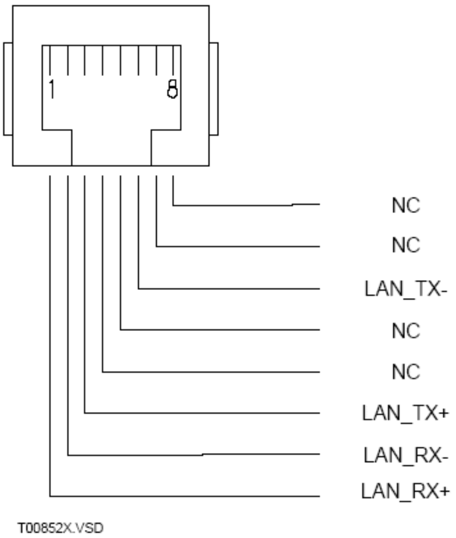


Figure 4-4. LAN interface connector

NOTE!

In order to conform to the requirements of EN50081-1 Class B it is recommended to use a STP cable for connection to the Management port. If a UTP cable is used the the unit conform to EN50081-1 Class A.

4.7.2 Parameters

The parameters on the Ethernet interface are in accordance with the specifications given in the Compliance chapter below.

Compliance

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 4.23. Ethernet compliance

4.8 ALARM INTERFACE

4.8.1 Connectors

The alarm interface connector is a 9 pin D- type connector, with the following pin-out:

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 4.24. Pin-out alarm interface connector

4.8.2 Parameters

Alarm input

Parameter	Value
Nominal open contact voltage	3.3V
Nominal closed contact current	1 mA
Max. closed contact resistance	0.8 kohm
Min. open contact resistance	10 kohm

Table 4.25. Electrical specification at alarm input

Alarm output

Parameter	Value
Maximum load bias referred to common return	+/-75V
Maximum load current	50mA
Common return to earth	+/-250V
Maximum contact resistance	50 ohm

Table 4.26. Electrical specification at alarm output

4.9 SYNCHRONISATION PORT

AXX155E has one 2048 kHz synchronisation output port and input port.

4.9.1 Connectors

Both input and output is provided on 8 pin RJ-45 connector, with the following pin-out:

Pin	Signal
1	SYNC_OUT+
2	SYNC_OUT-
3	GND
4	SYNC_IN+
5	SYNC_IN-
6	SYNC_SCREEN
7	NC
8	NC

Table 4.27. Pin-out synchronisation port

NOTE! *The outer screen is always connected to ground.*

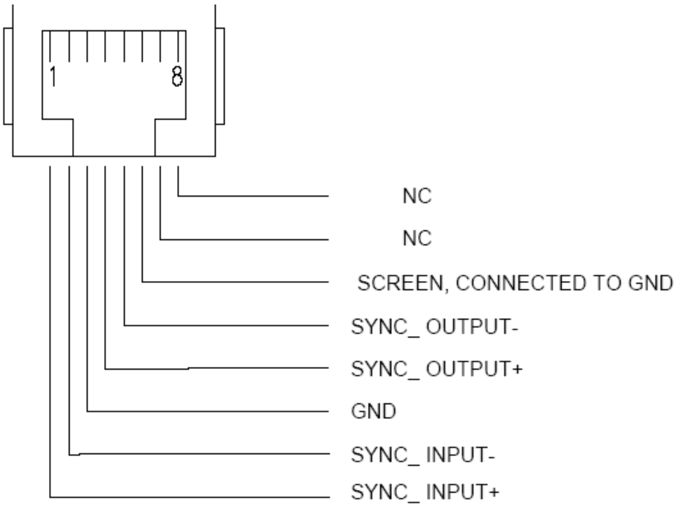


Figure 4-5. Synchronisation input/output connector

4.9.2 Parameters

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 4.28. Synchronisation input jitter parameters

Input reflection loss

Frequency	Reflection loss
2048 kHz	15 dB

Table 4.29. Synchronisation input reflection loss parameters

Output jitter

Filter bandwidth	Jitter output (p-p)
20 Hz - 100 kHz	< 0.05UI

Table 4.30. Synchronisation output jitter parameters

4.9.3 Compliance

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

Table 4.31. Synchronisation port compliance

4.10 CLI PORT

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

4.10.1 Connectors

The RS232 interface for AXX155E is provided using a RJ-45 connector, with the following pin-out:

Pin	Signal
1	GND
2	TxD
3	RxD
4	DB_TxD
5	NC
6	RTS
7	DB_RxD
8	NC

Table 4.32. Pin-out CLI connector

NOTE! *Pin 4 and 7 are only used for debug purposes.*

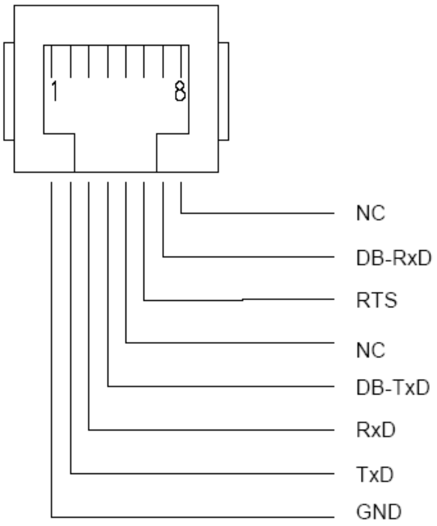


Figure 4-6. AXXCLI port connector

4.10.2 Parameters

The interface is running at a data rate of 19.200 baud. The interface is in accordance with the specifications given in table below.

Compliance

Standard	Comment
EIA RS-232	Physical interface

Table 4.33. CLI port compliance

4.11 POWER SUPPLY

AXX155E supports two different power supplies:

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

4.11.1 Connectors

The -48V DC supply input on the AXX155E is provided via a 4 pin power connector, with the following pin-out:

Pin	Signal
1	-48V (supply 1)
2	GND
3	0V (-48V return)
4	-48V (Supply 2)

Table 4.34. Pin-out power supply connector

The 220V mains supply input on the AXX155E is provided via a standard connector according to EN60320.

4.11.2 Parameters

The -48V DC input and the 220V mains input are according to the specifications given in the table below. See “AXX155E - Cabling” on page 1-13 and “Installation in Restricted Access Location (RAL)” on page 1-8 for details on DC power voltage range outside RAL.

.

Parameter	Limit
Power dissipation	Less than 40W
Fuse	1.5A
Battery voltage range	-36 to -72 [a]V DC
Mains voltage	-230V AC +/- 10%

[a] -60V outside of RAL

Table 4.35. Power supply parameters

Compliance

Standard	Comment
EN/IEC 60950	Single phase 230 V 50 Hz AC mains supply
ETS 300 132-2	Power supply interface at the input to the telecommunication equipment; Part 2: Operated at DC
ETS 300 253	Earthing and bonding of telecommunication equipment in telecommunication centers

Table 4.36. Power supply conformance

4.12 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.

4.12.1 Connector

The user channel interface for AXX155E 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 4.37. Pin-out user channel connector

Compliance

Standard	Comment
ITU-T V.11	

Table 4.38. User channel interface conformance

4.13 FAN UNIT

The main feature of the fan unit is to ventilate the 19"/ 1U cabinet used for AXX155E. The fan unit is a plug-in device consisting of a circuit board with two fans. The air is sucked in via two circular openings in the left sidewall, and emerges via holes in the right side cabinet wall. Two fans are used to improve reliability and give a lifetime of 10 years for this module

NOTE! *Make sure that there is minimum 10 cm free space around the air intake (placed in the left sidewall)*

4.13.1 Replacement

The fan module is easily replaceable from the front of the AXX155E unit without traffic affection. If the fan-unit must be replaced, this is done by open the screw found on the rear and gently pull the unit towards you with a pliers.

4.13.2 Fan operation

NOTE ! *When ambient temperature is below ~53^{o}C , none of the fans are running*

Fan operation is shown in the table below. Threshold temperatures are approximate and depend on ventilation conditions.

The ventilation holes must **NOT** be blocked.

Table 4.39. Fan operation and alarm

CONDITIONS:	MAIN FAN	STAND-BY FAN	ALARMS
Ambient temperature below lower (~53^{o}C)	Not running	Not running	No Alarm
Ambient temperature between (~53oC) and ~58^{o}C)	Running, the speed is increased with increasing temperature.	Not running	Temperature Alarm
Ambient temperature between (~58oC) and ~63^{o}C)	Running on full speed.	Running on full speed.	Temperature Alarm
Ambient temperature above ~63^{o}C)	Running on full speed.	Running on full speed.	Critical Temperature Alarm.
Every ~24-hours	Main and Stand-by roles are interchanged.		

MECHANICS & OTHER CHARACTERISTICS 5

AXX155E

5.1 MECHANICAL PARAMETERS

5.1.1 Mechanical characteristics AXX155E

Height (mm)	Width (mm)	Depth (mm)
44	445	240

Table 5.1. Mechanical characteristics

The weight of the unit is:

- 3,8 kg with WAN module.
- 3,7 kg without WAN module.

5.1.2 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
- +35oC ambient temperature
- Stress value 0.5.

Equipment	MTBF[a] [Years]
AXX155E non-redundant optics	40
AXX155E redundant optics	47

[a] MTBF : Mean Time Before Failure

Table 5.2. Reliability

5.2 OTHER CHARACTERISTICS

5.2.1 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 5.3. Specification of Climatic and Mechanical Environment

5.2.2 Storage and transport

The equipment meets the requirements in ETS 300 019, Class 1.1 and class 2.2. Supported storage temperature range : -40^{O}C to +70^{O}C.

5.2.3 Health and safety

The equipment meets the requirements in EN60950 and EN60825.

5.2.4 Environmental conditions

The equipment conforms to the requirement of product standard EN 300 386 for EMC related specifications. This standard defines tests for the equipment, which refers to the following standards:

Generic standards

- EN 50082-1
- EN 50081-1

Product family standards

- EN 55022
- EN 55024

Basic standards

- EN 61000-3-2
- EN 61000-3-3
- EN 61000-4-2
- EN 61000-4-3
- EN 61000-4-4
- EN 61000-4-5
- EN 61000-4-6
- EN 61000-4-11

The equipment operates under all environmental conditions detailed in ETSI EN 300 019-2-3 Class 3.2.

MANAGED OBJECTS

6

AXX155E

6.1 MANAGED OBJECTS OF AXX155E

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
AXX155E R3	AXX155E R3 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.
Interface	Logical IP interface on router.
IP/IPX Router	Routing of IP and IPX traffic including routing protocols.
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 6.1. Managed Objects

6.2 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, CRITICAL. This is not shown in the tables.

6.2.1 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 6.2. Alarm attributes

Alarm ID	Description
AUX	Alarm situation on alarm input port.

Table 6.3. Alarm input port alarm

6.2.2 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 6.4. AU-4 attributes

Alarm ID	Description
AIS	Alarm indication signal
LOP	Loss of pointer

Table 6.5. AU-4 alarms

6.2.3 AXX155E R3

Attribute	Access	Type	Description
DESCRIPTION	R	String	Device type (always AXX155E R3)
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
ADMINISTRATIVESYNC 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.
OPERATIONALSYNC SOURCE	R	string	Actual SDH synchronisation source. Same values as for AADMINISTRATIVE SYNC SOURCE, plus HOLDOVER
REMOTE DEVICE	R/W	IP address	IP address of the remote AXX155E.
ALARM REPORTING	R/W	choice	ENABLED or DISABLED. Set the alarm reporting capability for this object. The alarms are listed below.

Table 6.6. AXX155E R3 attributes

Alarm ID	Description
HWFAIL	Hardware failure
LOSSY	Loss of external synchronisation (Sync port)
TEMP	To high temperature in the unit
FAN	Failure of one or both fans

Table 6.7. AXX155E R3 alarms

6.2.4 Bridge

General Bridge Parameters

Attribute	Access	Type	Description
BRIDGE-ADDRESS	R	MAC	The device MAC address
BRIDGE-TYPE	R	string	Bridge Type, always "Transparent only" for AXX155E.
FORWARDING TABLE AGING TIME	R/W	integer	User-defined number of seconds the learned entries remain in the Forwarding Table(s) (minimum = 10 secs).

Table 6.8. General bridge attributes

The following attributes exist for each node or interface known to the bridge (Unicast Forwarding Table).

Attribute	Access	Type	Description
PORT	R/W	integer	Port through which the MAC has been learned.
MAC-ADDRESS	R/W	MAC	MAC address of the node.
VLAN-ID	R/W	integer	VLAN identifier to which theMAC address applies.
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), MGMT (the entry is a static set by the operator), or OTHER.
COUNT	R	integer	Current Unicast Forwarding Table size (per VLAN)

Table 6.9. Unicast Forwarding Table attributes

The following attributes exist for each multicast MAC address / VLAN-ID pair known to the bridge (Multicast Forwarding Table).

Attribute	Access	Type	Description
VLAN-ID	R	integer	VLAN identifier to which the multicast MAC address applies.
MAC-ADDRESS	R	MAC	Destination multicast MAC address.
EGRESS PORTS	R	list	Indicates a list of ports in a VLAN to be used to send frames to the multicast MAC address.
LEARNT	R	choice	Indicates the subset of ports from the list in EGRESS PORTS which were identified by IGMP snooping.

Table 6.10. Multicast Forwarding Table attributes

The following attributes exist for each VLAN-ID (Multicast Forward All Table).

Attribute	Access	Type	Description
VLAN-ID	R	integer	VLAN identifier of the Forward All Group.
EGRESS PORTS	R	list	Indicates a list of ports in a VLAN to be used to send frames to the multicast MAC address.
STATIC PORTS	R/W	list	Indicates a list of ports in a VLAN which can participate in a Forward All group.
FORBIDDEN PORTS	R/W	list	Indicates a list of ports in a VLAN which cannot participate in a Forward All group.

Table 6.11. Multicast Forward All Table attributes

The following attributes exist for each VLAN-ID (Multicast Forward Unregistered Table).

Attribute	Access	Type	Description
VLAN-ID	R	integer	VLAN identifier of the Forward Unregistered group.
EGRESS PORTS	R	list	Indicates a list of ports in a VLAN to be used to send frames to the multicast MAC address.
STATIC PORTS	R/W	list	Indicates a list of ports in a VLAN which can participate in a Forward All group.
FORBIDDEN PORTS	R/W	list	Indicates a list of ports in a VLAN which cannot participate in a Forward Unregistered group.

Table 6.12. Multicast Forward Unregistered Table attributes

The following attributes exist for each multicast MAC address / VLAN-ID pair known to the bridge (Multicast Static Table).

Attribute	Access	Type	Description
VLAN-ID	R/W	integer	VLAN identifier to which the multicast MAC address applies.
MULTICAST MAC ADDRESS	R/W	MAC	Destination multicast MAC address.
RECEIVE PORTS	R/W	choice	Indicates the port number of the port from which a packet must be received in order for this entry's filtering information to apply.
STATIC PORTS	R/W	list	Indicates a list of ports to which packets received from, and destined to, are always forwarded. This is regardless of the IGMP snooping setting.
FORBIDDEN PORTS	R/W	list	Indicates a list of ports to which packets received from, and destined to, must not be forwarded. This is regardless of the IGMP snooping setting.
STATUS	R/W	choice	Possible values are PERMANENT, DELETE ON RESET (the entry is deleted after a bridge reset), or DELETE ON TIMEOUT (the entry is deleted when it has timed out - aging mechanism).

Table 6.13. Multicast Static Table attributes

MAC Multicast Parameters (IGMP snooping)

Attribute	Access	Type	Description
MAC MULTICAST FILTERING ENABLE	R/W	choice	Enables multicast on a device. Legal values are TRUE or FALSE.
IGMP SNOOPING MIB VERSION	R	integer	Indicates the software version of IGMP that is running on the device.
IGMP SNOOPING ENABLE	R/W	choice	Enables IGMP learning on a device. Legal values are TRUE or FALSE.
IGMP SNOOPING HOST AGING TIME	R/W	integer	Indicates the amount of time (in seconds) before aging out an entry in the MAC Multicast Group Table.
IGMP SNOOPING ROUTER AGING TIME	R/W	integer	Indicates the amount of time (in seconds) before aging out an entry in the MAC Multicast Router Table.

Table 6.14. MAC Multicast General attributes

The following attributes exist for per VLAN (tag), per port and per MAC multicast address (MAC Multicast Group Table).

Attribute	Access	Type	Description
TAG	R	integer	Identifies the VLAN.
PORT	R	integer	Port number in the VLAN from which multicast group information was learned.
ADDRESS	R	MAC	MAC multicast group address.
EXPIRY TIME	R	integer	Indicates the (minimum) amount of time before the entry is aged out..

Table 6.15. MAC Multicast Group Table attributes

The following attributes exist for per VLAN (tag), and per port (MAC Multicast Router Table).

Attribute	Access	Type	Description
TAG	R	integer	Identifies the VLAN.
PORT	R	integer	Port number in the VLAN for which this entry contains information for an IP multicast Router.
EXPIRY TIME	R	integer	Indicates the (minimum) amount of time before the entry is aged out..

Table 6.16. MAC Multicast Router Table 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	perDevice or perVlan.
MUST-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
BRIDGE-MAX-AGE	R/W	integer	The maximum age (in seconds) of STP-information learned from the network on any port before it is discarded
BRIDGE-HELLO-TIME	R/W	integer	Time (in seconds) between transmission of config messages through a given port
BRIDGE-FORWARD-DELAY	R/W	integer	Amount of time a bridge remains in a listening and learning state before forwarding the packets.
STP-MIB-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
MAX-AGE	R	integer	The maximum age (in seconds) currently in use by all the bridges within the spanning tree.
HELLO-TIME	R	integer	Time (in seconds) between transmission of config messages through a given port currently in use by all the bridges within the spanning tree.
HOLD-TIME	R	integer	Minimum time (in seconds) between transmission of config messages through a given port (hard coded = 100 hundredths of sec, i.e. 1 sec).
FORWARD-DELAY	R	integer	Amount of time a bridge remains in a listening and learning state before forwarding the packets (value currently in use by all the bridges within the spanning tree).

Table 6.17. General STP 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	bridgeidentifier	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	bridgeidentifier	The Bridge Identifier, which this port considers to be the Designated Bridge for this port segment, with priority being included.
DESIGNATED-PORT	R	portIdentifier	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 6.18. STP port attributes

The following attributes exists per VLAN and per port of the bridge (port specific Rapid Spanning Tree Parameters):

Attribute	Access	Type	Description
VLAN	R	integer	VLAN ID.
PORT	R	integer	Port number.
STATUS	R/W	choice	Indicatres if the port is an edge port. Legal values are FALSE or TRUE.

Table 6.19. Rapid STP port attributes

The following attributes exists per VLAN (Rapid Spanning Tree Force Software Version Table):

Attribute	Access	Type	Description
VLAN	R	integer	VLAN ID.
STATE	R/W	choice	Specifies whether this Bridge uses the normal RSTP algorithm, or the STP Compatibility algorithm. Legal values are: STP COMPATIBILITY, or NORMAL RSTP.

Table 6.20. Rapid Spanning Tree Force Software Version attributes

The following attributes exists per port (Traffic Control Port Priority Table):

Attribute	Access	Type	Description
PORT	R	integer	Port number.
DEFAULT PRIORITY	R/W	integer	Indicates the default priority assigned to the ingress port. Packets are assigned this default priority if they are not tagged. Legal values are [0:7].
TRAFFIC CLASSES	R	integer	Indicates the number of traffic classes to which received packets can be mapped.

Table 6.21. Traffic Control Port Priority attributes

The following attributes exists per port and per priority (Traffic Class Table):

Attribute	Access	Type	Description
PORT	R	integer	Port number.
PRIORITY	R	integer	Priority level. Legal values are [0:7].
TRAFFIC CLASS	R/W	integer	Indicates the traffic class to which received packets with specified PRIORITY are mapped. Legal values are [0:3].

Table 6.22. Traffic Class attributes

The following attributes exists per port (Priority Group Table):

Attribute	Access	Type	Description
PORT	R	integer	Port number.
PRIORITY GROUP	R	integer	Indicates the group to which the PORT belongs. All ports belonging to a same group have the same User Priority to Traffic Class mapping

Table 6.23. Priority Group attributes

6.2.5 DCC

There are two DCC objects per SDH port, one for DCCR and one for DCCM. 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: NONE- IP BROADCAST IP ROUTING OSI ENCAPSULATION PPP
LAPD ROLE	R/W	choice	Defines the LAPD role on the DCC. Legal values are: NETWORK USER

Table 6.24. DCC attributes

6.2.6 Ethernet

Abstract object, no attribute defined.

6.2.7 Ethernet/VC12 Mapping

The following attributes exist for each WAN port.

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 2.1.1.
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 identifier pattern (15 char).
TRANSMIT-TI	R/W	string	Tx VC12 path trace identifier pattern (15 char).
CHANNEL-TI	R/W	choice	Represents the VC-12 (1-50) for which the received path trace identifier pattern is displayed in RECEIVED-TI.
RECEIVED-TI	R/W	string	Received trace identifier pattern for the VC-12 of the channel selected by RECEIVED-TI KLM.

Table 6.25. Ethernet/VC-12 mapping attributes

Alarm ID	Description
WANDELAY	Differential VC-12 delay for the WAN port is greater than +/-2ms

Table 6.26. WAN port alarms

6.2.8 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 6.27. Feature attributes

6.2.9 Firmware

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

Table 6.28. Firmware attributes

6.2.10 Interface

See IP Router and IPX Router.

6.2.11 IP/IPX Router

General parameters

Attribute	Access	Type	Description
FFT IP	R/W	choice	Enabling of IP Fast Forwarding Table. Legal values are ENABLE and DISABLE.
FFT IPX	R/W	choice	Enabling of IPX Fast Forwarding Table. Legal values are ENABLE and DISABLE.

Table 6.29. General IP/IPX attributes

IP Router parameters

Attribute	Acces s	Type	Description
IP REDUNDANCY ADMIN STATUS	R/W	choice	ENABLE or DISABLE
INACTIVE ARP TIME OUT	R/W	integer	Timeout value (in seconds) for entry in ARP table.
ARP PROXY	R/W	choice	ENABLE or DISABLE
ICMP ERROR MESSAGES	R/W	choice	ENABLE or DISABLE
RIP ADMIN STATUS	R/W	choice	ENABLE or DISABLE
RIP - LEAK OSPF ROUTES	R/W	choice	ENABLE or DISABLE
RIP - LEAK STATIC ROUTES	R/W	choice	ENABLE or DISABLE
OSPF ADMIN STATUS	R/W	choice	ENABLE or DISABLE
OSPF - ROUTER ID	R/W	IP address	Router ID (one of the router IP addresses).
OSPF - LEAK RIP ROUTES	R/W	choice	ENABLE or DISABLE
OSPF - LEAK STATIC ROUTES	R/W	choice	ENABLE or DISABLE
OSPF - LEAK EXTERNAL DIRECT ROUTES	R/W	choice	ENABLE or DISABLE
DHCP - SERVER	R/W	choice	ENABLE or DISABLE
DHCP - NEXT SERVER ADDRESS	R/W	IP address	DHCP server IP address.
DHCP - RELAY SECURITY THRESHOLD	R/W	integer	DHCP requests are relayed only if their SEC field is greater or equal to the threshold value.
DHCP - DNS IP ADDRESS	R/W	IP address	DNS server IP address
DHCP - PROBE	R/W	choice	ENABLE or DISABLE
DHCP - PROBE RETRIES	R/W	integer	Number of times the DHCP server sends an ICMP echo request.
DHCP - PROBE TIMEOUT	R/W	integer	The time in seconds the server waits for an acknowledgement from the host that the IP address was accepted.
DHCP - PRIMARY WINS SERVER	R/W	IP address	Primary WINS server IP address.
DHCP - SECONDARY WINS SERVER	R/W	IP address	Secondary WINS server IP address.
DHCP - NODE TYPE	R/W	choice	BROADCAST, POINT-TO-POINT, MIXED, or HYBRID
OSPF - NUMBER OF EXTERNAL LSAS	R	integer	Number of Link State Advertisements in the link-state database.
OSPF - EXTERNAL LS CHECKSUM SUM	R	integer	Sum of checksums of external Link State Advertisements contained in the Link State database.
TCP - ALGORITHM TYPE	R	choice	Algorithm used to determine the timeout value used for re-transmitting unacknowledged octets.
TCP - MINIMUM TIMEOUT	R	integer	Minimum value for re-transmission timeout in milliseconds.

Attribute	Acces s	Type	Description
TCP - MAXIMUM TIMEOUT	R	integer	Maximum value for re-transmission timeout in milliseconds.
TCP - MAXIMUM CONNECTIONS	R	integer	Maximum number of TCP connections the entity can support.

Table 6.30. General IP router attributes

IP Router Interface parameters.

One record per IP interface.

Attribute	Access	Type	Description
IP ADDRESS	R/W	IP address	IP address of the interface.
NETWORK MASK	R/W	IP address	Subnet mask.
INTERFACE NUMBER	R/W	integer	Physical or logical interface to which the IP address is mapped. A physical interface is an Ethernet port, while a logical interface can be a VLAN or the CLNP router.
FORWARD BROADCAST	R/W	choice	ENABLE or DISABLE
BROADCAST TYPE	R/W	choice	ONE-FILL or ZERO-FILL
ICMP - ADDRESS FOR ROUTER ADVERTISEMENT	R/W	IP address	IP destination address for multicast Router Advertisements sent from this interface.
ICMP - MAXIMUM ADVERTISEMENT INTERVAL	R/W	integer	Maximum time in seconds between advertisements.
ICMP - MINIMUM ADVERTISEMENT INTERVAL	R/W	integer	Minimum time in seconds between advertisements.
ICMP - ADVERTISEMENT LIFETIME	R/W	integer	Lifetime in seconds.
ICMP - ADVERTISE THIS INTERFACE	R/W	choice	TRUE or FALSE
ICMP - PREFERENCE LEVEL FOR THIS ADDRESS	R/W	integer	Preference level for this address as a default router address.
ICMP - CHANGE ALL PARAMETERS TO DEFAULT	R/W	choice	TRUE or FASLE
RIP - OUTGOING RIP	R/W	choice	RIP-V1, RIP-V2, or DO-NOT-SEND
RIP - INCOMING RIP	R/W	choice	RIP-V1, RIP-V2, or DO-NOT-RECEIVE
RIP - DEFAULT ROUTE METRIC	R/W	integer	Metric for the default route entry in RIP updates originated on this interface.
RIP - AUTO SEND	R/W	choice	ENABLE or DISABLE
RIP - VIRTUAL DISTANCE	R/W	integer	Virtual number of hops assigned to this interface.
RIP - STATUS	R/W	choice	VALID or INVALID
OSPF- ADMIN STATUS	R/W	choice	ENABLE or DISABLE
OSPF- PRIORITY	R/W	integer	Priority of the interface to become designated router.
OSPF- HELLO INTERVAL	R/W	integer	Seconds between hello packets.
OSPF- TIME BEFORE DECLARE ROUTER DEAD	R/W	integer	Number of seconds during which no hello packet for a router has been detected.
OSPF- INTERFACE AUTHENTICATION KEY	R/W	octet string	Interface Authentication Key.
OSPF- AUTHENTICATION TYPE	R/W	choice	NONE, SIMPLEPASSWORD, or MD5
OSPF- METRIC VALUE	R/W	integer	Metric for this type of service on this interface.
OSPF - AREA ID	R	IP address	IP address of the area.
OSPF - IF TYPE	R	integer	Sum of checksums of external Link State Advertisements contained in the Link State database.

Attribute	Access	Type	Description
OSPF - IF STATE	R	choice	DOWN, LOOPBACK, WAITING, POINT-TO-POINT, DESIGNATED-ROUTER, BACKUP-DESIGNATED-ROUTER, or OTHER-DESIGNATED-ROUTER.
OSPF - DESIGNATED ROUTER	R	IP address	IP address of the designated router.
OSPF - BACKUP DESIGNATED ROUTER	R	IP address	IP address of the backup designated router.

Table 6.31. IP router interface attributes

IP Router RIP Global Filter parameters.

One record per RIP global filter.

Attribute	Access	Type	Description
TYPE	R/W	choice	INPUT or OUTPUT
NETWORK ADDRESS	R/W	IP address	Network IP address to filter.
NUMBER OF MATCH BITS	R/W	integer	Number of bits to match the network address.
FILTER ACTION	R/W	choice	PERMIT or DENY

Table 6.32. RIP Global Filter attributes

IP Router RIP Interface Filter parameters.

One record per interface and RIP interface filter.

Attribute	Access	Type	Description
TYPE	R/W	choice	INPUT or OUTPUT
NETWORK ADDRESS	R/W	IP address	Network IP address to filter.
NUMBER OF MATCH BITS	R/W	integer	Number of bits to match the network address.
FILTER ACTION	R/W	choice	PERMIT or DENY
STATUS	R	string	VALID/INVALID

Table 6.33. RIP Interface Filter attributes

IP Router OSPF Area Table.

One record per OSPF area ID.

Attribute	Access	Type	Description
Area ID	R/W	IP address	The area ID
Import as External	R/W	choice	IMPORT-EXTERNAL or IMPORT-NO-EXTERNAL
Area Summary	R	choice	NO-AREA-SUMMARY or SEND-AREA-SUMMARY
Metric	R	integer	Metric for this type of service.
Metric Type	R	choice	Metric protocol type: OSPF-METRIC, or COMPARABLE-COST, or NON-COMPARABLE.

Table 6.34. OSPF Area Table attributes

IP Router OSPF Link State Database.

One record per link state database entry.

Attribute	Access	Type	Description
Area ID	R	IP address	Link IP address.
Link Type	R	choice	ROUTER-LINK, NETWORK-LINK, EXTERNAL-LINK, SUMMARY-LINK, or STUB-LINK.
Link ID	R	IP address	Identifies the routing domain.
Router ID	R	IP address	Identifies the originating router in the autonomous system.
Sequence Number	R	integer	The number for the link.
Age	R	integer	The age of the link state advertisement in seconds.
Checksum	R	integer	Checksum of the complete advertisement content, excluding the age value.

Table 6.35. OSPF Link State Database attributes

IP Router External OSPF Link State Database parameters

One record per link state database entry

Attribute	Access	Type	Description
Link Type	R	choice	ROUTER-LINK, NETWORK-LINK, EXTERNAL-LINK, SUMMARY-LINK, or STUB-LINK.
Link ID	R	IP address	Identifies the routing domain.
Origin Router ID	R	IP address	Identifies the originating router in the autonomous system.
OSPF Sequence Number	R	integer	The number for the link.
Link State Age	R	integer	The age of the link state advertisement in seconds.
Checksum	R	integer	Checksum of the complete advertisement content, excluding the age value.
Link State Advertisement	R	integer	The complete link state advertisement packet including the header.

Table 6.36. External OSPF Link State Database attributes

IP Router OSPF Neighbour Table

One record per interface and neighbour.

Attribute	Access	Type	Description
Neighbor Address	R	IP address	Neighbor IP address.
Router ID	R	IP address	Unique neighboring router identifier in the autonomous system.
Priority	R	integer	OSPF priority of the neighbor.
Neighbor State	R	choice	DOWN, ATTEMPT, INIT, TWO-WAYS, EXCHANGE-START, EXCHANGE, LOADING, or FULL.

Table 6.37. OSPF Neighbour Table attributes

IP Routing table

One entry per IP route.

Attribute	Access	Type	Description
Destination IP address	R/W	IP address	Destination IP address.
Destination network mask	R/W	IP address	Destination mask
Next Hop	R/W	IP address	IP address of the next system.
Interface Number	R/W	integer	Interface index through which the next hop can be reached.
Route Type	R/W	choice	REMOTE or REJECT
Metric	R/W	integer	Number of hops to the destination network.
Protocol	R	integer	Protocol through which the route is known.

Table 6.38. IP routing table attributes

IP Router ARP table

One record per ARP entry, i.e. IP address.

Attribute	Access	Type	Description
Interface	R/W	integer	Interface number to use to reach the IP/MAC address
IP Address	R/W	IP address	IP address
MAC Address	R/W	MAC	MAC address associated with the IP address
Class	R/W	choice	DYNAMIC or STATIC

Table 6.39. ARP table attributes

IP Router Redundancy Table

One record per IP redundancy entry.

Attribute	Access	Type	Description
Interface IP address	R/W	IP address	IP address running the redundancy feature.
Main Router Address	R/W	IP address	Router IP address that the device is backing up
Poll Interval	R/W	integer	Router polling interval in seconds.
Time Out	R/W	integer	Interval in seconds during which the router must signal.
Operating Status	R	choice	ACTIVE or INACTIVE

Table 6.40. Redundancy table attributes

IP Router DHCP Address Range

One record per IP address range.

Attribute	Access	Type	Description
IP address Interface	R/W	IP address	IP address of the interface.
IP Address From	R/W	IP address	First IP address allocated in this row.
IP Address To	R/W	IP address	Last IP address allocated in this row.
Default Router	R/W	IP address	Default router IP address.
Lease Time	R/W	integer	Maximum lease time for a new address.
Probe Enable	R/W	choice	ENABLE or DISABLE
Total addresses number	R	integer	Number of available IP addresses to choose from (including those already allocated).
Free addresses number	R	integer	Number of available IP addresses for new allocation.
DHCP addresses number	R	integer	Number of IP addresses currently used by DHCP.

Table 6.41. DHCP address range

IP Router DHCP Allocation Table

One record per IP address.

Attribute	Access	Type	Description
IP address	R/W	IP address	IP address allocated by DHCP.
MAC Address	R/W	MAC	MAC address.
Host name	R/W	string	Name of the host requesting the address.
Default Router	R/W	IP address	Default router IP address.
Configuration Server IP Address	R/W	IP address	TFTP server IP address.
Configuration File Name	R/W	string	Path and name of the configuration file on the TFTP server.
Mechanism	R	choice	AUTOMATIC, DYNAMIC, or MANUAL
Application	R	choice	DHCP or RIP
Age Time	R	integer	IP address age time.

Table 6.42. DHCP allocation table attributes

IP Router UDP Relay

One entry per UDP relay entry

Attribute	Access	Type	Description
UDP Destination Port	R/W	integer	UDP port of UDP frames to be relayed.
Source IP Address	R/W	IP address	Address of the input interface that relays UDP frames.
Destination IP Address	R/W	IP address	Address of the interface that receives UDP frame relays.

Table 6.43. UDP relay attributes

IP Router TCP Connections Table

One list per TCP connection.

Attribute	Access	Type	Description
Local Address	R	IP address	Local IP address for this TCP connection.
Local Port	R	integer	Local port number for this TCP connection.
Remote Address	R	IP address	Remote IP address for this TCP connection.
Remote Port	R	integer	Remote port number for this TCP connection.
Connection Sate	R	choice	Status of this TCP connection.

Table 6.44. TCP connection attributes

IPM Operating Parameters

Attribute	Access	Type	Description
IPM ROUTE ENABLE	R/W	choice	Enables IPM routing on a device. Legal values are EANBLED or DISABLED.

Table 6.45. IP Multicast (IPM) attribute

IGMP Operating Parameters

Attribute	Access	Type	Description
IGMP MIB VERSION	R	integer	Indicates the MIB software version for IGMP.

Table 6.46. IGMP General attribute

IGMP Interface Parameters

One list per port:

Attribute	Access	Type	Description
IFINDEX	R/W	integer	the ifIndex value of the interface for which IGMP is enabled.
QUERY INTERVAL	R/W	integer	The frequency at which IGMP Host-Query packets are transmitted on this interface.
VERSION	R/W	integer	Indicates the current software version of IGMP.
QUERIER	R	integer	The address of the IGMP Querier on the IP subnet to which this interface is attached. The multicast router with the lowest IP address is the multicast querier.
QUERY MAX RESPONSE TIME	R/W	integer	Indicates the maximum query response time advertised in IGMPv2 queries on this interface.
QUERY UP TIME	R	integer	Indicates the time since the Querier was last changed.
QUERY EXPIRY TIME	R	integer	Indicates the amount of time remaining before the Querier Present Timer expires. If the local system is the querier, the value is zero.
WRONG SOFTWARE VERSION QUERIES	R	integer	Indicates the number of queries received whose IGMP version does not match the VERSION on this interface. IGMP requires that all routers on a LAN be configured to run the same version of IGMP. Thus, if any queries are received with the wrong version, this indicates a configuration error.
JOIN	R	integer	Indicates the number of times a group membership has been added on this interface; that is, the number of times an entry for this interface has been added to the Cache Table.
PROXY IFINDEX	R	integer	Indicates that IGMP is performed by a proxy. IGMP Host Membership reports are sent on the interface identified by PROXY IFINDEX. A value of 0 indicates that IGMP proxying is not being performed.
GROUPS	R	integer	Indicates the current number of entries for this interface in the Cache Table.
ROBUSTNESS	R/W	integer	Allows tuning for the expected packet loss on a subnet. If a subnet is expected to be lossy, the Robustness Variable may be increased. Legal values are [1:255].
LAST MEMBER QUERY INTERVAL	R/W	integer	Indicates the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query messages. This value may be tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group.

Table 6.47. IGMP Interface attributes

IGMP cache Parameters

One list per port and per IP multicast address:

Attribute	Access	Type	Description
CACHE ADDRESS	R	IP Address	IP multicast group address to which the port is a member.
IFINDEX	R	integer	the ifIndex value of the interface for which IGMP is enabled.
CACHE SELF	R	integer	Indicates if the local system is member of this IP multicast group address on this interface.
LAST REPORTER	R	IP Address	Indicates the IP address of the source of the last membership report received for this IP Multicast group address on this interface. If no membership report has been received, this object has the value 0.0.0.0.
UP TIME	R	integer	Indicates the amount of time (in ticks) since the entry was created.
EXPIRY TIME	R	integer	Indicates the (minimum) amount of time (in ticks) remaining before the entry will be aged out.
STATUS	R	choice	Indicates the status of the entry. Legal values are ACTIVE, or DESTRUCTED.
VERSION1 HOST TIMER	R	integer	Indicates the time remaining until the local router will assume that there are no longer any IGMP version 1 members on the IP subnet attached to this interface.

Table 6.48. IGMP Cache attributes

IPM Routing Table Parameters

One list per IP multicast address (group) and per source (network address and network mask):

Attribute	Access	Type	Description
GROUP	R	IP Address	IP address of the multicast group.
SOURCE	R	IP Address	Indicates the network address which when combined with the corresponding value of SOURCE MASK identifies the sources for which this entry contains multicast routing information.
SOURCE MASK	R	IP Address	Indicates the network mask which when combined with the corresponding value of SOURCE identifies the sources for which this entry contains multicast routing information.
UPSTREAM NEIGHBOR	R	IP Address	Indicates the IP address of the upstream neighbor from which IP datagrams from these sources to this multicast address are received, or 0.0.0.0 if the upstream neighbor is unknown.
IN IFINDEX	R	integer	Indicates the value of ifIndex for the interface on which IP datagrams sent by these sources to this multicast address are received. A value of 0 indicates that datagrams are not subject to an incoming interface check, but may be accepted on multiple interfaces
UP TIME	R	integer	Indicates the time since the multicast routing information represented by this entry was learned by the router.
EXPIRY TIME	R	integer	Indicates the minimum amount of time remaining before this entry will be aged out. The value 0 indicates that the entry is not subject to aging.
PROTOCOL	R	choice	Indicates the multicast routing protocol via which this multicast forwarding entry was learned.
ROUTING MECHANISM	R	choice	Indicates the routing mechanism via which the route used to find the upstream or parent interface for this multicast forwarding entry was learned.
ROUTING ADDRESS	R	IP Address	Indicates the address portion of the route used to find the upstream or parent interface for this multicast forwarding entry.
ROUTE MASK	R	IP Address	Indicates the mask associated with the route used to find the upstream or parent interface for this multicast forwarding entry.
ROUTE TYPE	R	choice	Indicates the reason the given route was placed in the (logical) multicast Routing Information Base (RIB). A value of UNICAST means that the route would normally be placed only in the unicast RIB, but was placed in the multicast RIB (instead or in addition) due to local configuration, such as when running PIM over RIP. A value of MULTICAST means that the route was explicitly added to the multicast RIB by the routing protocol.

Table 6.49. IPM Routing attributes

IPM Next-Hop Table Parameters

One list per IP multicast address (group), per source (network address and network mask), per interface, and per next-hop address:

Attribute	Access	Type	Description
GROUP	R	IP Address	IP address of the multicast group for which this entry specifies a next-hop on an outgoing interface.
SOURCE	R	IP Address	Indicates the network address which when combined with the corresponding value of SOURCE MASK identifies the sources for which this entry specifies a next-hop on an outgoing interface.
SOURCE MASK	R	IP Address	Indicates the network mask which when combined with the corresponding value of SOURCE identifies the sources for which this entry specifies a next-hop on an outgoing interface.
IFINDEX	R	integer	Indicates the ifIndex of the interface for the outgoing interface for this next-hop.
NEXT-HOP ADDRESS	R	IP Address	Indicates the address of the next-hop specific to this entry. For most interfaces, this is identical to GROUP. NBMA interfaces, however, may have multiple next-hop addresses out a single outgoing interface.
STATE	R	choice	Indicates whether the outgoing interface and next-hop represented by this entry is currently being used to forward IP datagrams. The value 'FORWARDING' indicates it is currently being used; the value 'PRUNED' indicates it is not.
UP TIME	R	integer	Indicates the time since the multicast routing information represented by this entry was learned by the router.
EXPIRY TIME	R	integer	Indicates the minimum amount of time remaining before this entry will be aged out. If STATE is 'PRUNED', this object indicates the remaining time until the prune expires and the state reverts to 'FORWARDING'. Otherwise, it indicates the remaining time until this entry is removed from the table. The value 0 indicates that the entry is not subject to aging.
NEXT-HOP PROTOCOL	R	choice	Indicates the multicast routing protocol via which this next-hop entry was learned.

Table 6.50. IPM Next-Hop attributes

PIM Parameters

Attribute	Access	Type	Description
PIM MIB VERSION	R	integer	Indicates the MIB software version for PIM.
PIM ENABLE	R/W	choice	Enables PIM on a device. Legal values are EANBLED or DISABLED.

Table 6.51. PIM attributes

IPX Router RIP Global Filter parametes.

Attribute	Access	Type	Description
Type	R/W	choice	INPUT or OUTPUT
Network Address	R/W	octet string	IPX network address to filter.
Network Mask	R/W	octet string	IPX network mask.
Action	R/W	choice	PERMIT or DENY

Table 6.52. One record per RIP global filter.

IPX Router RIP Circuit Filter parameters

One record per circuit and per RIP circuit filter.

Attribute	Access	Type	Description
Type	R/W	choice	INPUT or OUTPUT
Network Address	R/W	octet string	IPX network address to filter.
Network Mask	R/W	octet string	IPX network mask.
Action	R/W	choice	PERMIT or DENY

Table 6.53. IPX RIP Circuit Filter attributes

IPX Router SAP Global Filter parameters

One record per SAP global filter.

Attribute	Access	Type	Description
Type	R/W	choice	INPUT or OUTPUT
Network Address	R/W	octet string	IPX network address to filter.
Network Mask	R/W	octet string	IPX network mask.
Service Type	R/W	integer	Type of server (in hex) the filter entry affects.
Service Name	R/W	string	Name of the server the filter entry affects.
Action	R/W	choice	PERMIT or DENY

Table 6.54. IPX Router SAP Global Filter parameters

PIM Route Table Parameters

One list per IP multicast address (group) and per source (network address and network mask):

Attribute	Access	Type	Description
GROUP	R	IP Address	IP address of the multicast group.
SOURCE	R	IP Address	Indicates the network address which when combined with the corresponding value of SOURCE MASK identifies the sources for which this entry contains multicast routing information.
SOURCE MASK	R	IP Address	Indicates the network mask which when combined with the corresponding value of SOURCE identifies the sources for which this entry contains multicast routing information.
UPSTREAM ASSERT TIMER	R	integer	Indicates the time remaining before the router changes its upstream neighbor back to its RPF (Reverse Path Forwarding) neighbor.
ASSERT METRIC	R	integer	Indicates the metric advertised by the assert winner (i.e. forwarding router) on the upstream interface. A value of 0 indicates that no assert was received.
ASSERT METRIC PREF	R	integer	Indicates the preference advertised by the assert winner (i.e. forwarding router) on the upstream interface. ASSET METRIC PREF is used when upstream routers run different unicast protocols. A value of 0 indicates that no assert is in effect.
ASSERT RPT BIT	R	integer	Indicates the value of the RPT-bit advertised by the assert winner (i.e. forwarding router) on the upstream interface.
FLAGS	R	choice	Indicates the PIM-specific flags related to a multicast state entry. Legal values are RPT and SPT.

Table 6.55. PIM Route attributes

PIM Next-Hop Table Parameters

One list per IP multicast address (group), per source (network address and network mask), per interface, and per next-hop address:

Attribute	Access	Type	Description
GROUP	R	IP Address	IP address of the multicast group for which this entry specifies a next-hop on an outgoing interface.
SOURCE	R	IP Address	Indicates the network address which when combined with the corresponding value of SOURCE MASK identifies the sources for which this entry specifies a next-hop on an outgoing interface.
SOURCE MASK	R	IP Address	Indicates the network mask which when combined with the corresponding value of SOURCE identifies the sources for which this entry specifies a next-hop on an outgoing interface.
IFINDEX	R	integer	Indicates the ifIndex of the interface for the outgoing interface for this next-hop.
NEXT-HOP ADDRESS	R	IP Address	Indicates the address of the next-hop specific to this entry. For most interfaces, this is identical to GROUP. NBMA interfaces, however, may have multiple next-hop addresses out a single outgoing interface.
PRUNE REASON	R	choice	Indicates why the downstream interface was pruned. Legal values are PRUNE (prune in response to prune message), ASSERT (prune due to PIM Assert processing), or OTHER.

Table 6.56. PIM Next-Hop attributes

IPX Router Interface parameters

One list per circuit number.

Attribute	Access	Type	Description
Interface number	R/W	integer	IfIndex used by this circuit.
Network Address	R/W	octet string	IPX network address of this circuit.
Time to Network	R/W	integer	Time to net value associated with this interface.
Layer 2 protocol	R/W	choice	Encapsulation method associated with this interface
NetBios	R/W	choice	ENABLE or DISABLE
Admin Status	R/W	choice	ON or OFF
RIP - Update interval	R/W	integer	RIP periodic update interval in seconds.
RIP - Age multiplier	R/W	integer	Holding multiplier for information received in RIP periodic updates.
RIP - Status	R/W	choice	ON or OFF
SAP - Update interval	R/W	integer	SAP periodic update interval in seconds.
SAP - Age multiplier	R/W	integer	Holding multiplier for information received in SAP periodic updates.
SAP - Respond to Get nearest server	R/W	choice	YES or NO
SAP - Status	R/W	choice	ON or OFF
Circuit number	R	integer	IPX circuit number
MAC address	R	MAC	MAC address

Table 6.57. IPX router interface attributes

IPX Router RIP Global Filter parameters.

One record per RIP global filter.

Attribute	Access	Type	Description
Type	R/W	choice	INPUT or OUTPUT
Network Address	R/W	octet string	IPX network address to filter.
Network Mask	R/W	octet string	IPX network mask.
Action	R/W	choice	PERMIT or DENY

Table 6.58. IPX RIP Global Filter attributes

IPX Router RIP Circuit Filter parameters

One record per circuit and per RIP circuit filter.

Attribute	Access	Type	Description
Type	R/W	choice	INPUT or OUTPUT
Network Address	R/W	octet string	IPX network address to filter.
Network Mask	R/W	octet string	IPX network mask.
Action	R/W	choice	PERMIT or DENY

Table 6.59. IPX RIP Circuit Filter attributes

IPX Router SAP Global Filter parameters

One record per SAP global filter.

Attribute	Access	Type	Description
Type	R/W	choice	INPUT or OUTPUT
Network Address	R/W	octet string	IPX network address to filter.
Network Mask	R/W	octet string	IPX network mask.
Service Type	R/W	integer	Type of server (in hex) the filter entry affects.
Service Name	R/W	string	Name of the server the filter entry affects.
Action	R/W	choice	PERMIT or DENY

Table 6.60. IPX SAP Global Filter attributes

IPX Router Circuit Filter parameters

One record per circuit and per SAP circuit filter.

Attribute	Access	Type	Description
Type	R/W	choice	INPUT or OUTPUT
Network Address	R/W	octet string	IPX network address to filter.
Network Mask	R/W	octet string	IPX network mask.
Service Type	R/W	integer	Type of server (in hex) the filter entry affects.
Service Name	R/W	string	Name of the server the filter entry affects.
Action	R/W	choice	PERMIT or DENY

Table 6.61. IPX Circuit Filter attributes

IPX Routing table

One record per IPX route.

Attribute	Access	Type	Description
Destination Network	R/W	octet string	Destination IPX network number
Hops to Net	R/W	integer	Number of hops on the route to the destination network.
Ticks to Net	R/W	integer	Time estimate to reach the destination network.
Forwarding Router Address	R/W	octet string	IPX node address of the next IPX router on the route to the destination network.
Circuit	R	integer	IPX circuit number used to reach the next hop.
Destination Protocol	R	choice	SATIC, LOCAL or RIP
Next Hop NetNum	R	octet string	Next hop IPX network number.
Status	R	choice	ON or OFF

Table 6.62. IPX routing table attributes

IPX Router SAP Table

One record per IPX server.

Attribute	Access	Type	Description
Server name	R/W	string	Name of the server.
Network	R/W	octet string	Network portion of the server IPX address.
Server address	R/W	octet string	Node portion of the server IPX address.
Socket	R/W	octet string	Socket portion of the server IPX address.
Server type	R/W	octet string	Type of service provided by the server.
Hops to server	R/W	integer	Number of hops on the route to the server.
Protocol type	R	choice	SATIC or SAP
Status	R	choice	ON or OFF

Table 6.63. IPX SAP table attributes

6.2.12 LAN

See Ethernet.

6.2.13 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 6.64. LED attributes

6.2.14 Mgmt Port

Attribute	Access	Type	Description
MODE	R/W	choice	Defines the use of the Management Port. Legal values are: NONE 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 6.65. Mgmt Port attributes

6.2.15 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	Errored 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 6.66. 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 6.67. MS alarms

6.2.16 The Point-to-Point Protocol

The PPP interface parameters are not managable via AXXCLI or any SNMP management solution supplied by AXXESSIT. However, the implementation is based on standard MIBs, RFC 1471 (PPP) and RFC 1473 (NCP).

Data Link Layer - PPP

In IP/PPP mode PPP is used as the Data Link Layer Protoccol on the DCC channel. The AXX155E R3 uses RFC 1662: PPP in HLDC like framing with the CRC-32 option. The CRC-16 option is not supported.

Link Control Protocol - LCP

The AXX155E R3 uses RFC 1661: The Point-toPoint-Protocol with the following options:

- Magic Number
- MRU = 1500

Once the LCP reach the opened state, Echo-Request and Echo-Reply messages are used as keep alive messages. The Echo-Request messages are sent with the negotiated Magic Number, zero if not negotiated. The AXX155E R3 uses an Echo-Request interval of 10 seconds. The AXX155E R3 will turn the interface down after missing 5 Echo-Reply messages.

After the LCP is established the AXX155E R3 will initiate NCP for IP, i.e. IPCP.

Internet Protocol Control Protocol - IPCP

The AXX155E R3 uses RFC 1332: The PPP Internet Protocol Control Protocol, with the following optins:

- IP-Address

The AXX155E R3 uses the IPCP negotiation phase to inform its peer of its own IP address. The peer must accesp this address.

The AXX155E R3 will accept any IP Address negotiated by the peer.

Once the IPCP reach the opened state, IP communications can take place.

6.2.17 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 6.68. General OSI stack attributes

OSI circuit attributes

One record per circuit:

Attribute	Access	Type	Description
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.
TOGGLE C/R	R/W	choce	ENABLED or DISABLED. Defines wheter the C/R bit in LAPD addressing should be toggled.
N201	R/W	integer	Sets the information field size of the LAPD frames.

Table 6.69. 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 6.70. 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 6.71. Reachable address attributes

6.2.18 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 6.72. Port attributes

6.2.19 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 seconds to wait before switching back to the preferred link after it has been restored (0,1, ...,12 minutes, default 5 min)
Preferred Link	R	string	Identifier of the preferred working link (always LINK A for AXX155E R3).
Commands	R/W	choice	CLEAR, LOCKOUT-OF-PROTECTION, FORCED-SWITCHED-TO-PROTECTION,FORCED-SWITCHED-TO-WORKING,MANUAL-SWITCHED-TO-PROTECTION,MANUAL-SWITCHED-TO-WORKINGEXERCISE, orNO-COMMAND
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 6.73. Protection attributes

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

Table 6.74. Protection alarm

6.2.20 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	Errored 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 RECEIVED TI	R	string	Actual Received Regenerator Section Trace Identifier, string (15 octets).
RS EXPECTED TI	R/W	string	Expected Regenerator Section Trace Identifier, string (15 octets).
RS TRANSMIT TI	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 6.75. 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 6.76. RS alarms

6.2.21 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 AXX155E 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 6.77. RTC attributes

6.2.22 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 6.78. 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 6.79. .SDH alarms

6.2.23 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 6.80. SNMP user attributes

6.2.24 Software

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

Table 6.81. Software attributes

6.2.25 Tributary

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 6.82. 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
UNASS	Trib activated without mapping to an available VC-12

Table 6.83. Tributary port alarms

6.2.26 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 6.84. TU-12 attributes

Alarm ID	Description
AIS	Alarm indication signal
LOP	Loss of pointer

Table 6.85. TU-12 alarms

6.2.27 Tunnel

Attribute	Access	Type	Description
OSI MODE	R/W	choice	GATEWAY or NE. Defines whether the AXX155E 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 6.86. Tunnel attributes

6.2.28 User Channel

Attribute	Access	Type	Description
ADMINISTRATIVE STATUS	R/W	choice	Defines if user channel is ENABLED or DISABLED.
AGGREGATE PORT	R/W	choice	Identifies 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 6.87. User Channel attributes

6.2.29 User Traffic Ethernet

Attribute	Access	Type	Description
CONNECTOR-TYPE	R	string	RJ45 or LC.
PORT-DESCRIPTOR	R	string	Always Ethernet in AXX155
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 assigned10 means force speed manually to 10 Mbit/s100 means force speed manually to 100 Mbit/s1000 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 6.88. User Traffic Ethernet attributes

Attribute	Access	Type	Description
MIRRORED PORT	R/W	choice	Indicates the port number from which all outgoing and incoming traffic is copied. Legal values are DISBALED, or a port number.
COPY PORT	R/W	choice	Indicates the port number to which all outgoing and incoming traffic from/to MIRRORED PORT is mirrored. Legal values are DISBALED, or a port number.

Table 6.89. Port Mirroring attributes

6.2.30 VC12

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	Errored 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 6.90. 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 6.91. VC-12 alarms

6.2.31 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	Errored 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 6.92. 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 6.93. VC-4 alarms

6.2.32 VLAN

Attribute	Access	Type	Description
SUPPORTED-TYPE	R	string	Indicates the type of VLAN currently supported.
SUPPORTED-TYPE-AFTER-RESET	R/W	choice	Indicates the type of VLAN supported after the device is reset. Legal values are "Per Port" or "Per Port And Per Protocol"

Table 6.94. VLAN attributes

The following attributes exist for each VLAN.

Attribute	Access	Type	Description
NAME	R/W	string	User defined VLAN name.
PRIORITY	R/W	integer	Indicates the value of the priority tag. Legal values are [0:7].
MAC-ADDRESS	R	MAC	Permanent VLAN MAC address (depends on ADDRESS-TYPE).
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 1-4000.
PROTOCOL-TYPE	R/W	choice	Indicates the type of protocol used to define the VLAN. Legal values are PREDEFINED or USER DEFINED. This parameter applies only for per Port and Protocol VLANs.
PROTOCOL	R/W	choice	Indicates the type of protocol used to define the VLAN. If PROTOCOL-TYPE = PREDEFINED, legal values are: IP, IPX RAW, IPX Ethernet, IPX LLC, IPX SNAP, DECNET, NETBIOS, SNA, or OTHER. If PROTOCOL-TYPE = USER DEFINED, legal values are defined by the user via the Ethernet User Defined Protocols (see). This parameter applies only for per Port and Protocol VLANs.

Table 6.95. 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.
FORBIDDEN EGRESS PORT	R/W	list	Indicates the ports which are forbidden to be included in the egress port list for this VLAN.

Table 6.96. VLAN port attributes

The following attributes exist for each Ethernet user defined protocol.

Attribute	Access	Type	Description
PROTOCOL NAME	R/W	string	User defined name.
ETHERNET TYPE	R/W	octet string	User defined Ethernet type.

Table 6.97. Ethernet user defined protocol attributes

Attribute	Access	Type	Description
GVRP STATUS	R/W	choice	Indicates if GVRP is enabled on the device. Legal values are ENABLED or DISABLED.

Table 6.98. GVRP attributes

The following attributes exist for each User Traffic Ethernet port.

Attribute	Access	Type	Description
PORT GVRP STATUS	R/W	choice	Indicates if GVRP is enabled on the port. Legal values are ENABLED or DISABLED.
JOIN TIME	R/W	integer	Maximum interval in milliseconds between GVRP PDUs.
LEAVE TIME	R/W	integer	Period of time in milliseconds that the device will wait in the Leaving state before transiting to the Empty state.
LEAVE ALL TIME	R/W	integer	Interval in milliseconds between LeaveAll PDUs.
FAILED REGISTRATIONS	R	integer	Indicates the total number of failed GVRP registrations, for any reason, on this port.
LAST PDU ORIGIN	R	octet string	Indicates the Source MAC Address of the last GVRP message received on this port.

Table 6.99. GVRP port attributes

6.2.33 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 6.100. VT100 user attributes

6.2.34 WAN

See Ethernet.

BOOTP APPLICATION NOTE

7

AXX155E

7.1 ABOUT THIS NOTE

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.

7.1.1 Copyright

Copyright © 2002 RADLAN Computer Communication Ltd., Atidim Technological Park Bldg. #4, Tel Aviv, Israel

All rights reserved. This information may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without the prior written consent of RADLAN. RADLAN reserves the right to make changes without further notices to any products or specifications referred to herein to improve reliability, functionality or design.

RADLAN does not convey any license under its intellectual property rights.

Reproduction, adaptation or translation without prior written permission is prohibited, except as allowed under the copyright laws.

7.2 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.

7.2.1 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.

7.3 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.

7.3.1 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.

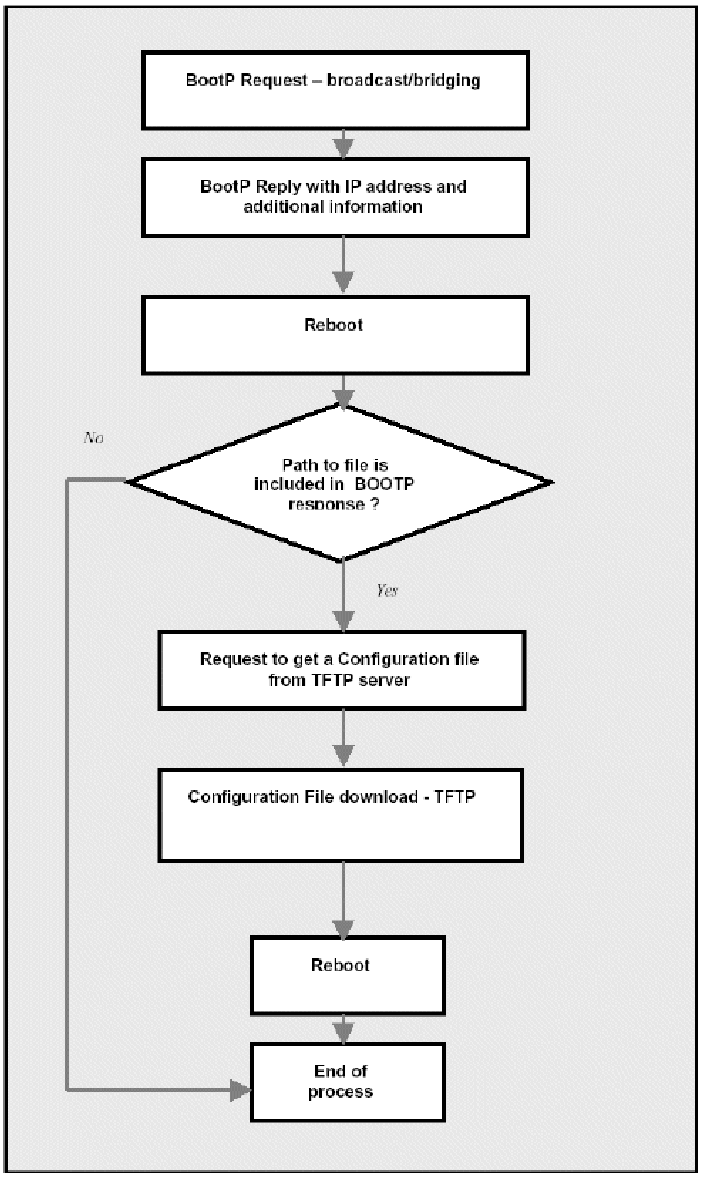

BootP Request – broadcast/bridging
BootP Reply with IP address and additional information
Reboot
No
Path to file is included in BOOTP response ?
Yes
Request to get a Configuration file from TFTP server
Configuration File download - TFTP
Reboot
End of process

Figure 7-1. Configuration process

A BOOTP process is initialized on a non-configured device (that is a device with no IP configured on it) 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.

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:

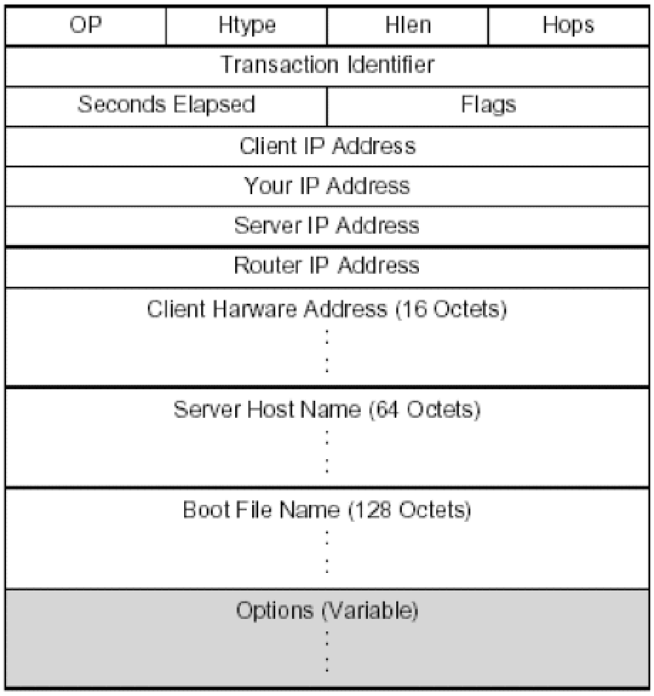
TFTP - IP address - get - configuration file location

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.*

7.4 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.



<table>
<tr><td>OP</td><td>Htype</td><td>Hlen</td><td>Hops</td></tr>
<tr><td colspan="4">Transaction Identifier</td></tr>
<tr><td colspan="2">Seconds Elapsed</td><td colspan="2">Flags</td></tr>
<tr><td colspan="4">Client IP Address</td></tr>
<tr><td colspan="4">Your IP Address</td></tr>
<tr><td colspan="4">Server IP Address</td></tr>
<tr><td colspan="4">Router IP Address</td></tr>
<tr><td colspan="4">Client Harware Address (16 Octets)
:
:</td></tr>
<tr><td colspan="4">Server Host Name (64 Octets)
:
:</td></tr>
<tr><td colspan="4">Boot File Name (128 Octets)
:
:</td></tr>
<tr><td colspan="4">Options (Variable)
:
:</td></tr>
</table>

Figure 7-2. BOOTP Message structure

The Options field format is:

Option ID - Option Length - Option Info

The following is an example of Radlan proprietary Options field:

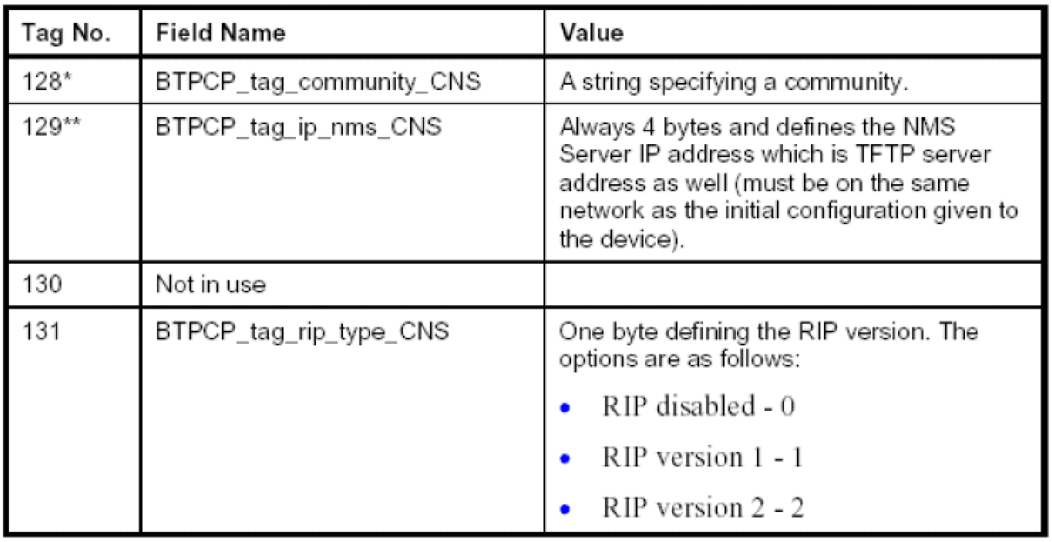
#define BTPCP_tag_community_CNS: 128

#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 7.1. BOOTP Fields

* Enter public in the community field

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

7.5 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.

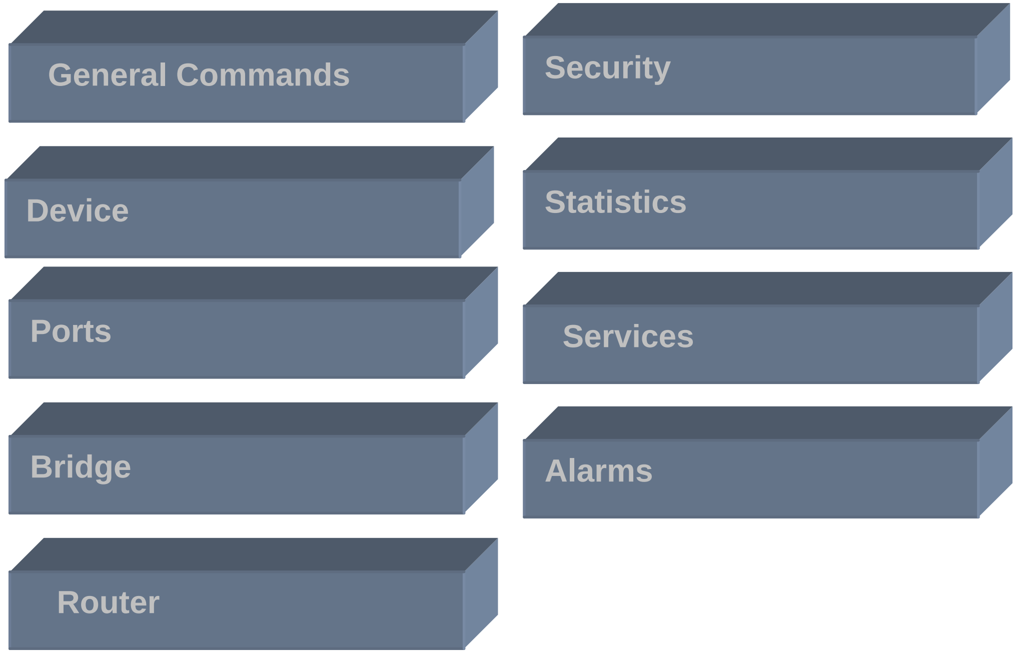
AXXCLI Command Hierarchy

8

AXX155E

8.1 INTRODUCTION

The following chapter contains the AXXCLI Command Hierarchy for AXX155E .



General Commands

Device

Ports

Bridge

Router

Security

Statistics

Services

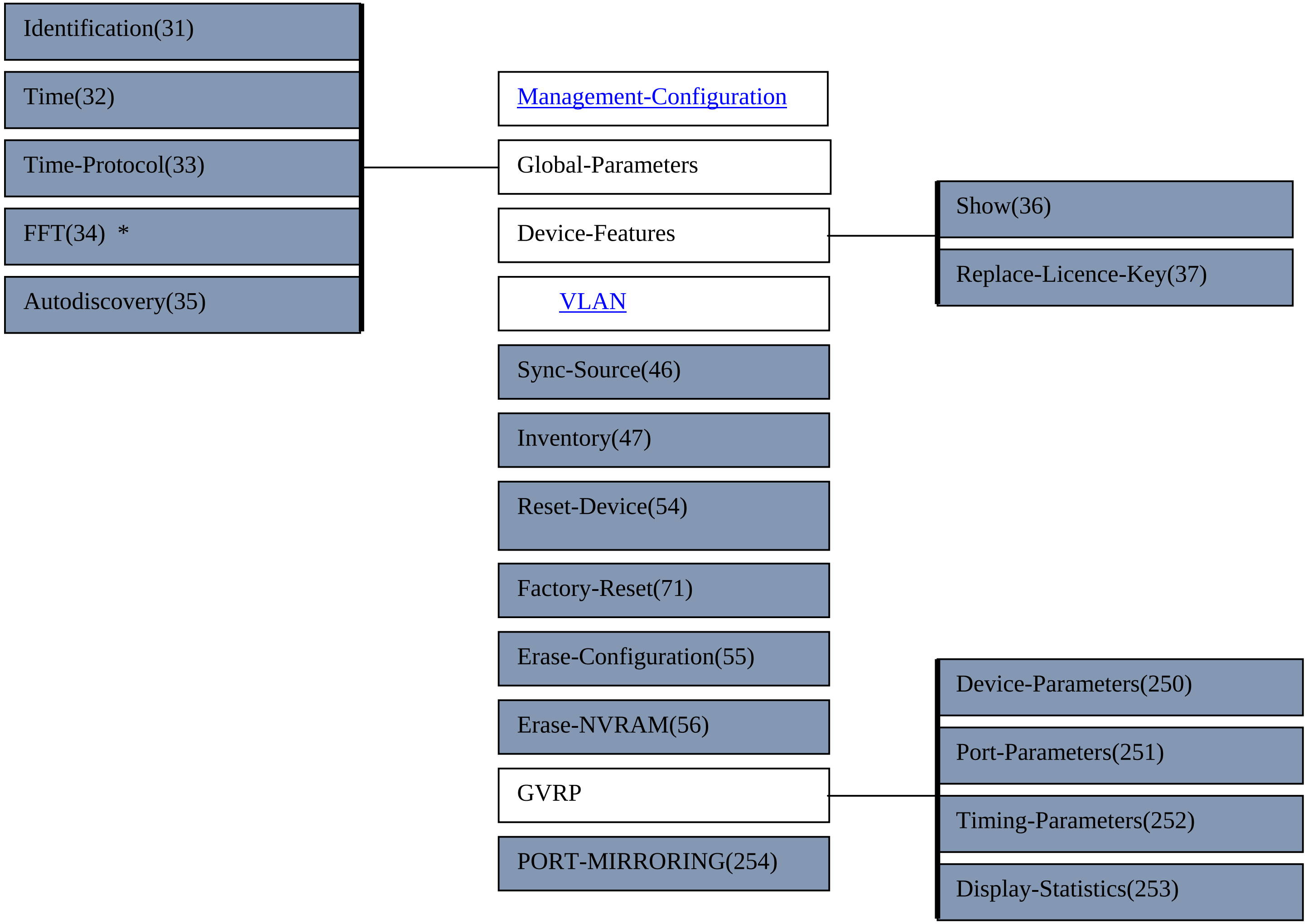
Alarms

General Commands

Running-Config(255)

Device

* Only if router licence



Identification(31)

Time(32)

Time-Protocol(33)

FFT(34) *

Autodiscovery(35)

Management-Configuration

Global-Parameters

Device-Features

VLAN

Sync-Source(46)

Inventory(47)

Reset-Device(54)

Factory-Reset(71)

Erase-Configuration(55)

Erase-NVRAM(56)

GVRP

PORT-MIRRORING(254)

Show(36)

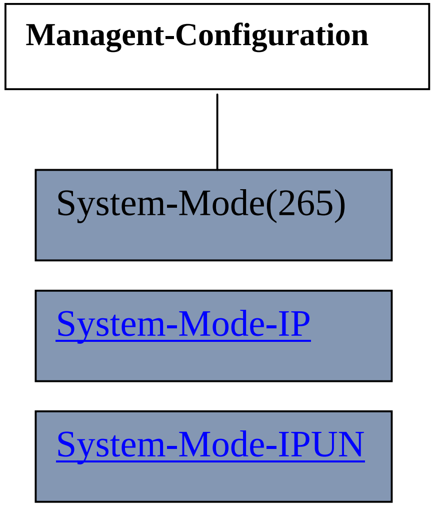
Replace-Licence-Key(37)

Device-Parameters(250)

Port-Parameters(251)

Timing-Parameters(252)

Display-Statistics(253)



Managent-Configuration

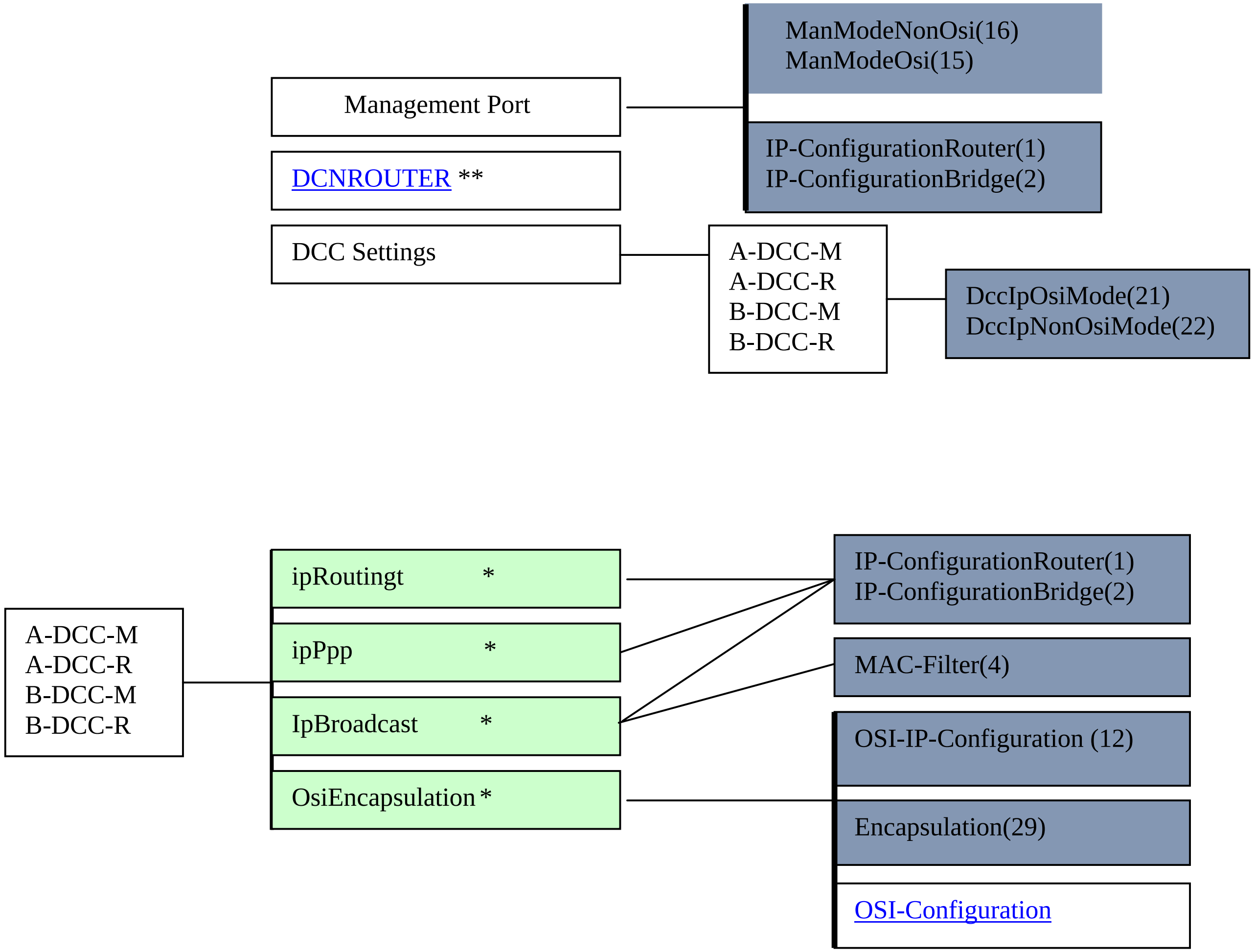
System-Mode(265)

System-Mode-IP

System-Mode-IPUN

* Current DCC Mode

System Mode IP



Management Port

DCNROUTER **

DCC Settings

ManModeNonOsi(16)
ManModeOsi(15)

IP-ConfigurationRouter(1)
IP-ConfigurationBridge(2)

A-DCC-M
A-DCC-R
B-DCC-M
B-DCC-R

DccIpOsiMode(21)
DccIpNonOsiMode(22)

A-DCC-M
A-DCC-R
B-DCC-M
B-DCC-R

ipRoutingt *

ipPpp *

IpBroadcast *

OsiEncapsulation *

IP-ConfigurationRouter(1)
IP-ConfigurationBridge(2)

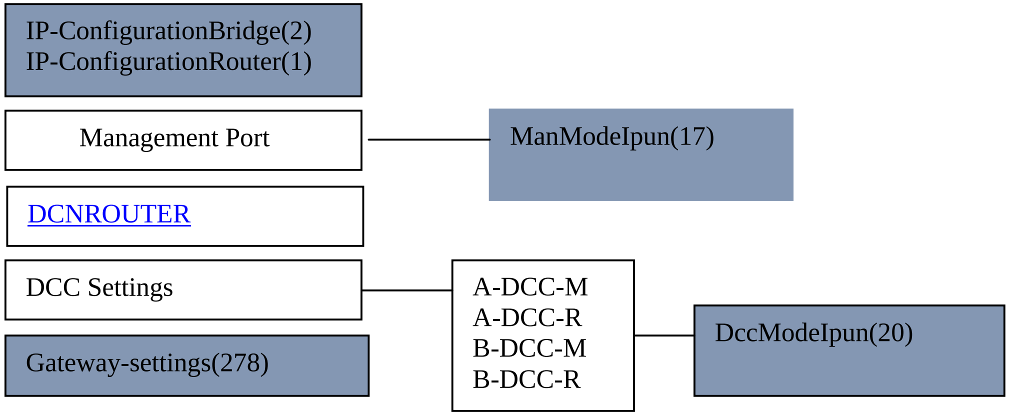
MAC-Filter(4)

OSI-IP-Configuration (12)

Encapsulation(29)

OSI-Configuration

System Mode IPUN



IP-ConfigurationBridge(2)
IP-ConfigurationRouter(1)

Management Port

ManModeIpun(17)

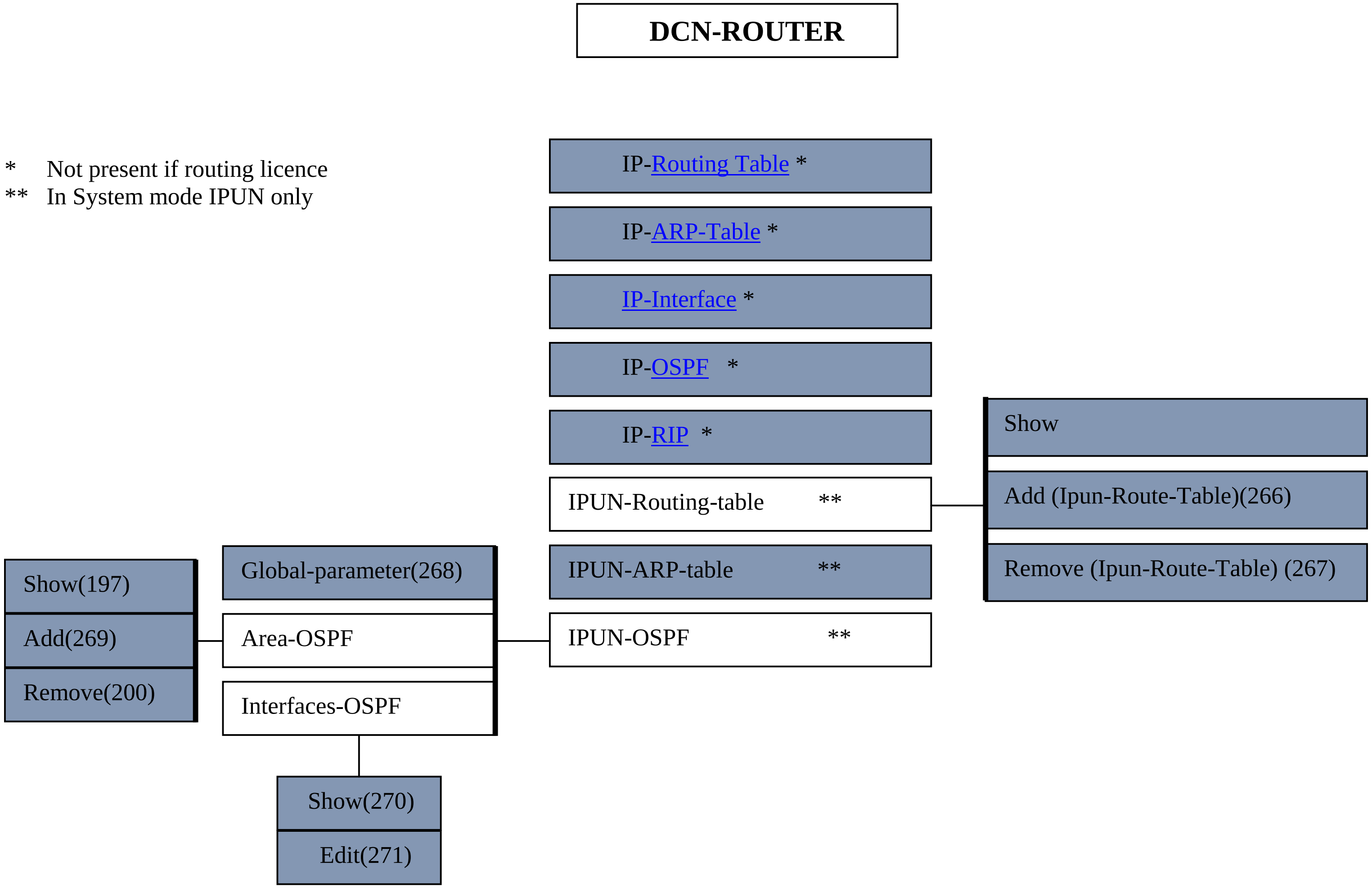
DCNROUTER

DCC Settings

A-DCC-M
A-DCC-R
B-DCC-M
B-DCC-R

DccModeIpun(20)

Gateway-settings(278)



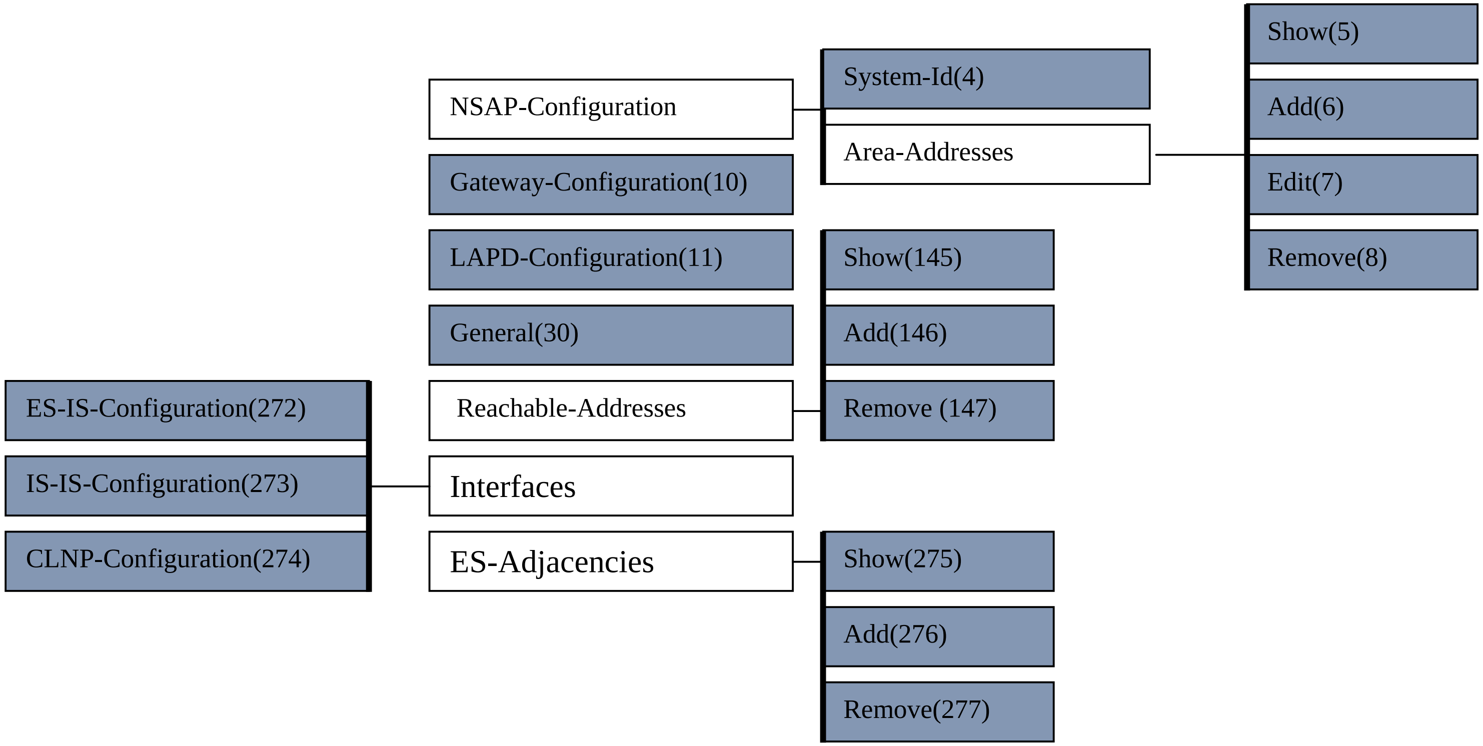
DCN-ROUTER

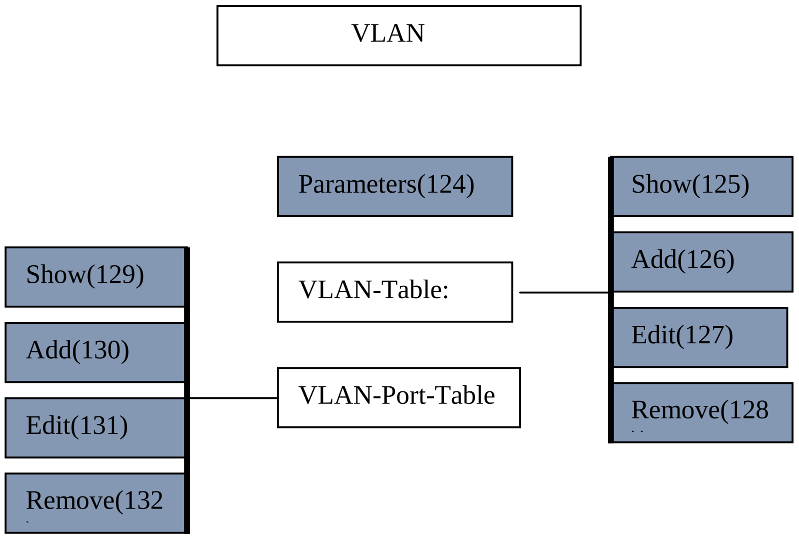
* Not present if routing licence

** In System mode IPUN only

- IP-Routing Table *
- IP-ARP-Table *
- IP-Interface *
- IP-OSPF *
- IP-RIP *
- IPUN-Routing-table **
  - Show
  - Add (Ipun-Route-Table)(266)
  - Remove (Ipun-Route-Table) (267)
- IPUN-ARP-table **
- IPUN-OSPF **
  - Global-parameter(268)
  - Area-OSPF
    - Show(197)
    - Add(269)
    - Remove(200)
  - Interfaces-OSPF
    - Show(270)
    - Edit(271)

OSI-Configuration




VLAN
Parameters(124)
VLAN-Table:
VLAN-Port-Table
Show(125)
Add(126)
Edit(127)
Remove(128
Show(129)
Add(130)
Edit(131)
Remove(132

Ports

Ethernet-Ports

TRIB-Port

Aggregate-Port

Alarm-Port-Properties(62)

User-Channel-Port-Properties(63)

Ethernet-Ports

- Main(49)
- Other(50)
- VLAN-Properties(51)
- IP-Properties(52)
- IPX-Properties(53)
- WAN-Port
- WANX-Port

WAN-Port

- General(73)
- Add-VC12-channel(74)
- Edit-VC12-channel(75)
- Remove-VC12-channel(76)

WANX-Port

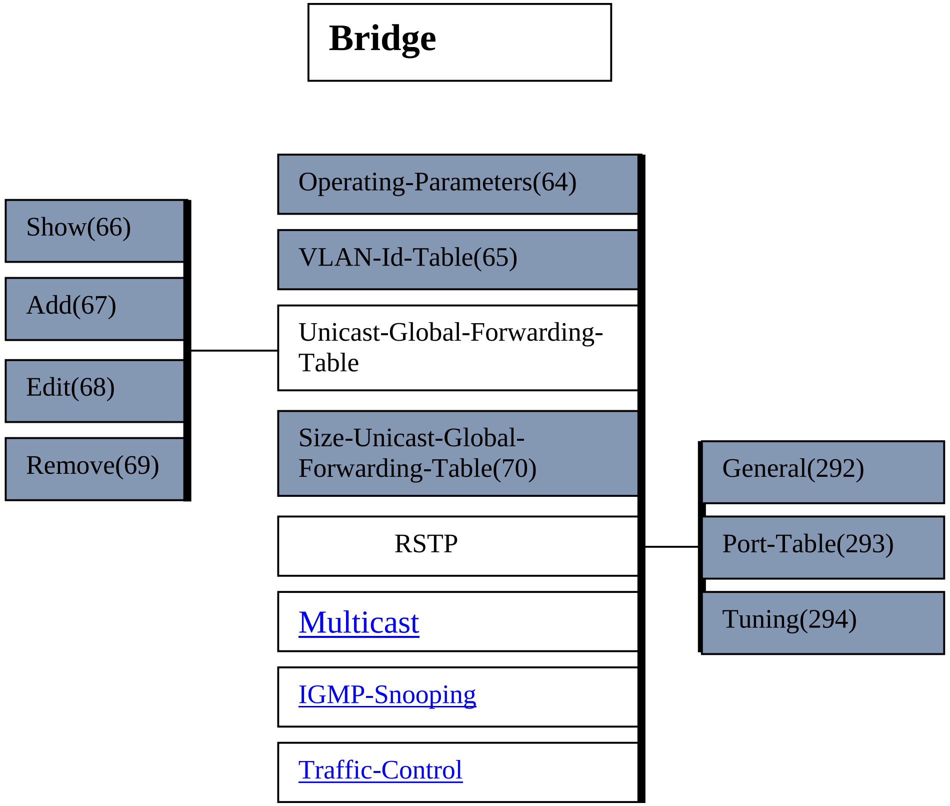
- show(279)
- General(280)
- Add-VC3-VC12-channel(281)
- Remove-VC3-VC12-channel(282)
- Free-VC12VC3-List(283)
- Used-VC12VC3-List(284)

TRIB-Port

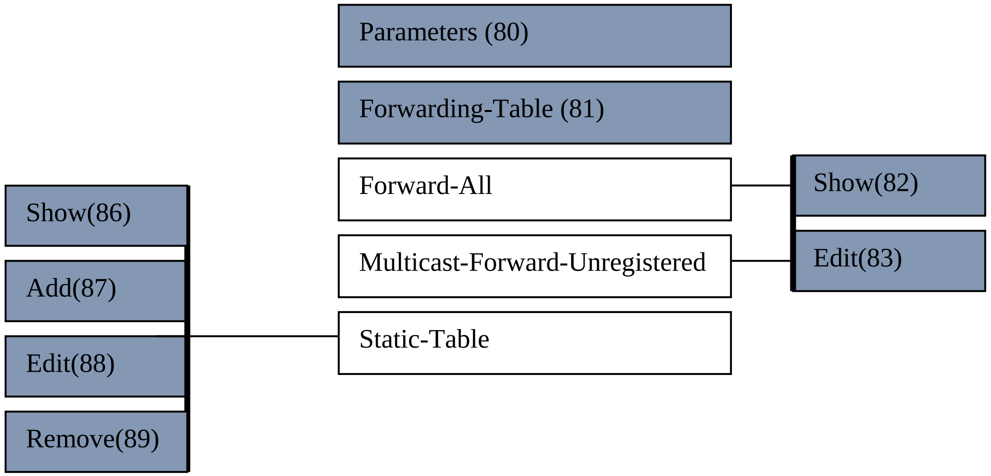
- General(77)
- Assign-VC12-Channel(78)
- Deassign-VC12-Channel(79)
- General(58)
- Protection(59)
- VC4-Path-Trace(60)
- RS-Path-Trace(61)

Aggregate Port

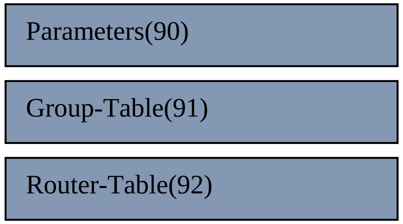
- General(58)
- TUG3-mapping(286)
- Show-VC3-VC12-Mapping(287)
- List-VC3-VC12-Usage(288)
- Protection(289)
- VC4-Path-Trace(290)
- RS-Path-Trace(291)


Bridge
Operating-Parameters(64)
VLAN-Id-Table(65)
Unicast-Global-Forwarding-Table
Size-Unicast-Global-Forwarding-Table(70)
RSTP
Multicast
IGMP-Snooping
Traffic-Control
Show(66)
Add(67)
Edit(68)
Remove(69)
General(292)
Port-Table(293)
Tuning(294)

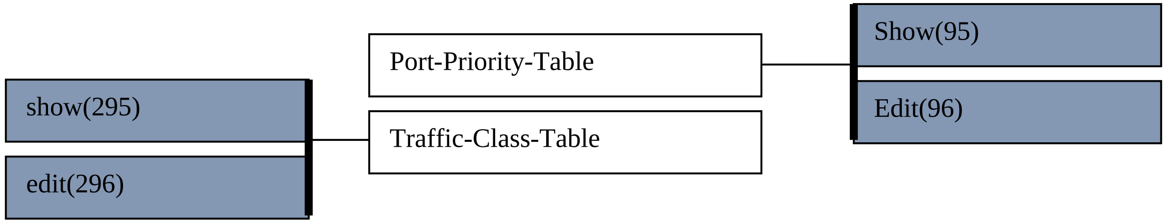
Multicast


Parameters (80)
Forwarding-Table (81)
Forward-All
Multicast-Forward-Unregistered
Static-Table
Show(82)
Edit(83)
Show(86)
Add(87)
Edit(88)
Remove(89)

IGMP-Snooping


Parameters(90)
Group-Table(91)
Router-Table(92)

Traffic-Control

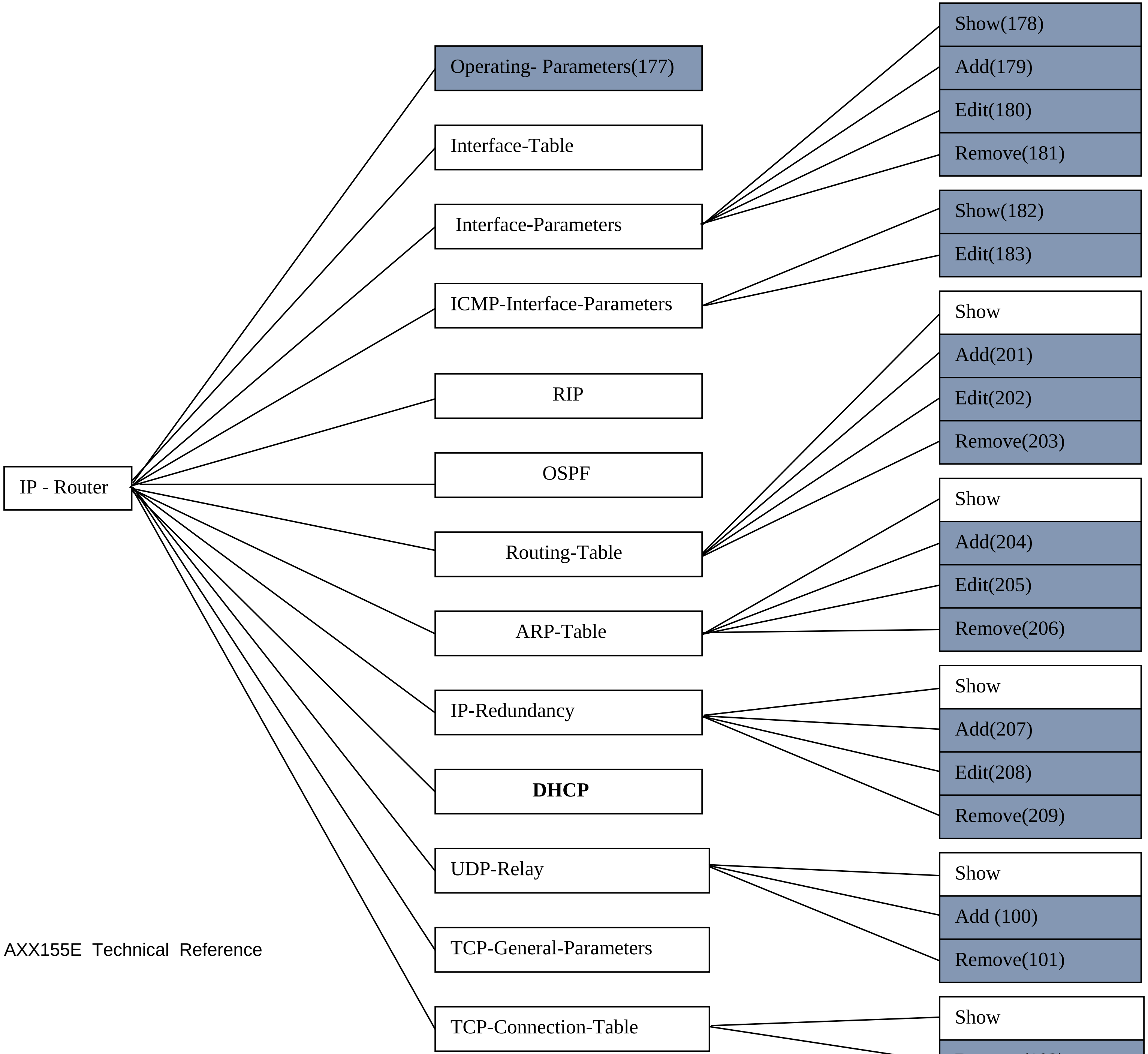

Port-Priority-Table
Traffic-Class-Table
Show(95)
Edit(96)
show(295)
edit(296)

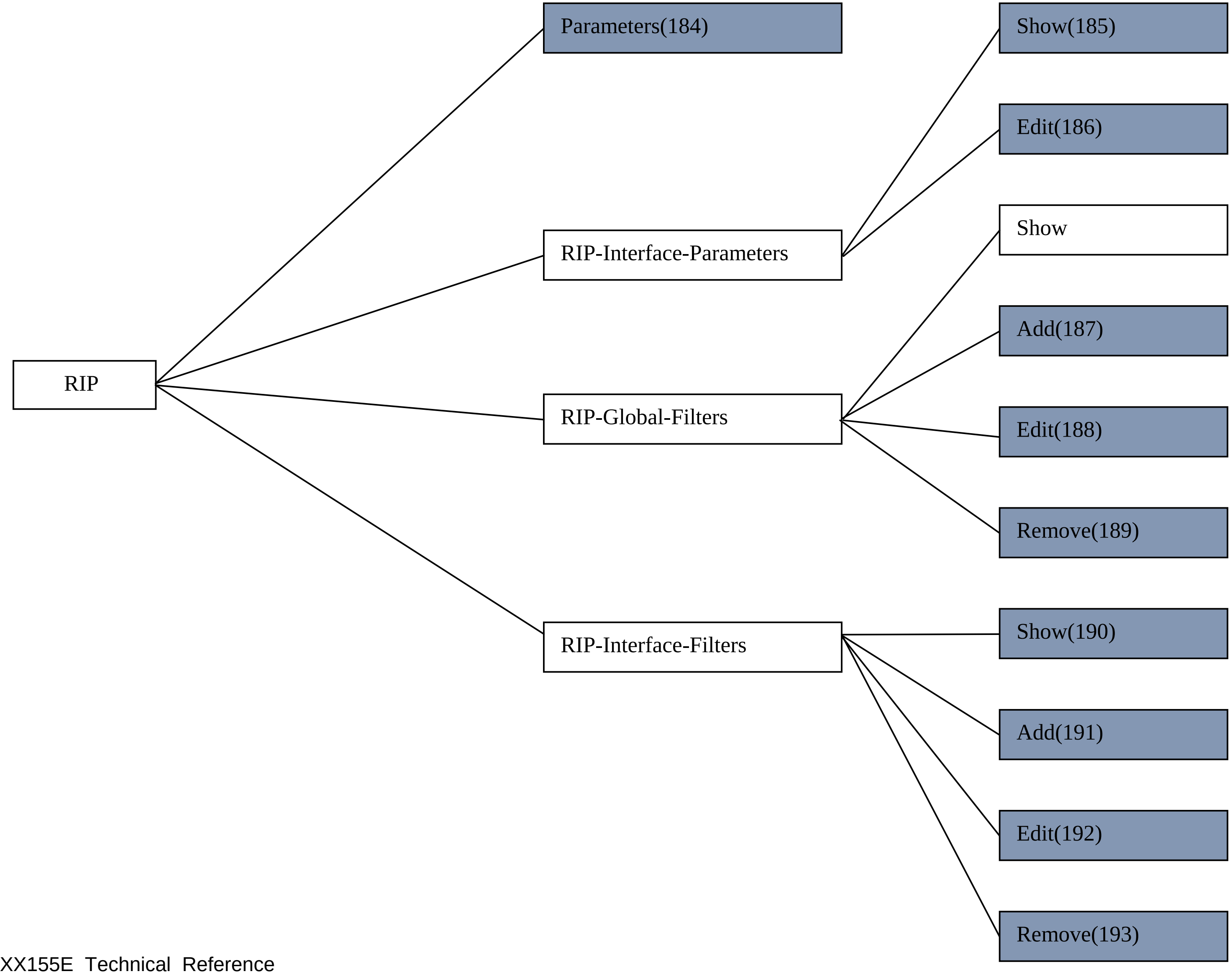
Router

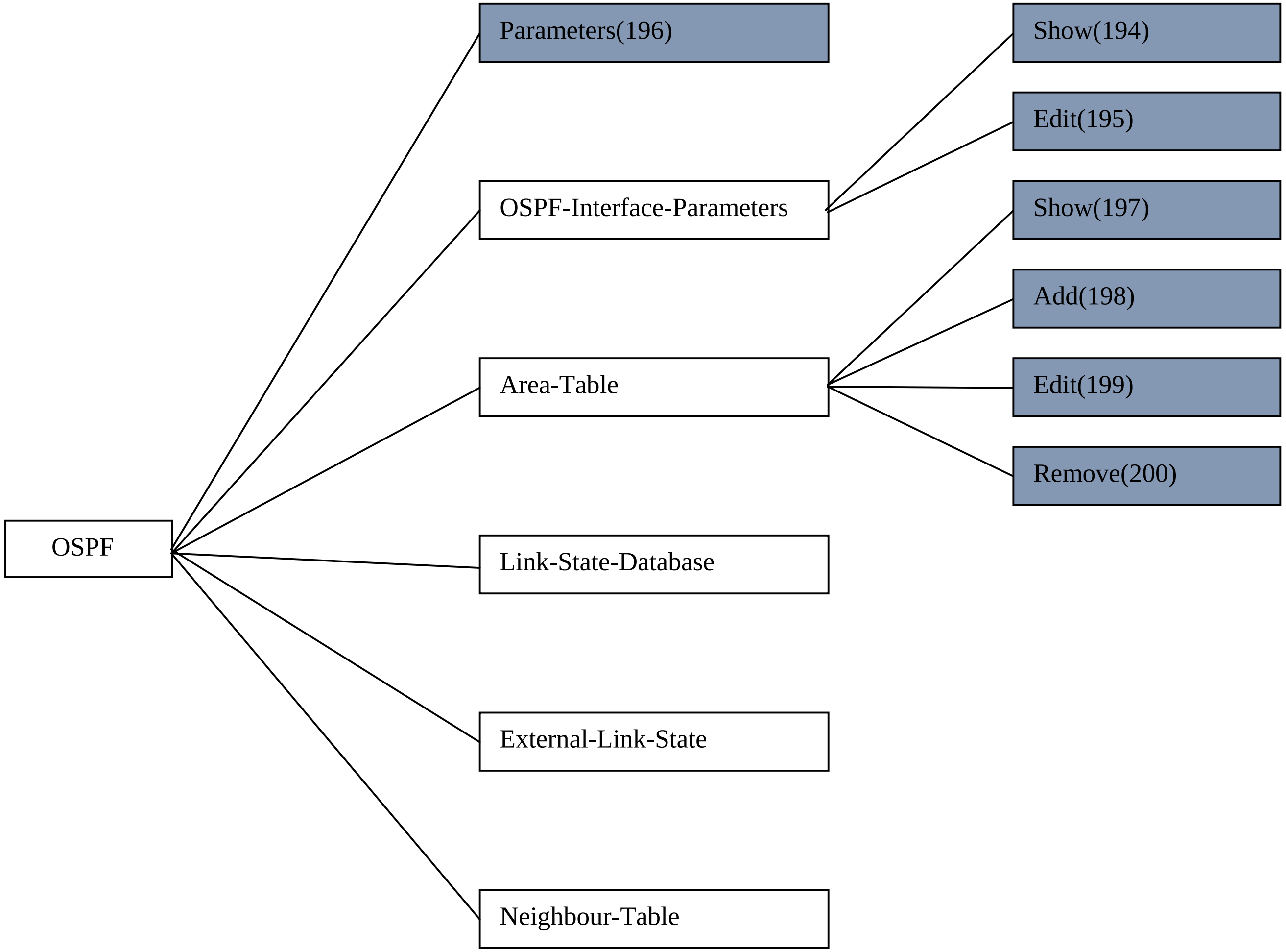
IP - Router

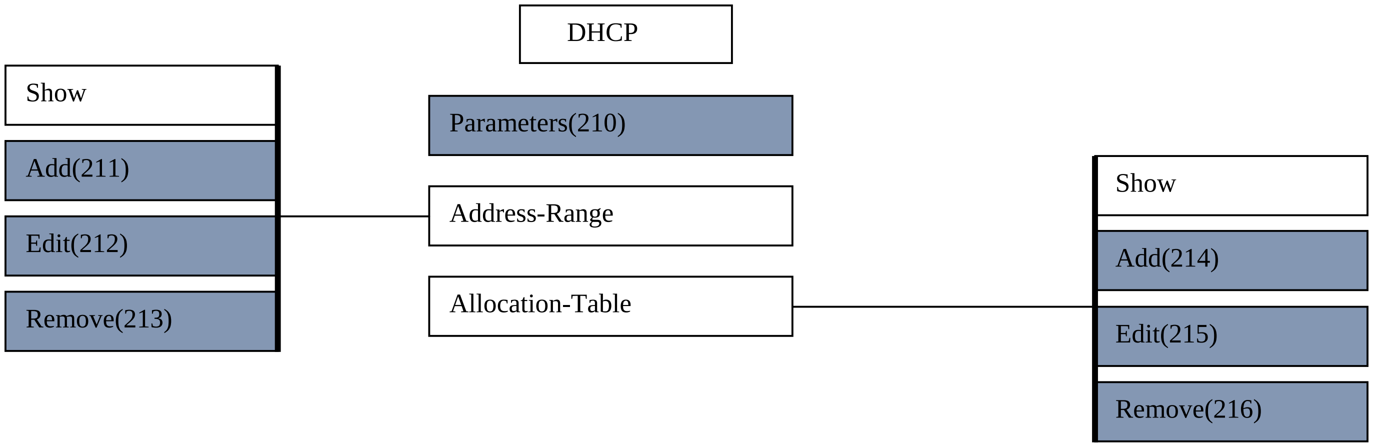
IPX - Router

IPM

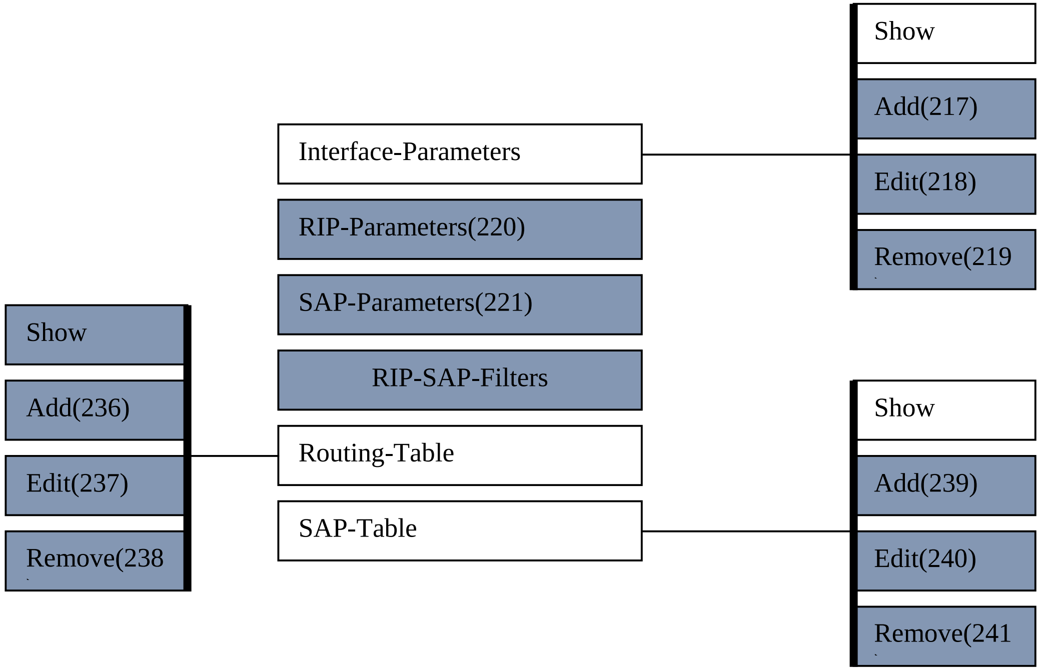

IP - Router
Operating- Parameters(177)
Interface-Table
Interface-Parameters
ICMP-Interface-Parameters
RIP
OSPF
Routing-Table
ARP-Table
IP-Redundancy
DHCP
UDP-Relay
TCP-General-Parameters
TCP-Connection-Table
Show(178)
Add(179)
Edit(180)
Remove(181)
Show(182)
Edit(183)
Show
Add(201)
Edit(202)
Remove(203)
Show
Add(204)
Edit(205)
Remove(206)
Show
Add(207)
Edit(208)
Remove(209)
Show
Add (100)
Remove(101)
Show

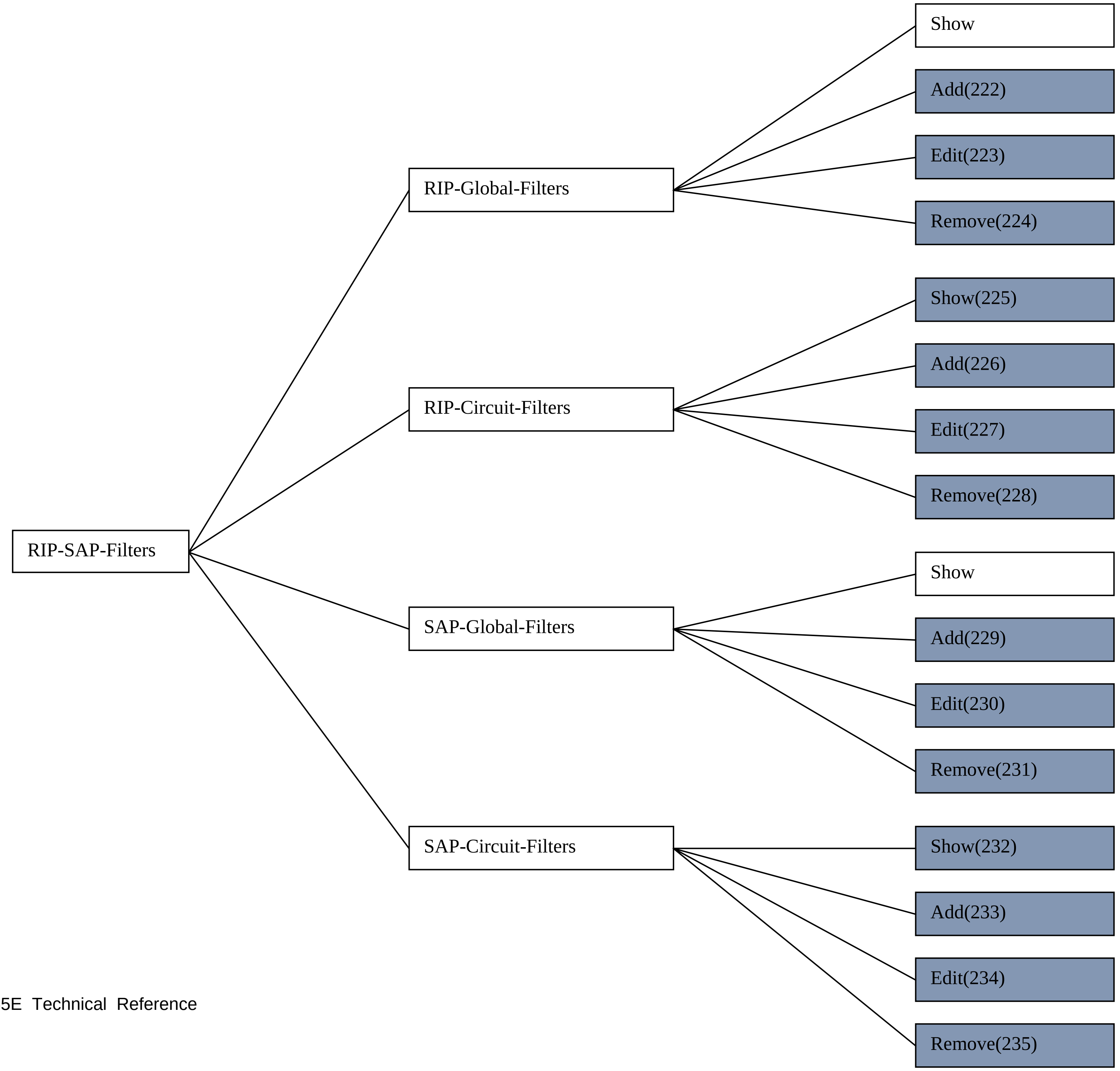

RIP
Parameters(184)
RIP-Interface-Parameters
RIP-Global-Filters
RIP-Interface-Filters
Show(185)
Edit(186)
Show
Add(187)
Edit(188)
Remove(189)
Show(190)
Add(191)
Edit(192)
Remove(193)

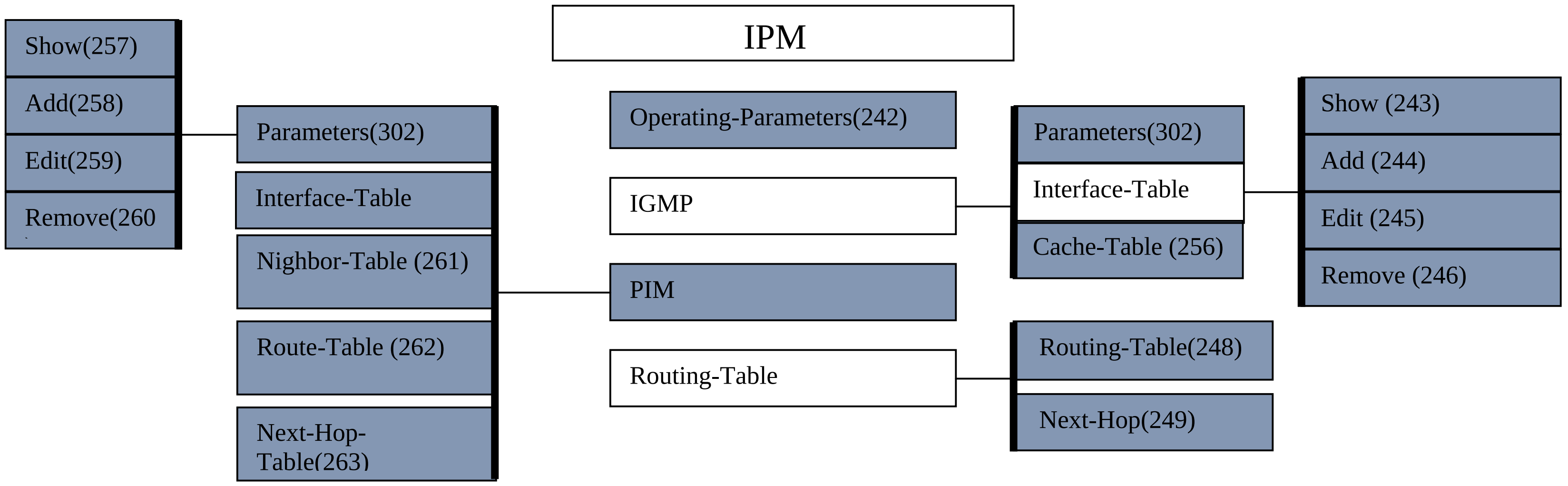

OSPF
Parameters(196)
OSPF-Interface-Parameters
Area-Table
Link-State-Database
External-Link-State
Neighbour-Table
Show(194)
Edit(195)
Show(197)
Add(198)
Edit(199)
Remove(200)


DHCP
Parameters(210)
Address-Range
Allocation-Table
Show
Add(211)
Edit(212)
Remove(213)
Show
Add(214)
Edit(215)
Remove(216)

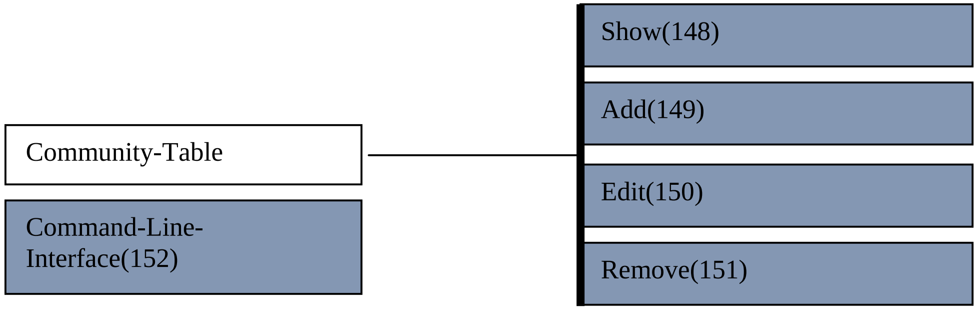
IPX - Router


Show
Add(217)
Edit(218)
Remove(219
Interface-Parameters
RIP-Parameters(220)
SAP-Parameters(221)
RIP-SAP-Filters
Routing-Table
SAP-Table
Show
Add(236)
Edit(237)
Remove(238
Show
Add(239)
Edit(240)
Remove(241

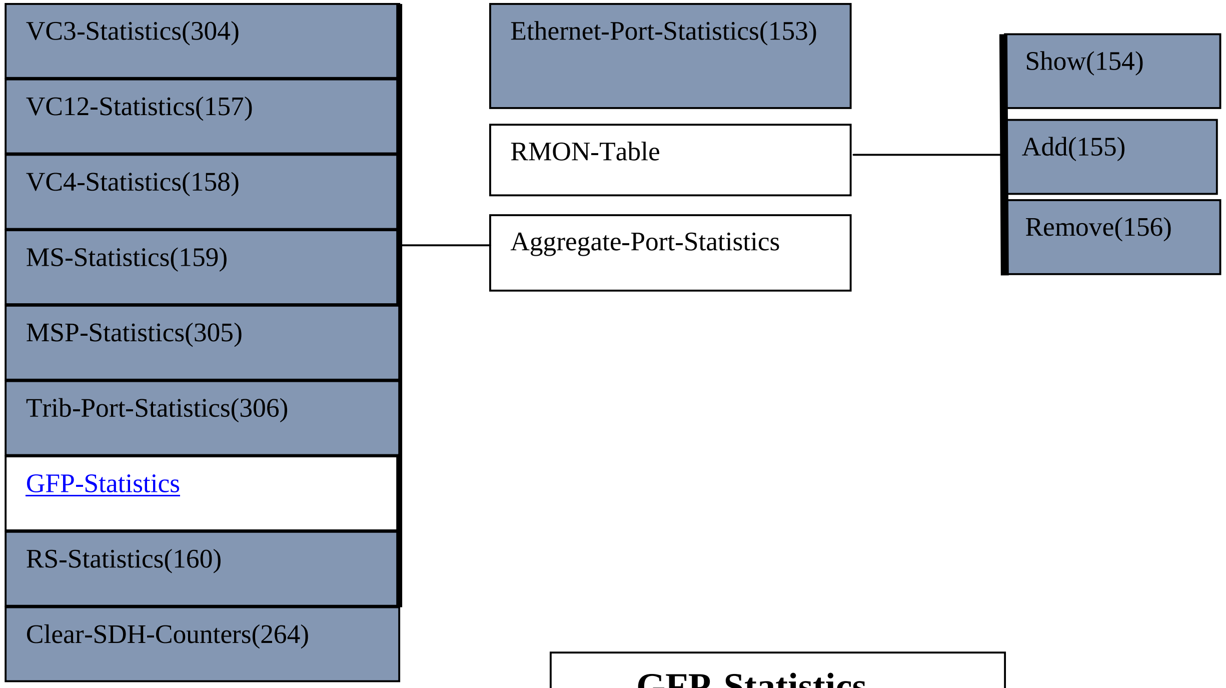

RIP-SAP-Filters
RIP-Global-Filters
Show
Add(222)
Edit(223)
Remove(224)
RIP-Circuit-Filters
Show(225)
Add(226)
Edit(227)
Remove(228)
SAP-Global-Filters
Show
Add(229)
Edit(230)
Remove(231)
SAP-Circuit-Filters
Show(232)
Add(233)
Edit(234)
Remove(235)


IPM
Show(257)
Add(258)
Edit(259)
Remove(260
Parameters(302)
Interface-Table
Nighbor-Table (261)
Route-Table (262)
Next-Hop-Table(263)
Operating-Parameters(242)
IGMP
PIM
Routing-Table
Parameters(302)
Interface-Table
Cache-Table (256)
Show (243)
Add (244)
Edit (245)
Remove (246)
Routing-Table(248)
Next-Hop(249)

Security


Community-Table
Command-Line-Interface(152)
Show(148)
Add(149)
Edit(150)
Remove(151)

Statistics



VC3-Statistics(304)

VC12-Statistics(157)

VC4-Statistics(158)

MS-Statistics(159)

MSP-Statistics(305)

Trib-Port-Statistics(306)

GFP-Statistics

RS-Statistics(160)

Clear-SDH-Counters(264)

Ethernet-Port-Statistics(153)

RMON-Table

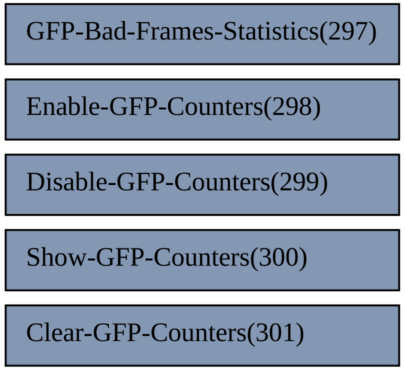
Aggregate-Port-Statistics

Show(154)

Add(155)

Remove(156)

GFP-Statistics



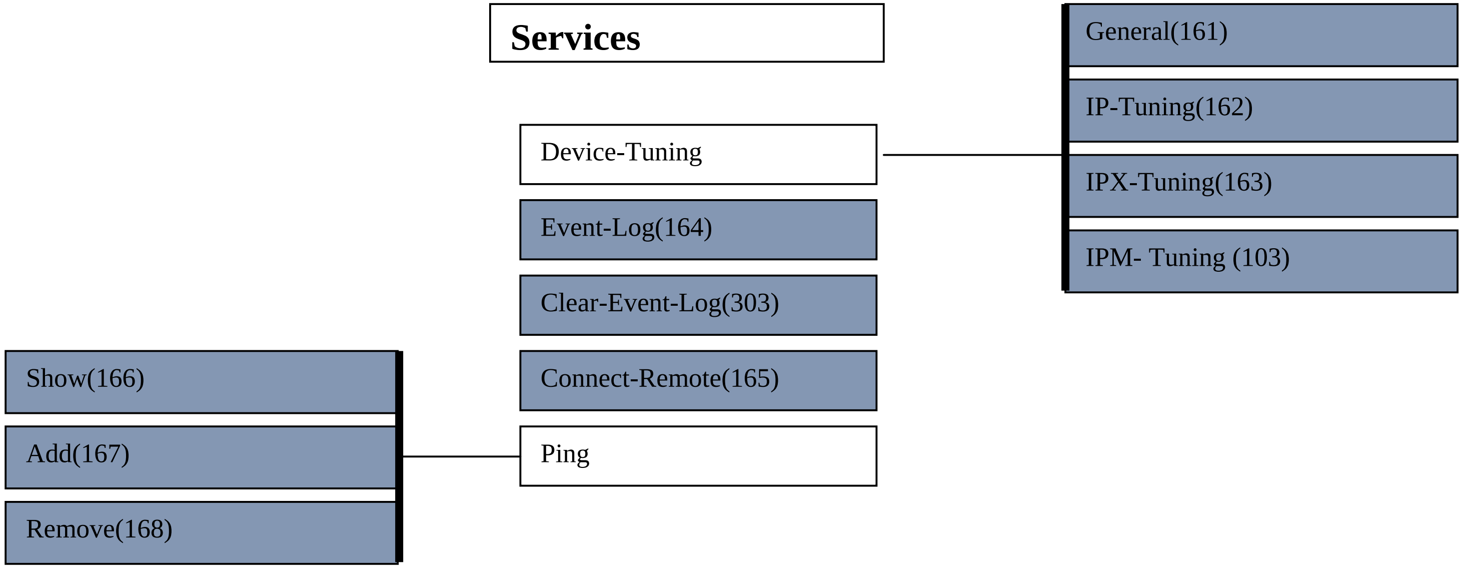
GFP-Bad-Frames-Statistics(297)

Enable-GFP-Counters(298)

Disable-GFP-Counters(299)

Show-GFP-Counters(300)

Clear-GFP-Counters(301)



Services

Device-Tuning

General(161)

IP-Tuning(162)

IPX-Tuning(163)

IPM- Tuning (103)

Event-Log(164)

Clear-Event-Log(303)

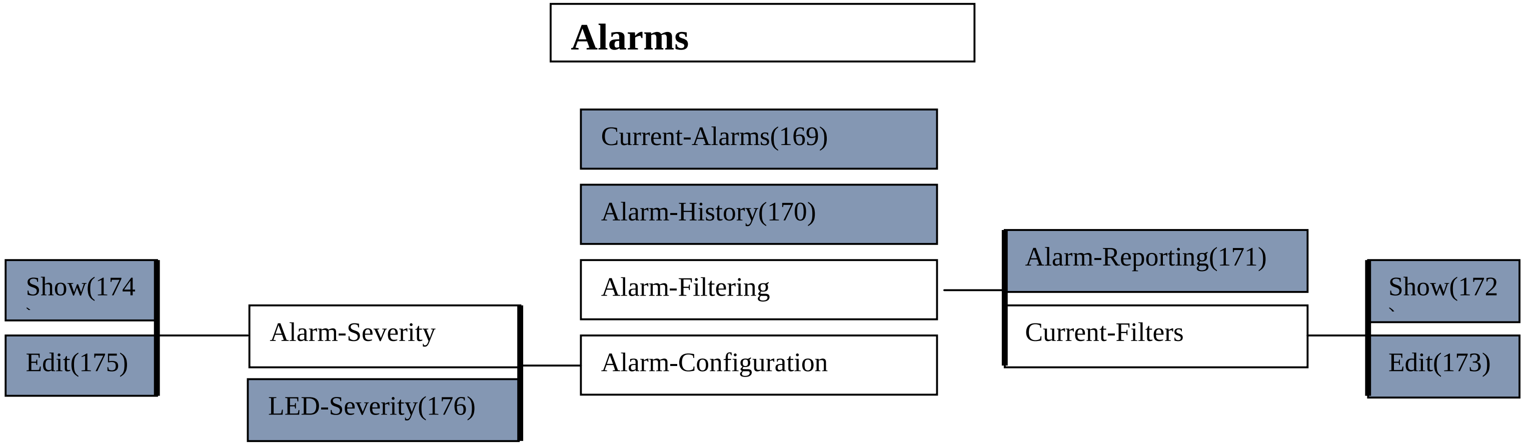
Connect-Remote(165)

Ping

Show(166)

Add(167)

Remove(168)



Alarms

Current-Alarms(169)

Alarm-History(170)

Alarm-Filtering

Alarm-Reporting(171)

Current-Filters

Show(172
`

Edit(173)

Alarm-Configuration

Alarm-Severity

Show(174
`

Edit(175)

LED-Severity(176)

Command	Parameters
1. IP-ConfigurationRouter	[IP-ADDRESS=<IP address>] [SUBNET-MASK=<IP address>]
2. IP-ConfigurationBridge	[IP-ADDRESS=<IP address>] [SUBNET-MASK=<IP address>] [DEFAULT-GATEWAY=<IP address>]
3. MAC-Filter	[MAC-FILTER-SWITCH=<enabled | disabled>]
4. System-Id	[SYSTEM-ID=<NSAP system ID - hexString[2:16]>] [NSEL=<NSAP selector - hexString[2:2]>]
5. Show	<none>
6. Add	AREA-ADDRESS=<NSAP area address - hexString[4:36]>
7. Edit	INDEX=<integer value 1:3> AREA-ADDRESS=<NSAP area address - hexString[4:36]>
8. Remove	INDEX=<integer value 1:3>
9. ModeOsi	MODE=<notUsed|ip|clnp|ipAndClnp>>
10. Gateway-Configuration	[NSAP-ADDRESS=<NSAP address - hexString[6:40]>] [STATUS=<enabled|disabled>]
11. LAPD-Configuration	[LAPD-ROLE=<network|user>] [TOGGLE-CR=<enabled|disabled>] [N201=<integer value 0:65535>]
12. OSI-IP-ConfigurationRouter	[OSI-IP-ADDRESS=<IP address>] [OSI-SUBNET-MASK=<IP address>]
13. DccIpNonOsiMode	[MODE=<notUsed|ipBroadcast|ipRouting|ipPppCrc16|ipPppCrc32>]
14. IP-Configuration	[IP-ADDRESS=<IP address>] [SUBNET-MASK=<IP address>]
15. ManModeOsi	[[MODE=<notUsed|ip|clnp|ipAndClnp>]
16. ManModeNonOsi	[[MODE=<notUsed|ip|>]
17. ManModeIpun	[MODE=<notUsed|ip>]
18. OSI-IP-ConfigurationBridge	[OSI-IP-ADDRESS=<IP address>] [OSI-SUBNET-MASK=<IP address>] [OSI-DEFAULT-GATEWAY=<IP address>]
19. OsiMode	[MODE=<notUsed|ip|clnp|ipAndClnp>]
20. DccModeIpun	[[MODE=<notUsed|ipPppCrc16|ipPppCrc32>]
21. DccIpOsiMode	[MODE=<notUsed|ipBroadcas|ipRouting|osiEncapsulation|ipPppCrc16|ipPppCrc32>]
22. DccIpNonOsiMode	[MODE=<notUsed|ipBroadcast|ipRouting|ipPppCrc16|ipPppCrc32>]
23. Add	IP-ADDRESS=<IP address> IF-NUM=<integer value> SUBNET-MASK=<IP address> [DEFAULT-GATEWAY=<IP address>]
24. Edit	IP-ADDRESS=<IP address> [IF-INDEX=<integer value>] [SUBNET-MASK=<IP address>] [DEFAULT-GATEWAY=<IP address>]
25. Remove	IP-ADDRESS=<IP address>
26. Show	IP-ADDRESS=<IP address>
27. PPP-IP-Routing	[IP-ADDRESS=<IP address>][SUBNET-MASK=<IP address>]
28. PPP-IP-Routing	[IP-ADDRESS=<IP address>] [SUBNET-MASK=<IP address>] [DEFAULT-GATEWAY=<IP address>]

Command	Parameters
29. Encapsulation	[HELLO-INTERVAL=<integer value 0:65535>]
30. General	[L1-LSP=<integer value 0:1492>] [L2-LSP=<integer value 0:1492>] [IS-MODE=<disabled|is|l1Is|l2Is>]
31. Identification	[NAME=<string[0:160]>] [LOCATION=<string[0:160]>] [CONTACT=<string[0:160]>]
32. Time	[TIME=<hh:mm:ss>] [DATE=<yyyy-mm-dd>]
33. Time-Protocol	[SERVER-IP-ADDRESS=<IP address>] [SYNC-INTERVAL=<integer value 0:2147483647>] [UTC-DELTA=<integer value -720:720>]
34. FFT	[IP-FASTFORWARDING=<enable|disable>] [IPX-FASTFORWARDING=<enable|disable>]
35. Autodiscovery	[STATUS=<enabled|disabled>] [TRAP-FREQUENCY=<integer value 0:2147483647>]
36. Show	<none>
37. Replace-Licence-Key	LICENCE-KEY=<string[1:50]>
38. Show	[VLAN-NUMBER=<integer>]
39. Add	NAME=<string> [ADDRESS-TYPE=<default|reserve>] [TAG=<integer>]
40. Edit	VLAN-NUMBER=<integer> [NAME=<string>] [ADDRESS-TYPE=<default|reserve>] [TAG=<integer>]
41. Remove	VLAN-NUMBER=<integer>
42. Show	[VLAN-NUMBER=<integer>]
43. Add	VLAN-NUMBER=<integer> ETHERNET-PORTS=<portList> [TAGGING=<enable|disable>]
44. Edit	VLAN-NUMBER=<integer> ETHERNET-PORTS =<portList> TAGGING=<enable|disable>
45. Remove	VLAN-NUMBER=<integer> ETHERNET-PORTS =<portList>
46. Sync-Source	[ADMIN-SOURCE=<Trib1|Trib2|Trib3|Trib4|Trib5|Trib6|Trib7|Trib8|Trib9|Trib10| Trib11|Trib12|Aggr1|Aggr2|Active|Local|External>]
47. Inventory	<none>
48. Remote-Device-Identification	[REMOTE-DEVICE=<IP address>]
49. Main	[ETHERNET-PORT=<integer value 1:8>] [SPEED-ADMIN-MODE=<10M|100M>] [ADMINISTRATIVE-STATUS=<on|off>] [DESCRIPTION=<string[0:64]>] [DUPLEX-ADMIN-MODE=<none|half|full>] [PHYSICAL-ADDRESS-ASSIGNMENT=<default|reserve>] [AUTONEGOTIATION-MODE=<enabled|disabled>]
50. Other	[ETHERNET-PORT=<integer value 1:8>] [BACK-PRESSURE-MODE=<enable|disable>] [FLOW-CONTROL-MODE=<on|off|autoNegotiation>]
51. VLAN-Properties	[ETHERNET-PORT=<integer value 1:8>]
52. IP-Properties	[ETHERNET-PORT=<integer value 1:8>]
53. IPX-Properties	[ETHERNET-PORT=<integer value 1:8>]

Command	Parameters
54. Reset-Device	<none>
55. Erase-Configuration	<none>
56. Erase-NVRAM	<none>
57. 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>]
58. General	AGGREGATE-PORT=<integer value 1:2> [ADMINISTRATIVE-STATUS=<enable|disable>] [DESCRIPTION=<string[0:64]>] [CONNECTED-TO=<string[0:160]>]
59. 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>]
60. VC4-Path-Trace	[PATH-TRACE=<enabled|disabled>] [EXPECTED-TI=<string[1:15]>] [HEX-EXPECTED-TI=<string[2:44]>] [TRANSMIT-TI=<string[1:15]>] [HEX-TRANSMIT-TI=<string[2:44]>]
61. RS-Path-Trace	AGGREGATE-PORT=<integer value 1:2> [PATH-TRACE=<enabled|disabled>] [EXPECTED-TI=<string[1:15]>] [HEX-EXPECTED-TI=<string[2:44]>] [TRANSMIT-TI=<string[1:15]>] [HEX-TRANSMIT-TI=<string[2:44]>]
62. Alarm-Port-Properties	[ALARM-PORT=<integer value 1:4>] [MODE=<enabled|disabled>] [DESCRIPTION=<string[0:64]>] [TRIGGERED-WHEN=<opens|closes>]
63. User-Channel-Port-Properties	[ADMINISTRATIVE-STATUS=<enabled|disabled>] [DESCRIPTION=<string[0:64]>] [AGGREGATE-PORT=<SDH-A|SDH-B|ACTIVE>] [DATA-RATE=<sync64000|async19200>]
64. Operating-Parameters	[FORWARDING-TABLE-AGING-TIME=<integer value 10:1000000>] [BRIDGE-MODE=<normal|provider>]
65. VLAN-Id-Table	ETHERNET-PORT=<integer value 1:8>
66. Show	<none>

67. Add	VLAN-TAG-ID=<integer value 1:4000>
	MAC-ADDRESS=<MAC address - hexString[12:12]>
	ETHERNET-PORT=<integer value 1:8>
	[STATUS=<permanent|deleteOnReset>]

68. Edit	VLAN-TAG-ID=<integer value 1:4000>
	MAC-ADDRESS=<MAC address - hexString[12:12]>
	ETHERNET-PORT=<integer value 1:8>
	[STATUS=<permanent|deleteOnReset>]

Command	Parameters

69. Remove	VLAN-TAG-ID=<integer value 1:4000>
	MAC-ADDRESS=<MAC address - hexString[12:12]>
	ETHERNET-PORT=<integer value 1:8>

70. Size-Unicast-Global-Forwarding-Table	<none>
71. Factory-Reset	<none>
72. Show	[IP-ADDRESS=<IP address>]
73. General	[WAN-PORT=<integer value 5:8>] [PATH-TRACE=<enabled|disabled>][EXPECTED-TI=<string[1:15]>] [HEX-EXPECTED-TI=<string[2:44]>][TRANSMIT-TI=<string[1:15]>][HEX-TRANSMIT-TI=<string[2:44]>] [CHANNEL-TI=<integer value 0:50>]
74. Add-VC12-channel	WAN-PORT=<integer value 5:8> [KLM=<K.L.M - integer value 1:3.integer value 1:7.integer value 1:3>] [ADMIN-STATUS=<enabled|disabled>] [NUMBER-TO-ADD=<integer value 1:50>] [SORT-MODE=<LEX|G707>]
75. Edit-VC12-channel	[WAN-PORT=<integer value 5:8>] [WAN-CHANNEL=<integer value 1:50>] [ADMIN-STATUS=<enabled|disabled>]
76. Remove-VC12-channel	WAN-PORT=<integer value 5:8> [NUMBER-TO-REMOVE=<integer value 1:50>]
77. General	[[TRIB-PORT=<integer value 1:12>] [DESCRIPTION=<string[0:64]>] [ADMINISTRATIVE-STATUS=<enable|disable>] [MODE=<TRA|PRA>] [LOOP-MODE=<NONE|LL2|LL3>] [PATH-TRACE=<enabled|disabled>] [EXPECTED-TI=<string[1:15]>] [HEX-EXPECTED-TI=<string[2:44]>] [TRANSMIT-TI=<string[1:15]>] [HEX-TRANSMIT-TI=<string[2:44]>]
78. Assign-VC12-Channel	TRIB-PORT=<integer value 1:12> [KLM=<K.L.M - integer value 1:3.integer value 1:7.integer value 1:3>] [NUMBER-TO-ADD=<integer value 1:12>] [SORT-MODE=<LEX|G707>]
79. Deassign-VC12-Channel	TRIB-PORT=<integer value 1:12> [NUMBER-TO-REMOVE=<integer value 1:12>]
80. Parameters	[MULTICASTING-ENABLE=<true|false>]
81. Forwarding-Table	[[VLAN-TAG-ID=<integer value 1:4000>] [MULTICAST-ADDRESS=<MAC address - hexString[12:12]>]
82. Show	[[VLAN-TAG-ID=<integer value 0:8>]
83. Edit	[VLAN-TAG-ID=<integer value 1:4000> [STATIC-PORTS=<integer value 0:8,...>] [FORBIDDEN-PORTS=<integer value 0:8,...>]
84. Show	[[VLAN-TAG-ID=<integer value 1:4000>]
85. Edit	[VLAN-TAG-ID=<integer value 1:4000> [STATIC-PORTS=<integer value 0:8,...>] [FORBIDDEN-PORTS=<integer value 0:8,...>]
86. Show	[[VLAN-TAG-ID=<integer value 1:4000>] [MULTICAST-ADDRESS=<MAC address - hexString[12:12]>]

Command	Parameters
87. Add	[VLAN-TAG-ID=<integer value 1:4000> MULTICAST-ADDRESS=<MAC address - hexString[12:12]> [EGRESS-PORTS=<integer value 0:8,...>] [FORBIDDEN-PORTS=<integer value 0:8,...>] [STATUS=<other|invalid|permanent|deleteOnReset|deleteOnTimeout>]
88. Edit	[VLAN-TAG-ID=<integer value 1:4000> MULTICAST-ADDRESS=<MAC address - hexString[12:12]> [EGRESS-PORTS=<integer value 0:8,...>] [FORBIDDEN-PORTS=<integer value 0:8,...>] [STATUS=<other|invalid|permanent|deleteOnReset|deleteOnTimeout>]
89. Remove	[VLAN-TAG-ID=<integer value 1:4000> MULTICAST-ADDRESS=<MAC address - hexString[12:12]>
90. Parameters	[IGMP-ENABLE=<true|false>] [HOST-AGING-TIME-IGMP=<integer value>] [ROUTER-AGING-TIME-IGMP=<integer value>]
91. Group-Table	[VLAN-TAG-ID =<integer value 1:4000>] [PORT=<integer value 1:8>] [MULTICAST-ADDRESS=<MAC address - hexString[12:12]>]
92. Router-Table	[VLAN-TAG-ID =<integer value 1:4000>] [PORT=<integer value 1:8>]
93. Show	[PORT=<integer value 1:8>] [TYPE-OF-PROTOCOL=<notUsed|preDefined|ethUserDefined|llcUserDefined>] [PROTOCOL=<NotUsed|Other|IP|RESERVED|IPX_RAW|IPX_Ethernet|IPX_LLC|IPX_SNAP| DECNET|DECLAT|NETBIOS|APPLETALK|XNS|SNA>]
94. Edit	PORT=<integer value 1:8> TYPE-OF-PROTOCOL=<notUsed|preDefined|ethUserDefined|llcUserDefined> PROTOCOL=<NotUsed|Other|IP|RESERVED|IPX_RAW|IPX_Ethernet|IPX_LLC|IPX_SNAP| DECNET|DECLAT|NETBIOS|APPLETALK|XNS|SNA> [DEFAULT-PRIOR=<integer value 0:7>] [TRAFFIC-CLASSES=<integer value 1:8>]
95. Show	[PORT=<integer value 1:8>]
96. Edit	PORT=<integer value 1:8> [DEFAULT-PRIOR=<integer value 0:7>]
97. Priority-Group-Table	[PORT=<integer value 1:8>]
98. Port-Table	[VLAN-TAG=<integer value 1:4000>] [ETHERNET-PORT=<integer value 1:8>] [STATUS=<true|false>]
99. Forced-SW-Version-Table	[VLAN-TAG=<integer value 1:4000>] [STATE=<STPCompatibility|NormalRSTP>]
100. Add	UDP-DEST-PORT=<integer value> SOURCE-IP-ADDRESS=<IP address> DEST-IP-ADDRESS=<IP address>
101. Remove	UDP-DEST-PORT=<integer value> SOURCE-IP-ADDRESS=<IP address> DEST-IP-ADDRESS=<IP address>
102. Remove	LOCAL-IP-ADDR=<IP address> LOCAL-PORT=<integer value 0:65535> REMOTE-IP-ADDR=<IP address> REMOTE-PORT=<integer value 0:65535>
103. IPM- Tuning	[FFT-ENTRIES-AFTER-RESET=<integer value>] [NEIGBOUR-ENTRIES-AFTER-RESET=<integer value>] [ROUTE-ENTRIES-AFTER-RESET=<integer value>] [INTERFACE-ENTRIES-AFTER-RESET=<integer value>] [IGMP-ENTRIES-AFTER-RESET=<integer value>]
104.	
105.	

Command	Parameters
106.	
107.	
108.	
109.	
110.	
111.	
112.	
113.	
114.	
115.	
116.	
117.	
118.	
119.	
120.	
121.	
122.	
123.	
124. Parameters	[VLAN-SUPPORTED-TYPE-AFTER-RESET=<perPort|perProtAndPort>]
125. Show	[IF-INDEX.=<integer value>]
126. Add	NAME=<string[0:20]> [ADDRESS-TYPE=<default|reserve>] [TAG=<integer value 1:4000>]
127. Edit	IF-INDEX=<integer value> [NAME=<string[0:20]>] [ADDRESS-TYPE=<default|reserve>]
128. Remove	IF-INDEX=<integer value>
129. Show	[IF-INDEX=<integer value>]
130. Add	IF-INDEX=<integer value> ETHERNET-PORTS=<integer value 1:8,...> [TAGGING=<enable|disable>] [EGRESS-FORBIDDEN=<true|false>]
131. Edit	IF-INDEX=<integer value> ETHERNET-PORTS=<integer value 1:8,...> [TAGGING=<enable|disable>] [EGRESS-FORBIDDEN=<true|false>]
132. Remove	IF-INDEX=<integer value> ETHERNET-PORTS=<integer value 1:8,...>
133. Show	[INDEX=<integer value>]
134. Add	PROTOCOL-NAME=<string[0:20]> PROTOCOL-NUM=<string[4:4]> [PROTOCOL-MASK=<string[4:4]>]
135. Edit	INDEX=<integer value> [PROTOCOL-NAME=<string[0:20]>] [PROTOCOL-NUM=<string[4:4]>] [PROTOCOL-MASK=<string[4:4]>]

Command	Parameters
136. Remove	INDEX=<integer value>
137. Show	[VLAN-IF-INDEX.=<integer value>]
138. Add	TYPE-OF-PROTOCOL=<preDefined_protocols|ethUserDefined_protocols> NAME=<string[0:20]> [PROTOCOL=< |Other|IP|IPX_RAW|IPX_Ethernet|IPX_LLC|IPX_SNAP|DECNET|NETBIOS|SNA>] [ADDRESS-TYPE=<default|reserve>] [TAG=<integer value 1:4000>] **If TYPE-OF-PROTOCOL = ethUserDefined_protocols, PROTOCOL input not needed(taken from vlanEthUserDefProtEntry**)
139. Edit	VLAN-IF-INDEX.=<integer value> [NAME=<string[0:20]>] [ADDRESS-TYPE=<default|reserve>]
140. Remove	VLAN-NUMBER=<integer value>
141. Show	[VLAN-NUMBER=<integer value>]
142. Add	VLAN-NUMBER=<integer value> ETHERNET-PORTS=<integer value 1:8,...> [TAGGING=<enable|disable>] [EGRESS-FORBIDDEN=<true|false>]
143. Edit	VLAN-NUMBER=<integer value> ETHERNET-PORTS=<integer value 1:8,...> [TAGGING=<enable|disable>] [EGRESS-FORBIDDEN=<true|false>]
144. Remove	VLAN-NUMBER=<integer value> ETHERNET-PORTS=<integer value 1:8,...>
145. Show	<none>
146. Add	PREFIX=<NSAP area address - hexString[4:36]>
147. Remove	PREFIX=<NSAP area address - hexString[4:36]>
148. Show	[MANAGER=<IP address>]
149. Add	MANAGER=<IP address> COMMUNITY=<string[1:20]> ACCESS=<readOnly|readWrite|super> TRAPS=<enable|disable>
150. Edit	MANAGER=<IP address> COMMUNITY=<string[1:20]> [ACCESS=<readOnly|readWrite|super>] [TRAPS=<enable|disable>]
151. Remove	MANAGER=<IP address> COMMUNITY=<string[1:20]>
152. Command-Line-Interface	[XXXCLI-PASSWORD=<string[6:12]>] [TELNET-PASSWORD=<string[6:12]>] [DISPLAY-LINES=<integer value 0:999>] [ALLOW-MESSAGES=<YES|NO>]
153. Ethernet-Port-Statistics	ETHERNET-PORT=<integer value 1:8>
154. Show	<none>
155. Add	ETHERNET-PORT=<integer value 1:8>
156. Remove	ETHERNET-PORT=<integer value 1:8>
157. VC12-Statistics	KLM=<K.L.M - integer value 1:3.integer value 1:7.integer value 1:3>
158. VC4-Statistics	<none>
159. MS-Statistics	AGGREGATE-PORT=<integer value 1:2>

Command	Parameters
160. RS-Statistics	AGGREGATE-PORT=<integer value 1:2>
161. General	[BRIDGE-FORWARDNG-TABLE-AFTER-RESET=<integer value>] [RMON-LOG-TABLE-AFTER-RESET=<integer value>] [GVRP-VLAN-ENTRIES-AFTER-RESET=<integer value>] [RULES-POLICY-MIB-AFTER-RESET=<integer value>] [PROFILES-POLICY-MIB-AFTER-RESET=<integer value>] [VLAN-ENTRIES-AFTER-RESET=<integer value>] [ERROR-REPORT-LEVEL=<integer value>]
162. IP-Tuning	[IP-RIP-MAX-ENTRIES-AFTER-RESET=<integer value>] [ARP-FORWARDING-MAX-ENTRIES-AFTER-RESET=<integer value>] [IP-FFT-MAX-ENTRIES-AFTER-RESET=<integer value>] [DHCP-MAX-CONNECTION-AFTER-RESET=<integer value>] [IP-FFT-UPPER-LIMIT=<integer value 0:100>] [IP-FFT-LOWER-LIMIT=<integer value 0:100>]
163. IPX-Tuning	[IPX-RIP-MAX-ENTRIES-AFTER-RESET=<integer value>] [IPX-SAP-MAX-ENTRIES-AFTER-RESET=<integer value>] [IPX-FFT-MAX-ENTRIES-AFTER-RESET=<integer value>][IPX-FFT-UPPER-LIMIT=<integer value 1:100>] [IPX-FFT-LOWER-LIMIT=<integer value 0:100>]
164. Event-Log	<none>
165. Connect-Remote	<none>
166. Show	[IP-ADDRESS=<IP address>]
167. Add	IP-ADDRESS=<IP address> [COUNT=<integer value 1:2147483647>] [SIZE=<integer value>] [TIMEOUT=<integer value 0:3600000>] [DELAY=<integer value 0:3600000>]
168. Remove	IP-ADDRESS=<IP address>
169. Current-Alarms	<none>
170. Alarm-History	<none>
171. Alarm-Reporting	[ALARM-REPORTING=<enabled|disabled>]
172. Show	[OBJECT-TYPE=<DEVICE|GFP|VCATLC|ALARM|TRIB|SPI|RST|MST|MSP|VC-4|AU-4|TU-12| VC-12|TU-3|VC-3>]

Command	Parameters
173. Edit	OBJECT-TYPE=<DEVICE|GFP|VCATLC|ALARM|TRIB|SPI|RST|MST|MSP|VC-4|AU-4|TU-12| VC-12|TU-3|VC-3> [ALARM-REPORTING=<enabled|disabled>] [PORT=<integer value 1:12>] [PERSISTENCY-ON=<integer value 0:255>] [PERSISTENCY-OFF=<integer value 0:255>] [SD-THRESHOLD=<integer value 6:9>] [AIS=<enabled|disabled>] [RDI=<enabled|disabled>]
174. Show	[ALARM-ID=<unknownAlarmId|hwFail|losSy|aux|losTx|aisRx|lfaRx|lfaTx|los|lof| td|tf|exc|deg|csf|tim|ais|rdi|msp|lom|lop|uneq|plm|fan|temp|unass| wanDelay|syncHoldOver|seqFail|plc|tlc|degFcs|degtHec|upm|clos|lfd| exm|pfm|sqnc|sqm|loa|loaNoTraf|acMstTimeout|rsAckTimeout| eosMultiple|eosMissing|sqNonCont|sqMultiple|sqOor|gidErr|ctrlOor| lcasCrc|nonLcas|mnd|fopr|plcr|tlcr|plct|tlct|info|lanOn|lanOff| rxOverflowHWFault|txOverflowHWFault|routeTableOverflow| resetRequired|endTftp|abortTftp|startTftp|faultBackUp|mainLinkUp| ipxRipTblOverflow|ipxSapTblOverflow|facsAccessVoilation| autoConfigurationCompleted|forwardingTabOverflow| framRelaySwitchConnectionUp|framRelaySwitchConnectionDown| errorsDuringInit|vlanDynPortAdded|vlanDynPortRemoved| rsSDclientsTableOverflow|rsSDinactiveServer| rsIpZhrConnectionsTableOverflow|rsIpZhrReqStaticConnNotAccepted| rsIpZhrVirtualIpAsSource|rsIpZhrNotAllocVirtualIp| rsSnmpSetRequestInSpecialCfgState|rsPingCompletion| pppSecurityViolation|frDLCIStatudChange|papFailedCommunication| chapFailedCommunication|rsWSDRedundancySwitch| rsDhcpAllocationFailure|rlIgmpTableOverflow|rlPimTableOverflow| rlIpFftStnOverflow|rlIpFftSubOverflow|rlIpxFftStnOverflow| rlIpxFftSubOverflow|rlIpmFftOverflow|rlPhysicalDescriptionChanged| rldot1dStpPortStateForwarding|rldot1dStpPortStateNotForwarding| rlPolicyDropPacketTrap|rlPolicyForwardPacketTrap>]

Command	Parameters

175. Edit	ALARM-ID=<unknownAlarmId|hwFail|losSy|aux|losTx|aisRx|lfaRx|lfaTx|los|lof|tdtf|exc|deg|csf|tim|ais|rdi|msp|lom|lop|uneq|plm|fan|temp|unass|wanDelay|syncHoldOver|seqFail|plc|tlc|degFcs|degtHec|upm|clos|lfd|exm|pfm|sqnc|sqm|loa|loaNoTraf|acMstTimeout|rsAckTimeout|eosMultiple|eosMissing|sqNonCont|sqMultiple|sqOor|gidErr|ctrlOor|lcasCrc|nonLcas|mnd|fopr|plcr|tlcr|plct|tlct|info|lanOn|lanOff|rxOverflowHWFault|txOverflowHWFault|routeTableOverflow|resetRequired|endTftp|abortTftp|startTftp|faultBackUp|mainLinkUp|ipxRipTblOverflow|ipxSapTblOverflow|facsAccessVoilation|autoConfigurationCompleted|forwardingTabOverflow|framRelaySwitchConnectionUp|framRelaySwitchConnectionDown|errorsDuringInit|vlanDynPortAdded|vlanDynPortRemoved|rsSDclientsTableOverflow|rsSDinactiveServer|rsIpZhrConnectionsTableOverflow|rsIpZhrReqStaticConnNotAccepted|rsIpZhrVirtualIpAsSource|rsIpZhrNotAllocVirtualIp|rsSnmpSetRequestInSpecialCfgState|rsPingCompletion|pppSecurityViolation|frDLCIStatudChange|papFailedCommunication|chapFailedCommunication|rsWSDRedundancySwitch|rsDhcpAllocationFailure|rlIgmpTableOverflow|rlPimTableOverflow|rlIpFftStnOverflow|rlIpFftSubOverflow|rlIpxFftStnOverflow|rlIpxFftSubOverflow|rlIpmFftOverflow|rlPhysicalDescriptionChanged|rldot1dStpPortStateForwarding|rldot1dStpPortStateNotForwarding|rlPolicyDropPacketTrap|rlPolicyForwardPacketTrap>
	ALARM-POINT=<unknownAlarmPoint|device|sdhPhysical|rst|mst|msp|au4|vc4|tu12|vc12|trib|aux|ethernet|wan|tu3|vc3|wanx|gfp|lcas|vcat>
	[SEVERITY=<critical|major|minor|warning>]
	[DESCRIPTION=<string[0:160]>]

176. LED-Severity	[CUSTOMER-LED-MIN-SEVERITY=<critical|major|minor|warning>] [OPERATOR-LED-MIN-SEVERITY=<critical|major|minor|warning>]
177. Operating- Parameters	[IP-REDUNDANCY-ADMIN-STATUS=<enable|disable>] [ARP-INACTIVE-TIMEOUT=<integer value>] [ARP-PROXY=<enable|disable>] [ICMP-ERROR-MSG=<enable|disable>]
178. Show	[IP-ADDRESS=<IP address>]

Command	Parameters
179. Add	IP-ADDRESS=<IP address> SUBNET-MASK=<IP address> IF-NUMBER=<integer value> [FWD-BROADCAST=<enable|disable>] [BROADCAST-TYPE=<ZERO-FILL|ONE-FILL>] [ARP-SERVER=<enable|disable>]
180. Edit	IP-ADDRESS=<IP address> [SUBNET-MASK=<IP address>] [IF-NUMBER=<integer value>] [FWD-BROADCAST=<enable|disable>] [BROADCAST-TYPE=<ZERO-FILL|ONE-FILL>] [ARP-SERVER=<enable|disable>]
181. Remove	IP-ADDRESS=<IP address>
182. Show	[IP-ADDRESS=<IP address>]
183. Edit	IP-ADDRESS=<IP address> [DESTINATION=<ALL-SYSTEMS-MULTICAST|LIMITED-BROADCAST>] [MAX-INTERVAL=<integer value 4:1800>] [MIN-INTERVAL=<integer value 3:1800>] [LIFETIME=<integer value 4:9000>] [ADVERTISE=<enable|disable>] [PREFERENCE-LEVEL=<integer value>] [DEFAULT-VALUES=<TRUE|FALSE>]
184. Parameters	[ADMINISTRATIVE-STATUS=<enable|disable>] [LEAK-OSPF=<enable|disable>] [LEAK-STATIC=<enable|disable>]
185. Show	[IP-ADDRESS=<IP address>]
186. Edit	IP-ADDRESS=<IP address> [OUTGOING-RIP=<doNotSend|ripVersion1|rip1Compatible|ripVersion2|ripV1Dem ripV2Demand>] [INCOMING-RIP=<rip1|rip2|rip1OrRip2|doNotRecieve>] [DEFAULT-METRIC=<integer value 0:15>] [AUTO-SEND=<enable|disable>] [VIRTUAL-DISTANCE=<integer value>] [STATUS=<valid|invalid>]
187. Add	TYPE=<input|output> NETWORK-ADDRESS=<IP address> NUM-MATCH-BITS=<integer value 1:32> ACTION=<deny|permit>
188. Edit	TYPE=<input|output> NUMBER=<integer value> [NETWORK-ADDRESS=<IP address>] [NUM-MATCH-BITS=<integer value 1:32>] [ACTION=<deny|permit>]
189. Remove	TYPE=<input|output> NUMBER=<integer value>
190. Show	[IP-ADDRESS=<IP address>]
191. Add	IP-ADDRESS=<IP address> TYPE=<input|output> NETWORK-ADDRESS=<IP address> NUM-MATCH-BITS=<integer value 1:32> ACTION=<deny|permit>
192. Edit	IP-ADDRESS=<IP address> TYPE=<input|output> NUMBER=<integer value> [NETWORK-ADDRESS=<IP address>] [NUM-MATCH-BITS=<integer value 1:32>] [ACTION=<deny|permit>]
193. Remove	IP-ADDRESS=<IP address> TYPE=<input|output> NUMBER=<integer value>
194. Show	[IP-ADDRESS=<IP address>]

Command	Parameters
195. Edit	IP-ADDRESS=<IP address> [AREA-ID=<IP address>] [IF-TYPE=<broadcast|nbma|pointToPoint|pointToMultipoint>] [ADMINISTRATIVE-STATUS=<enabled|disabled>] [PRIORITY=<integer value 0:255>] [HELLO-INTERVAL=<integer value 1:65535>] [ROUTER-DEAD-INTERVAL=<integer value 0:2147483647>] [IF-AUTHENTICATION-KEY=<string[0:8]>] [AUTHENTICATION-TYPE=<none|password>] [METRIC-VALUE=<integer value 0:65535>]
196. Parameters	[ADMINISTRATIVE-STATUS=<enabled|disabled>] [ROUTER-ID=<IP address>] [LEAK-RIP=<enable|disable>] [LEAK-STATIC=<enable|disable>] [LEAK-EXTERNAL=<enable|disable>]
197. Show	[AREA-ID=<IP address>]
198. Add	AREA-ID=<IP address> IMPORT-AS-EXTERN=<importExternal|importNoExternal|importNssa> [METRIC=<integer value 0:16777215>]
199. Edit	AREA-ID=<IP address> [IMPORT-AS-EXTERN=<importExternal|importNoExternal|importNssa>] [METRIC=<integer value 0:16777215>]
200. Remove	AREA-ID=<IP address>
201. Add	DEST-IP-ADDRESS=<IP address> DEST-SUBNET-MASK=<IP address> NEXT-HOP=<IP address> IF-NUMBER=<integer value> ROUTE-TYPE=<remote|reject> METRIC=<integer value>
202. Edit	DEST-IP-ADDRESS=<IP address> DEST-SUBNET-MASK=<IP address> NEXT-HOP=<IP address> METRIC=<integer value>
203. Remove	DEST-IP-ADDRESS=<IP address> DEST-SUBNET-MASK=<IP address> NEXT-HOP=<IP address>
204. Add	IF-NUMBER=<integer value> IP-ADDRESS=<IP address> MAC-ADDRESS=<MAC address - hexString[0:320]>
205. Edit	IF-NUMBER=<integer value> IP-ADDRESS=<IP address> MAC-ADDRESS=<MAC address - hexString[0:320]>
206. Remove	IF-NUMBER=<integer value> IP-ADDRESS=<IP address>
207. Add	IF-IP-ADDRESS=<IP address> MAIN-ROUTER-IP-ADDRESS=<IP address> [POLL-INTERVAL=<integer value>] [TIMEOUT=<integer value>]
208. Edit	IF-IP-ADDRESS=<IP address> MAIN-ROUTER-IP-ADDRESS=<IP address> [OPERATIONAL-STATUS=<active|inactive>] [POLL-INTERVAL=<integer value>] [TIMEOUT=<integer value>]
209. Remove	IF-IP-ADDRESS=<IP address> MAIN-ROUTER-IP-ADDRESS=<IP address>
210. Parameters	[SERVER-ENABLE=<enable|disable>] [NEXT-SERVER-ADDRESS=<IP address>] [SECURITY-THRESHOLD=<integer value>] [DNS-IP-ADDRESS=<IP address>] [PROBE-ENABLE=<enable|disable>] [PROBE-RETRIES=<integer value>] [PROBE-TIMEOUT=<integer value>] [PRIMARY-WINS-SERVER=<IP address>] [SECONDARY-WINS-SERVER=<IP address>] [NODE-TYPE=<BROADCAST|POINT-TO-POINT|HYBRID|MIXED>]
211. Add	IF-IP-ADDRESS=<IP address> IP-ADDRESS-FROM=<IP address> IP-ADDRESS-TO=<IP address> DEFAULT-ROUTER=<IP address> LEASE-TIME=<integer value> PROBE-ENABLE=<enable|disable>

Command	Parameters
212. Edit	IF-IP-ADDRESS=<IP address> IP-ADDRESS-FROM=<IP address> IP-ADDRESS-TO=<IP address> [DEFAULT-ROUTER=<IP address>] [LEASE-TIME=<integer value>] [PROBE-ENABLE=<enable|disable>]
213. Remove	IF-IP-ADDRESS=<IP address> IP-ADDRESS-FROM=<IP address> IP-ADDRESS-TO=<IP address>
214. Add	IP-ADDRESS=<IP address> MAC-ADDRESS=<MAC address - hexString[0:320]> HOST-NAME=<string[0:20]> DEFAULT-ROUTER=<IP address> CONFIG-SERVER-IP=<IP address> CONFIG-FILE-NAME=<string[0:128]>
215. Edit	IP-ADDRESS=<IP address> [MAC-ADDRESS=<MAC address - hexString[0:320]>] [HOST-NAME=<string[0:20]>] [DEFAULT-ROUTER=<IP address>] [CONFIG-SERVER-IP=<IP address>] [CONFIG-FILE-NAME=<string[0:128]>]
216. Remove	IP-ADDRESS=<IP address>
217. Add	IF-NUMBER=<integer value> NETWORK-ADDRESS=<IPX network number - hexString[8:8]> TIME-TO-NETWORK=<integer value 1:65535> LAYER2-ENCAP=<novell|ethernet|llc|snap|none> NETBIOS=<enabled|disabled> ADMINISTRATIVE-STATUS=<off|on|sleeping>
218. Edit	CIRCUIT-NUMBER=<integer value> [TIME-TO-NETWORK=<integer value 1:65535>] [LAYER2-ENCAP=<novell|ethernet|llc|snap|none>] [NETBIOS=<enabled|disabled>] [ADMINISTRATIVE-STATUS=<off|on|sleeping>]
219. Remove	CIRCUIT-NUMBER=<integer value>
220. RIP-Parameters	CIRCUIT-NUMBER=<integer value> [UPDATE-INTERVAL=<integer value>] [AGE-MULTIPLIER=<integer value>] [STATUS=<off|on>]
221. SAP-Parameters	CIRCUIT-NUMBER=<integer value> [UPDATE-INTERVAL=<integer value>] [AGE-MULTIPLIER=<integer value>] [RESPOND-TO-GET-SERVER=<no|yes>] [STATUS=<off|on>]
222. Add	TYPE=<input|output> NETWORK-ADDRESS=<IPX network number - hexString[8:8]> NETWORK-MASK=<IPX network number - hexString[8:8]> ACTION=<deny|permit>
223. Edit	TYPE=<input|output> NUMBER=<integer value> [NETWORK-ADDRESS=<IPX network number - hexString[8:8]>] [NETWORK-MASK=<IPX network number - hexString[8:8]>] [ACTION=<deny|permit>]
224. Remove	TYPE=<input|output> NUMBER=<integer value>
225. Show	[CIRCUIT-NUMBER=<integer value>]
226. Add	CIRCUIT-NUMBER=<integer value> TYPE=<input|output> NETWORK-ADDRESS=<IPX network number - hexString[8:8]> NETWORK-MASK=<IPX network number - hexString[8:8]> ACTION=<deny|permit>
227. Edit	CIRCUIT-NUMBER=<integer value> TYPE=<input|output> NUMBER=<integer value> [NETWORK-ADDRESS=<IPX network number - hexString[8:8]>] [NETWORK-MASK=<IPX network number - hexString[8:8]>] [ACTION=<deny|permit>]
228. Remove	CIRCUIT-NUMBER=<integer value> TYPE=<input|output> NUMBER=<integer value>

Command	Parameters
229. Add	TYPE=<input|output> NETWORK-ADDRESS=<IPX network number - hexString[8:8]> NETWORK-MASK=<IPX network number - hexString[8:8]> SERVICE-TYPE=<IPX server type - hexString[4:4]> SERVICE-NAME=<string[1:48]> ACTION=<deny|permit>
230. Edit	TYPE=<input|output> NUMBER=<integer value> [NETWORK-ADDRESS=<IPX network number - hexString[8:8]>] [NETWORK-MASK=<IPX network number - hexString[8:8]>] [SERVICE-TYPE=<IPX server type - hexString[4:4]>] [SERVICE-NAME=<string[1:48]>] [ACTION=<deny|permit>]
231. Remove	TYPE=<input|output> NUMBER=<integer value>
232. Show	[CIRCUIT-NUMBER=<integer value>]
233. Add	CIRCUIT-NUMBER=<integer value> TYPE=<input|output> NETWORK-ADDRESS=<IPX network number - hexString[8:8]> NETWORK-MASK=<IPX network number - hexString[8:8]> SERVICE-TYPE=<IPX server type - hexString[4:4]> SERVICE-NAME=<string[1:48]> ACTION=<deny|permit>
234. Edit	CIRCUIT-NUMBER=<integer value> TYPE=<input|output> NUMBER=<integer value> [NETWORK-ADDRESS=<IPX network number - hexString[8:8]>] [NETWORK-MASK=<IPX network number - hexString[8:8]>] [SERVICE-TYPE=<IPX server type - hexString[4:4]>] [SERVICE-NAME=<string[1:48]>] [ACTION=<deny|permit>]
235. Remove	CIRCUIT-NUMBER=<integer value> TYPE=<input|output> NUMBER=<integer value>
236. Add	DEST-NETWORK=<IPX network number - hexString[8:8]> CIRCUIT-NUMBER=<integer value> NEXT-HOP=<IPX network number - hexString[8:8]> [TICKS-TO-NET=<integer value>] [HOPS-TO-NET=<integer value>] [FORWARDING-ROUTER=<MAC address - hexString[12:12]>]
237. Edit	DEST-NETWORK=<IPX network number - hexString[8:8]> CIRCUIT-NUMBER=<integer value> [TICKS-TO-NET=<integer value>] [HOPS-TO-NET=<integer value>] [FORWARDING-ROUTER=<IPX node address - hexString[12:12]>] [NEXT-HOP=<IPX network number - hexString[8:8]>]
238. Remove	DEST-NETWORK=<IPX network number - hexString[8:8]>CIRCUIT-NUMBER=<integer value>
239. Add	SERVER-NAME=<string[1:48]> SERVER-TYPE=<IPX server type - hexString[4:4]> NETWORK=<IPX network number - hexString[8:8]> SERVER-ADDRESS=<IPX node address - hexString[12:12]> SOCKET=<IPX socket type - hexString[4:4]> HOPS-TO-SERVER=<integer value>
240. Edit	SERVER-NAME=<string[1:48]> SERVER-TYPE=<IPX server type - hexString[4:4]> [NETWORK=<IPX network number - hexString[8:8]>] [SERVER-ADDRESS=<IPX node address - hexString[12:12]>] [SOCKET=<IPX socket type - hexString[4:4]>] [HOPS-TO-SERVER=<integer value>]
241. Remove	SERVER-NAME=<string[1:48]> SERVER-TYPE=<IPX server type - hexString[4:4]>
242. Operating-Parameters	[IPM-ENABLE=<enabled|disabled>]
243. Show	[IF-INDEX=<integer value>]

Command	Parameters
244. Add	IF-INDEX=<integer value> [QUERY-INTERVAL=<integer value>] [VERSION=<integer value>] [MAX-RESPONSE-TIME=<integer value 0:255>] [ROBUSTNESS=<integer value 1:255>] [LAST-MEMBER-QUERY-INTVL=<integer value 0:255>]
245. Edit	IF-INDEX=<integer value> [QUERY-INTERVAL=<integer value>] [VERSION=<integer value>] [MAX-RESPONSE-TIME=<integer value 0:255>] [ROBUSTNESS=<integer value 1:255>] [LAST-MEMBER-QUERY-INTVL=<integer value 0:255>
246. Remove	[IF-INDEX=<integer value>]
247. Cache-Table	[CACHE-ADDRESS=<IP address>] [IF-INDEX=<integer value>]
248. Routing-Table	[GROUP=<IP address>] [SOURCE=<IP address>] [MASK=<IP address>]
249. Next-Hop	[GROUP=<IP address>] [SOURCE=<IP address>] [MASK=<IP address>] [IF-INDEX=<integer value>] [ADDRESS=<IP address>]
250. Device-Parameters	[GVRP-STATUS=<enabled|disabled>]
251. Port-Parameters	[PORT-NUMBER=<integer value 1:8>] [GVRP-STATUS=<enabled|disabled>]
252. Timing-Parameters	[PORT-NUMBER=<integer value 1:8>] [JOIN-TIME=<integer value>] [LEAVE-TIME=<integer value>] [ALL-LEAVE-TIME=<integer value>]
253. Display-Statistics	[PORT-NUMBER=<integer value 1:8>]
254. PORT-MIRRORING	[MIRRORED-PORT=<disabled|1|2|3|4|5|6|7|8>] [COPY-PORT=<disabled|1|2|3|4|5|6|7|8>]
255. Running-Config	[SECTION-LIST=<integer value 1:9,...>] No input parameter starts all sections. 1 - Section 1 General information. 2 - Section 2 Alarms. 3 - Section 3 Routing(IP) information. 4 - Section 4 Management configuration. 5 - Section 5 Bridge configuration. 6 - Section 6 Ports configuration. 7 - Section 7 VLAN configuration. 8 - Section 8 Statistics. 9 - Section 9 Compressed status report.
256. Used	[SORT-MODE=<LEX|G707>]
257. Show	[IF-INDEX=<integer value>]
258. Add	IF-INDEX=<integer value> [JOIN-PRUNE-INTV=<integer value>] [MODE=<dense|sparse|sparseDense>] [HELLO-INTV=<integer value>]
259. Edit	IF-INDEX=<integer value> [JOIN-PRUNE-INTV=<integer value>] [MODE=<dense|sparse|sparseDense>] [HELLO-INTV=<integer value>]

Command	Parameters
260. Remove	[IF-INDEX=<integer value>]
261. Nighbor-Table	[ADDRESS=<IP address>]
262. Route-Table	[GROUP=<IP address>] [SOURCE=<IP address>] [MASK=<IP address>]
263. Next-Hop-Table	[GROUP=<IP address>] [SOURCE=<IP address>] [MASK=<IP address>] [IF-INDEX=<integer value>] [ADDRESS=<IP address>]
264. Clear-SDH-Counters	<none>
265. System-Mode	[SYSTEM-MODE=<ip|ip-unnumbered>]

266. Add (Ipun-Route-Table)	DEST-IP-ADDR=<IP address>
	SUBNET-MASK=<IP address>
	NEXT-HOP=<IP address>
	[METRIC=<integer value>]

267. Remove (Ipun-Route-Table)	DEST-IP-ADDR=<IP address>
	SUBNET-MASK=<IP address>
	NEXT-HOP=<IP address>

268. Global-parameter	[OSPF-IPUN-ADMINISTRATIVE-STATUS=<enabled|disabled>] [LEAK-STATIC-ROUTES-TO-OSPF=<enable|disable>] [LEAK-EXTERNAL-ROUTES-TO-OSPF=<enable|disable>]
269. Add	AREA-ID=<IP address>
270. Show	[IP-ADDRESS=<IP address>] [IF-INDEX=<integer value>]
271. Edit	IP-ADDRESS=<IP address> IF-INDEX=<integer value> [AREA-ID=<IP address>] [ADMIN-STATUS=<enabled|disabled>] [ROUTER-PRIORITY=<integer value 0:255>] [RETRANSMISSION-INTERVAL=<integer value 0:3600>] [HELLO-INTERVAL=<integer value 1:65535>] [TRANSMISSION-DELAY=<integer value 0:3600>] [ROUTER-DEAD-INTERVAL=<integer value 0:2147483647>]

Command	Parameters
272. ES-IS-Configuration	[STATUS=<enabled|disabled>] [ES-HOLD-TIMER=<integer value 0:65535>] [ES-REPORT-TIMER=<integer value 0:65535>] [IS-HOLD-TIMER=<integer value 0:65535>] [IS-REPORT-TIMER=<integer value 0:65535>] [SUGGESTED-TIMER=<integer value 0:65535>]
273. IS-IS-Configuration	[STATUS=<enabled|disabled>] [L1-METRIC=<integer value 1:63>] [L2-METRIC=<integer value 1:63>] [CIRCUIT-OUTSIDE-DOMAIN=<enabled|disabled>] [IS-IS-HELLO-TIMER=<integer value 0:65535>] [L1-DIS-PRIORITY=<integer value 1:127>] [L2-DIS-PRIORITY=<integer value 1:127>] [DIS-IIH-TIMER=<integer value 0:65535>]
274. CLNP-Configuration	[MAXIMUM-CLNP-PDU-LIFETIME=<integer value 0:65535>] [MAXIMUM-CLNP-REASSEMBLY-TIME=<integer value 0:65535>]
275. Show	<none>
276. Add	NSAP=<NSAP address - hexString[6:40]>
277. Remove	NSAP=<NSAP address - hexString[6:40]>
278. Gateway-settings	[GATEWAY-ENABLED=<true|false>]
279. show	WANX-PORT=<integer value 6:8>

Command	Parameters
280. General	WANX-PORT=<integer value 6:8> [CONCATENATION=<vcatvc12|vcatvc3|axxessit>] [CHANNEL-TI/SIGNAL-LABEL=<integer value 0:50>] [PATH-TRACE=<enabled|disabled>] [EXPECTED-TI=<string[1:15]>] [HEX-EXPECTED-TI=<string[2:44]>] [TRANSMIT-TI=<string[1:15]>] [HEX-TRANSMIT-TI=<string[2:44]>] [LCAS-OPERATIONAL-MODE=<lcas|nolcas|nolcasbidirectional>] [ADMIN-UPSTREAM-CAPASITY=<integer value>] [ADMIN-DOWNSTREAM-CAPASITY=<integer value>] [PAYLOAD-FCS-INDICATOR=<FCS-ENABLED|FCS-DISABLED>] [QTAG-STATUS=<transparentPriority|extractPriority|disabled>] [FLOW-CONTROL=<enabled|disabled>] [PROTOCOL-TUNNELING=<enabled|disabled>]
281. Add-VC3-VC12-channel	WAN-PORT=<integer value 6:8> [KLM=<K.L.M - integer value 1:3.integer value 1:7.integer value 1:3>] [ADMIN-STATUS=<enabled|disabled>] [NUMBER-TO-ADD=<integer value 1:50>] [SORT-MODE=<LEX|G707>]
282. Remove-VC3-VC12-channel	WAN-PORT=<integer value 6:8> [NUMBER-TO-REMOVE=<integer value 1:50>]
283. Free-VC12VC3-List	<none>
284. Used-VC12VC3-List	<none>
285. General	AGGREGATE-PORT=<integer value 1:2> [ADMINISTRATIVE-STATUS=<enable|disable>] [DESCRIPTION=<string[0:64]>] [CONNECTED-TO=<string[0:64]>]
286. TUG3-mapping	[K=<integer value 1:3>] [STRUCTURE=<tu3|tu12x21>]
287. Show-VC3-VC12-Mapping	<none>
288. List-VC3-VC12-Usage	[SORT-MODE=<LEX|G707>]

Command	Parameters
289. Protection	[MSP-STATUS=<enabled|disabled>] [PROTECTION-TYPE=<unidirectional|bidirectional>] [REVERTING-STATUS=<enabled|disabled>] [WAIT-TO-RESTORE-TIME=<integer value 0:2147483647>] [SWITCHING-COMMAND=<clear|exercise|manualSwitchToProtection| manualSwitchToWorking|forcedSwitchToProtection| forcedSwitchToWorking|lockoutProtection>]
290. VC4-Path-Trace	[PATH-TRACE=<enabled|disabled>] [EXPECTED-TI=<string[1:15]>] [HEX-EXPECTED-TI=<string[2:44]>] [TRANSMIT-TI=<string[1:15]>] [HEX-TRANSMIT-TI=<string[2:44]>]
291. RS-Path-Trace	AGGREGATE-PORT=<integer value 1:2> [PATH-TRACE=<enabled|disabled>] [EXPECTED-TI=<string[1:15]>] [HEX-EXPECTED-TI=<string[2:44]>] [TRANSMIT-TI=<string[1:15]>] [HEX-TRANSMIT-TI=<string[2:44]>]
292. General	[SPANNING-TREE-ENABLED=<true|false>] [FORCED-PROTOCOL=<stpCompatible|rstp>] [BELONG-TO-VLAN=<true|false>] [PRIORITY=<integer value 0:65535>] [MAX-AGE=<integer value>] [HELLO-TIME=<integer value>] [FORWARD-DELAY=<integer value>]
293. Port-Table	[ETHERNET-PORT=<integer value 1:8>] [PRIORITY=<integer value 0:255>] [ENABLE=<enabled|disabled>] [PATH-COST=<integer value 0:200000000>] [EDGE-PORT=<true|false>] [POINT-POINT=<forceTrue|forceFalse|auto>] [PROTOCOL-MIGRATION=<true|false>]
294. Tuning	<none>
295. show	<none>

Command	Parameters

296. edit	PRIORITY=<integer value 0:7>
	TRAFFIC-CLASS=<integer value 0:3>

297. GFP-Bad-Frames-Statistics	[WANX-PORT=<integer value 6:8>]
298. Enable-GFP-Counters	WANX-PORT=<integer value 6:8>
299. Disable-GFP-Counters	WANX-PORT=<integer value 6:8>
300. Show-GFP-Counters	[WANX-PORT=<integer value 6:8>]
301. Clear-GFP-Counters	<none>
302. Parameters	<none>
303. Clear-Event-Log	<none>
304. VC3-Statistics	K=<integer value 1:3> [SHOW-ALL-INTERVALS=<FALSE|TRUE>]
305. MSP-Statistics	<none>
306. Trib-Port-Statistics	TRIB-PORT=<integer value 1:12> [SHOW-ALL-INTERVALS=<FALSE|TRUE>]

9

GLOSSARY

AXX155E

9.1 NUMERICS

10BaseT - 10 Mbps baseband Ethernet (twisted-pair Cat. 3, 4, or 5)

100BaseT - 100 Mbps baseband Fast Ethernet (UTP wiring)

100BaseTX - 100 Mbps baseband Fast Ethernet (UTP or STP wiring)

802.x - Set of IEEE standards for LAN protocols

9.2 ALPHABETICAL

A

AC - Alternate Current

ADM - Add Drop Multiplexer

ADSL - asymmetric digital subscriber line.

AIS - Alarm Indication Signal

AMT - Address Mapper Table

ANSI - American National Standards Institute

ARP - Address Resolution Protocol

AS - Autonomous System

ASCII - American Standard Code for Information Interchange

ASIC - Application-specific integrated circuit

AU - Administrative Unit

AU-PTR - Administrative Unit Pointer

AXXCLI - The AXXESSIT CLI application

B

BAT - Battery

BER - Bit Error Rate

BOOTP - Bootstrap Protocol

BPDU - Bridge Protocol Data Unit

bps - bits per second

Brigde - Device to connect two network segments (Layer 2)

C

CCITT - International Telegraph and Telephone

CIR - Committed Information Rate

CLI - Command Line Interface

CLNP - Connectionless Network Protocol

CMI - Coded Mark Inversion

CO - Central Office

CoS - class of service.

CPE - Customer Premises Equipment

CPU - Central Processing Unit

CRC - Cyclic Redundancy Check

D

DC - Direct Current

DCC - Data Communications Channel

DCE - Data Circuit-terminal Equipment

DCN - Data Communications Network

DHCP - Dynamic Host Configuration Protocol.

DL - Downlink (towards user)

DLAS - Degraded Laser

DNU - Do Not Use

DTMF - Dual Tone Multi-Frequency

E

E1 - European Hierarchy Primary Rate Access: 2048 Mbit/s

ECT - Equipment Craft Terminal

EEPROM - Electrical Erase Programmable Read Only Memory

EMC - Electromagnetic Compatibility

EOW - Engineering Order Wire

EPROM - Erase Programmable Read Only Memory

ES1 - End System

ES2 - Errored Seconds

ESH - End System Hello

ES-IS - End System-to-Intermediate System.

ET - Exchange Termination

ETSI - European Telecommunications Standards Institute

F

F1 - Optical line interface

F2 - Electrical 2 Mbit/s interface

FA - Frame Alignment

FAQ - Frequently Asked Questions

FC - Failure Condition

FC/PC - Optical Connector

FE - Fast Ethernet

FPGA - Field Programmable Gate Arraey

FTP - File Transfer Protocol

FW - Firmware

G

GFP - Generic Frame Procedure

GNE - Gateway Network Element

GND - Ground

GUI - Graphical User Interface

H

HBER - High Bit Error Rate

HO - Hold Over

HTTP - Hyper Text Transfer Protocol

HW - Hardware

I

ICMP - Internet Control Message Protocol

ICMP - Internet Control Message Protocol

ICS - Item Change Status, AXXESSIT version number

ID - Identifier

IEEE - Institute of Electrical and Electronics Engineers

IGMP - Internet Group Management Protocol

IIH - IS-IS Hello

IP - Internet Protocol

IPX - Internetwork Packet Exchange

IS - Intermediate System

ISDN - Integrated Services Digital Network

IS-IS - Intermediate System-to-Intermediate System

ISO - International Organization for Standardization

ISP - Internet service provider

ITU-T - International Telecommunication Union Standardisation Bureau

J

K

KLM - Numbering scheme for containers in SDH

L

LAN - Local Area network

LAP-D - Link Access Procedure on the D channel

LAPS - Link Access Procedure SDH

LBER - Low Bit Error Rate

LCAS - Link Capacity Adjustment Scheme

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

LLC - Logical Link Control

LOS - Loss of Signal

LTE - Line Termination Equipment

M

MAC - Medium Access Control

MCN - Management Communication Network

MF - Multiframe (G.704)

MIB - Management Information Base

MS - Multiplex Section

MSOH - Multiplex Section OverHead

MTBF - Mean Time Between Failure

MTU - Maximum Transmission Unit

MUX - Multiplexer

N

NC - Not Connected

NE - Network Element

NET - Network

NMS - Network Management System

NSAP - Network Service Access Point

NSEL - Network Select

NTE - Network Termination Equipment

O

OC - Operating Centre

OCT - Office Craft Terminal

OH - Overhead

OID - Object Identifier

OLOS - Optical LOS

OPOL - Optical Power out of Limit

OSI - Open Systems Interconnection

OSPF - Open Shortest Path First

P

p2mp - point-to-multipoint

p2p - point-to-point

PABX - Private Automatic Branch Exchange

PBX - Private Branch Exchange

PC - Personal Computer

PDH - Plesiochronous Digital Hierarchy (ITU-T Rec. G.702)

PIR - Peak Information Rate

POP - Point Of Presence

PPP - Point-to-Point Protocol

PPS - Packet Per Second

PRA - Primary Rate Access

proxy ARP - proxy Address Resolution Protocol

PSTN - Public Switched Telephone Network

Q

QL - Quality Level

R

RAM - Random-Access Memory

RIP - Routing Information Protocol

RLS - Received signal level

RMON - Remote monitoring

RS - Regenerator Section

RSOH - Regenerator Section OverHead

S

SDH - Synchronous Digital Hierarchy

SDRAM - Synchronous Dynamic Random Access Memory

SEMF - SDH Equipment Management Function

SES - Severely Errored Second

SETS - Station Equipment Timing Synchronisation

SF - Signal Failure

SNMP - Simple Network Management Protocol

SOHO - Small Office, Home Office

STA - Spanning-Tree Algorithm

STP1 - Spanning-Tree Protocol

STP2 - Shielded Twisted-Pair

SPX - Sequenced Packet Exchange

STM-1 - Synchronous Transport Module level 1

SW - Software

T

T0 - Timing information for internal NE synchronization

T3 - Timing information derived from a 2 MHz station clock (T12) input

T4 - Timing information towards a 2 MHz station clock (T12) output

TCP - Transmission Control Protocol

TCP/IP - Transmission Control Protocol/Internet Protocol

TDM - Time-Division Multiplexing

TE - Terminal Equipment

TFTP - Trivial File Transfer Protocol

TTL - Time To Live

TU - Tributary Unit

TUG-n - (n=12, 3, 4) Tributary Unit Group

U

UDP - User Datagram Protocol

UTP - Unshielded Twisted-Pair

V

VC-n - (n=12, 3, 4) Virtual Container

VCTIP - Virtual Container termination/IP mapper device

VID - VLAN ID

VLAN - Virtual LAN

VLSM - Variable-Length Subnet Mask

VPN - Virtual Private Network

VT-100 - Terminal standard

W

WAN - Wide-Area Network

WTR - Wait To Restore

X

Y

Z

9.3 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.813	Timing characteristics of SDH equipment slave clocks (SEC)
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

ETSI Documents	
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

IEEE Documents	
IEEE 802.1q	IEEE standard for local and metropolitan area networks: Virtual Bridged Local Area Networks
IEEE 802.1d	IEEE Standard for Information technology--Telecommunications and information exchange between systems--IEEE standard for local and metropolitan area networks--Common specifications--Media access control (MAC) Bridges
IEEE 802.2	IEEE Standard for Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements--Part 2: Logical Link Control
IEEE 802.3	Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements--Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications