1643 Access Multiplexer and 1643 Access Multiplexer Small (Formerly Metropolis® AM and Metropolis® AMS)

Release 1.0 through 7.2

User Operations Guide
365-312-807R7.2
CC109635813
Issue 10 | July 2013

Alcatel-Lucent - Proprietary
Use pursuant to applicable agreements
Legal notice

Alcatel, Lucent, Alcatel-Lucent and the Alcatel-Lucent logo are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners.

The information presented is subject to change without notice. Alcatel-Lucent assumes no responsibility for inaccuracies contained herein.

Copyright © 2013 Alcatel-Lucent. All rights reserved.

Contains proprietary/trade secret information which is the property of Alcatel-Lucent and must not be made available to, or copied or used by anyone outside Alcatel-Lucent without its written authorization.

Not to be used or disclosed except in accordance with applicable agreements.

Notice

Every effort has been made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change. This IP describes certain hardware, software, features, and capabilities of Alcatel-Lucent products that may not be the same as the equipment that you have. The IP is for information purposes, and you are cautioned that it may not describe your specific equipment.

Declaration of Conformity

The Declaration of Conformity (DoC) for this product can be found in the Applications and Planning Guide (APG) chapter “Quality and reliability”, or at: http://www.lucent.de/ecl.

Electrostatic Sensitive Devices

The equipment described in this guide contains static sensitive devices. Electrostatic Discharge Precautions should be taken when operating or working on this equipment.

Special handling precautions apply whenever installing or removing parts of the equipment include:

- Leaving components or equipment in original packaging until required for use.
- Removing plug-in units with previously discharged hands (e.g. using grounded wrist straps connected to the ESD Bonding Point on the Cabinet).
- Returning items for repair in suitable antistatic packaging.

Ordering information

The order number of this document is 365-312-807R7.2.

Technical support

Please contact your Alcatel-Lucent Local Customer Support Team (LCS) for technical questions about the information in this document.

Information product support

To comment on this information product online, go to http://www.lucent-info.com/comments or email your comments to comments@alcatel-lucent.com.
# Contents

## About this document

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>xxi</td>
</tr>
<tr>
<td>Reason for reissue</td>
<td>xxi</td>
</tr>
<tr>
<td>Safety information</td>
<td>xxiv</td>
</tr>
<tr>
<td>Intended audience</td>
<td>xxiv</td>
</tr>
<tr>
<td>How to use this information product</td>
<td>xxv</td>
</tr>
<tr>
<td>Conventions used</td>
<td>xxvii</td>
</tr>
<tr>
<td>Related documentation</td>
<td>xxix</td>
</tr>
<tr>
<td>Related training</td>
<td>xxx</td>
</tr>
<tr>
<td>Customer Documentation Subnetwork Controller Related</td>
<td>xxx</td>
</tr>
<tr>
<td>Documented feature set</td>
<td>xxxi</td>
</tr>
<tr>
<td>Intended use</td>
<td>xxxi</td>
</tr>
<tr>
<td>Optical safety</td>
<td>xxxi</td>
</tr>
<tr>
<td>Technical Documentation</td>
<td>xxxiv</td>
</tr>
<tr>
<td>How to comment</td>
<td>xxxiv</td>
</tr>
</tbody>
</table>

## 1 Safety

### General notes on safety

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>1-1</td>
</tr>
</tbody>
</table>

## 1-1 Overview
## Contents

Specific safety areas

- Overview .......................................................... 1-12
- Laser safety ...................................................... 1-13
- Laser product classification .............................. 1-17
- Electrostatic discharge ...................................... 1-21

## 2 Getting Started

Overview .................................................................... 2-1

### Installing the ITM-CIT

Overview .......................................................... 2-3
Install ITM-CIT software .......................................... 2-4

### Main menu and buttons

Overview .................................................................. 2-8
The ITM-CIT main menu .......................................... 2-9
Frequently used buttons .......................................... 2-16

### Login to a NE

Overview .................................................................. 2-18
Login to a Network Element .................................... 2-19

### Change NE date and time

Overview .................................................................. 2-21
Change NE Date and Time ....................................... 2-22
Parameters for Changing NE Date and Time ............ 2-23

### Log out of an NE

Overview .................................................................. 2-24
Logout procedure .................................................. 2-25

## 3 Security administration

Overview .................................................................. 3-1
## View the access control parameters

Overview ................................................................. 3-2  
Viewing Access Control Parameters ................................................................. 3-3  
Parameters for viewing the access control parameters .................................................. 3-4

## Change the lock state

Overview ................................................................. 3-5  
Changing the lock state ................................................................. 3-6  
Parameters for changing the lock state ................................................................. 3-7

## Change the inactivity time

Overview ................................................................. 3-8  
Changing the inactivity time ................................................................. 3-9  
Parameters for changing the inactivity time ................................................................. 3-10

## Configure or change a password

Overview ................................................................. 3-11  
Configuring or changing a password ................................................................. 3-12  
Parameters for configuring or changing a password ................................................................. 3-13

## Force a logout

Overview ................................................................. 3-14  
Forcing a logout ................................................................. 3-15  
Parameters for forcing a logout ................................................................. 3-16

## Management communication setup

Overview ................................................................. 4-1

## Concepts

Overview ................................................................. 4-3

## Basic DCN principles

DCN configurations ................................................................. 4-7
## Contents

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCN addresses</td>
<td>4-11</td>
</tr>
<tr>
<td>NSAP address format</td>
<td>4-12</td>
</tr>
<tr>
<td>Data communication channels</td>
<td>4-15</td>
</tr>
<tr>
<td>Dual stack with tunneling (DSwT)</td>
<td>4-18</td>
</tr>
<tr>
<td>Example of dual stack with tunneling</td>
<td>4-24</td>
</tr>
<tr>
<td>DSwT tunnel auto provisioning (TAP)</td>
<td>4-28</td>
</tr>
<tr>
<td>DSwT connecting areas with manual TAP tunnels</td>
<td>4-30</td>
</tr>
<tr>
<td>Partition repair</td>
<td>4-31</td>
</tr>
<tr>
<td>Partition repair guidelines</td>
<td>4-33</td>
</tr>
<tr>
<td><strong>Configuring a Data Communication Network (DCN)</strong></td>
<td></td>
</tr>
<tr>
<td>Overview</td>
<td>4-36</td>
</tr>
<tr>
<td>Create new or modify existing DCC terminations</td>
<td>4-37</td>
</tr>
<tr>
<td>Provisioning DCN information</td>
<td>4-39</td>
</tr>
<tr>
<td>Parameters for provisioning DCN information</td>
<td>4-41</td>
</tr>
<tr>
<td>Managing the DCC</td>
<td>4-44</td>
</tr>
<tr>
<td>Parameters for managing the DCC</td>
<td>4-46</td>
</tr>
<tr>
<td>Creating a transparent DCC cross-connection</td>
<td>4-47</td>
</tr>
<tr>
<td><strong>Procedures regarding login into remote NEs</strong></td>
<td></td>
</tr>
<tr>
<td>Overview</td>
<td>4-49</td>
</tr>
<tr>
<td>Adding a remote accessible NE to the configured nodes list</td>
<td>4-50</td>
</tr>
<tr>
<td>Editing remote NEs in the configured nodes list</td>
<td>4-52</td>
</tr>
<tr>
<td>Parameters for adding and editing remote logins in the configured nodes list</td>
<td>4-54</td>
</tr>
<tr>
<td>Remote login via configured nodes list</td>
<td>4-55</td>
</tr>
<tr>
<td>Remote login via neighbors option</td>
<td>4-57</td>
</tr>
<tr>
<td>Remote login via Area option</td>
<td>4-59</td>
</tr>
</tbody>
</table>
Contents

Provision NE tunnel information

Overview .................................................................................................................. 4-61
Editing provisioned IP parameters .......................................................................... 4-62
Adding manual route ............................................................................................... 4-63
Editing local/manual route ...................................................................................... 4-64
Editing TAP properties ............................................................................................ 4-65
Parameters for provisioning NE tunnel information .............................................. 4-67

Provision SNMP management

Overview .................................................................................................................. 4-70
Provision SNMP management ................................................................................. 4-71

Equipment provisioning

Overview .................................................................................................................. 5-1

Concepts

Overview .................................................................................................................. 5-4
Provisioning methods ............................................................................................. 5-5
Addressing and management concepts ................................................................... 5-8
1643 AM or 1643 AMS configuration possibilities ............................................... 5-9
Node creation ........................................................................................................... 5-11
Miscellaneous discrete inputs and outputs .............................................................. 5-12
Local alarms signaling ............................................................................................. 5-13
Centralized alarm signaling ..................................................................................... 5-14
Centralized MDI signaling ...................................................................................... 5-15

Create a node

Overview .................................................................................................................. 5-16
Creating a node ........................................................................................................ 5-17
Parameters for creating a node ................................................................................ 5-19
Provision slots

Overview .................................................................................................................. 5-21
Provisioning slots ................................................................................................. 5-22
Parameters for provisioning slots .................................................................. 5-24

Confirm the MIB

Overview .................................................................................................................. 5-25
Confirming the MIB ............................................................................................... 5-26
Parameters for confirming the MIB ............................................................... 5-28

Retrieve NE slot information

Overview .................................................................................................................. 5-30
Viewing NE slot information ........................................................................... 5-31
Parameters for viewing NE slot information ............................................... 5-32

Retrieve shelf display

Overview .................................................................................................................. 5-33
Viewing the shelf display ................................................................................. 5-34
Parameters for viewing shelf display .......................................................... 5-35

View hardware inventory

Overview .................................................................................................................. 5-37
Viewing hardware inventory - shelf ............................................................... 5-38
Viewing hardware inventory - slot ................................................................. 5-39
Parameters for viewing hardware inventory ............................................. 5-41

View SFP inventory data

Overview .................................................................................................................. 5-42
Viewing SFP inventory ...................................................................................... 5-43
Parameters for viewing SFP inventory data .................................................. 5-44
View and edit node details
Overview .............................................................................................................................................. 5-48
Viewing and editing node details ........................................................................................................ 5-49
Parameters for viewing or editing node details ................................................................................. 5-51

View and edit MDI information
Overview .............................................................................................................................................. 5-53
Viewing and editing MDI information ............................................................................................. 5-54
Parameters for viewing or editing MDI information ........................................................................ 5-56

View or edit MDO information
Overview .............................................................................................................................................. 5-57
Viewing or editing MDO information ............................................................................................. 5-59
Parameters for viewing or editing MDO information ........................................................................ 5-61

Provision ports
Overview .............................................................................................................................................. 5-62
Provisioning ports .................................................................................................................................. 5-63
Parameters for Port Provisioning ........................................................................................................ 5-65

Alarm management
Overview .............................................................................................................................................. 6-1

Concepts
Overview .............................................................................................................................................. 6-4
Events origin and flow ........................................................................................................................ 6-5
Event properties .................................................................................................................................. 6-8
Event display ........................................................................................................................................ 6-12
Alarm supervision concepts .................................................................................................................. 6-13
Event history ......................................................................................................................................... 6-14
Contents

Alarm identification

Overview ................................................................. 6-15
View alarm summary .............................................. 6-16
Set up filters ............................................................. 6-17
View current alarms ................................................. 6-18
View alarm details .................................................... 6-20
Archive cleared alarms ............................................ 6-22
Parameters for identifying the alarms ....................... 6-23

Provision alarm options

Overview ................................................................. 6-28
Setting the alarm options ......................................... 6-29
Parameters for setting the alarm options ................. 6-30

Provision alarm severity assignment profiles (ASAP)

Overview ................................................................. 6-32
Create a new ASAP .................................................. 6-33
Modifying an existing ASAP ................................. 6-35
Delete an existing ASAP ......................................... 6-37
Retrieve an existing ASAP ........................................ 6-38
Assign an ASAP ....................................................... 6-39
Retrieve an assignment list for a specified ASAP ....... 6-44
Retrieve assigned ASAPs for a specified managed object 6-45
Parameters for “ASAP Assignment” ......................... 6-46
Alarm Severity Assignment Profile ......................... 6-47

Alarm supervision

Overview ................................................................. 6-64
Supervise alarms ..................................................... 6-65
Contents

Parameters for supervising alarm ................................................................. 6-72

View historical data
Overview ........................................................................................................ 6-77
Historical data ................................................................................................ 6-78
Retrieving historical data ............................................................................. 6-79
Parameters for retrieving historical data ...................................................... 6-81

Timing provisioning
Overview ........................................................................................................ 7-1

Concepts
Overview ........................................................................................................ 7-3
NE timing ....................................................................................................... 7-4
Network synchronization ............................................................................... 7-7
Timing quality levels ...................................................................................... 7-9
Priorities ......................................................................................................... 7-11
Example of network Timing ........................................................................ 7-13
Timing loop ................................................................................................... 7-14
Re-timing ....................................................................................................... 7-15
Timing configuration ..................................................................................... 7-17

Provisioning
Overview ........................................................................................................ 7-19
Provisioning timing sources .......................................................................... 7-20
Parameters for provisioning timing sources .................................................. 7-26
Provisioning system timing .......................................................................... 7-32
Parameters for provisioning system timing .................................................... 7-35
Provisioning station clock output .................................................................. 7-39
Parameters for provisioning station clock output ........................................... 7-43
Traffic provisioning

Overview ........................................................................................................................................... 8-1

Cross-connection management

Overview ........................................................................................................................................... 8-5

Transmission Plan ............................................................................................................................. 8-6

Cross Connections .......................................................................................................................... 8-8

VC-3 concatenation ......................................................................................................................... 8-10

VC-12 concatenation ....................................................................................................................... 8-11

SHDSL feature .................................................................................................................................. 8-12

Path protection

Overview ........................................................................................................................................... 8-17

Sub-Network Connection Protection (SNCP) .................................................................................. 8-18

Line Protection

Overview ........................................................................................................................................... 8-20

Multiplexer Section Protection ....................................................................................................... 8-21

Ethernet concepts

Overview ........................................................................................................................................... 8-23

Ethernet over SDH .......................................................................................................................... 8-24

Virtual concatenation ..................................................................................................................... 8-41

Spanning tree protocol (STP) ......................................................................................................... 8-47

GARP VLAN Registration Protocol (GVRP) .................................................................................. 8-54

Ethernet over SDH applications ........................................................................................................ 8-56

Operational modes .......................................................................................................................... 8-64

Tagging modes ................................................................................................................................ 8-75
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet mapping schemes</td>
<td>8-81</td>
</tr>
<tr>
<td><strong>Ethernet engineering rules and guidelines</strong></td>
<td></td>
</tr>
<tr>
<td>Overview</td>
<td>8-83</td>
</tr>
<tr>
<td>Port provisioning</td>
<td>8-84</td>
</tr>
<tr>
<td>Quality of Service (QoS) overview</td>
<td>8-90</td>
</tr>
<tr>
<td>Classification, queueing, and scheduling</td>
<td>8-94</td>
</tr>
<tr>
<td>Quality of Service provisioning</td>
<td>8-103</td>
</tr>
<tr>
<td>Performance monitoring</td>
<td>8-105</td>
</tr>
<tr>
<td><strong>Provision Ethernet over SDH</strong></td>
<td></td>
</tr>
<tr>
<td>Overview</td>
<td>8-106</td>
</tr>
<tr>
<td>Provisioning Ethernet services</td>
<td>8-107</td>
</tr>
<tr>
<td>Parameters of the window “View SDH Channel / VCG Information”</td>
<td>8-112</td>
</tr>
<tr>
<td>Provisioning a virtual switch in repeater (promiscuous) mode</td>
<td>8-113</td>
</tr>
<tr>
<td>Provisioning a virtual switch in LAN interconnect mode</td>
<td>8-116</td>
</tr>
<tr>
<td>Provisioning a virtual switch in MLAN (VPN) mode</td>
<td>8-119</td>
</tr>
<tr>
<td>Provisioning a virtual switch in MLAN (VPN) mode with QoS</td>
<td>8-123</td>
</tr>
<tr>
<td>Provisioning a virtual switch in spanning tree mode</td>
<td>8-132</td>
</tr>
<tr>
<td>Parameters for provisioning a LAN unit in repeater mode</td>
<td>8-143</td>
</tr>
<tr>
<td>Parameters for provisioning LAN unit in spanning tree mode</td>
<td>8-147</td>
</tr>
<tr>
<td><strong>Provision MAC address tables</strong></td>
<td></td>
</tr>
<tr>
<td>Overview</td>
<td>8-153</td>
</tr>
<tr>
<td>Provision static MAC address table</td>
<td>8-154</td>
</tr>
<tr>
<td>Provision the MAC address learning mode</td>
<td>8-157</td>
</tr>
<tr>
<td>Provision the MAC address aging pass timer</td>
<td>8-159</td>
</tr>
<tr>
<td><strong>Provision Quality of Service (QoS)</strong></td>
<td></td>
</tr>
<tr>
<td>Overview</td>
<td>8-160</td>
</tr>
</tbody>
</table>
### Contents

- Provision the QoS profile definitions ................................................................. 8-161
- Parameters for provisioning a QoS profile ........................................................... 8-162
- View QoS profile information ............................................................................. 8-165
- View the details of a LAN/WAN port QoS parameters ......................................... 8-166
- Edit QoS mode ..................................................................................................... 8-167
- Provision QoS Flow Identification Table ............................................................. 8-169
- Parameters for provisioning Flow Identification Tables ........................................ 8-172
- Edit the QoS egress details .................................................................................. 8-177
- Ingress rate control .............................................................................................. 8-178

**Provision cross connections without protection**

- Overview ............................................................................................................... 8-179
- Creating cross connections without protection .................................................... 8-180
- Deleting cross connections .................................................................................. 8-182
- Parameters for provisioning cross connections without protection ...................... 8-183

**Provision cross connections with SNC protection**

- Overview ............................................................................................................... 8-184
- Add SNC/N protection to an unprotected cross-connection .................................... 8-185
- Remove protection from an SNC/N protected cross-connection ............................. 8-187
- Delete an existing cross-connection ..................................................................... 8-189
- Parameters for provisioning a cross-connection with SNC protection .................... 8-191

**View or Edit the LTU information**

- Overview ............................................................................................................... 8-192
- View the LTU information .................................................................................... 8-193
- Edit the LTU Information ..................................................................................... 8-194
- Parameters for viewing or editing LTU information ............................................. 8-195
Contents

View or Edit the SHDSL connection information
Overview ........................................................................................................................................................................ 8-196
View the SHDSL connections ............................................................................................................................................. 8-197
Update the SHDSL connection list ................................................................................................................................ 8-198
Details of the SHDSL Connection List .......................................................................................................................... 8-199
Parameters for viewing or editing the SHDSL connections list ......................................................................................... 8-200

View or Edit the NTU information
Overview ........................................................................................................................................................................ 8-201
Update the NTU information ............................................................................................................................................. 8-202
View the NTU information ........................................................................................................................................... 8-203
Edit the NTU information ............................................................................................................................................... 8-204
View or Edit NTU's General Configuration ...................................................................................................................... 8-205
Remote SHDSL Power Supply (RPS) ................................................................................................................................. 8-207
VC 12 termination point information ............................................................................................................................. 8-208
Update the VC 12 termination point information window ............................................................................................... 8-209
Report the VC 12 termination point information list ......................................................................................................... 8-210
Edit the VC 12 termination point information list .............................................................................................................. 8-211
Parameters for viewing or editing NTU information and VC 12 termination point information .................................. 8-213
Provisioning the SHDSL on the NT10ETH modem ........................................................................................................... 8-215

View SNC protection
Overview ........................................................................................................................................................................ 8-216
Viewing SNC protection .................................................................................................................................................. 8-217
Parameters for viewing SNC protection ........................................................................................................................... 8-218

Edit SNC protection
Overview ........................................................................................................................................................................ 8-219
Editing a SNC protection .................................................................................................................................................. 8-220
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters for editing SNC protection</td>
<td>8-221</td>
</tr>
<tr>
<td><strong>View MSP protection</strong></td>
<td></td>
</tr>
<tr>
<td>Overview</td>
<td>8-222</td>
</tr>
<tr>
<td>Viewing MSP protection</td>
<td>8-223</td>
</tr>
<tr>
<td>Parameters for viewing MSP protection</td>
<td>8-224</td>
</tr>
<tr>
<td><strong>Edit MSP protection</strong></td>
<td></td>
</tr>
<tr>
<td>Overview</td>
<td>8-225</td>
</tr>
<tr>
<td>Editing MSP protection</td>
<td>8-226</td>
</tr>
<tr>
<td>Parameters for editing MSP protection</td>
<td>8-228</td>
</tr>
<tr>
<td><strong>Add MSP protection</strong></td>
<td></td>
</tr>
<tr>
<td>Overview</td>
<td>8-230</td>
</tr>
<tr>
<td>Adding MSP protection</td>
<td>8-231</td>
</tr>
<tr>
<td>Parameters for adding MSP protection</td>
<td>8-233</td>
</tr>
<tr>
<td><strong>Traffic maintenance</strong></td>
<td>9</td>
</tr>
<tr>
<td>Overview</td>
<td>9-1</td>
</tr>
<tr>
<td><strong>Concepts</strong></td>
<td></td>
</tr>
<tr>
<td>Overview</td>
<td>9-3</td>
</tr>
<tr>
<td>Port types</td>
<td>9-4</td>
</tr>
<tr>
<td>Termination points (TPs)</td>
<td>9-7</td>
</tr>
<tr>
<td><strong>Provision termination points</strong></td>
<td></td>
</tr>
<tr>
<td>Overview</td>
<td>9-9</td>
</tr>
<tr>
<td>Provisioning termination points</td>
<td>9-10</td>
</tr>
<tr>
<td>Parameters for provisioning termination points</td>
<td>9-12</td>
</tr>
<tr>
<td><strong>Provision a path trace</strong></td>
<td></td>
</tr>
<tr>
<td>Overview</td>
<td>9-14</td>
</tr>
<tr>
<td>Provisioning a path trace</td>
<td>9-15</td>
</tr>
</tbody>
</table>
Parameters for provisioning a path trace ................................................................. 9-17

Provision degraded signal thresholds

Overview ..................................................................................................................... 9-19

Selecting the threshold for a signal ........................................................................ 9-20

Changing the threshold values ................................................................................ 9-22

Parameters for provisioning degraded signal thresholds .......................................... 9-23

Switch SNC protection

Overview ..................................................................................................................... 9-24

Switching SNC protection ........................................................................................ 9-25

Parameters for switching SNC protection ................................................................. 9-27

Switch MSP protection

Overview ..................................................................................................................... 9-28

Switching MSP protection ........................................................................................ 9-29

Parameters for switching MSP protection ................................................................. 9-30

Performance monitoring

Overview ..................................................................................................................... 10-1

Concepts

Overview ..................................................................................................................... 10-3

Introduction ............................................................................................................... 10-4

The performance monitoring process ..................................................................... 10-7

Performance measurements ..................................................................................... 10-8

Ethernet performance monitoring .......................................................................... 10-13

Available PM data ................................................................................................... 10-27

Configuration of the ITM-CIT ................................................................................. 10-35

Data Storage and Recovery ...................................................................................... 10-37
12 **Software upgrade**

Overview ................................................................................................................................................................................... 12-1

Concepts

Overview ................................................................................................................................................................................... 12-3

Software upgrade ..................................................................................................................................................................... 12-4

View software stored in an NE

Overview ................................................................................................................................................................................... 12-6

View software stored in the NE .............................................................................................................................................. 12-7

Parameters for viewing the software stored in the NE ........................................................................................................... 12-8

Upgrade NE software

Overview ................................................................................................................................................................................... 12-9

Loading NE software from CD-ROM to ITM CIT ..................................................................................................................... 12-10

Upgrading the software of an NE ........................................................................................................................................... 12-12

Parameters for upgrading the software of an NE ................................................................................................................... 12-15

Switch the stores in an NE

Overview ................................................................................................................................................................................... 12-17

Switch the software stores ....................................................................................................................................................... 12-18

Parameters for switching the software Stores ...................................................................................................................... 12-20

13 **Engineering orderwire concepts**

Overview ................................................................................................................................................................................... 13-1

Engineering orderwire .............................................................................................................................................................. 13-2

Glossary

Index
About this document

Purpose

The network element (NE) User Operations Guide (UOG) is a network management oriented guide. This guide instructs the user how to operate the network element using an ITM-CIT, including provisioning and maintenance tasks.

The whole masking tree describes the following standards:

- ITU-T recommendation G.783, issue April 1997
- ETSI standard ETS 300 417-1-1, issue January 1996
- ETSI standard ETS 300 417-2-1, issue April 1997
- ETSI standard ETS 300 417-3-1, issue June 1997
- ETSI standard ETS 300 417-3-1, issue June 1997.

Reason for reissue

A new version of this document was needed to address all features supported by 1643 AM and 1643 AMS Release 1.0 through 7.2.

Note: The 1643 AM and 1643 AMS User Operations Guide contains images with old logos and will be updated in the forthcoming releases.

Previous versions and features are listed below:

<table>
<thead>
<tr>
<th>Release</th>
<th>GA</th>
<th>Features added</th>
</tr>
</thead>
<tbody>
<tr>
<td>UOG</td>
<td>365-312-807R7.2</td>
<td>Issue 10 July 2013 Alcatel-Lucent - Proprietary Use pursuant to applicable agreements</td>
</tr>
<tr>
<td>Ruby 1.0</td>
<td>December 2000</td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
<td></td>
</tr>
<tr>
<td>• One or Two STM-1 or two STM-4 optical line interface pairs (transmit/receive)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Up to sixteen 2 Mbit/s interface ports - G.703 interface - G.704/G.706 interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Remote and local software downloading</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• General VC-11/VC-12 SNC/N protection or VC-3 SNC/N protection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1+1 MSP protection (STM-1 aggregate only) in terminal applications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Performance Monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• E1 or DS1 or E3 or DS3 or X.21 loopbacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Cross-connect loopbacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Four Miscellaneous Discrete Inputs (MDI)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Four Miscellaneous Discrete Outputs (MDO)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Dual fiber pair working</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• IP Tunneling in the DCC channels for the management of elements (TCP/IP protocol)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Space-efficient for simple and rapid installation within street cabinets or in customer premises</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Supported by the user-friendly Integrated Transmission Management (ITM) network management and element management systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• AC/DC or DC/DC converter</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Working in large temperature range</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Optional additional sixteen 1.5 Mbit/s ports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Optional additional sixteen 2 Mbit/s ports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Optional additional two 34 Mbit/s ports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Optional additional two 45 Mbit/s ports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Optional additional four 2 Mbit/s X.21 ports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Optional additional four 10/100Base-T LAN interfaces</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Topaz 2.0</th>
<th>July 2001</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Optional additional two optical STM-1 tributary signals</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Pearl 2.2</th>
<th>July 2002</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Optional additional two electrical STM-1 tributary signals</td>
<td></td>
</tr>
<tr>
<td>• Spanning tree protocol</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Garnet 3.1</th>
<th>May 2003</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Rapid spanning tree protocol</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Garnet 3.2</th>
<th>July 2003</th>
</tr>
</thead>
<tbody>
<tr>
<td>• introduction of 1643 AMS</td>
<td></td>
</tr>
<tr>
<td>• introduction of Network Termination Unit (NTU)</td>
<td></td>
</tr>
<tr>
<td>• Optional additional twelve SHDSL interfaces</td>
<td></td>
</tr>
</tbody>
</table>
| Venus 4.0        | September 2003 | • X8PL option card  
|                 |                | • LCAS functionality for VC-12 and VC-3  
|                 |                | • AITS operation (DCC\textsubscript{m})  
|                 |                | • Transparent DCC\textsubscript{r}  

| Earth 5.0 (current release) | April 2004 | • Support of SNMP management  
|                            |            | • Advanced SFP data retrieve capability  
|                            |            | • Enhanced VLAN tagging  
|                            |            | • Enhanced Ethernet port provisioning  
|                            |            | • Provisionable LSP size  

| Mars 6.1        | June 2005 | The following features are implemented in this release:  
|                 |            | • Enhanced flow classification (Port, VID, UP) on E/FE units  
|                 |            | • QoS in IEEE 802.1Q & IEEE 802.1ad mode on E/FE units, i.e. flow classification, rate control and traffic class handling  
|                 |            | • Oversubscription in IEEE mode  
|                 |            | • SHDSL Performance Monitoring  
|                 |            | • 3rd party NTU support for E1 and Ethernet applications  
|                 |            | • Port Loopback alarming  
|                 |            | • J0 support on STM-n lines  
|                 |            | • E1 non-intrusive monitoring  
|                 |            | • E1 PDH AIS  
|                 |            | • 1643 AMS with integrated AC power supply  
|                 |            | • Increased SFP support (STM-1e, single fiber)  
|                 |            | • New SHDSL option card with R6.1 Features, e.g. SW Download to NTUs.  

| Uranus Release 7.1 | November 2006 | The following features are implemented in this release:  
|                   |               | • Optional TransLAN card - X51P, FSP12AMS support  
|                   |               | • Ethernet PM counter enhancements  
|                   |               | • PM counter for Congestion monitoring  
|                   |               | • Round trip time/delay measurement  
|                   |               | • Static MAC address table configuration and retrieval  
|                   |               | • Provisionable CBS  
|                   |               | • Flow classification based on DA-MAC and IP-TOS/DSCP  
|                   |               | • SHDSL enhancements  

---

About this document

---

UOG 365-312-807R7.2
Issue 10  July 2013
The following features are implemented in this release:

- Alarm Severity Assignment Profile (ASAP)
- X5IP option card enhancements
- Outloops on Ethernet ports in repeater mode
- Ethernet PM counter enhancements
- PM counter for congestion monitoring
- Roundtrip time / delay measurement
- Static MAC@ table configuration & retrieval
- Provisionable CBS
- Supported by the Lucent OMS Release 5.0.2 and Wavestar® ITM-CIT - Release 18.0
- Digital Diagnostics Monitoring (DDM) on SFPs

The following features are implemented in this release:

- X12SHDSL-V3 option card

For your safety, this document contains safety statements. Safety statements are given at points where risks of damage to personnel, equipment, and operation may exist. Failure to follow the directions in a safety statement may result in serious consequences.

For personnel who need to operate the network element. It is assumed that personnel have some knowledge about operating the ITM-CIT. For more information on this topic, refer to chapter “ITM-CIT Tutorial”.

Provisioning personnel have to perform the tasks:
- Install the ITM-CIT software on a local workstation
- Install new hardware in the network element
- Configure the network element using the ITM-CIT
- Perform tests.

Maintenance personnel have to perform the tasks:
- Identify alarms and/or performance degradation
- Gather information about the alarms and/or performance degradation
- Interpret alarm information
- Resolve alarms
- Perform preventive maintenance.
How to use this information product

The network element User Operations Guide (UOG) is divided into a number of chapters. Through this readers can quickly select the subject of their interest and need.

This guide is divided into the chapters:

- About this Information Product (IP). This chapter describes the structure and organization of the User Operations Guide (UOG).
- Safety. This chapter comprises safety admonishments, especially laser safety instructions.
- Security administration. This chapter allows the user to control access to the network element and to the ITM-CIT, for example:
  - Viewing the Access Control Parameters
  - Changing the Lock State
  - Changing the Inactivity Time
  - Configuring or changing a Password
  - Forcing a Logout.
- Management communication setup. This chapter covers setting up management communication, for example:
  - Creating a node
  - Managing the Data Communication Channels
  - Remote logins
  - Provisioning Data Communication Channels in MSP mode
  - Provisioning Data Communication Network information.
- Equipment provisioning. In this chapter, the user is starting with either an NE with no information about the equipment, or an NE with complete provisioning information on the equipment (including equipment protection).

The end result is an NE with the complete provisioning information on the equipment, including the equipment protection, according to the user's needs.

Examples:
  - Modify equipment information
  - Modify equipment defaults
  - Provision the equipment protection
  - Define automatic laser shutdown settings
  - Provision the miscellaneous discrete inputs and outputs.
- Alarm management. This chapter provides instructions for the user to:
  - Set the alarm reporting states (alarm severities)
  - Get more information on the alarm and previous alarms
– Store and archive alarms
– Make sure some alarms will not disappear into the history list without an explicit acknowledgment.

• Timing provisioning. This chapter provides instructions for the user to deliver a timing signal with predefined quality. This includes for example:
  – Provisioning network element timing
  – Provision timing marker settings.

• Traffic provisioning. This chapter provides instructions for tasks such as setting a path, creating low-level cross connections, and modifying an existing path.

Input to traffic provisioning is a request for a path, while output is a path (including its protection through the network).

The user can use the network to transport traffic using various paths. In this chapter, the user gets support for setting up the path, including its protection. This chapter needs to be used in conjunction with the next chapter (Traffic Maintenance).

Supported tasks include the following:
  – View the present cross connections and protection
  – Create new cross connections with or without the different types of protection
  – Change existing cross connections and/or existing protection.

• Traffic maintenance. This chapter provides instructions for the user to set up the maintenance for the path and check the path, including its protection.

Input to traffic maintenance is a path through the network, including its protection. Output includes a tested and protected path with all the performance monitoring and alarm thresholds set.

Examples of traffic maintenance tasks are:
  – Set termination points to be monitored
  – Create Traffic Ports, both physically and logically
  – Create Termination points
  – Verify the path using trail trace
  – Set the signal degradation threshold for the path (the signal degradation thresholds determines whether or not to generate an alarm and whether or not a protective switch will take place)
  – Switch the protection of the path
  – Verify the protection path using trail trace.

• Performance monitoring. The provider performs Performance Monitoring in order to detect flaws early on, before the alarms arise.
This chapter enables the user to:
- Create a monitoring point
- Write performance data to another medium
- Retrieve performance data from the NE.

- Engineering order wire and user channel provisioning. This chapter allows the user to view/create/modify the engineering order wire and the user channels.

- Software upgrade. This chapter allows the user to:
  - Find out what software versions are loaded in the network element
  - Download a new software image
  - Check whether software download was successful
  - Switch stores.

- Concepts. The concepts chapter(s) contains all knowledge information. The user can use this chapter(s) when they do not understand a task.

- ITM-CIT tutorial. In this chapter, the user learns how to operate the user interface. For example:
  - View alarms
  - Acknowledge alarms
  - Display alarm reports
  - Workstation installation
  - Workstation operation.

- Back matter: Glossary and Index

Conventions used

These conventions are used in this document:

**Numbering**

The chapters of this document are numbered consecutively. The page numbering restarts at “1” in each chapter. To facilitate identifying pages in different chapters, the page numbers are prefixed with the chapter number. For example, page 2-3 is the third page in chapter 2.

**Cross-references**

Cross-reference conventions are identical with those used for numbering, i.e. the first number in a reference to a particular page refers to the corresponding chapter.

**Keyword blocks**

This document contains so-called keyword blocks to facilitate the location of specific text passages. The keyword blocks are placed to the left of the main text and indicate the contents of a paragraph or group of paragraphs.
Typographical conventions

Special typographical conventions apply to elements of the graphical user interface (GUI), file names and system path information, keyboard entries, alarm messages etc.

- Elements of the graphical user interface (GUI)
  These are examples of text that appears on a graphical user interface (GUI), such as menu options, window titles or push buttons:
  - **Provision**, **Delete**, **Apply**, **Close**, **OK** (push-button)
  - **Provision Timing/Sync** (window title)
  - **View Equipment Details...** (menu option)
  - **Administration → Security → User Provisioning...** (path for invoking a window)

- File names and system path information
  These are examples of file names and system path information:
  - `ItmCit.exe`
  - `C:\Program Files\Lucent Technologies\ITM-CIT 13.0`

- Keyboard entries
  These are examples of keyboard entries:
  - **F1, Esc X, Alt-F, Ctrl-D, Ctrl-Alt-Del** (simple keyboard entries)
    A hyphen between two keys means that both keys have to be pressed simultaneously. Otherwise, a single key has to be pressed, or several keys have to be pressed in sequence.
  - **copy abc xyz** (command)
    A complete command has to be entered.

- Alarms and error messages
  These are examples of alarms and error messages:
  - **Loss of Signal**
  - **Circuit Pack Failure**
  - **HP-UNEQ, MS-AIS, LOS, LOF**
  - **Not enough disk space available**

Abbreviations

Abbreviations used in this document can be found in the “Glossary” unless it can be assumed that the reader is familiar with the abbreviation.

Approval mark

The following CE approval mark applies to this product.
CE Marking is the indicator for products conform with relevant European Community (EC) Directives. CE stands for Conformité Européenne. The CE-marked transmission equipment is compliant with one EC Directive: 89/336/EEC - Electro-magnetic compatibility (EMC). In this manual you will find several chapters in relation with the CE-marking, for example the use of EMC closed connector Hoods, filtered connectors, and warnings to use a wrist strap when handling equipment.

Related documentation

This section briefly describes the documents that are included in the 1643 AM and 1643 AMS documentation set.

- Installation Guide
  The 1643 AM and 1643 AMS Installation Guide (IG) is a step-by-step guide to system installation and setup. It also includes information needed for pre-installation site planning and post-installation acceptance testing.

- Applications and Planning Guide
  The 1643 AM and 1643 AMS Applications and Planning Guide (APG) is for use by network planners, analysts, and managers. It is also for use by the Alcatel-Lucent Account Team. It presents a detailed overview of the system, describes its applications, gives planning requirements, engineering rules, ordering information, and technical specifications.

- User Operations Guide

- Alarm Messages and Trouble Clearing Guide
  The 1643 AM and 1643 AMS Alarm Messages and Trouble Clearing Guide (AMTCG) gives detailed information on each possible alarm message. Furthermore, it provides procedures for routine maintenance, troubleshooting, diagnostics, and component replacement.

- The WaveStar® ITM-SC Release 11.0 Provisioning Guide (Application 1643 AM and 1643 AMS)
The WaveStar® ITM-SC Provisioning Guide (Application 1643 AM and 1643 AMS) gives instructions on how to perform system provisioning, operations, and administrative tasks by use of ITM-SC.

The following table lists the documents included in the 1643 AM and 1643 AMS documentation set.

<table>
<thead>
<tr>
<th>Document title</th>
<th>Document code</th>
</tr>
</thead>
<tbody>
<tr>
<td>1643 AM and 1643 AMS Release 1.0 through 7.2 Applications and Planning Guide</td>
<td>109635771 (365-312-801R7.2)</td>
</tr>
<tr>
<td>1643 AM and 1643 AMS Release 1.0 through 7.2 User Operations Guide</td>
<td>109635813 (365-312-807R7.2)</td>
</tr>
<tr>
<td>1643 AM and 1643 AMS Release 1.0 through 7.2 Alarm Messages and Trouble Clearing Guide</td>
<td>109635763 (365-312-803R7.2)</td>
</tr>
<tr>
<td>1643 AM and 1643 AMS Release 1.0 through 7.2 Installation Guide</td>
<td>109635797 (365-312-802R7.2)</td>
</tr>
<tr>
<td>WaveStar® OMS Provisioning Guide 1643 AM and 1643 AMS Release 1.0 through 7.2</td>
<td>109635805 (365-312-877R7.2)</td>
</tr>
<tr>
<td>CD-ROM Documentation 1643 AM and 1643 AMS Release 1.0 through 7.2 (all manuals on a CD-ROM)</td>
<td>109635789 (365-312-811R7.2)</td>
</tr>
</tbody>
</table>

Related training

For detailed information about the training courses that are related to 1643 AM and 1643 AMS please refer to 1643 AM and 1643 AMS Applications and Planning Guide, chapter 8 Product support - Training courses.

Customer Documentation Subnetwork Controller Related

The following documents are Subnetwork Controller related:

- The ITM-SC APPLICATION AND PLANNING GUIDE provides an understanding of what the ITM-SC is and how and how to plan to use and order it.
- The ITM-SC INSTALLATION GUIDE instructs the user how to install the ITM-SC and configure the running environment.
- The ITM-SC ADMINISTRATION GUIDE instructs the user how to administer the ITM-SC.
- The ITM-SC MAINTENANCE GUIDE Instructs the user how to maintain the ITM-SC and network.
• The ITM-SC PROVISIONING GUIDE for the network element instructs the user how to use the ITM-SC to provision network equipment.
• The ITM-SC ALARM MESSAGES AND TROUBLE CLEARING GUIDE instructs the user how to respond to alarms and fix problems with the ITM-SC.

### Documented feature set

This manual describes 1643 AM and 1643 AMS Release 1.0 through 7.2. For technical reasons some of the documented features might not be available until later software versions. For precise information about the availability of features, please consult the Software Release Description (SRD) that is distributed with the network element software. This provides details of the status at the time of software delivery.

### Intended use

This equipment shall be used only in accordance with intended use, corresponding installation, and maintenance statements as specified in this documentation. Any other use or modification is prohibited.

### Optical safety

#### IEC Customer Laser Safety Guidelines

Alcatel-Lucent declares that this product is compliant with all essential safety requirements as stated in IEC 60825-Part 1 and 2 “Safety of laser products” and “Safety of optical fibre telecommunication systems”. Furthermore Alcatel-Lucent declares that the warning statements on labels on this equipment are in accordance with the specified laser radiation class.

#### Optical Safety Declaration (if laser modules used)

Alcatel-Lucent declares that this product is compliant with all essential safety requirements as stated in IEC 60825-Part 1 and 2 “Safety of Laser Products” and “Safety of Optical Fiber Telecommunication Systems”. Furthermore Alcatel-Lucent declares that the warning statements on labels on this equipment are in accordance with the specified laser radiation class.

#### Optical Fiber Communications

This equipment contains an Optical Fiber Communications semiconductor laser/LED transmitter. The following Laser Safety Guidelines are provided for this product.

#### General Laser Information

Optical fiber telecommunication systems, their associated test sets, and similar operating systems use semiconductor laser transmitters that emit infrared (IR) light at wavelengths between approximately 800 nanometers (nm) and 1600 nm. The emitted light is above the red end of the visible spectrum, which is normally not visible to the human eye. Although
radiant energy at near-IR wavelengths is officially designated invisible, some people can see the shorter wavelength energy even at power levels several orders of magnitude below any that have been shown to cause injury to the eye.

Conventional lasers can produce an intense beam of monochromatic light. The term “monochromaticity” means a single wavelength output of pure color that may be visible or invisible to the eye. A conventional laser produces a small-size beam of light, and because the beam size is small the power density (also called irradiance) is very high. Consequently, lasers and laser products are subject to federal and applicable state regulations, as well as international standards, for their safe operation.

A conventional laser beam expands very little over distance, or is said to be very well collimated. Thus, conventional laser irradiance remains relatively constant over distance. However, lasers used in lightwave systems have a large beam divergence, typically 10 to 20 degrees. Here, irradiance obeys the inverse square law (doubling the distance reduces the irradiance by a factor of 4) and rapidly decreases over distance.

Lasers and Eye Damage

The optical energy emitted by laser and high-radiance LEDs in the 400-1400 nm range may cause eye damage if absorbed by the retina. When a beam of light enters the eye, the eye magnifies and focuses the energy on the retina magnifying the irradiance. The irradiance of the energy that reaches the retina is approximately 10^5, or 100,000 times more than at the cornea and, if sufficiently intense, may cause a retinal burn.

The damage mechanism at the wavelengths used in an optical fiber telecommunications is thermal in origin, i.e., damage caused by heating. Therefore, a specific amount of energy is required for a definite time to heat an area of retinal tissue. Damage to the retina occurs only when one looks at the light long enough that the product of the retinal irradiance and the viewing time exceeds the damage threshold. Optical energies above 1400 nm cause corneal and skin burns, but do not affect the retina. The thresholds for injury at wavelengths greater than 1400 nm are significantly higher than for wavelengths in the retinal hazard region.

Classification of Lasers

Manufacturers of lasers and laser products in the U.S. are regulated by the Food and Drug Administration's Center for Devices and Radiological Health (FDA/CDRH) under 21 CFR 1040. These regulations require manufacturers to certify each laser or laser product as belonging to one of four major Classes: I, II, IIA, IIIa, IIIb, or IV. The International Electro-technical Commission is an international standards body that writes laser safety standards under IEC-60825. Classification schemes are similar with Classes divided into Classes 1, 1M, 2, 2M, 3R, 3B, and 4. Lasers are classified according to the accessible emission limits and their potential for causing injury. Optical fiber telecommunication systems are generally classified as Class 1/1 because, under normal operating conditions, all energized laser transmitting circuit packs are terminated on optical fibers which enclose the laser energy with the fiber sheath forming a protective housing. Also, a
A protective housing/access panel is typically installed in front of the laser circuit pack shelves. The circuit packs themselves, however, may be FDA/CDRH Class I, IIIb, or IV or IEC Class 1, 1M, 3R, 3B, or 4.

**Laser Safety Precautions for Optical Fiber Telecommunication Systems**

In its normal operating mode, an optical fiber telecommunication system is totally enclosed and presents no risk of eye injury. It is a Class I/1 system under the FDA and IEC classifications.

The fiber optic cables that interconnect various components of an optical fiber telecommunication system can disconnect or break, and may expose people to laser emissions. Also, certain measures and maintenance procedures may expose the technician to emission from the semiconductor laser during installation and servicing. Unlike more familiar laser devices such as solid-state and gas lasers, the emission pattern of a semiconductor laser results in a highly divergent beam. In a divergent beam, the irradiance (power density) decreases rapidly with distance. The greater the distance, the less energy will enter the eye, and the less potential risk for eye injury. Inadvertently viewing an un-terminated fiber or damaged fiber with the unaided eye at distances greater than 5 to 6 inches normally will not cause eye injury, provided the power in the fiber is less than a few milliwatts at the near IR wavelengths and a few tens of milliwatts at the far IR wavelengths. However, damage may occur if an optical instrument such as a microscope, magnifying glass, or eye loupe is used to stare at the energized fiber end.

![⚠️⚠️ CAUTION](CAUTION)

Laser hazard

*Use of controls, adjustments, and procedures other than those specified herein may result in hazardous laser radiation exposure.*

**Laser Safety Precautions for Enclosed Systems**

Under normal operating conditions, optical fiber telecommunication systems are completely enclosed; nonetheless, the following precautions shall be observed:

1. Because of the potential for eye damage, technicians should not stare into optical connectors or broken fibers
2. Under no circumstance shall laser/fiber optic operations be performed by a technician before satisfactorily completing an approved training course
3. Since viewing laser emissions directly in excess of Class I/1 limits with an optical instrument such as an eye loupe greatly increases the risk of eye damage, appropriate labels must appear in plain view, in close proximity to the optical port on the protective housing/access panel of the terminal equipment.
Laser Safety Precautions for Unenclosed Systems

During service, maintenance, or restoration, an optical fiber telecommunication system is considered unenclosed. Under these conditions, follow these practices:

1. Only authorized, trained personnel shall be permitted to do service, maintenance and restoration. Avoid exposing the eye to emissions from un-terminated, energized optical connectors at close distances. Laser modules associated with the optical ports of laser circuit packs are typically recessed, which limits the exposure distance. Optical port shutters, Automatic Power Reduction (APR), and Automatic Power Shut Down (APSD) are engineering controls that are also used to limit emissions. However, technicians removing or replacing laser circuit packs should not stare or look directly into the optical port with optical instruments or magnifying lenses. (Normal eye wear or indirect viewing instruments such as Find-R-Scopes are not considered magnifying lenses or optical instruments.)

2. Only authorized, trained personnel shall use optical test equipment during installation or servicing since this equipment contains semiconductor lasers (Some examples of optical test equipment are Optical Time Domain Reflectometers (OTDR’s), Hand-held Loss Test Sets.)

3. Under no circumstances shall any personnel scan a fiber with an optical test set without verifying that all laser sources on the fiber are turned off.

4. All unauthorized personnel shall be excluded from the immediate area of the optical fiber telecommunication systems during installation and service.


Technical Documentation

The technical documentation as required by the Conformity Assessment procedure is kept at Alcatel-Lucent location which is responsible for this product. For more information please contact your local Alcatel-Lucent representative.

How to comment

Note to reviewers: The following "How to comment" text will appear in the final document when it is published. However, the feedback method described below is for use only on final documents. Please send your review comments to the author using the process you were given when you received this draft document.

To comment on this document, go to the Online Comment Form (http://infodoc.alcatel-lucent.com/comments/) or e-mail your comments to the Comments Hotline (comments@alcatel-lucent.com).
1 Safety

Overview

Purpose

The aim of this chapter on safety is to provide users of 1643 AM and 1643 AMS systems with the relevant information and safety guidelines to safeguard against personal injury. Furthermore, this chapter may be useful to prevent material damage to the equipment.

The present chapter on safety must be read by the responsible technical personnel before carrying out relevant work on the system. The valid version of this document must always be kept close to the equipment.

Potential sources of danger

The 1643 AM and 1643 AMS equipment has been developed in line with the present state-of-the-art and fulfills the current national and international safety requirements. It is provided with a high degree of operational safety resulting from many years of development experience and continuous stringent quality checks in our company.

The equipment is safe in normal operation. There are, however, some potential sources of danger that cannot be completely eliminated. In particular, these arise during the:

- opening of housings or equipment covers,
- manipulation of any kind within the equipment, even if it has been disconnected from the power supply,
- disconnection of optical or electrical connections,

through possible contact with the following:

- live parts,
- laser light,
- hot surfaces, or
- sharp edges
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General notes on safety</strong></td>
<td>1-3</td>
</tr>
<tr>
<td>Structure of safety statements</td>
<td>1-4</td>
</tr>
<tr>
<td>Structure of safety instructions</td>
<td>1-6</td>
</tr>
<tr>
<td>Basic safety aspects</td>
<td>1-9</td>
</tr>
<tr>
<td><strong>Specific safety areas</strong></td>
<td>1-12</td>
</tr>
<tr>
<td>Laser safety</td>
<td>1-13</td>
</tr>
<tr>
<td>Laser product classification</td>
<td>1-17</td>
</tr>
<tr>
<td>Electrostatic discharge</td>
<td>1-21</td>
</tr>
</tbody>
</table>
General notes on safety

Overview

Purpose

This section provides general information on the structure of safety instructions and summarizes general safety requirements.

Contents

<table>
<thead>
<tr>
<th>Structure of safety statements</th>
<th>1-4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Structure of safety instructions</td>
<td>1-6</td>
</tr>
<tr>
<td>Basic safety aspects</td>
<td>1-9</td>
</tr>
</tbody>
</table>
Structure of safety statements

Overview

This topic describes the components of safety statements that appear in this document.

General structure

Safety statements include the following structural elements:


Lifting this equipment by yourself can result in injury due to the size and weight of the equipment.

Always use three people or a lifting device to transport and position this equipment.

<table>
<thead>
<tr>
<th>Item</th>
<th>Structure element</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Safety alert symbol</td>
<td>Indicates the potential for personal injury (optional)</td>
</tr>
<tr>
<td>2</td>
<td>Safety symbol</td>
<td>Indicates hazard type (optional)</td>
</tr>
<tr>
<td>3</td>
<td>Signal word</td>
<td>Indicates the severity of the hazard</td>
</tr>
<tr>
<td>4</td>
<td>Hazard type</td>
<td>Describes the source of the risk of damage or injury</td>
</tr>
<tr>
<td>5</td>
<td>Safety message</td>
<td>Consequences if protective measures fail</td>
</tr>
<tr>
<td>6</td>
<td>Avoidance message</td>
<td>Protective measures to take to avoid the hazard</td>
</tr>
<tr>
<td>7</td>
<td>Identifier</td>
<td>The reference ID of the safety statement (optional)</td>
</tr>
</tbody>
</table>
Signal words

The signal words identify the hazard severity levels as follows:

<table>
<thead>
<tr>
<th>Signal word</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>DANGER</td>
<td>Indicates an extremely hazardous situation which, if not avoided, will result in death or serious injury.</td>
</tr>
<tr>
<td>WARNING</td>
<td>Indicates a hazardous situation which, if not avoided, could result in death or serious injury.</td>
</tr>
<tr>
<td>CAUTION</td>
<td>Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.</td>
</tr>
<tr>
<td>NOTICE</td>
<td>Indicates a hazardous situation not related to personal injury.</td>
</tr>
</tbody>
</table>
Structure of safety instructions

General structure

All safety instructions include a warning symbol and a signal word that classify the danger, and a text block that contains descriptions of the type and cause of the danger, the consequences of ignoring the safety instruction and the measures that can be taken to minimise the danger.

Example:

⚠️ ⚠️ DANGER

Electric-shock hazard

Arcing can cause burns to the hands and damage to the eyes.

Ensure that the line circuit breaker on the Power Interface (PI) is in the “OFF” position before removing or inserting the power supply plug.

Danger classification

There are three classes of safety instructions: “DANGER”, “WARNING” and “CAUTION”. Which class is relevant depends on the consequences of ignoring the safety instruction:

<table>
<thead>
<tr>
<th>Class</th>
<th>Consequence Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DANGER</td>
<td>Serious injury is definite or likely.</td>
</tr>
<tr>
<td>WARNING</td>
<td>Serious injury is possible.</td>
</tr>
<tr>
<td>CAUTION</td>
<td>Minor injury is definite, likely or possible, or material damage to the product or in the product environment is definite or likely.</td>
</tr>
</tbody>
</table>
Warning symbols

These warning symbols are defined for safety instructions:

1. General warning of danger
2. Electric shock
3. Hazard of laser radiation
4. Components sensitive to electrostatic discharge (ESD)
5. Electromagnetic radiation
6. Flammable material / Risk of fire
7. Service disruption hazard
8. Laceration hazard
9. Corrosive substance
10. Hazard caused by batteries
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Hot surface</td>
</tr>
<tr>
<td>12</td>
<td>Heavy overhead load</td>
</tr>
<tr>
<td>13</td>
<td>Noxious substance</td>
</tr>
<tr>
<td>14</td>
<td>Explosion hazard</td>
</tr>
<tr>
<td>15</td>
<td>Falling object hazard</td>
</tr>
<tr>
<td>16</td>
<td>Risk of suffocation</td>
</tr>
<tr>
<td>17</td>
<td>Pinch hazard</td>
</tr>
<tr>
<td>18</td>
<td>Lifting hazard, heavy object</td>
</tr>
<tr>
<td>19</td>
<td>Inhalation hazard</td>
</tr>
<tr>
<td>20</td>
<td>Slip hazard</td>
</tr>
<tr>
<td>20</td>
<td>Slip hazard</td>
</tr>
<tr>
<td>21</td>
<td>Trip hazard</td>
</tr>
<tr>
<td>22</td>
<td>Hazard of falling</td>
</tr>
</tbody>
</table>
Basic safety aspects

General safety requirements

In order to keep the technically unavoidable residual risk to a minimum, it is imperative to observe the following rules:

- Transport, storage, and operation of the system must be under the *permissible conditions only*.
  
  See accompanying documentation and information on the system.

- Installation, configuration, and disassembly must be carried out only by *expert personnel* and *with reference to the respective documentation*.
  
  Due to the complexity of the system, the personnel requires *special training*.

- The system must be operated by *expert and authorised users only*.
  
  The user must operate the system only after having *read and understood* this chapter on safety and the parts of the documentation relevant to operation. For complex systems, additional training is recommended. Any obligatory training for operating and service personnel must be carried out and documented.

- The system must not be operated unless it is in perfect working order.
  
  Any faults and errors that might affect safety must be reported *immediately* by the user to a person in responsibility.

- The system must be operated only with the connections and under the environmental conditions as described in the documentation.

- Any conversions or changes to the system or parts of the system (including the software) must be carried out by qualified Alcatel-Lucent personnel or by expert personnel authorised by Alcatel-Lucent.
  
  All changes carried out by other persons lead to a *complete exemption from liability*.

  No components/spare parts must be used other than those recommended by the manufacturer and those listed in the procurement documents.

- The removal or disabling of safety facilities, the clearing of faults and errors, and the maintenance of the equipment must be carried out by *specially qualified personnel only*.
  
  The respective parts of the documentation must be strictly observed. The documentation must also be consulted during the selection of measuring and test equipment.

- Calibrations, special tests after repairs and regular safety checks must be carried out, documented and archived.
• Non-system software is used at one’s own risk. The use/installation of non-system software can adversely affect the normal functioning of the system.

• Only use tested and virus-free data carriers (floppy disks, streamer tapes, ...).

Summary of important safety instructions

Especially observe the following safety instructions, they are of particular importance for 1643 AM and 1643 AMS systems:

• This equipment is to be installed only in Restricted Access Areas in business and customer premises.

Applications in accordance with Articles 110-16, 110-17 and 110-18 of the National Electrical Code, ANSI/NFPA No. 70. Other installations exempt from the enforcement of the National Electrical Code may be engineered according to the accepted practices of the local telecommunications utility.

• This product should only be operated from the type of power source indicated on the marking label.

• This equipment must be provided with a readily accessible disconnect device as part of the building installation.

• Disconnect up to four (4) power supply connections when removing power from the system.

• Installation must include an independent frame ground drop to the building ground. Refer to the 1643 AM and 1643 AMS Installation Guide.

• For information on proper mounting instructions, consult the 1643 AM and 1643 AMS Installation Guide.

• Install only equipment identified in the 1643 AM and 1643 AMS Installation Guide provided with this product. Use of other equipment may result in improper connection of circuitry leading to fire or injury to persons.

• To reduce the risk of electrical shock, do not disassemble this product. Installation and service should be performed by trained personnel only. Opening or removing covers and/or circuit boards may expose you to dangerous voltages or other risks. Incorrect re-assembly can cause electrical shock when the unit is subsequently used.

• Slots and openings in this product are provided for ventilation. To protect the product from overheating, these openings must not be blocked or covered. This product should not be placed in a built-in installation unless proper ventilation is provided.

• Never push objects of any kind into this product through slots as they may touch dangerous voltage points or short-cut parts that could result in a risk of fire or electrical shock. Never spill liquids of any kind on the product.
CAUTION: This equipment is designed to permit the connection of the grounded conductor of the DC supply circuit to the grounding conductor at the equipment.

1. This equipment shall be connected directly to the DC supply system grounding electrode conductor or to a bonding jumper from a grounding terminal bar or bus to which the DC supply system grounding electrode conductor is connected.

2. This equipment shall be located in the same immediate area (such as, adjacent cabinets) as any other equipment that has a connection between the grounded conductor of the same DC supply circuit and the grounding conductor, and also the point of grounding of the DC system. The DC system shall not be grounded elsewhere.

3. The DC supply source is to be located within the same premises as this equipment.

4. There shall be no switching or disconnection devices in the grounded circuit conductor between the DC source and the point of connection of the grounding electrode conductor.
Specific safety areas

Overview

Purpose

The aspects of “laser safety” and “handling of components sensitive to electrostatic discharge (ESD)” are of vital importance for the 1643 AM and 1643 AMS equipment. Therefore, the key safety instructions for these subjects are summarised in the following.

Contents

<table>
<thead>
<tr>
<th>Laser safety</th>
<th>1-13</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laser product classification</td>
<td>1-17</td>
</tr>
<tr>
<td>Electrostatic discharge</td>
<td>1-21</td>
</tr>
</tbody>
</table>
Laser safety

Optical fiber telecommunication systems, their associated test sets, and similar operating systems use semiconductor laser transmitters that emit infrared (IR) light at wavelengths between approximately 800 nanometers and 1600 nanometers. The emitted light is above the red end of the visible spectrum, which is normally not visible to the human eye. Although radiant energy at near-IR wavelengths is officially designated invisible, some people can see the shorter wavelength energy even at power levels several orders of magnitude below any that have been shown to cause injury to the eye.

Conventional lasers can produce an intense beam of monochromatic light. The term monochromaticity means a single wavelength output of pure color that may be visible or invisible to the eye. A conventional laser produces a small-size beam of light, and because the beam size is small the power density (also called irradiance) is very high. Consequently, lasers and laser products are subject to federal and applicable state regulations as well as international standards for their safe operation.

A conventional laser beam expands very little over distance, or is said to be very well collimated. Thus, conventional laser irradiance remains relatively constant over distance. However, lasers used in light wave systems have a large beam divergence, typically 10 to 20 degrees. Here, irradiance obeys the inverse square law (doubling the distance reduces the irradiance by a factor of 4) and rapidly decreases over distance.

System design

The 1643 AM and 1643 AMS system complies with the Food and Drug Administration’s Center for Devices and Radiological Health (FDA/CDRH) regulations FDA/CDRH 21 CFR 1040.10 and 1040.11 as a Class I and with IEC 60825-1 as a Class 1 Optical Fiber Telecommunication laser product.

The system has been designed to ensure that the operating personnel is not endangered by laser radiation during normal system operation. The safety measures specified in the FDA/CDRH regulations and the international standards IEC 60825 and DIN/EN 60825 respectively are met. Please also refer to “Laser product classification” (p. 1-17).

Laser classes

The maximum output power of laser radiation depends on the type of laser diode used. The international standards IEC 60825 and DIN/EN 60825 respectively as well as the FDA/CDRH regulations define the maximum output power of laser radiation for each laser class in accordance with the wavelength.

The classification scheme is based on the ability of the laser emission or the reflected laser emission to cause injury to the eye or skin during normal operating conditions. Please also refer to “Laser product classification” (p. 1-17).
IEC Customer Laser Safety Guidelines

Alcatel-Lucent declares that this product is compliant with all essential safety requirements as stated in IEC 60825-Part 1 and 2 “Safety of laser products” and “Safety of optical fibre telecommunication systems”. Furthermore, Alcatel-Lucent declares that the warning statements on labels on this equipment are in accordance with the specified laser radiation class.

Optical Safety Declaration (if laser modules used)

Alcatel-Lucent declares that this product is compliant with all essential safety requirements as stated in IEC 60825-Part 1 and 2 “Safety of Laser Products” and “Safety of Optical Fiber Telecommunication Systems”. Furthermore, Alcatel-Lucent declares that the warning statements on labels on this equipment are in accordance with the specified laser radiation class.

Potential sources of danger

Beware of the following potential sources of danger which will remain despite all safety measures taken:

- Laser radiation can cause damage to the skin and eyes.
- Laser radiation from optical transmission systems is in a wavelength range that is invisible to the human eye.

Lasers and Eye Damage

The optical energy emitted by laser and high-radiance LEDs in the 400-1400 nm range may cause eye damage if absorbed by the retina. When a beam of light enters the eye, the eye magnifies and focuses the energy on the retina magnifying the irradiance. The irradiance of the energy that reaches the retina is approximately 105, or 100,000 times more than at the cornea and, if sufficiently intense, may cause a retinal burn.

The damage mechanism at the wavelengths used in an optical fiber telecommunications is thermal in origin, i.e., damage caused by heating. Therefore, a specific amount of energy is required for a definite time to heat an area of retinal tissue. Damage to the retina occurs only when one looks at the light long enough that the product of the retinal irradiance and the viewing time exceeds the damage threshold. Optical energies above 1400 nm cause corneal and skin burns, but do not affect the retina. The thresholds for injury at wavelengths greater than 1400 nm are significantly higher than for wavelengths in the retinal hazard region.

Laser Safety Precautions for Optical Fiber Telecommunication Systems

In its normal operating mode, an optical fiber telecommunication system is totally enclosed and presents no risk of eye injury. It is a Class I/1 system under the FDA and IEC classifications.
The fiber optic cables that interconnect various components of an optical fiber telecommunication system can disconnect or break, and may expose people to laser emissions. Also, certain measures and maintenance procedures may expose the technician to emission from the semiconductor laser during installation and servicing. Unlike more familiar laser devices such as solid-state and gas lasers, the emission pattern of a semiconductor laser results in a highly divergent beam. In a divergent beam, the irradiance (power density) decreases rapidly with distance. The greater the distance, the less energy will enter the eye, and the less potential risk for eye injury. Inadvertently viewing an un-terminated fiber or damaged fiber with the unaided eye at distances greater than 5 to 6 inches normally will not cause eye injury, provided the power in the fiber is less than a few milliwatts at the near IR wavelengths and a few tens of milliwatts at the far IR wavelengths. However, damage may occur if an optical instrument such as a microscope, magnifying glass, or eye loupe is used to stare at the energized fiber end.

**CAUTION**

Laser hazard

*Use of controls, adjustments, and procedures other than those specified herein may result in hazardous laser radiation exposure.*

**Laser Safety Precautions for Enclosed Systems**

Under normal operating conditions, optical fiber telecommunication systems are completely enclosed; nonetheless, the following precautions shall be observed:

1. Because of the potential for eye damage, technicians should not stare into optical connectors or broken fibers
2. Under no circumstance shall laser/fiber optic operations be performed by a technician before satisfactorily completing an approved training course
3. Since viewing laser emissions directly in excess of Class I/1 limits with an optical instrument such as an eye loupe greatly increases the risk of eye damage, appropriate labels must appear in plain view, in close proximity to the optical port on the protective housing/access panel of the terminal equipment.

**Laser safety precautions for unenclosed systems**

During service, maintenance, or restoration, an optical fiber telecommunication system is considered unenclosed. Under these conditions, follow these practices:

1. Only authorized, trained personnel shall be permitted to do service, maintenance and restoration. Avoid exposing the eye to emissions from un terminated, energized optical connectors at close distances. Laser modules associated with the optical ports of laser circuit packs are typically recessed, which limits the exposure distance. Optical port shutters, Automatic Power Reduction (APR), and Automatic Power Shut Down
Laser safety

Laser safety instructions

Observe the following instructions to avoid exposing yourself and others to risk:

- Read the relevant descriptions in the manuals before taking equipment into operation or carrying out any installation and maintenance work on the optical port units, and follow the instructions. Ignoring the instructions may result in hazardous laser radiation exposure.

- Do not view directly into the laser beam with optical instruments such as a fiber microscope, because viewing of laser emission in excess of Class 1 limits significantly increases the risk of eye damage.

- Never look into the end of an exposed fiber or an open connector as long as the optical source is still switched on.

- Ensure that the optical source is switched off before disconnecting optical fiber connectors.

- In the event of doubt, check that the optical source is switched off by measuring with an optical power meter.

CAUTION

Laser hazard

Use of controls, adjustments, and procedures other than those specified herein may result in hazardous laser radiation exposure.
Laser product classification

Standards compliance

The 1643 AM and 1643 AMS product complies with the applicable IEC standards and the Food and Drug Administration’s Center for Devices and Radiological Health (FDA/CDRH) regulations.

FDA/CDRH regulations

Laser products are classified in accordance with the FDA/CDRH - 21 CFR 1010 and 1040. The classification scheme is based on the ability of the laser emission to cause injury to the eye or skin during normal operating conditions.

In the United States, lasers and laser systems in the infrared wavelength range (greater than 700 nm) are assigned to one of the following classes (please refer to “FDA/CDRH laser classification” (p. 1-18)):

- Class I,
- Class IIIb, or
- Class IV.

Laser classification is dependent upon operating wavelength, output power, and fiber mode field diameter (core diameter).

IEC requirements

The International Electro-Technical Commission (IEC) establishes standards for the electrical and electronic industries. The IEC 60825 standard has been established for the worldwide safety of laser products.

According to the IEC classification, lasers and laser systems in the infrared wavelength range (greater than 700 nm) are assigned to one of the following classes (please refer to “IEC laser classification” (p. 1-18)):

- Class 1,
- Class 1M,
- Class 3R,
- Class 3B, or
- Class 4.

There are some major differences between the FDA/CDRH regulations and the IEC requirements:

1. The Accessible Emission Limits (AEL) are different.
2. Class 1M applies to all wavelengths.
3. Class 3B requires strict engineering controls.

4. Classification is under single fault conditions.

FDA/CDRH laser classification

The following table provides an overview of laser classes for wavelengths of 1310 nm and 1550 nm in accordance with the FDA/CDRH regulations.

<table>
<thead>
<tr>
<th>Laser class</th>
<th>Wavelength</th>
<th>Max. output power of laser radiation</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>1310 nm</td>
<td>1.53 mW +1.85 dBm</td>
</tr>
<tr>
<td></td>
<td>1550 nm</td>
<td>8.52 mW +9.3 dBm</td>
</tr>
<tr>
<td>IIIb</td>
<td>1310 nm</td>
<td>500 mW +27 dBm</td>
</tr>
<tr>
<td></td>
<td>1550 nm</td>
<td>500 mW +27 dBm</td>
</tr>
<tr>
<td>IV</td>
<td>1310 nm</td>
<td>&gt; 500 mW +27 dBm</td>
</tr>
<tr>
<td></td>
<td>1550 nm</td>
<td>&gt; 500 mW +27 dBm</td>
</tr>
</tbody>
</table>

Explanatory note: In the United States, lasers and laser systems are assigned to one of the following classes: Roman numerals I, IIa, II, IIIa, IIIb, and IV. Classes I, IIIb, and IV apply to lasers of all wavelengths. Classes IIa, II, and IIIa apply only to those lasers operating within the visible wavelength range (400-700 nm). Alcatel-Lucent laser products typically operate in the infrared wavelength range (greater than 700 nm) and, therefore, are primarily in the Class I or Class IIIb classifications.

IEC laser classification

The following table provides an overview of laser classes for wavelengths of 1310 nm and 1550 nm in accordance with the IEC 60825-1 Ed. 1.2 (2001) standard. The precise power limits depend on the mode field diameter and the numerical aperture (NA) of the laser source.

<table>
<thead>
<tr>
<th>Laser class</th>
<th>Wavelength</th>
<th>Max. output power of laser radiation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1310 nm</td>
<td>15.6 mW +11.93 dBm</td>
</tr>
<tr>
<td></td>
<td>1550 nm</td>
<td>10 mW +10 dBm</td>
</tr>
<tr>
<td>1M</td>
<td>1310 nm</td>
<td>50.84 mW +17.06 dBm</td>
</tr>
<tr>
<td></td>
<td>1550 nm</td>
<td>121.20 mW +20.84 dBm</td>
</tr>
<tr>
<td>3R</td>
<td>1310 nm</td>
<td>86 mW +18.92 dBm</td>
</tr>
<tr>
<td></td>
<td>1550 nm</td>
<td>_1</td>
</tr>
<tr>
<td>3B</td>
<td>1310 nm</td>
<td>500 mW +27 dBm</td>
</tr>
<tr>
<td></td>
<td>1550 nm</td>
<td>500 mW +27 dBm</td>
</tr>
</tbody>
</table>
Laser class | Wavelength | Max. output power of laser radiation
---|---|---
4 | 1310 nm | > 500 mW > +27 dBm
| 1550 nm | > 500 mW > +27 dBm

Notes:
1. Class 3R only exists if the maximum power is within five times the Accessible Emission Limit (AEL) of Class 1.

In earlier editions of the IEC 60825 standard the following laser classes and corresponding power limits were defined for wavelengths of 1310 nm and 1550 nm.

<table>
<thead>
<tr>
<th>Laser class</th>
<th>Wavelength</th>
<th>Max. output power of laser radiation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1310 nm</td>
<td>8.85 mW +9.5 dBm</td>
</tr>
<tr>
<td></td>
<td>1550 nm</td>
<td>10 mW +10 dBm</td>
</tr>
<tr>
<td>3A</td>
<td>1310 nm</td>
<td>24 mW +13.8 dBm</td>
</tr>
<tr>
<td></td>
<td>1550 nm</td>
<td>50 mW +17 dBm</td>
</tr>
<tr>
<td>3B</td>
<td>1310 nm</td>
<td>500 mW +27 dBm</td>
</tr>
<tr>
<td></td>
<td>1550 nm</td>
<td>500 mW +27 dBm</td>
</tr>
<tr>
<td>4</td>
<td>1310 nm</td>
<td>&gt; 500 mW &gt; +27 dBm</td>
</tr>
<tr>
<td></td>
<td>1550 nm</td>
<td>&gt; 500 mW &gt; +27 dBm</td>
</tr>
</tbody>
</table>

Notes:
1. Corresponding laser warning labels can still be found on equipment manufactured before publication of the IEC 60825-1 Ed. 1.2 (2001) standard.

Hazard level assignment

“Hazard level” refers to the potential hazard from laser emission at any location in an end-to-end optical fiber communication system that may be accessible during service or in the event of a failure. The assignment of hazard level uses the AELs for the classes.

Hazard levels for optical transmission equipment are assigned in either of the following two ways:
- the actual output power from the connector or fiber cut.
- if automatic power reduction is used, the output power at the connector or fiber cut at one second after automatic power reduction takes place, provided that maximum output and restart conditions are met.
Classification of optical telecommunication equipment

Optical telecommunication equipment is generally classified as IEC Class 1 or FDA/CDRH Class I, because under normal operating conditions the transmitter ports terminate on optical fiber connectors. These are covered by a front panel to ensure protection against emissions from any energized, unterminated transmitter.

The circuit packs themselves, however, may be IEC Class 1 or 1M or FDA/CDRH Class I or Class IIIb.

Optical specifications of the internal laser circuit packs:

<table>
<thead>
<tr>
<th>Laser circuit pack code</th>
<th>Wavelength (nm)</th>
<th>Output power (mW)</th>
<th>Fiber type core/cladding diameter (µm)</th>
<th>Connector type</th>
<th>FDA class/IEC hazard level</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1.1</td>
<td>1310</td>
<td>0.16</td>
<td>SM(9/125)</td>
<td>SC, FC, ST</td>
<td>I/1</td>
</tr>
<tr>
<td>S4.1</td>
<td>1310</td>
<td>0.16</td>
<td>SM(9/125)</td>
<td>SC, FC, ST</td>
<td>I/1</td>
</tr>
<tr>
<td>L1.2</td>
<td>1550</td>
<td>1.6</td>
<td>SM(9/125)</td>
<td>SC, FC, ST</td>
<td>I/1</td>
</tr>
<tr>
<td>L4.2</td>
<td>1550</td>
<td>1.6</td>
<td>SM(9/125)</td>
<td>SC, FC, ST</td>
<td>I/1</td>
</tr>
</tbody>
</table>

Alcatel-Lucent 1643 AM and 1643 AMS complies with FDA/CDRH 21 CFR 1040.10 and 1040.11 as Class I and IEC 60825-1 as a Class 1 Laser Product.
Electrostatic discharge

Introduction

Electrostatic discharge (ESD), caused by touching with the hand for example, can destroy semiconductor components. The correct operation of the complete system is then no longer assured.

Industry experience has shown that all semiconductor components can be damaged by static electricity that builds up on work surfaces and personnel. The electrostatic discharge can also affect the components indirectly via contacts or conductor tracks. The electrostatic charges are produced by various charging effects of movement and contact with other objects. Dry air allows greater static charges to accumulate. Higher potentials are measured in areas with low relative humidity, but potentials high enough to cause damage can occur anywhere.

The barred-hand symbol

Circuit packs containing components that are especially sensitive to electrostatic discharge are identified by warning labels bearing the barred-hand symbol.

ESD instructions

Observe the following ESD instructions to avoid damage to electrostatic-sensitive components:

- Wear working garment made of 100% cotton to avoid electrostatic charging.
- Touch the circuit packs at the edges or the insertion and removal facilities only.
- Ensure that the rack is grounded.
- Wear conductively connected wrist straps and connect them to the rack ESP bonding point.
- Work in an area which is protected against electrostatic discharge. Use conducting floor and bench mats which are conductively connected to the rack ESP bonding point.
- Conductively connect all test equipment and trolleys to the rack ESP bonding point.
Store and ship circuit packs and components in their shipping packing. Circuit packs and components must be packed and unpacked only at workplaces suitably protected against build-up of charge.

- Whenever possible, maintain the relative humidity of air above 20%.
2 Getting Started

Overview

Purpose

Using the ITM-CIT provides information on how to use the Integrated Transport Management-Craft Interface Terminal.

Objective

Locally install, test, or provision a network element.

Outcome

A working network element or an inactive network element.

Intended use

This chapter explains the basics of using the ITM-CIT, such as the installing of software, window handling, use of the ITM-CIT main menu and procedures.

Contents

<table>
<thead>
<tr>
<th>Installing the ITM-CIT</th>
<th>2-3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install ITM-CIT software</td>
<td>2-4</td>
</tr>
<tr>
<td><strong>Main menu and buttons</strong></td>
<td>2-8</td>
</tr>
<tr>
<td>The ITM-CIT main menu</td>
<td>2-9</td>
</tr>
<tr>
<td>Frequently used buttons</td>
<td>2-16</td>
</tr>
<tr>
<td><strong>Login to a NE</strong></td>
<td>2-18</td>
</tr>
<tr>
<td>Login to a Network Element</td>
<td>2-19</td>
</tr>
<tr>
<td><strong>Change NE date and time</strong></td>
<td>2-21</td>
</tr>
<tr>
<td>Change NE Date and Time</td>
<td>2-22</td>
</tr>
</tbody>
</table>
### Getting Started

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters for Changing NE Date and Time</td>
<td>2-23</td>
</tr>
<tr>
<td>Log out of an NE</td>
<td>2-24</td>
</tr>
<tr>
<td>Logout procedure</td>
<td>2-25</td>
</tr>
</tbody>
</table>
Installing the ITM-CIT

Overview

Purpose

The purpose of this section is to describe the installation procedures of the ITM-CIT application software on a PC and to explain how to use the ITM-CIT. This section provides information which must be known by the user before performing specific tasks.

Main topics

The main topics in this section are the hard- and software requirements and the installation procedures. Further, this section describes how to start and stop the ITM-CIT application, how to login and logout of a Network Element and the layouts of the windows of the ITM-CIT. Finally, it also presents a menu structure overview of the ITM-CIT application.

Target group

This subject is intended for personnel responsible for installation of the ITM-CIT software on a PC and for first-time user of the ITM-CIT application.

Note

The windows shown in this section are merely meant as an example. The contents can slightly differ from what is shown on the screen.

Contents

Install ITM-CIT software 2-4
Install ITM-CIT software

When to use

Use this procedure to install the ITM CIT software onto a new system.

Required equipment

For the ITM CIT a personal computer is necessary which fulfills the following minimum requirements:

- Pentium® processor with 450 MHz or higher
- 128 MB RAM or higher
- Keyboard
- Mouse
- 300 MB of free hard-disk drive space
- CD-ROM drive
- Display set to 1024x768, 16 million colors recommended)
- RS-232 communication port (serial asynchronous port)
- Ensure that the RS232 interface of the PC that is running the ITM CIT is able to handle the RTS (ready to send) line correctly. Otherwise the ITM CIT would not detect a recovery of the SC. This would cause the ITM CIT to "hang" while the SC is recovering.
- Windows XP® or Windows® 2000 operating system
- ITM-CIT connector (F-interface) cable (one end RS-232 and the other end RJ-45 modular jack).

The performance can be enhanced by using a higher performance personal computer. Independent of the requirements listed above the minimum requirements of the operating system must be fulfilled. A CD-ROM containing the WaveStar® ITM-CIT software must be available.

Before you begin

Before installing the software, the software release number must be known.

The installation program cannot install system files or update shared files if they are in use by other programs. For this reason the user must stop as many Windows applications as possible before starting with the installation procedures.
Installation procedure

Complete the following steps to install the WaveStar® ITM-CIT software on your PC:

1. On the Windows® desktop, click with the left button of the mouse on Start.
   
   **Result:** The Start menu appears.

2. Click with the left button of the mouse on the Run item.
   
   **Result:** The Run window appears.

3. Click on the Browse button.
   
   **Result:** The Browse window appears.

4. Insert the CD-ROM containing the WaveStar® ITM-CIT application into the CD-ROM drive and click with the left button of the mouse on the CD-ROM item.

5. Select the required directory and click on the executable file SETUP.exe and then click Open.

6. Click OK to run the executable file on the CD-ROM.
   
   **Result:** The InstallShield Wizard window appears.

7. Click Next to continue with the installation of the WaveStar® ITM-CIT software.
   
   **Result:** The WaveStar® ITM-CIT files are extracted. This will take a few minutes. Then the Welcome window appears.

8. Click Next.
   
   **Result:** The Software License Agreement window appears.

9. Click Yes.
Result: The Select Language window appears. Here the language of the Online Help is defined.

<table>
<thead>
<tr>
<th>If</th>
<th>then</th>
</tr>
</thead>
<tbody>
<tr>
<td>you want to install WaveStar® ITM-CIT with default setting <strong>English</strong> (English Online Help)</td>
<td>click <strong>Next</strong>. <strong>Result:</strong> The Select Components window appears.</td>
</tr>
<tr>
<td>you want to install a different language</td>
<td>run <strong>SETUP.exe</strong> again and select the required language (right now in english available only). <strong>Result:</strong> The Select Components window appears.</td>
</tr>
</tbody>
</table>

11 Select the component(s) you wish to be installed. It is recommended to leave the default setting and install the ITM CIT including the Online Help files.

12 Click **Next** to install the WaveStar® ITM-CIT software in the default directory (C:\..\ITM-CIT).

**Important!** It is strictly recommended to use the default directory for installing the ITM CIT software.

When the (current) NE SW is going to be installed the ITM CIT version that fits to the NE version is 'hard coded' in the installation routine. This means, in case there's no according directory available (for example, C:\..\Lucent Technologies\ITM CIT\<<version identifier>>\Isd\), the installer will create exactly this directory and puts the extracted “isd” directory below this directory.

**Additional info** If for any reason you must install the ITM CIT on a different drive you can click on the Browse button to select or create a different directory for the WaveStar® ITM-CIT software.

Additionally you can check the available disk space for all available drives by clicking on Disk Space... Leave the window Available Disk Space by clicking OK or Cancel.

Activating Disk Space... may change the default directory to another drive.

13 It is optional to define a password. Fill in a password, if required and confirm it.. Then click **Next**.
Result: The **Select Program Folder** window appears.

14 Leave the default setting, select, or create a folder in which the program icons will be installed. Click **Next**.

   Result: The *WaveStar®* ITM-CIT is installed. This will take a few minutes. Then the **Restarting Windows** window appears.

15 Choose one of the given options and click **OK** to finish the setup.

   **Important!** It is recommended to reboot the PC before starting up the *WaveStar®* ITM-CIT, but make sure to restart the computer only if other *Windows®* programs have been closed before.
Main menu and buttons

Overview

Purpose

In this section the basics of the ITM-CIT application are discussed. This is done in three parts.

In the first part the simple procedures, such as logging in and out, are described step by step. The second part gives an overview of the main menu and its features. And in the third part the most frequently used buttons and their functions are listed.

The screens presented in this chapter are examples and may slightly differ from the screens presented on the ITM-CIT.

User roles

A user of the ITM-CIT can login in three different roles, called admin, config and view.

When logged in as admin, the user can perform all ITM-CIT administration and configure a network element.

If the user is logged in as config, it is possible to perform all transmission related tasks and retrieve and edit all network element related data.

Finally, if the user logs in as view, it is only possible to view the network element configuration, it cannot be altered.

Contents

<table>
<thead>
<tr>
<th>The ITM-CIT main menu</th>
<th>2-9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequently used buttons</td>
<td>2-16</td>
</tr>
</tbody>
</table>
The ITM-CIT main menu

Introduction

The main menu of the ITM-CIT contains several bars that either provide information about the current status of the network element, or that can be used to manage the network element.

Bars of the main menu

The main menu contains the following bars:

- Title bar
- Menu bar
- Status bar
- Toolbar
- Alarm Summary bar.

ITM CIT main menu

Although the Alarm Summary bar is not a default feature. It can be switched on or off depending on the user’s preference.
**Title bar**

For a local session, the title bar shall contain the name, the type and the location of the network element.

If the session is remote, also the name, the type and the location of the network element will be shown.

**Menu bar**

Via the menu bar it is possible to manage the network element. It consist of several buttons that have one or more submenus attached to it. By clicking a menu bar button, the submenus will scroll down and the submenu that is required can be selected. These submenus can, on their part, contain several sub-submenus as well.
All these submenus are discussed in the following chapters, they are not relevant for Getting Started. Of course with the exception of the menu items in File and Window, which are already discussed. And with the exception of the Help submenu, through which an on-line Help feature is reached.

**Menu bar structure**

The structure underlying the menu bar is as follows:

<table>
<thead>
<tr>
<th>File</th>
<th>NE Login</th>
<th>Login</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>DCC Neighbours List</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network Area Members List</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Add Accessible NE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Alarm Subscription</td>
</tr>
<tr>
<td>NE Logout</td>
<td>NE Logout</td>
<td>Alarm Unsubscription</td>
</tr>
<tr>
<td>Print</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Options</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View</td>
<td>Status bar</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Toolbar</td>
<td></td>
</tr>
<tr>
<td>Session</td>
<td>Local Session</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Remote Session</td>
<td></td>
</tr>
<tr>
<td>Provisioning</td>
<td>Equipment</td>
<td>Provisioned NE Components</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MDI</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MDO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NE Software Configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Shelf Display</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RPS</td>
</tr>
<tr>
<td>Transport</td>
<td>Ports</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Termination Point</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DEG Thresholds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cross Connection</td>
<td></td>
</tr>
<tr>
<td>Timing</td>
<td>Timing Sources</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System Timing</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Subcategory</td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Output Timing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LAN Management</td>
<td>LAN Unit</td>
<td></td>
</tr>
<tr>
<td>Virtual Switch</td>
<td>VCG</td>
<td></td>
</tr>
<tr>
<td>QoS Profile</td>
<td>Flow Pool List</td>
<td></td>
</tr>
<tr>
<td>SHDSL</td>
<td>SHDSL LTU</td>
<td></td>
</tr>
<tr>
<td>Connection / NTU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td>Node Creation</td>
<td></td>
</tr>
<tr>
<td>Node Details</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Control</td>
<td>Parameters</td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td>CIT Access List</td>
<td></td>
</tr>
<tr>
<td>Overlay Comms Network</td>
<td>DCN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DCC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DCC in MSP Mode</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP Tunneling</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transparent DCC</td>
<td></td>
</tr>
<tr>
<td>Overhead Byte Channel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMP Manager</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Datacom Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Stack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protection Equipment</td>
<td>MAIN 1+1</td>
<td></td>
</tr>
<tr>
<td>Transmission</td>
<td>MSP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SNC</td>
<td></td>
</tr>
<tr>
<td>Alarms</td>
<td>Current Alarms</td>
<td></td>
</tr>
<tr>
<td></td>
<td>History Alarms</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Alarm Summary</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Alarm Reporting Severity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Instances with Specific Settings</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NE Alarm Control</td>
<td></td>
</tr>
</tbody>
</table>
The ITM-CIT main menu

<table>
<thead>
<tr>
<th>Button</th>
<th>Button name</th>
<th>Access from menu bar</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="NE Login icon" /></td>
<td>NE Login</td>
<td>File -&gt; NE Login</td>
</tr>
<tr>
<td><img src="image2" alt="NE Logout icon" /></td>
<td>NE Logout</td>
<td>File -&gt; NE Logout</td>
</tr>
<tr>
<td><img src="image3" alt="Alarm Summary icon" /></td>
<td>Alarm Summary</td>
<td>Alarms -&gt; Alarm Summary</td>
</tr>
</tbody>
</table>
### Button Table

<table>
<thead>
<tr>
<th>Button</th>
<th>Button name</th>
<th>Access from menu bar</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Current Alarms</td>
<td>Alarms -&gt; Current Alarms</td>
</tr>
<tr>
<td></td>
<td>Provisioned NE Components</td>
<td>Provisioning -&gt; Equipment -&gt; Provisioned NE Components</td>
</tr>
<tr>
<td></td>
<td>Cross Connection</td>
<td>Provisioning -&gt; Transport -&gt; Cross Connection</td>
</tr>
<tr>
<td></td>
<td>Termination Point</td>
<td>Provisioning -&gt; Transport -&gt; Termination Point</td>
</tr>
<tr>
<td></td>
<td>Ports</td>
<td>Provisioning -&gt; Transport -&gt; Ports</td>
</tr>
<tr>
<td></td>
<td>SNC</td>
<td>Protection -&gt; Transmission -&gt; SNC</td>
</tr>
<tr>
<td></td>
<td>Time</td>
<td>Management -&gt; Time</td>
</tr>
<tr>
<td></td>
<td>Local Session</td>
<td>Session -&gt; Local Session</td>
</tr>
<tr>
<td></td>
<td>Remote Session</td>
<td>Session -&gt; Remote Session</td>
</tr>
<tr>
<td></td>
<td>Virtual Switch</td>
<td>Provisioning -&gt; LAN Management -&gt; Virtual Switch</td>
</tr>
<tr>
<td></td>
<td>VCG</td>
<td>Provisioning -&gt; LAN Management -&gt; VCG</td>
</tr>
<tr>
<td></td>
<td>QoS Profile</td>
<td>Provisioning -&gt; LAN Management -&gt; QoS Profile</td>
</tr>
<tr>
<td></td>
<td>Shelf Display</td>
<td>Provisioning -&gt; Equipment -&gt; Shelf Display</td>
</tr>
<tr>
<td></td>
<td>Print</td>
<td>File -&gt; Print</td>
</tr>
</tbody>
</table>

### Status bar

This is a Characteristic of the Windows™ operating system. It is divided into panels that display:

- The current computer time settings, correlated to the local time.
- The operators capability.
• A progress/abort message. This appears when a command is invoked, which leads to data interchange between the CIT and the network element. At the same time the mouse pointer will change into an hourglass.

The only commands that will not have the progress/abort message displayed in the status bar are the following:
  – Alarm Automatic Update
  – Test Request
  – Software Download
  – Get NE Configuration
  – Send NE Configuration.

Alarm summary bar

By selecting the Alarm Summary, either via the menu bar or the toolbar, the user can either disable or enable the Alarm Summary to be displayed in the main menu. As the name indicates, it summarizes the number and severity of the current alarms. For more details, see the section “Alarms”.

Frequently used buttons

Introduction

The ITM-CIT guides the user through the procedures by means of windows. These are either view windows, windows that provide information about the status of the network element, or they are edit windows, in which the user can alter parameters.

In general these windows will contain the following buttons:

OK

Executes changes that are made in an edit window and closes the window.

Cancel

Discards all changes that are made in an edit window and closes the window.

Update

If a window has been open for a while, it may display data that is not current any more. By clicking Update the user obtains the most recent information.

Apply

Allows the user to commit changes in a window without closing the window. This button is often made available in situations where a number of separate edit operations want to be evoked. It ensures that the user does not have to reopen the window after each alteration.

Close

Closes a window.

Edit

Is available on view windows that contain provisionable data. If it is clicked, an Edit window will appear in which the data can be altered.

Details

In some view windows it is not possible to show all relevant information. Usually the window will then contain a list of objects. By selecting an object and clicking Details, the user can obtain specified information of that object.
Filter

By using the Filter button, the user can make a selection of a set of objects to be shown in a view window. By specifying one or more constraints on the objects or their properties, a subset can be chosen from a complete set of objects.
Login to a NE

Overview

Purpose

Use this procedure to login into an NE to start managing the NE.

Contents

<table>
<thead>
<tr>
<th>Login to a Network Element</th>
<th>2-19</th>
</tr>
</thead>
</table>
Login to a Network Element

When to use
To configure the NE

Related information
No related information is available.

Before you begin
Before starting the ITM-CIT application and login in to a NE make sure that:
- the PC is connected to the network element (NE)
- the PC is rebooted at least once after installation.

Procedure
Follow these steps to login to a network element:

1. Start the ITM-CIT application.
   Result: The main ITM-CIT window appears

2. Select File -> NE Login -> Login in the main menu.
   Result: The NE Login window appears.

3. Select the correct COM port. Usually this is COM1.

4. Select Edit to set the correct baudrate.
   The baudrate to be used is 115k.
   AM1 (plus), TM1 do operate on a baudrate of 115k, the ADM16/1 family, and the 1643 AM is working with 114k.

5. Select Login.
   Result: The Password Required window appears.

6. Select the user role from the capability field.
Selectable user roles are:

- Admin (for ITM-CIT administration and configuration of an NE)
- Config (to configure an NE)
- View (only to view NE configuration)

Fill in the required password (if configured, to configure or change a password see procedure: Configuring and changing a password) and click **OK**.

**Result:** The ITM-CIT is logged into the NE.
Change NE date and time

Overview

Purpose

The purpose of this procedure is to change the date and time of an NE. The date and time are important for registration of alarms and PM data.

Contents

| Change NE Date and Time       | 2-22 |
| Parameters for Changing NE Date and Time | 2-23 |
Change NE Date and Time

When to use

To update the date and time information.

Related information

No related information is available.

Before you begin

The current date and time information must be known. If there is an association with the WaveStar® ITM-SC, then the date and time are automatically set when the association is established and will be repeated every 24 hours (at night).

Procedure

Follow this procedure to change the date and time of the NE.

1 Select Management --> Time, in the main menu.
   Result: The NE Date and Time window appears.

2 Click Edit.
   Result: The Edit Date and Time window appears.

3 Select the desired Edit Mode. Fill in the date and time (when the manual setting is chosen) and click OK.
   Result: The Edit Date and Time window disappears.

END OF STEPS
Parameters for Changing NE Date and Time

Date

The date field is used to set the date when the manual setting edit mode is chosen.

Edit Mode

The two edit modes provide a choice of methods by which the date and time can be changed. The possible values are described in the table below:

<table>
<thead>
<tr>
<th>Edit Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sync to CIT Time</td>
<td>The date and time are set automatically by using the local time and date from the CIT (PC). This information is sent to the NE and the time and date are set.</td>
</tr>
<tr>
<td>Manual Set</td>
<td>To manually set the date and time.</td>
</tr>
</tbody>
</table>

Time

The time field is used to set the time when the manual setting edit mode is chosen.
Log out of an NE

Overview

Purpose

Use this procedure to log out of an NE to stop managing NEs or to switch to another NE.

Contents

<table>
<thead>
<tr>
<th>Logout procedure</th>
<th>2-25</th>
</tr>
</thead>
</table>

Logout procedure

When to use

When managing the NE by the ITM-CIT must be stopped or another NE must be managed by this ITM-CIT.

Related information

No related information is available.

Before you begin

The NE name must be known.

Procedure

Follow this procedure to log out of an NE:

1. Select File -> NE Logout -> Logout in the main menu.
   Result: The ITM-CIT Warning window appears.

2. Click Yes.
   Result: The ITM-CIT is logged out of the NE and another NE can be connected via File -> NE Login -> Login in

END OF STEPS
3 Security administration

Overview

Purpose

This chapter discusses how to do some security administration tasks.

Contents

| View the access control parameters       | 3-2 |
| View Access Control Parameters          | 3-3 |
| Parameters for viewing the access control parameters | 3-4 |
| Change the lock state                   | 3-5 |
| Changing the lock state                 | 3-6 |
| Parameters for changing the lock state  | 3-7 |
| Change the inactivity time              | 3-8 |
| Changing the inactivity time            | 3-9 |
| Parameters for changing the inactivity time | 3-10 |
| Configure or change a password          | 3-11|
| Configuring or changing a password      | 3-12|
| Parameters for configuring or changing a password | 3-13|
| Force a logout                          | 3-14|
| Forcing a logout                        | 3-15|
| Parameters for forcing a logout         | 3-16|
View the access control parameters

Overview

Purpose

The only user that can perform administrative tasks, is the administrator. Most of these tasks are security tasks, such as configuring passwords for the different users and locking users.

The other users can get the administrative information, but they cannot alter it.

In this section, these administrative tasks will be treated.

The purpose of this procedure is to allow all users, not only an administrator, to see who, in what user role, is logged in on a network element.

Contents

| Viewing Access Control Parameters | 3-3 |
| Parameters for viewing the access control parameters | 3-4 |
Viewing Access Control Parameters

When to use

Use this procedure to view the parameters for the different user roles.

Related information

Related procedures are:
- Changing the lock state
- Changing the inactivity time
- Configuring and changing a password

Before you begin

No prerequisites or precautions are needed when performing this procedure.

Procedure

Follow this procedure to view the access control parameters:


Result: The Access Control Parameters window appears.

END OF STEPS
Parameters for viewing the access control parameters

Lock state

Specifies whether the user is locked. The value is either Locked or Unlocked.

Capability

This field lists the user roles. The possible values are described in the table below:

<table>
<thead>
<tr>
<th>Capability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>The user can perform all ITM-CIT administration tasks and configure a network element.</td>
</tr>
<tr>
<td>Config</td>
<td>The user can perform all transmission related tasks and retrieve and edit all network element related data.</td>
</tr>
<tr>
<td>View</td>
<td>The user can only view the network element configuration, it cannot be altered.</td>
</tr>
</tbody>
</table>

Inactivity time

Defines after which time the workstation will be locked if the user is inactive. The value is an integer between 0 and 60. If the value is 0, the user will never be logged out.
Change the lock state

Overview

Purpose

The purpose of this procedure is to change the lock state for a specific user role.

Contents

<table>
<thead>
<tr>
<th>Changing the lock state</th>
<th>3-6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters for changing the lock state</td>
<td>3-7</td>
</tr>
</tbody>
</table>
Changing the lock state

When to use

Use this procedure to lock a certain user out of the network element. The profile of the user will still exist, but the user will not be able to login.

Related information

A related procedure is Viewing Access Control Parameters.

Before you begin

Changing of the lock state can only be done when logged in as administrator.

Procedure

Follow this procedure to change the lock state for a specific user role.

   
   **Result:** The Access Control Parameters window appears.

2. Click on the capability that needs to be edited. If there are more users than can fit in the window, click on the scroll buttons (the arrow button) and scroll to the desired user.

3. Click **Edit**.
   
   **Result:** The Edit Access Control Parameters window appears.

4. Either tick or untick **Lock Access** and click **OK**.
   
   **Result:** The Access Control Parameters window reappears.

5. Click **Close**.
   
   **Result:** The Access Control Parameters window disappears.

**END OF STEPS**
Parameters for changing the lock state

**Lock state**

Specifies whether the user is locked. The value is either locked or unlocked.

**Capability**

This field lists the user roles. The possible values are described in the table below:

<table>
<thead>
<tr>
<th>Capability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>The user can perform all ITM-CIT administration tasks and configure a network element.</td>
</tr>
<tr>
<td>Config</td>
<td>The user can perform all transmission related tasks and retrieve and edit all network element related data.</td>
</tr>
<tr>
<td>View</td>
<td>The user can only view the network element configuration, it cannot be altered.</td>
</tr>
</tbody>
</table>

**Lock access**

Checking this box will lock a selected user (capability) out of the network element. The profile of the user still exists, but the user will not be able to log in.
Change the inactivity time

Overview

Purpose

The purpose of this procedure is to change the inactivity time for the different user roles.

Contents

<table>
<thead>
<tr>
<th>Changing the inactivity time</th>
<th>3-9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters for changing the inactivity time</td>
<td>3-10</td>
</tr>
</tbody>
</table>
Changing the inactivity time

When to use

Use this procedure to change the inactivity time, and by specifying after which time a user will be logged out do not do any action with CIT. If the value is 0, the user will never be logged out.

Related information

A related procedure is viewing access control parameters.

Before you begin

Changing of the lock state can only be done when logged in as administrator.

Procedure

Follow this procedure to change the inactivity time:

   
   **Result:** The Access Control Parameters window appears.

2. Click on the capability that needs to be edited. If there are more users than can fit in the window, click on the scroll buttons (the arrow button) and scroll to the desired user.

3. Click **Edit**.

   **Result:** The Edit Access Control Parameters window appears.

4. Change the **Inactivity time**. This can be done by deleting the old time and filling in a new time. It can also be changed by clicking on the increase or decrease button (the arrow buttons). Click **OK** to set the changes.

   **Result:** The Access Control Parameters window reappears.

5. Click **Close**.

   **Result:** The Access Control Parameters window disappears.

**END OF STEPS**
Parameters for changing the inactivity time

Lock state

Specifies whether the user is locked. The value is either locked or unlocked.

Capability

This field lists the user roles. The possible values are described in the table below:

<table>
<thead>
<tr>
<th>Capability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>The user can perform all ITM-CIT administration tasks and configure a network element.</td>
</tr>
<tr>
<td>Config</td>
<td>The user can perform all transmission related tasks and retrieve and edit all network element related data.</td>
</tr>
<tr>
<td>View</td>
<td>The user can only view the network element configuration, it cannot be altered.</td>
</tr>
</tbody>
</table>

Inactivity time

Defines after which time the workstation will be locked if the user is inactive. The value is an integer between 0 and 60. If the value is 0, the user will never be logged out.
Configure or change a password

Overview

Purpose

The purpose of this procedure is to change or configure the password used when logging in to a NE.

Contents

<table>
<thead>
<tr>
<th>Configuring or changing a password</th>
<th>3-12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters for configuring or changing a password</td>
<td>3-13</td>
</tr>
</tbody>
</table>
Configuring or changing a password

When to use

Use this procedure to change or configure the password for the different user roles (view, config, or admin). The use of a password is optional.

Related information

The procedure login to a network element is related.

Before you begin

This procedure can only be performed when logged in as an administrator.

Procedure

Follow this procedure to configure or change a password for the different user roles:

   
   **Result:** The Access Control Parameters window appears.

2. Select the capability to edit and click **Edit**.
   
   **Result:** The Edit Access Control Parameters window appears.

3. Enter the new password in the Enter Password field. Retype the password in the Confirm Password field and click **OK**.
   
   **Result:** If the two passwords are the same and legal: at least have six letters, the new password is set and the Access Control Parameters window reappears. If the passwords did not match, an error message is displayed and the screen is left intact.

4. Click **Close**.
   
   **Result:** The Access Control Parameters window disappears.

END OF STEPS
Parameters for configuring or changing a password

Lock state

Specifies whether the user is locked. The value is either locked or unlocked.

Capability

This field lists the user roles. The possible values are described in the table below:

<table>
<thead>
<tr>
<th>Capability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>The user can perform all ITM-CIT administration tasks and configure a network element.</td>
</tr>
<tr>
<td>Config</td>
<td>The user can perform all transmission related tasks and retrieve and edit all network element related data.</td>
</tr>
<tr>
<td>View</td>
<td>The user can only view the network element configuration, it cannot be altered.</td>
</tr>
</tbody>
</table>

Enter password

Sets the password for the selected capability.

Confirm password

Field to confirm the password typed in the enter password field.
Force a logout

Overview

Purpose

The purpose of this procedure is to force a specific user role to logout from an NE.

Contents

<table>
<thead>
<tr>
<th>Forcing a logout</th>
<th>3-15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters for forcing a logout</td>
<td>3-16</td>
</tr>
</tbody>
</table>
Forcing a logout

When to use

Use this procedure to force a session to logout from an NE. This action can only be performed by an administrator.

Related information

There is no information related to this procedure.

Before you begin

This procedure can only be performed by an administrator.

Procedure

Follow this procedure to force a session to logout:

   Result: The CIT Access List window appears.

2. Select the session that is to logout.

3. Click Force Logout.
   Result: A message will appear on the screen with the lines:
   Are you sure you wish to complete this operation? This will terminate the selected session. Do you want to proceed?

4. Click Yes.
   Result: The selected session is terminated.

END OF STEPS
Parameters for forcing a logout

NE name
Displays the name of the network element.

Force logout
Forces a session to logout.

Capability
This field lists the user roles. The possible values are described in the table below:

<table>
<thead>
<tr>
<th>Capability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>The user can perform all ITM-CIT administration tasks and configure a network element.</td>
</tr>
<tr>
<td>Config</td>
<td>The user can perform all transmission related tasks and retrieve and edit all network element related data.</td>
</tr>
<tr>
<td>View</td>
<td>The user can only view the network element configuration, it cannot be altered.</td>
</tr>
</tbody>
</table>

Lock state
Specifies whether the user is locked. The value is either locked or unlocked.

Access start time
Displays the time and date of the login of the displayed session.
4 Management communication setup

Overview

Purpose
The purpose of management communication setup is to provision the Data Communication Network (DCN) parameters for a network element.

Objective
The objective of provisioning the DCN parameters is to optimize the communication between network elements and the management system.

Outcome
An optimized DCN in which the exchange of routing data is minimized with full management of NEs.

Intended use
This chapter explains the concepts of provisioning the DCN. After the concepts the procedures used for DCN Management are described.

Contents

<table>
<thead>
<tr>
<th>Concepts</th>
<th>4-3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic DCN principles</td>
<td>4-4</td>
</tr>
<tr>
<td>DCN configurations</td>
<td>4-7</td>
</tr>
<tr>
<td>DCN addresses</td>
<td>4-11</td>
</tr>
<tr>
<td>NSAP address format</td>
<td>4-12</td>
</tr>
<tr>
<td>Data communication channels</td>
<td>4-15</td>
</tr>
<tr>
<td>Dual stack with tunneling (DSwT)</td>
<td>4-18</td>
</tr>
<tr>
<td>Example of dual stack with tunneling</td>
<td>4-24</td>
</tr>
</tbody>
</table>
Management communication setup

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSwT tunnel auto provisioning (TAP)</td>
<td>4-28</td>
</tr>
<tr>
<td>DSwT connecting areas with manual TAP tunnels</td>
<td>4-30</td>
</tr>
<tr>
<td>Partition repair</td>
<td>4-31</td>
</tr>
<tr>
<td>Partition repair guidelines</td>
<td>4-33</td>
</tr>
<tr>
<td><strong>Configuring a Data Communication Network (DCN)</strong></td>
<td>4-36</td>
</tr>
<tr>
<td>Create new or modify existing DCC terminations</td>
<td>4-37</td>
</tr>
<tr>
<td>Provisioning DCN information</td>
<td>4-39</td>
</tr>
<tr>
<td>Parameters for provisioning DCN information</td>
<td>4-41</td>
</tr>
<tr>
<td>Managing the DCC</td>
<td>4-44</td>
</tr>
<tr>
<td>Parameters for managing the DCC</td>
<td>4-46</td>
</tr>
<tr>
<td>Creating a transparent DCC cross-connection</td>
<td>4-47</td>
</tr>
<tr>
<td><strong>Procedures regarding login into remote NEs</strong></td>
<td>4-49</td>
</tr>
<tr>
<td>Adding a remote accessible NE to the configured nodes list</td>
<td>4-50</td>
</tr>
<tr>
<td>Editing remote NEs in the configured nodes list</td>
<td>4-52</td>
</tr>
<tr>
<td>Parameters for adding and editing remote logins in the configured nodes list</td>
<td>4-54</td>
</tr>
<tr>
<td>Remote login via configured nodes list</td>
<td>4-55</td>
</tr>
<tr>
<td>Remote login via neighbors option</td>
<td>4-57</td>
</tr>
<tr>
<td>Remote login via Area option</td>
<td>4-59</td>
</tr>
<tr>
<td><strong>Provision NE tunnel information</strong></td>
<td>4-61</td>
</tr>
<tr>
<td>Editing provisioned IP parameters</td>
<td>4-62</td>
</tr>
<tr>
<td>Adding manual route</td>
<td>4-63</td>
</tr>
<tr>
<td>Editing local/manual route</td>
<td>4-64</td>
</tr>
<tr>
<td>Editing TAP properties</td>
<td>4-65</td>
</tr>
<tr>
<td>Parameters for provisioning NE tunnel information</td>
<td>4-67</td>
</tr>
<tr>
<td><strong>Provision SNMP management</strong></td>
<td>4-70</td>
</tr>
<tr>
<td>Provision SNMP management</td>
<td>4-71</td>
</tr>
</tbody>
</table>
Concepts

Overview

Purpose

This section explains the concepts of provisioning the Data Communications Network (DCN). To complete the procedures in this chapter, the user should first be acquainted with the concepts contained in this section.

Contents

<table>
<thead>
<tr>
<th>Concept</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic DCN principles</td>
<td>4-4</td>
</tr>
<tr>
<td>DCN configurations</td>
<td>4-7</td>
</tr>
<tr>
<td>DCN addresses</td>
<td>4-11</td>
</tr>
<tr>
<td>NSAP address format</td>
<td>4-12</td>
</tr>
<tr>
<td>Data communication channels</td>
<td>4-15</td>
</tr>
<tr>
<td>Dual stack with tunneling (DSwT)</td>
<td>4-18</td>
</tr>
<tr>
<td>Example of dual stack with tunneling</td>
<td>4-24</td>
</tr>
<tr>
<td>DSwT tunnel auto provisioning (TAP)</td>
<td>4-28</td>
</tr>
<tr>
<td>DSwT connecting areas with manual TAP tunnels</td>
<td>4-30</td>
</tr>
<tr>
<td>Partition repair</td>
<td>4-31</td>
</tr>
<tr>
<td>Partition repair guidelines</td>
<td>4-33</td>
</tr>
</tbody>
</table>
Basic DCN principles

Purpose

This subsection serves as an entry point, it describes the basic DCN principles. The following subsection describes common DCN configurations. DCN configuration guidelines for 1643 AM products, NSAP address formats, and other related information are provided thereafter.

A Data Communication Network (DCN) is used for the exchange of management data. This section provides an overview of the Data Communication Network and describes the type of communication between the nodes in the network and the used protocols.

SDH management network

The SDH management network is an overlay of the transmission network. The Element Management System (EMS) and the Network Elements (NEs) together are the nodes of this network. The 10/100BaseT and Data Communication Channel (DCC) provide the physical connection between the nodes.

DCN physical components

The figure below illustrates a Data Communications Network (DCN) as defined by the Open Systems Interconnection (OSI) model. This figure refers to the physical components and connections in the DCN. It does not give information on the logical configuration of the DCN.
The figure of the OSI-DCN consists of two LANs and a number of DCC channels in an SDH transmission network with point-to-point configuration and two rings connected to an EMS. The management system server is used as an EMS. The management system is connected to the transmission network via Gateway Network Elements (GNEs) by the LAN. The network elements are connected to each other by DCC channels.

**LCN**

In the case where there is no DCC connectivity between nodes, a Local Communications Network (LCN) can be used to connect the nodes to each other. See the LCN on the right side of the figure.

**DCN communication protocols**

Communication protocols used in the Data Communications Network (DCN) between the nodes include:

- Ethernet (on the 10BaseT) LAPD (on the DCC channels)
- OSI Network Protocol (DCN wide)

The OSI Network Protocol (OSI-DCN) is used for routing management data between nodes in the DCN.
ISO-OSI network protocol

The network protocol used between nodes is the ISO-OSI Network Protocol (ISO/IEC 8648). According to this protocol a node in the network can behave as an End System (ES) or as an Intermediate System (IS), sometimes called a router.

End systems

Nodes behaving as End Systems perform no forwarding of data packets. They communicate with each other on an end-to-end basis via Intermediate Systems.

Intermediate systems

Intermediate Systems are used for routing data between nodes and (sub) networks. The End System - Intermediate System (ES-IS) protocol is responsible for the exchange of data between an End System and Intermediate System. A network element can act both as an End System as well as an Intermediate System. However, an ITM-SC, for example, can only act as End System.

IS - IS protocol

The Intermediate System to Intermediate System (IS-IS) protocol is used between Intermediate Systems in the DCN. The IS-IS protocol maintains the IS Routing Information Base (RIB). The information in this information base is used for the routing of management data packets in the DCN by the Intermediate Systems.

Routing information base and LSPs

Each RIB comprises a number of tables. These tables contain information on Network Service Access Point (NSAP) addresses of nodes in the network and ports of the IS through which these nodes can be reached. Intermediate Systems exchange routing information regularly with one another as part of the IS-IS protocol by the use of Link State Protocol Data Units (LSPs).

The LSPs contain the information on the NSAP addresses of nodes used in the tables of the RIBs.
DCN configurations

Hierarchical routing
Hierarchical routing is used for large networks when the number of NSAP entries in the RIB databases of the Intermediate Systems is too large. When this happens, it causes an exponential increase of exchanged LSPs between Intermediate Systems. This in turn causes the performance of the DCN to decrease due to the computation of the shortest path first algorithm.

Hierarchical routing definition
In hierarchical routing, the DCN addressing domain is divided into a number of areas. Each area is assigned a unique identifier. The value of the Area Identifier of each node's NSAP address is set according to the area the node is part of.

Level 1, Level 2 definition
Each area contains a number of:
- End Systems,
- first level (Level 1) Intermediate Systems and,
- second level (Level 2) Intermediate Systems.

Level 1 Intermediate Systems provide interconnectivity between nodes within the same area. Level 2 Intermediate Systems provide interconnectivity between nodes belonging to different areas.

Level 2 subdomain
The complete set of Level 2 Intermediate Systems is also referred to as the Level 2 Subdomain. All areas in a network are connected via the Level 2 Subdomain.

Area-divisioning of a DCN
Partitioning is configuration of the DCN in such a way that the exchange of LSPs between Intermediate Systems is limited.

When networks are partitioned into areas, the RIB database(s) in the systems are much smaller and hence the routing overhead is significantly reduced. Intermediate Systems in an area only exchange information (LSPs) on nodes with other systems in their own area. Information on other areas is exchanged by Level 2 Intermediate Systems only and maintained by the Level 2 Intermediate Systems of the area.

In this way, the data management load in the network is strongly reduced, while keeping the dynamic re-routing capabilities of Intermediate Systems in case of failures intact. It is important to notice that although the DCN is divided into areas, ES-ES communication between all nodes in the DCN is still possible.
The figure below illustrates how a network can be partitioned into areas, connected by Level 2 Intermediate Systems. Each area has at least one Level 2 Intermediate System assigned and can have a number of Level 1 Intermediate Systems and End Systems.

Routing management data

The following scenario describes routing management data in a divisioned network. Suppose a node A wants to send messages to another node. If this node is in its own area (determined by the Area Id part in the Area Address field), the messages from A to this particular node (B) are routed directly using the Level 1 Intermediate System. (See previous figure)

Alternatively, if the required destination is in a different area (C), the messages are sent to a second, higher level (Level 2) Intermediate System. This Intermediate System routes the messages coming from node A to other Level 2 Intermediate Systems until they reach a Level 2 Intermediate System attached to the destination area of C. From there it is routed within the area using Level 1 Intermediate Systems to node C.

Notice that in both of the above cases the ES-ES communication between nodes in the same or in different areas is still possible.
OSI-DCN networks types

In general the OSI-DCN network can be classified in three types:

- Undivided
- IS-IS Clustered
- IS-IS Area Divided network

The three types are illustrated in the figure below:

**Undivided network definition**

An undivided network consists of a single routing domain. There is no division between the nodes at the network protocol level. All nodes in the network and especially the Intermediate Systems can exchange routing information with each other. Although a network element can only be managed by one ITM-SC at a time, the IS-IS protocol is running between all nodes in the network. This leads to the exchange of LSPs between all Intermediate Systems of the network.

**IS-IS clustered DCN**

In order to avoid the decrease of performance, the exchange of LSPs over a certain port can be disabled in some nodes. A node can exchange LSPs over its DCC or LAN (10BaseT) ports. The exchange of LSPs over the DCC channel can be disabled. However, this also prevents the exchange of management data over this port and prevents the use of this DCC port for re-routing in case of a failure of another port.

**Disabling exchange of LSPs**

Another option is to disable the exchange of LSPs over the LAN (10BaseT) port. This can be done by choosing the IS to have a NO-IS-IS port. This node is also referred to as a NO-IS-IS (gateway) node. If this is done for all Intermediate Systems on a LAN, the
LAN becomes a NO-IS-IS LAN. In NO-IS-IS LANs, the IS-IS protocol is not run on the 10BaseT. This prevents the exchange of LSPs between Intermediate Systems on a 10BaseT. This results in a network which comprises several clusters of nodes. Between the clusters there is no IS-IS traffic.

**ES-ES communication**

Within a cluster the ES-ES, ES-IS, and IS-IS communication is still possible. There is however no communication possible between nodes in different clusters. For example a Craft Interface Terminal (CIT) can be connected to a node in a cluster for maintenance activities on nodes within a cluster. However, it is then not possible to do a remote login from this node to a node of another cluster.

**Management system connections**

The management system connected to the 10BaseT can still communicate with all nodes in the clusters since the ES-IS protocol on the 10BaseT is not disabled. Important to notice is that the nodes in a Remote Cluster lose their association with the management system when NO-IS-IS is chosen on the gateway node of the remote cluster. It is advised to connect the management system to the 10BaseT that connects the clusters to each other and to assign NO-IS-IS only to nodes on this LAN.

**IS-IS area divided DCN**

The division of the DCN in areas by introducing Level 2 Intermediate Systems is similar to disabling the IS-IS protocol over the 10BaseT port of nodes, as described earlier. Similar to clustering, the exchange of Level 1 LSPs between Intermediate Systems in different areas is prevented. However Level 2 LSPs are still exchanged between Level 2 Intermediate Systems.
DCN addresses

The system has two addresses in the DCN:

- Ethernet address
- NSAP address

**Ethernet address**

The Ethernet address is the unique 6-byte address of a Network Element. Sometimes it is also referred to as the hardware or physical address of the node. The Ethernet address has only local meaning on the LAN and cannot be used for routing purposes. It does not contain the information on where the node is in the data communications network.

**NSAP address**

The Network Service Access Point (NSAP) address is used by the network protocol for location information. The NSAP address of a node is its DCN wide identifier which uniquely identifies the node in the network.
NSAP address format

Background
The following three NSAP formats can be distinguished:

- ISO-DCC NSAP address format. This format is used by most Alcatel-Lucent network element types in the network,
- Local-Lucent NSAP address format. This format is also used by some Alcatel-Lucent network element types in the network,
- Flexible NSAP address format. An alternative to the previous two formats.

Although different NSAP address formats exist, preferably all nodes in a network should use the same address format.

ISO-DCC NSAP address format
The ISO-DCC NSAP address format is presented below.

ISO-DCC NSAP address fields
This ISO-DCC NSAP address format is hierarchical and consists of the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Function It Provides</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area Address</td>
<td>Has three parts:</td>
</tr>
<tr>
<td></td>
<td>- AFI (Authority and Format Identifier) is equal to 39 (HEX).</td>
</tr>
<tr>
<td></td>
<td>- The fixed part is equal to 00008000000000000000 (HEX).</td>
</tr>
<tr>
<td></td>
<td>- Area Id indicates the area to which a node belongs and thus its logical location in the network.</td>
</tr>
<tr>
<td>System Identifier (SID)</td>
<td>Identifies the node. In most network element types, the Ethernet address is copied into the SID address field and this makes the NSAP address unique throughout the DCN.</td>
</tr>
</tbody>
</table>
### Field Function It Provides

<table>
<thead>
<tr>
<th>Field</th>
<th>Function It Provides</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selector (Sel)</td>
<td>Set to 01 (HEX) for the network elements.</td>
</tr>
</tbody>
</table>

**Local-Lucent NSAP address format**

The Local-Lucent NSAP address format is presented below.

```
  1 Byte  2 Bytes  6 Bytes  1 Byte
  AFI     Area Id   System Id  Sel

  Area Address
  3 Bytes

  Node Address
  10 Bytes
```

**Local-Lucent NSAP address fields**

The Local-Lucent NSAP address format has the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Function It Provides</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area Address</td>
<td>Has two predefined parts:</td>
</tr>
<tr>
<td></td>
<td>• AFI (Authority and Format Identifier) field, equal to 49 (HEX).</td>
</tr>
<tr>
<td></td>
<td>• Area Id indicates the area to which a node belongs and thus its logical location in the network.</td>
</tr>
<tr>
<td>System Identifier (SID)</td>
<td>Identifies the node. In most network element types, the Ethernet address is copied into the SID address field and this makes the NSAP address unique throughout the DCN.</td>
</tr>
<tr>
<td>Selector (Sel)</td>
<td>Set to 01 (HEX) for the network elements.</td>
</tr>
</tbody>
</table>

There is no fixed part in this address type.

**Flexible NSAP address format**

The flexible NSAP address format is presented below.
Flexible NSAP address fields

The flexible NSAP address has the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Function It Provides</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area Address</td>
<td>Has two provisionable parts:</td>
</tr>
<tr>
<td></td>
<td>• AFI (Authority and Format Identifier) field, which may vary between 10 and 99 (HEX).</td>
</tr>
<tr>
<td></td>
<td>• Flexible part, which may vary from 0 to 12 bytes.</td>
</tr>
<tr>
<td>System Identifier (SID)</td>
<td>Identifies the node. In most network element types, the Ethernet address is copied into the SID address field and this makes the NSAP address unique throughout the DCN.</td>
</tr>
<tr>
<td>Selector (Sel)</td>
<td>Set to 01 (HEX) for the network elements.</td>
</tr>
</tbody>
</table>

In this way, the flexible NSAP address can vary from 8 to 20 bytes.

Notice that the flexible NSAP address format can be used to derive the other formats.
Data communication channels

Data Communication Channels (DCC)

The Data Communication Channels (DCC) are part of the Data Communications Network (DCN). The channels are used to exchange management data between the management system and the Network Elements. The channels are also used for communication between the different Network Elements (for example remote logins). DCC channels (D1 - D12) are provided by reserved bytes in the regenerator section (RS) and the multiplexer section (MS) overhead of the STM-N signal.

Transparent DCC

The Transparent DCC Cross-Connect feature allows to transparently pass-through certain DCC channels which cannot or should not be processed by the system.

Transparent DCC Cross-Connect are to be used when there is a router on one side of the SDH/SONET network which uses the DCC to transport some IP-based protocol to a router on the other side of the network. This feature can be used to avoid interworking with equipment from a different vendor in a common routing domain.

The Transparent DCC Cross-Connect path is transparent. This means that no processing at all will be done as the data travels along the path. Therefore, the entire Transparent DCC Cross-Connect path counts as a single hop for the network elements at the ends of the path.

The Transparent DCC Cross-Connections are completely independent from the Transmission Cross-Connections. There is no relation between the number of "normal" (terminated) DCC channels and the number of Transparent DCC channels. They are taken from different pools.

Therefore, enabling a "normal" (terminated) DCC channel does not reduce the number of available Transparent DCC channels, and vice versa.

For each DCC channel, Transparent DCC Crossconnection and traditional DCC processing on the CTL/DCF are mutually exclusive.

Functional requirements

The following functional requirements to the transparent DCC channels:

- the number of bidirectional transparent DCC channels is limited to 25.
- it is possible to use transparent DCC cross-connect for RS-DCC and MS-DCC.

Establishing Transparent DCC Crossconnection

Transparent DCC cross connection are to be established by identification of the two ports of an NE that are to be cross-connected and the DCC type (RS-DCC or MS-DCC).
The LAPD protocol, which controls communication between the network elements, operates in either of the following modes:

- **Network Side**
  
  The LAPD is assigned as Network. This mode complies with the standards and interoperates successfully with other LAPDs operating in user_side mode.

- **User Side**
  
  The LAPD is assigned as User. This mode complies with the standards and interoperates successfully with other LAPDs operating in network_side mode.

Please note that the DCCs work according to the master/slave principle, i.e. the LAPD modes of two interconnected SDH ports must be set differently. A corresponding “User-Network Side Failure” alarm will be generated if the LAPD mode is the same at both ends of a DCC.

### AITS and UITS supported

1643 AM or 1643 AMS network elements support the Acknowledged Information Transfer Service (AITS) and the Unacknowledged Information Transfer Service (UITS) as the basis for the LAPD or LinkID protocol with the UITS mode being the default mode of operation. AITS should only be used if required by other NE types. UITS is furthermore used for link protocol at the same time when AITS is chosen.

### AITS and UITS functional principles

In the LAPD protocol, all PDUs are sent with a checksum to verify that the data has not been corrupted during the transmission over the DCC link. If a PDU is received with a bad checksum, it is not acknowledged and will be resent:

- In the **Unacknowledged Information Transfer Service** (UITS) (default), corrupted PDUs are ignored and no further actions taken. Upper layers of the OSI stack are responsible for recovery actions.

- In the **Acknowledged Information Transfer Service** (AITS), PDUs are numbered and transmitted sequentially, and acknowledgment PDUs are sent back from the receiver to the sender. If a PDU is lost, that is, if the sender gets no acknowledgment, the PDU is retransmitted.
Functional principle of the AITS

Node A  PDU 3 corrupted  Node B

Ack. 1  Ack. 2

retransmission of 3

no  Ack. 3

Ack. 3
Dual stack with tunneling (DSwT)

Introduction

The Dual Stack with Tunneling (DSwT) feature provides a way to manage IP devices through the DCN network.

An IP EMS (Element Management System) is used to manage NEs which use IP based management protocols (IP NEs).

Dual stack

Dual Stack means adding an IP Router stack to an existing OSI stack.

Tunnel

A tunnel is a unidirectional path through the OSI domain capable of transporting IP packets. The tunnel consists of an endpoint in the OSI domain (NSAP) and the encapsulation/decapsulation mechanism to transport an IP packet in an OSI network. The actual path taken by the encapsulated IP packet is completely determined by the normal OSI routing mechanisms.

TCP/IP tunneling

This feature is intended to forward IP traffic between IP managed equipment at the borders of the SDH network and their IP-based management system.

In order to use the tunneling feature it is necessary to provision the following using the ITM-SC or the ITM-CIT:

- map a “tunnel far-end” to each (masked) IP-destination, where all IP-addresses are implied that fulfill the most significant bits (non-masked) part of the IP-destination. Only the far-end of a tunnel needs to be identified through its NSAP address (the near-end is implicitly this NE). Resources for a maximum of 50 tunnels must be provided.
- provision its own IP-address in the NE.
- enable IP routing.
- add routing information for forwarding towards an external IP router, when the IP-destination is not connected to the QLAN of the NE.
- enable (when desired) automatic creation of tunnels, towards all other NE’s in this area that have automatic creation enabled. Note that manual provisioning of tunnels as in ”1” is needed for a tunnel that spans a number of areas, while subsequent tunneling within the destination area can make use of automatically created tunnels.

Network architecture

The network architecture in the figure is used in this example.
IP tunnel architecture

The IP Tunnel architecture in the figure is used in this example.

Tunnel configuration

A tunnel can be seen as a set of two static routing entries in nodes on the edge of the OSI network and the corresponding static entries in the routing table. The term tunnel may be misleading because it is often associated with connections which must be set up in advance. In this case, only some routing and mapping information needs to be provisioned and no communication between two systems is needed to set up the “tunnel”
between them. To avoid confusion, it is better to speak of encapsulation and to think of the OSI network as a non broadcast multiple access (NBMA) subnetwork within the IP network.

The NEs need to be configured with one IP address on the LAN side, connected to the IP subnet with the IP NEs. The LAN can be used for both OSI and IP traffic. The same Ethernet address will be used for both protocols.

**IP encapsulation**

The IP packets are encapsulated in Connectionless Network Protocol (CLNP) packets which are routed through the OSI-only node which routes the CLNP packets as normal, totally oblivious of the CLNP packets contents.

**IP and DCC**

A benefit of the tunneling approach, is that IP need not to be carried on the DCC. Only the CLNP packets (possibly carrying IP) go on to the DCC.

**IP routing**

In the Dual Stack with Tunnelling configuration, a second network layer entity (the IP router) is added alongside the existing OSI network layer entity (CLNP). The CLNP entity has the routing tables and the mechanisms to automatically populate them - namely the IS-IS and ES-IS dynamic routing protocols.

This is not the case for the IP routing tables since there is no IP dynamic routing protocol to populate the IP routing tables. IP routing tables have to be manually provisioned by the operator.

**DSwT routing table**

A Routing Table, IP, or OSI, is divided into two columns:

- “Final Destinations” of each Network Node,
- for each Final Destination, the identity of the “Next Hop” which is the next network node in the path towards the Final Destination.

The table below shows a simplified IP routing table for IP router in a DSwT stack. It is divided into two main columns. These two parts of the routing table will be discussed separately.

<table>
<thead>
<tr>
<th>Final Destination</th>
<th>Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>130.44.5.0/24</td>
<td>LAN 0</td>
</tr>
<tr>
<td>120.23.4.0 / 24</td>
<td>LAN 0</td>
</tr>
<tr>
<td></td>
<td>130.44.5.8</td>
</tr>
</tbody>
</table>
Final destination

This column of the Routing Table is a list of all the final destination nodes. When a packet is received at this node, then the destination address in that packet is checked against the list of destinations in the destination column of the routing table. If there is no entry in the table for the packet destination, then the node will not know how to route the packet and will execute the error procedure (which involves discarding the packet and trying to send an error message packet back to the source). If a match is found, the next hop towards the destination can be looked up in the “Next Hop” column.

IP prefixes

An IP Prefix is a mechanism of identifying a collection of IP addresses with some common root. The general principle is to choose a mask which identifies a suitable first part of the IP address which summarizes a number of addresses. For example, the addresses 120.10.2.1, 120.10.2.5 and 120.10.2.13 can be summarized by the IP Prefix: 120.10.2.0 / 24. The 24 identifies the first 24 bits of the address. Summarizing IP addresses is a very powerful way to reduce the number of entries in a Routing Table.

Next hop

Two pieces of information are needed in order to identify the next hop node:
• on which subnetwork (for example on which exit port) is the next hop node,
• which node on that subnetwork is the next hop.

This is shown in the figure below.
To send a packet to the destination Dest, the Source must identify the node Next Hop. This is identified by the subnetwork (on Port 2 of Source) and then the node on that subnetwork (identified by B). In OSI terminology the address B is known as a Subnetwork Point of Attachment (SNPA), which is the point that the node is attached to the subnetwork.

The second column in the Routing Table is the next hop and is divided into two parts:

- the Next Hop Subnetwork
- the Next Hop Node.

Next hop subnetwork

A router, by its nature, must be connected to multiple subnetworks. Each subnetwork is connected to a separate port on that router. The Next Hop Port identifies the subnetwork to exit this node for the next hop towards the destination.

For the DSwT IP router entity, there are two types of port/subnetwork:

1. LAN: This is the Ethernet (common subnetwork type for IP routers).
2. CLNP-Tunnel: This is a logical subnetwork created by the OSI CLNP network itself. From the IP router perspective, this subnetwork is seen as a “Non-Broadcast Multiple Access” (NBMA) subnetwork. The IP router simply sees all the neighbor IP router entities connected together to this NBMA. It does not see any of the OSI CLNP nodes inside this network.

Next hop node

Once the correct exit port (subnetwork) has been identified, the correct node on that subnetwork must be identified by its SNPA. This could be an Ethernet address (for a LAN), or an X.121 address for an X.25 subnetwork. When the subnetwork is a point-to-point link then there is no need to identify the Next Hop. There are various ways to identify the Next Hop Node, and they depend on the type of subnetwork that node is attached to. The following table provides an overview:
### Management communication setup

#### Concepts

<table>
<thead>
<tr>
<th>Subnetwork Type</th>
<th>Next Hop Node (Identity Type)</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN</td>
<td>IP address or none if the destination is actually on this LAN (there is no Next Hop Node).</td>
</tr>
<tr>
<td>CLPN-Tunnel</td>
<td>NSAP</td>
</tr>
</tbody>
</table>
Example of dual stack with tunneling

Network architecture

The network architecture in the figure is used in this example.

Routing tables for IP host nodes

Not only IP router nodes but also IP host nodes have Routing Tables. The Routing Table is used for every IP packet generated by this IP host. As can be seen in the table below, each node has two routing entries. These two routing entries will be discussed separately.

The routing tables for nodes I1, I2, I3, I4, and I5, see the previous figure:

<table>
<thead>
<tr>
<th>IP Host Node</th>
<th>Final Destination</th>
<th>Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Port</td>
</tr>
<tr>
<td>I1</td>
<td>120.2.1.0 / 24</td>
<td>LAN</td>
</tr>
<tr>
<td></td>
<td>0.0.0.0 / 0</td>
<td>LAN</td>
</tr>
<tr>
<td>I2</td>
<td>120.1.2.0 / 24</td>
<td>LAN</td>
</tr>
<tr>
<td></td>
<td>0.0.0.0 / 0</td>
<td>LAN</td>
</tr>
<tr>
<td>I3</td>
<td>120.2.3.0 / 24</td>
<td>LAN</td>
</tr>
<tr>
<td></td>
<td>0.0.0.0 / 0</td>
<td>LAN</td>
</tr>
</tbody>
</table>
### Local route

The first routing entry in the IP host node routing table is called the Local Route and is often generated automatically after the node’s interface is configured with an IP address and a subnet mask. This IP Prefix is simply the subnet address (IP address with subnet mask) of the locally attached subnet. This entry says that every packet generated with destination address of the local subnet will be sent out on the local LAN. There is no “Next Hop Node”. Instead <Local Subnet> is simply a flag which says to take the destination IP address from the IP packet and resolve it directly on the local LAN. Notice this routing entry would be essential in nodes I4 and I5 if they wished to communicate with each other. There is one Local Route entry for each interface. These IP Hosts only have a single interface and so only a single Local Route entry.

### Default route

The second routing entry in the IP host node routing table is the IP Prefix 0.0.0.0 / 0, which is called the Default Route. This prefix will match every destination IP address and so in effect, this routing entry says that every packet generated will be sent to the specified next hop. In all cases, the specified next hop is the DSwT node which is identified by its IP address. Notice that routes for the local subnet also match the Default Route. Of course this is not the intention so there is another essential rule for all routing tables, which says that match with the longest prefix route must be selected. This is fundamental to IP Routing Tables and must be followed in all cases.

### Routing table for external routers

For external routers there are two possible hop ports (LAN 1 and LAN 2). The <Local subnet> routes can be added automatically when the router interfaces are configured (assigned IP address and subnet mask).

The routing tables for routers C1 and C2, see the previous figure:
Routing table for DSwT nodes

These Routing Tables have been completed with a specific application in mind: namely the management of IP based fringe equipment. In this example, only routes between I1 and I2, I3, I4, I5 are necessary: I3 does not need to communicate with I2 for example. This has been done to minimize the routes in the routing table and give a realistic indication of what the operator must provision to get the application to work.

The routing tables for DSwT nodes D1, D2, D3, and D4, see the previous figure:
In the Routing Tables for DSwT nodes, the Subnet CLNP-Tunnel is seen for next hops across the OSI (CLNP) DCN. Whenever the subnet is a CLNP-Tunnel, the Next Hop Node is identified by the NSAP address of that node. As can be seen, nodes D2, D3, D4 have routes (tunnels) back to D1 only and D1 has routes to D2, D3, D4.

Notice nodes D1 and D4 have an extra route. This is because another router is involved; the extra route points to the subnet at the far side of the router. This route must be added since, unlike the Local Route, there is no way to add this route automatically (without a full blown Dynamic Routing Protocol).
DSwT tunnel auto provisioning (TAP)

Introduction

Provisioning all the entries in the Routing Tables of all the nodes can be a considerable effort and is error prone, particularly when networks comprise hundreds of nodes. It would be desirable to have a mechanism which reduces some of the necessary provisioning to alleviate this problem. Such a mechanism has been designed. It is an Alcatel-Lucent proprietary mechanism called “Tunnel Auto Provisioning” (TAP).

TAP principle

The principle behind TAP is that IP routes known by DSwT nodes at the edge of the OSI network are advertised across the OSI network to the other DSwT nodes which can then insert these routes into their own Routing Tables. This basic principal is illustrated in the figure below.

Example of two DSwT nodes advertising the IP networks they can reach. Each Node learns the others advertised routes it hears and places them in its Routing Table.
Notice that the advertising node is not limited to giving one IP prefix but could provide a list of all the IP prefixes it can reach, if appropriate, each one resulting in a routing table entry.
DSwT connecting areas with manual TAP tunnels

Introduction

The TAP mechanism does not work across IS-IS Areas because it distributes information using IS-IS Level 1 LSPs. However, it is likely to have a considerable number of nodes in the OSI network and multiple areas.

Connecting areas

To allow DSwT nodes to communicate across IS-IS Areas enjoying the benefits of the auto-provisioning, a pair of “tunnels” must be manually configured between the areas. This principle is illustrated in the following figure.

Connecting areas principle

A pair of provisioned “Tunnels” connecting any two nodes, one from each area, provides bi-directional communication between the Areas.

NOTE: TAP “Tunnels” are not transitive. That is a “Tunnel” connecting Areas A and B, and a “Tunnel” connecting Areas B and C does NOT connect Areas A and C. A separate “Tunnel” between Areas A and C is needed.
Partition repair

Partition-repair

The partition-repair is needed to allow management DCNs for large multi-ring networks to be designed such that single points of failure are avoided. The use of partition-repair is restricted to those cases where the current mechanisms cannot avoid a single point of failure, even though a physical backup route is available.

Partition-repair provides a way to enhance the robustness of the DCN by providing the capability to repair intra-area routing using connections via nodes outside the area. This is done by creating a path outside the area, between two level 2 nodes (which are provisioned to be partition capable level 2 nodes) that belong to distinct partitions of the same IS-IS area. Level 1 IS-IS PDUs and CLNP PDUs are encapsulated and transferred over the level 2 path.

Note that network element types that do not support partition-repair, can exist in the “repaired” areas; however, these network element types cannot be part of the level 2 repair path (they cannot be part of the level 1 tunnel through the level 2 domain).

A network element (NE) is a physical box that contains a physical piece of equipment. A network element can contain one or more nodes. A node is a logical part of the DCN and is the basic building block of the DCN. Both intermediate systems and end systems are considered to be nodes. Each node is identified by exactly one NSAP. An NSAP, or network service access point, is the address of a node. Each node has exactly one NSAP that is unique in the entire network (usually the NSAP is even globally unique). Routing and forwarding in each node of a network is done using the target NSAP.

The terminology that is used in relation to partition-repair requires some explanation. A node can be partition-repair capable, partition-repair compatible, and partition-repair designated. These terms are described below:

- A node is partition-repair capable if it is provisioned as such. Only possible end points of partition-repair tunnels need to be provisioned as partition-repair capable. Such possible end points must be attached level 2 nodes. (A level 2 node is attached if it can forward packets to a different area, even if the level 2 node itself is not on an area boundary).
- A node is partition-repair compatible if a partition-repair path can pass through the node. No provisioning is needed or required to make a node partition repair-compatible. Many of the older network element types, are not partition-repair compatible.
- A node is partition-repair designated if it is selected as such by all the other nodes in its area that are still connected to it via a level 1 path. The election is done by choosing one node from the set of still-connected nodes that are partition-repair capable. If a partition-repair designated node of a certain area learns (by listening to level 2 communication) that there is another partition repair designated node in the
same area, both of these nodes conclude that their area is partitioned. These nodes will then establish a partition-repair path between them. The partition-repair path is a virtual level 1 connection between the two partition-repair designated nodes that runs through the level 2 domain. Level 1 packets are tunneled through this virtual connection; this removes the area partitioning.
Partition repair guidelines

When to use partition repair

Only provision nodes to be Partition Repair Capable in an area, if a Single Point of Failure otherwise cannot be avoided for that area. If more than one Level-2 entry into an area is used, partition repair is a valid mechanism.

How to use partition repair

To allow the healing of a partitioned area, two nodes must be provisioned as Partition Repair Capable as follows:

- At the area boundary, connecting Level-2 node(s) in (an) other area(s)
- The potential virtual link (tunnel) should reduce the SPF’s in the area to a minimum.

In case an area is partitioned due to a single failure, the two partition repair capable level-2 nodes in each partition will establish a level-1 tunnel through the level-2 subdomain, in order to repair level-1 connectivity between all nodes in the two related partitions.
NE type restrictions

Observe the following NE type restrictions:

- All NE-types, managers, and other OSI nodes (like external OSI-routers) are allowed as Level-1 IS nodes or as ES-only nodes, in an area with Partition Repair Capable NE’s.

  When a repair tunnel is established, the partition repair designated NE’s will advertise information such, that the tunnel is identified as a normal level-1 route within the area.

- All NE-types and other OSI nodes (like external OSI-routers) are allowed as Level-2 nodes in the Level-2 subdomain, as long as they are not part of the shortest inter-area path between two Partition Repair Capable NE’s in an area.

  The network is expected to be designed for full management connectivity in case of a single failure. In case of two failures, including a partitioned area and a failure in the shortest potential tunnel route, the network is allowed to drop management connections. Therefore not all OSI-nodes in the Level-2 subdomain need to be partition compatible.
Large network restrictions

Observe the following restrictions regarding large networks:

- The manager connections that are tunneled through a Level-2 node in case of a single failure, are counted as connections and must therefore be subtracted (like all other rerouted connections through this node) from the maximum number as specified in S-111 in order to identify the maximum number of acceptable connections in the case that the network is in its normal (failure-free) state.

  If 50 manager connections can be tunneled in case of a failure, and 150 manager connections are forwarded in a failure-free network, through one of the nodes in the potential tunnel, the related node must be capable of forwarding 200 manager connections.

  The total number of managed NE’s in an area can be tunneled through the Level-2 subdomain with regard to the maximum number of manager connections that can be forwarded by a node. Only the shortest inter-area route between two Partition Repair Capable nodes in an area has to be taken into account.

- The manager connections that are received, encapsulated and forwarded into a partition-repair tunnel, are counted as normal connections. If 100 manager connections can be tunneled in case of a failure, the related partition designated node must be capable of forwarding 100 manager connections.

- All areas can be provisioned to have one or more Partition Repair Capable node(s).

  Each area with one or more Partition Repair Capable nodes requires an extra entry in the routing table (RIB), because of initial selection of a partition repair designated node per area.

- Avoid the use of partition repair capable NE’s in large areas.

  A DCN network design that selects small level-1 areas to use partition repair, while the large areas are rings that need no partition repair, will be easier to understand. Also it is easier to check that all rules are obeyed.

Partitioning restrictions

A maximum of nine partition repair capable NEs per area is allowed. This implies that the partition repair capable NEs can terminate a maximum of eight partition repair tunnels. A single cable cut may imply many fiber cuts, of which more than 7 of those fiber cuts may imply partitioning of the same area. A fiber cut between two DWDM nodes may imply a cut of many DCC channels. The Network design shall not use partition repair to cover such topologies.
Configuring a Data Communication Network (DCN)

Overview

Purpose

This section describes the individual procedures to be used to configure the Data Communication Network (DCN).

Contents

| Create new or modify existing DCC terminations | 4-37 |
| Provisioning DCN information | 4-39 |
| Parameters for provisioning DCN information | 4-41 |
| Managing the DCC | 4-44 |
| Parameters for managing the DCC | 4-46 |
| Creating a transparent DCC cross-connection | 4-47 |
Create new or modify existing DCC terminations

When to use

Use this procedure to create new or modify existing DCC terminations.

Related information

For related information, please refer to:
- “Concepts” (p. 4-3)

Before you begin

Prior to performing this task, you must have an overview of the current network topology.

Furthermore, you must:
1. log into the ITM® CIT, and
2. connect to the NE.

Required privilege codes

You must have at least a privilege code of:
- S1
to view the currently enabled DCC terminations,
- S4
to create new or modify existing DCC terminations.

Required equipment

The following equipment is required to perform this task:
- ITM® CIT

Instructions

Complete the following steps to create a new DCC termination or to modify an existing DCC termination.

1 Select **Management → Overlay Comms Networks → DCC** from the main menu.
   
   **Result:** The **DCC list** window is displayed.

2 In the **DCC list** window select the port for which you want to create a new DCC termination or to modify an existing DCC termination.
   
   Click on **Edit**.
Management communication setup
Configuring a Data Communication Network (DCN)

Create new or modify existing DCC terminations

---

**Result:** The Edit DCC window is displayed.

---

3. In the **Edit DCC** window either enable or disable DCC termination for the selected port by selecting the respective radio button.

---

4. In the **LAPD Side** group box, choose the **LAPD Role** (either **USER-SIDE** (default) or **NETWORK-SIDE**) by selecting the respective radio button.

---

5. In the **LAPD Mode** group box, choose the **LAPD Mode** (either **UITS** (default) or **AITS**) by selecting the respective radio button.

---

6. Click on **Ok**.

---

7. Provision the DCN information for the DCC termination.

   **Reference:** Refer to “Provisioning DCN information” (p. 4-39).

---

END OF STEPS
Provisioning DCN information

The purpose of this procedure is to view, provision, or modify the NE DCN information.

When to use

Use this procedure to view, provision or modify the DCN information.

Related information

Section DCN management concepts.

Before you begin

Before changing DCN information notice the following precautions:

- When the IS-IS parameters are changed this may cause the network element to restart, resulting in a temporary loss of association. If the network element is participating in a GR scheme this may cause an automatic protection switch. A warning message is displayed.
- If the values of the IS-IS parameters are incorrect this may cause instabilities in the DCN and may result in many network elements becoming unmanageable. A warning message is displayed.
- Do not create an area with the area ID 0000, because this is already the default area ID for all newly created NEs.
- Choosing the static value for the connection type option makes the gateway network element a single point of failure in the management of the network element.
- When the LAN IS-IS Level is set to None (NO-IS-IS) a network element cluster that is not directly connected to the management system LAN (10BaseT) may become unmanageable when None is chosen for the cluster gateway. None also prevents traffic from one cluster from being routed to another cluster over the LAN.
- The value of the designated router priority is composed in a specialized plan, so do not change it unless this plan is available.
- If an additional manual area address is provisioned when the computed area address table (CAAT) is full, this may cause a loss of entries in the CAAT which results in a loss of association. If the network element is participating in a GR scheme this may cause an automatic protection switch. A warning message is displayed.
- Before starting to change the provisioned network element information, all information about the DCN must be available.
Provisioning DCN information

Procedure

Complete the following procedure to view, provision, or modify the NE DCN information.

1. Select Management -> Overlay Comms Network -> DCN.
   
   **Result:** The Provisioned NE DCN Information window appears.

2. Click **Edit** to modify the DCN information.
   
   **Result:** The Edit Provisioned DCN Information window appears.

3. Set the DCN parameters as desired.
   
   **Result:** The DCN parameters are selected.
   
   **Reference:** The DCN parameters and their function are described in “Parameters for provisioning DCN information” (p. 4-41).

4. Click **OK** to confirm the current changes.
   
   **Result:** When the Area ID has been changed, a window will appear with the message:

   Changing the IS-IS parameter on the NE will cause the NE to restart resulting in a temporary loss of ITM management association as well as a loss of any remote logins.

5. Click **OK** to proceed.
   
   **Result:** The information is sent to the NE.

6. Click **Close** to finish the activities in this window.

**END OF STEPS**
Parameters for provisioning DCN information

Node isolated

The node isolated indicates whether the network element is isolated from the DCN or not.

Max. LSP Size

The system is provisionable to either operate with a maximum LSP PDU size of 512 byte (standard in Alcatel-Lucent products) or 1492 bytes (default of ISO8473). Default value is 512 byte.

**Important!** This parameter has to be set to the same value for all NEs in the network.

NSAP format

The NSAP address of a node is its DCN wide identifier which uniquely identifies the node in the network. The different formats are described in the table below:

<table>
<thead>
<tr>
<th>NSAP format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed 20 byte</td>
<td>40 hexadecimal digits.</td>
</tr>
<tr>
<td>Fixed 10 byte</td>
<td>20 hexadecimal digits.</td>
</tr>
<tr>
<td>Flexible</td>
<td>Else (16 - 40 hexadecimal digits).</td>
</tr>
</tbody>
</table>

Area ID

The Area ID indicates the area to which a node belongs and thus its logical location in the network. Area ID for fixed 20 byte and fixed 10 byte NSAP format: 4 hexadecimal digits (2 bytes).

SID

The SID is a unique identifier of the system. Normally this is equal to the Ethernet Address.

Full NSAP

Area address for flexible NSAP format: 2 - 26 hexadecimal digits (1-13 bytes).

Additional manual area addresses

A synonymous Area Address associated with an Intermediate System. Together with the SID and SEL fields, it is a valid synonymous NSAP address for an Intermediate System. This address can be used to connect subnetworks to the OSI-DCN with nodes having a different NSAP format than the formats supported. For example nodes from other
vendors. In addition to the Area Address that can be provisioned in the Area ID or Area Address field, two manual Area Address fields may be added to the NE. The Additional Manual Area Address field is used to assign the second or a third (Hex) Area address of the NE. Valid values are empty or 2-26 Hex (even numbers of digits only).

NE IS-IS level

The NE IS-IS level field changes the IS-IS level of the network element. The possible IS-IS level values for an NE are described in the table below:

<table>
<thead>
<tr>
<th>IS-IS Functionality of NE</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>Provides interconnectivity between network elements in the same area.</td>
</tr>
<tr>
<td>Level 1+2</td>
<td>Provides interconnectivity between areas and between network elements in the same area.</td>
</tr>
<tr>
<td>Level 1+2 Area Repair Access</td>
<td>Provides interconnectivity between areas and between network elements in the same area and enables area partition repair access.</td>
</tr>
</tbody>
</table>

LAN IS-IS level

The LAN IS-IS level field changes the IS-IS level on the LAN port. The possible LAN IS-IS level values are described in the table below:

<table>
<thead>
<tr>
<th>LAN IS-IS Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Follow NE IS-IS</td>
<td>The LAN IS-IS level is the same as the level of the network element provisioned in IS-IS level of NE. Under normal circumstances the network element should use this value.</td>
</tr>
<tr>
<td>Level 2</td>
<td>The LAN IS-IS level is set to level 2. This value should only be used temporarily during upgrade activities.</td>
</tr>
<tr>
<td>None</td>
<td>Disables the LAN (10BaseT) port of a network element for the IS-IS protocol (NO-IS-IS). This value is used in combination with static routing to the management system.</td>
</tr>
</tbody>
</table>

Designated router priority

The designated router priority is a value which indicates the priority of the designated router connected to the LAN (10BaseT). A higher number has priority over a lower one. Valid values are 0-127. The default value is 64. This value is composed in a specialized plan, so do not change it unless this plan is available.
Computed area address

A computed area address associated with an intermediate system. Together with the SID and SEL fields, it is a valid synonymous NSAP address for an intermediate system. Valid addresses can be empty or 2-26 Hex (even numbers of digits only).
Managing the DCC

When to use

The purpose of this procedure is to change the DCC status in the Regenerator Section (RS) and Multiplexer Section (MS) of each STM-N port.

Use this procedure to reduce the exchange of routing data between network elements. Reduction of the exchange of management data is done in order to optimize the Data Communications Network (DCN). The DCC status can be set to enabled or disabled in order to achieve this.

Related information

Refer to “Concepts” (p. 4-3).

Before you begin

Pay attention to the following:

- Disabling DCC can cause permanent loss of association between the management system (ITMCIT) and the network element. In that case the DCC ports can be enabled by a local login with the Local Workstation.
- Enabling DCC can cause instability in the Data Communications Network (DCN).
- A data communications network plan must be available.

Procedure

Complete the following procedure to view and change the status of the DCC.

1. Select Management --> Overlay Comms Network --> DCC.
   Result: The DCC List window appears.

2. Select the port for which the DCC status must be changed and click Edit.
   Result: The Edit DCC window for this port appears.

3. Select the DCC status for the selected port.
   Result: The required values are selected.

4. Click OK to confirm the current settings.
Result: In case Disabled is selected a pop up window will appear with the message:

WARNING

Are you sure you want to complete this operation? Disabling the DCC Channel may result in a loss of ITM-SC management association for this or any remote NEs as well as loss of any remote login.

5 Click OK to proceed with the operation.

Result: The new DCC settings are sent to the network element.

6 Click Close to finish the activities in this window.

END OF STEPS
Parameters for managing the DCC

Port

Shows the line and tributary ports on which DCC is available. If the port is part of an MSP scheme running in slave mode, both ports involved with the protection scheme are shown on the same entry.

DCC channel

Shows which channel the DCC is running over.

DCC status

Shows the current status of the DCC or the slaved pair. Values can be enabled or disabled. The meaning of these values are described in the table below:

<table>
<thead>
<tr>
<th>DCC Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>The DCC communication on this port is stopped. No D-bytes will be exchanged on this port within this network element and his neighbors.</td>
</tr>
<tr>
<td>Enabled</td>
<td>This port can be used in DCC communication for exchanging management data between the network elements.</td>
</tr>
</tbody>
</table>

Important

Maximum 32 DCC channels can be enabled.
Creating a transparent DCC cross-connection

Functional description

Transparent DCC Cross-connect are to be used when there is a router on one side of the SDH network which uses the DCC to transport some IP-based protocol to a router on the other side of the network. This feature can be used to avoid interworking with equipment from a different vendor in a common routing domain. The Transparent DCC Cross-connect is only supported for STM-1 line interfaces.

The Transparent DCC Cross-connect performs a relay function between 2 DCC RS channels. When provisioned those 2 DCC channels are not available for reaching the involved NE.

This feature can be used to create a "pass-through" mechanism through a NE for the following reasons:

• Non-interworking at the Network Layer (due to different N-layer protocols/settings).
• Separation of the Network Layer routing domains.

Related information

For related information, please refer to:

• “Transparent DCC” (p. 4-15)

Before you begin

Prior to performing this task, you must have an overview of the current network topology. Furthermore, you must:

1. log into the ITM CIT, and
2. connect to the NE.

Required equipment

The following equipment is required to perform this task:

• ITM CIT

Instructions

Complete the following steps for the two ports of the NE that are to be cross-connected.

1. Invoke the DCC Selection Filter window from the main menu via Management → Overlay Comms Networks → Transparent DCC.

2. Click on Add.
Result: The Add Transparent DCC Channel screen is displayed.

3 In the DCC channel box select the channel for which you want to create a new DCC termination.

4 Select the ports to be used for the DCC Transparent Cross Connection using the group boxes Port A and Port B.

   Additional info If a DCC channel is selected, then the combo box is populated with the not yet connected TPs that support DCC connection, else the box is greyed out. The ‘not yet connected TP’ means that the DCC of the TP is not enabled and the TP is not connected by transparent DCC channel.

5 Click OK and confirm your changes in the confirmation window.

   Result: The newly created DCC Transparent Cross Connection is displayed in the DCC Transparent Cross Connections window.

END OF STEPS
Procedures regarding login into remote NEs

Overview

Purpose

This section describes procedures to login into a network element in the network via the network element to which the ITM-CIT is connected locally.

Contents

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding a remote accessible NE to the configured nodes list</td>
<td>4-50</td>
</tr>
<tr>
<td>Editing remote NEs in the configured nodes list</td>
<td>4-52</td>
</tr>
<tr>
<td>Parameters for adding and editing remote logins in the configured nodes list</td>
<td>4-54</td>
</tr>
<tr>
<td>Remote login via configured nodes list</td>
<td>4-55</td>
</tr>
<tr>
<td>Remote login via neighbors option</td>
<td>4-57</td>
</tr>
<tr>
<td>Remote login via Area option</td>
<td>4-59</td>
</tr>
</tbody>
</table>
Adding a remote accessible NE to the configured nodes list

Remote login is the possibility to connect via the local network element to another network element in the network. It can be used to configure network elements without actually having to go to the physical location of the network element.

When to use

Use this procedure to add remote assessable network elements to the configured nodes list. By selecting the node added to the configured nodes list a remote login can be established.

Related information

Remote login by using the Configured Nodes list.
Refer to “Concepts” (p. 4-3).

Before you begin

Pay attention to the following:

- When an already specified NSAP is used an error message will be displayed, and upon the user selecting OK, then will be prompted to re-enter the NSAP value.
- When an incorrect NSAP is specified for example if the characters are not hexadecimal characters an error message will be displayed, and upon the user selecting OK, then will be prompted to re-enter the NSAP value.

Procedure

Follow this procedure to add remote logins to the configured nodes list:

1. Login to the network element to which the ITM-CIT is physically connected.
   
   **Result:** A connection is established.

2. Select File —> NE Login —> Login.
   
   **Result:** The NE login window appears.

3. Click Add.
4 Select Add NE Manually and fill in:
   • NE Name (user defined).
   • NE NSAP (fixed 20 bytes).
   • Comment (user defined, optional).

   **Result:** The parameters needed to establish a remote login are filled in.

5 Click **OK**.

   **Result:** The information is stored and the *Add Accessible Network Element* window disappears.

6 The *NE login* window appears.

   **Result:** The remote login on specified network element is now possible by selecting the network element from the lower part of the configured nodes list.

7 Click **Close** to finish the activities in this window.

**END OF STEPS**
Editing remote NEs in the configured nodes list

When to use

Use this procedure to edit existing accessible remote network elements in the configured nodes list. By selecting the node edited in the configured nodes list a remote login can be established.

Related information

Remote login by using the Configured Nodes list.
Refer to “Concepts” (p. 4-3).

Before you begin

Pay attention to the following:

- When an already specified NSAP is used an error message will be displayed, and upon the user selecting OK, then will be prompted to re-enter the NSAP value.
- When an incorrect NSAP is specified for example if the characters are not hexadecimal characters an error message will be displayed, and upon the user selecting OK, then will be prompted to re-enter the NSAP value.

Procedure

Follow this procedure to add remote logins to the configured nodes list:

1. Login to the network element to which the ITM-CIT is physically connected.
   
   Result: A connection is established.

2. Select File —> NE Login —> Login.
   
   Result: The NE login window appears.

3. Click Edit.
   
   Result: The Edit Accessible Network Element window appears.

4. Fill in the fields that need to be modified.
   
   Result: The parameters needed to establish a remote login are changed.

5. Click OK.
**Result:** The information is stored and the *Edit Accessible Network Element* window disappears.

6 **The NE login** window appears.

**Result:** The remote login on specified network element is now possible by selecting the network element from the lower part of the configured nodes list.

7 Click **Close** to finish the activities in this window.

**END OF STEPS**
Parameters for adding and editing remote logins in the configured nodes list

**NE name**

Name of the network element. The value can be up to 20 uppercase or lowercase characters.

**NE NSAP**

The NSAP of the NE. This is a 16-40 HEX digits string. Mandatory field. This field should be unique to the NE.

**Comment**

The comment field is used to note additional information which may consist of 100 characters or less. The field is typically used to define the NE configuration type.
Remote login via configured nodes list

Remote login is the possibility to connect via the local network element to another network element in the network.

When to use

Use this procedure to configure network elements via a remote login from a local network element to another network element in the network.

Related information

Related procedures and information are:

- Managing the DCC
- Adding remote logins to the configured nodes list
- Remote login via neighbors option
- Remote login via area option
- “Concepts” (p. 4-3).

Before you begin

It is only possible to set up a remote session if no other remote session already exists.

Procedure

Follow this procedure to perform a remote login by selecting a network element from the lower part of the configured nodes list:

1. Login to the network element to which the ITM-CIT is physically connected.
   
   **Result:** A connection is established.

2. Select File —> NE Login —> Login.
   
   **Result:** The NE login window appears.

3. Select the network element to remote login to. These nodes are presented in the configured nodes list, in the lower part of this window.
   
   **Result:** An NE to remote login to is selected.

4. Click Login.
Management communication setup

Procedures regarding login into remote NEs

---

**Result:** The remote login is established.

---

5. Click **Close** to finish the activities in this window.

---

END OF STEPS
Remote login via neighbors option

Remote login is the possibility to connect via the local network element to another network element in the network. It can be used to configure network elements without actually having to go to the physical location of the network element.

When to use

Use the following procedure to perform a remote login by using the neighbors option. With this option all neighboring nodes, from the network element to which the ITM-CIT is physically connected, are identified. This makes it possible to perform a remote login without having to fill in the NSAP address of these neighboring nodes.

Related information

Related procedures and information are:
- Managing the DCC
- Adding remote logins to the configured nodes list
- Remote login via configured nodes list
- Remote login via area option
- "Concepts" (p. 4-3).

Before you begin

It is only possible to set up a remote session if no other remote session already exists.

Procedure

Follow this procedure to perform a Remote login by using the neighbors option:

1. Login to the network element to which the ITM-CIT is physically connected.
   
   **Result:** A connection is established.

2. Select File —> NE Login —> Login.
   
   **Result:** The *NE login* window appears.

3. Click *Neighbours*. 
Result: The DCC Neighbours List Filter window appears.

4 Select which slot and port are to be used to find any neighboring connected NEs. Then click **OK**.

**Result:** The DCC Neighbor List window appears displaying all neighboring NEs for which it is possible to remotely login to.

5 Select the network element to remotely login to from the list. Then click **Login**.

**Result:** The remote login is established.

6 Click **Close** to finish the activities in this window.

END OF STEPS
Remote login via Area option

Remote login is the possibility to connect via the local network element to another network element in the network. It can be used to configure network elements without actually having to go to the physical location of the network element.

When to use

Use this procedure to make a remote login to a network element that is in the same area as the local network element to which the CIT is physically connected. This makes it possible to perform a remote login without having to fill in the NSAP address of these nodes.

Related information

Related procedures are:
- Managing the DCC
- Adding remote logins to the configured nodes list
- Remote login via configured nodes list
- Remote login via Neighbors option
- “Concepts” (p. 4-3).

Before you begin

It is only possible to set up a remote session if no other remote session already exists.

Procedure

Follow these steps to perform a remote login by using the area option:

1. Login to the network element to which the ITM-CIT is physically connected.
   
   **Result:** A connection is established.

2. Select File —> NE Login —> Login.
   
   **Result:** The *NE login* window appears.

3. Click Area.
Management communication setup
Procedures regarding login into remote NEs

**Result:** The *Network Area Members List* window appears, displaying all network elements in the same area as the local network element.

4 Select the NSAP address of the network element to login to. Then click **Login**.

**Result:** The remote login is established.

5 Click **Close** to finish the activities in this window.

**END OF STEPS**
Provision NE tunnel information

Overview

Purpose

The purpose of this procedure to setup a path through the DCN capable of transporting IP packets.

Contents

<table>
<thead>
<tr>
<th>Editing provisioned IP parameters</th>
<th>4-62</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding manual route</td>
<td>4-63</td>
</tr>
<tr>
<td>Editing local/manual route</td>
<td>4-64</td>
</tr>
<tr>
<td>Editing TAP properties</td>
<td>4-65</td>
</tr>
<tr>
<td>Parameters for provisioning NE tunnel information</td>
<td>4-67</td>
</tr>
</tbody>
</table>
Editing provisioned IP parameters

When to use

Use this section to provision or change the NE tunnel information.

Related information

“Concepts” (p. 4-3).

Before you begin

Before changing provisioned NE tunnel information a network plan must be available.

Procedure

Complete the following procedure to edit the Local IP Parameters.

...................................................................................................................................................................................................

1 Select Management --> Data Comm Interface.

Result: The Datacom Interface Information window appears.

...................................................................................................................................................................................................

2 Click Edit.

Result: The Edit Datacom Interface Information window appears.

...................................................................................................................................................................................................

3 Make the changes as desired.

Result: The desired values are selected.

...................................................................................................................................................................................................

4 Click OK to confirm the current settings.

Result: A pop up window will appear with the message: “The local IP configuration (IP address and/or subnetwork mask) has updated. This will cause the NE to restart and will result in the loss of ITM-CIT session. Do you wish to continue?”. 

...................................................................................................................................................................................................

5 Click OK to proceed with the operation.

...................................................................................................................................................................................................

6 Click Close to finish the activities in this window.

END OF STEPS
Adding manual route

When to use

Use this section to change the provisioned NE Tunnel information.

Related information

“Concepts” (p. 4-3).

Before you begin

Before changing provisioned NE tunnel information a network plan must be available.

Procedure

Complete the following procedure to add a manual route.

   
   **Result:** The Provisioned NE Tunnel Information window appears.

2. Click **Add** in the IP Tunnel Routing Table box.
   
   **Result:** The Add Manual route window appears.

3. Set the parameters as desired.
   
   **Result:** The parameters are set.

4. Click **OK** to confirm the current settings.
   
   **Result:** A pop up window will appear with the message: “Are you sure you wish to complete this operation”.

5. Click **Close** to finish the activities in this window.

**END OF STEPS**
**Editing local/manual route**

**When to use**

Use this section to provision or change the provisioned NE tunnel information.

**Related information**

“Concepts” (p. 4-3).

**Before you begin**

Before changing provisioned NE tunnel information a network plan must be available.

**Procedure**

Complete the following procedure to edit the local or manual route.

   **Result:** The *Provisioned NE Tunnel Information* window appears.

2. Select the route to be changed from the IP Routing Table box.
   **Result:** The route to be changed is selected.

3. Click **Edit** in the IP Tunnel Routing Table box.
   **Result:** The *Edit Local/Manual route* window appears.

4. Set the parameters as desired.
   **Result:** The parameters are set.

5. Click **OK** to confirm the current settings.
   **Result:** A pop up window will appear with the message: “Are you sure you wish to complete this operation”.

6. Click **Close** to finish the activities in this window.

END OF STEPS
Editing TAP properties

When to use

Use this section to provision or change the provisioned NE tunnel information.

Related information

“Concepts” (p. 4-3).

Before you begin

Before changing provisioned NE tunnel information a network plan must be available.

Procedure

Complete the following procedure to edit TAP properties.


   **Result:** The Provisioned NE Tunnel Information window appears.

2. | IF                     | THEN                                                                 |
   |------------------------|----------------------------------------------------------------------|
   | you want to enable TAP Advertise and TAP Learning | Click **Edit** in the TAP Properties box.  
   |                         | In the *Edit TAP Properties* window select the respective radio buttons (*enabled*) and click **OK**.  
   |                         | In the **Provisioned NE Tunnel Information**, in the group box **IP Tunnel Routing Table** select the respective route and click **Edit**.  
   |                         | In the now opened **Edit Local/Manual Route** window select the **Advertise the route** check box and click **OK**  
   |                         | **Result:** TAP Advertise and TAP Learning are enabled. |

   | you want to disable TAP Advertise and TAP Learning | In the **Provisioned NE Tunnel Information**, in the group box **IP Tunnel Routing Table** select the respective route and click **Edit**.  
   |                                                       | In the now opened **Edit Local/Manual Route** window de-select the **Advertise the route** check box and click **OK**  
   |                                                       | Click **Edit** in the TAP Properties box.  
   |                                                       | In the *Edit TAP Properties* window de-select the respective radio buttons (*enabled*) and click **OK**.  
   |                                                       | **Result:** TAP Advertise and TAP Learning are disabled. |
3 Click **OK** to confirm the current settings.

**Result:** A pop up window will appear with the message: “Disabling TAP parameters or changing the TAP group may lead to loss of IP connections! Do you wish to continue?”

4 Click **OK** to proceed with the operation.

5 Click **Close** to finish the activities in this window.

**END OF STEPS**
Parameters for provisioning NE tunnel information

IP address

IP address of the NE. The IP address consists of 32 bits broken into 4 logical bytes. Each byte is converted into the decimal equivalent. For example, the equivalent dotted decimal notation of the address 10000011 1101011 00000000 00000001 is 131.107.0.1. Values: a, b, c and d in the range 0..255. The default value is 0.0.0.0.

Subnet mask

Filter setting for most significant bits. Values: 8..32. The default value for the subnet mask is 16, in which case only the most significant bits (first part) of the IP address will be checked. This field will be grayed out and empty when the tunnel status is disabled.

IP tunnel status

The status of the tunneling feature, which can be enabled or disabled. The default value is disabled.

Filter

Allows the user to filter the list with routes. Possible values are local/manual routes or all routes.

The different values are described in the table below:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local/Manual Routes</td>
<td>When the filter is set to local/manual routes, only routes entered in the table after the node's interface is configured with an IP address and a subnet mask or routes entered by the operator are displayed.</td>
</tr>
<tr>
<td>All Routes</td>
<td>When the filter is set to all routes, all routes entered in the table after the node's interface is configured with an IP address and a subnet mask, routes entered by the operator and routes entered by the TAP provisioning protocol are displayed.</td>
</tr>
</tbody>
</table>

Destination prefix

The address of the destination to which packets can be sent. The destination prefix consists of the subnet address and subnet mask.

Subnetwork

Indicates the next hop subnetwork type. Possible values are LAN or CLNP-tunnel.
The different values are described in the table below:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN</td>
<td>When the subnetwork type is LAN, the next hop address is an IP address.</td>
</tr>
<tr>
<td>CLNP-Tunnel</td>
<td>When the subnetwork type is CLNP-tunnel, the next hop address is a full NSAP address.</td>
</tr>
</tbody>
</table>

**Next hop IP/NSAP**

Lists the next hop full NSAP address or IP address.

**Important!** For IP communication the selector of the NSAP should be 04 instead of the 01 for OSI.

**Owner**

Identifies the originator of the routing entry. Possible values are local, manual, or TAP.

The different values are described in the table below:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>A route automatically entered into the table after the node's interface is configured with an IP address and a subnet mask. This route cannot be deleted or manipulated in any way.</td>
</tr>
<tr>
<td>Manual</td>
<td>Routes entered by the operator. These are the only routes the operator can manipulate. This value always applies to added entries.</td>
</tr>
<tr>
<td>TAP</td>
<td>Routes entered by the TAP provisioning protocol.</td>
</tr>
</tbody>
</table>

**Cost**

Displays the cost of the route.

**TAP advertise**

The status of the automatic provisioning protocol. The possible values are enabled or disabled. The default value is disabled.

**TAP learn**

The learning status of the automatic provisioning protocol. The possible values are enabled or disabled. When set to enabled the NE shall process the option field in incoming LSPs and store the learned routes in the routing table. The default value for TAP Learn is disabled.
TAP group

The TAP group to which the system belongs. Possible values are: 0..65535. The default value is 0.
Provision SNMP management

Overview

Purpose

SNMP stands for Simple Network Management Protocol and is a protocol standardized by the Internet Engineering Task Force (IETF) which is commonly used to manage data devices like switches and routers.

The NE needs to have an IP address assigned so that it can be addressed.

Contents

| Provision SNMP management | 4-71 |
Provision SNMP management

When to use

Use this section to provision SNMP management.

Procedure

Complete the following procedure to edit the local or manual route.

1. Select Management → SNMP Manager List
   
   Result: The SNMP Manager List window appears.

2. To add an SNMP manager click on Add, to modify an SNMP manager click on Edit.
   
   Result: The Add IP Address window appears.

3. Add/modify the IP address and click OK.
   
   Result: The Add IP Address window is closed.

4. Click Close to close the SNMP Manager List window.

END OF STEPS
5 Equipment provisioning

Overview

Purpose

Equipment provisioning provides the configuration data for the 1643 AM and 1643 AMS. Provisioning is the preparatory work that is done to ensure that a network element (NE) properly functions so that the NE may be included in a network. After initial provisioning, any subsequent changes in the NE’s equipment mean that provisioning must once more be performed.

Objective

The correct configuration data is provided for the 1643 AM and 1643 AMS.

Outcome

The objective of equipment provisioning is to eventually include a network element in an SDH network. To enable the 1643 AM and 1643 AMS to become a functioning part of a network, it must first be provided with the correct configuration data.

Intended use

This chapter provides all procedures needed to provision the equipment of a 1643 AM and 1643 AMS network element when using the ITM-CIT. Conceptual information about equipment provisioning can be found in “Concepts” (p. 5-4).

Contents

<table>
<thead>
<tr>
<th>Concepts</th>
<th>5-4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning methods</td>
<td>5-5</td>
</tr>
<tr>
<td>Addressing and management concepts</td>
<td>5-8</td>
</tr>
<tr>
<td>1643 AM or 1643 AMS configuration possibilities</td>
<td>5-9</td>
</tr>
<tr>
<td>Node creation</td>
<td>5-11</td>
</tr>
<tr>
<td>Task</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Miscellaneous discrete inputs and outputs</td>
<td>5-12</td>
</tr>
<tr>
<td>Local alarms signaling</td>
<td>5-13</td>
</tr>
<tr>
<td>Centralized alarm signaling</td>
<td>5-14</td>
</tr>
<tr>
<td>Centralized MDI signaling</td>
<td>5-15</td>
</tr>
<tr>
<td>Create a node</td>
<td>5-16</td>
</tr>
<tr>
<td>Creating a node</td>
<td>5-17</td>
</tr>
<tr>
<td>Parameters for creating a node</td>
<td>5-19</td>
</tr>
<tr>
<td>Provision slots</td>
<td>5-21</td>
</tr>
<tr>
<td>Provisioning slots</td>
<td>5-22</td>
</tr>
<tr>
<td>Parameters for provisioning slots</td>
<td>5-24</td>
</tr>
<tr>
<td>Confirm the MIB</td>
<td>5-25</td>
</tr>
<tr>
<td>Confirming the MIB</td>
<td>5-26</td>
</tr>
<tr>
<td>Parameters for confirming the MIB</td>
<td>5-28</td>
</tr>
<tr>
<td>Retrieve NE slot information</td>
<td>5-30</td>
</tr>
<tr>
<td>Viewing NE slot information</td>
<td>5-31</td>
</tr>
<tr>
<td>Parameters for viewing NE slot information</td>
<td>5-32</td>
</tr>
<tr>
<td>Retrieve shelf display</td>
<td>5-33</td>
</tr>
<tr>
<td>Viewing the shelf display</td>
<td>5-34</td>
</tr>
<tr>
<td>Parameters for viewing shelf display</td>
<td>5-35</td>
</tr>
<tr>
<td>View hardware inventory</td>
<td>5-37</td>
</tr>
<tr>
<td>Viewing hardware inventory - shelf</td>
<td>5-38</td>
</tr>
<tr>
<td>Viewing hardware inventory - slot</td>
<td>5-39</td>
</tr>
<tr>
<td>Parameters for viewing hardware inventory</td>
<td>5-41</td>
</tr>
<tr>
<td>View SFP inventory data</td>
<td>5-42</td>
</tr>
<tr>
<td>Viewing SFP inventory</td>
<td>5-43</td>
</tr>
<tr>
<td>Parameters for viewing SFP inventory data</td>
<td>5-44</td>
</tr>
<tr>
<td>View and edit node details</td>
<td>5-48</td>
</tr>
<tr>
<td>Viewing and editing node details</td>
<td>5-49</td>
</tr>
<tr>
<td>Parameters for viewing or editing node details</td>
<td>5-51</td>
</tr>
<tr>
<td>View and edit MDI information</td>
<td>5-53</td>
</tr>
<tr>
<td>Viewing and editing MDI information</td>
<td>5-54</td>
</tr>
<tr>
<td>Parameters for viewing or editing MDI information</td>
<td>5-56</td>
</tr>
<tr>
<td>View or edit MDO information</td>
<td>5-57</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Viewing or editing MDO information</td>
<td>5-59</td>
</tr>
<tr>
<td>Parameters for viewing or editing MDO information</td>
<td>5-61</td>
</tr>
<tr>
<td><strong>Provision ports</strong></td>
<td>5-62</td>
</tr>
<tr>
<td>Provisioning ports</td>
<td>5-63</td>
</tr>
<tr>
<td>Parameters for Port Provisioning</td>
<td>5-65</td>
</tr>
</tbody>
</table>
Overview

Purpose

This chapter explains the concepts of equipment provisioning. The information in this chapter can be used as background information for equipment provisioning.

Contents

<table>
<thead>
<tr>
<th>Provisioning methods</th>
<th>5-5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addressing and management concepts</td>
<td>5-8</td>
</tr>
<tr>
<td>1643 AM or 1643 AMS configuration possibilities</td>
<td>5-9</td>
</tr>
<tr>
<td>Node creation</td>
<td>5-11</td>
</tr>
<tr>
<td>Miscellaneous discrete inputs and outputs</td>
<td>5-12</td>
</tr>
<tr>
<td>Local alarms signaling</td>
<td>5-13</td>
</tr>
<tr>
<td>Centralized alarm signaling</td>
<td>5-14</td>
</tr>
<tr>
<td>Centralized MDI signaling</td>
<td>5-15</td>
</tr>
</tbody>
</table>
Provisioning methods

Provisioning methods

Providing provisioning information to the network element, the management system, or both the NE and the management system can be accomplished in three different ways.

- Using an NE template.
- Using a pre-provisioned NE.
- Performing an MIB upload.

Management information base

The Management Information Base (MIB) is the provisioning information stored in the database of the NE. This includes the configuration of the units within the NE, the name and type of the NE, as well as addressing and network information necessary for management.

MIB image

As suggested by the name, the MIB image is a copy of the data stored in the MIB. The MIB image is stored in the ITM-SC thereby enabling the ITM-SC to manage the NE.

Templates

A template is a collection of configuration data. There are two types of templates, default and user-defined. In the system software of the WaveStar® ITM-SC are a set of default templates, which have the essential units already provisioned. User-defined templates are templates created by the user, and they may use a default template as a basis. All of these templates can be used to pre-provision and provision network elements.

The provisioning information contained in a template includes only data concerning the network element contents; it does not include any information regarding the position of the NE within the network. For this reason, the templates are a basic provisioning tool capable of serving as the basis for pre-provisioning or provisioning an NE.

Pre-provisioning

Pre-provisioning allows a network elements configuration data to be stored on the management system before an actual association with this NE is established. Thus, creating a pre-provisioned NE prepares for the provisioning of an NE by storing a dummy NE on the management system. This data, stored as a pre-provisioned NE, is accessed later when the actual network element is installed and ready to be provisioned.
A template serves as the basis for creation of a pre-provisioned NE; however, the MIB image created by pre-provisioning an NE includes not only the information from the template, it also has the essential information concerning the network element’s place in the network.

Creating an MIB image

An MIB image is created during pre-provisioning; however, it may also be created from an existing network element already provisioned with its configuration data. For example, an MIB could have been created for an NE using the ITM CIT. In this case, the NE is provisioned, but it is not yet under control of the ITM-SC. Once a physical connection exists between the NE and the ITM-SC, the ITM-SC can assume management of the NE by creating an MIB image from the network element’s MIB.

Overview of provisioning methods

In the figure below, the methods of provisioning using the ITM-SC are illustrated. As discussed above, templates can be used as the basis for creation of the MIB images of pre-provisioned or provisioned NEs. Pre-provisioned NEs have the same provisioning information as a provisioned NE, and thus they can be used to quickly create the provisioned NE because no additional information must be entered. Finally, an MIB image can be created from the MIB of an existing NE.

MIB = Management Information Base
Provisioning outcomes

A properly completed template will appear in the list of NE templates.

After successfully pre-provisioning an NE, the proper equipment configuration data for the network element is stored in the management system. The NE is displayed on the network map with a blue color, indicating that it is a pre-provisioned network element.

Finally, a fully provisioned NE is integrated into the network and is displayed on the network map in green.
Addressing and management concepts

Introduction

To enable management, the WaveStar® ITM-SC must have addressing and management connection information for each NE under its control. The basic information concerning such topics as addressing and management connection information are given in this section; however, much more detailed information about all of these Data Communications Network (DCN) concepts can be found in Chapter 4, “Management communication setup”.

Data communications network

The Data Communications Network (DCN) is a general name for the collection of various communication means between network management devices, such as the ITM-SC, and the NEs. By providing the communication between management systems and the NEs, the DCN makes management possible. For further information, Chapter 4, “Management communication setup” discusses this network in depth.

DCN addresses

The NE has two addresses in the DCN:

- Ethernet address
- NSAP address

Ethernet address

The Ethernet address is the unique 6-byte address of a network element. Sometimes it is also referred to as the hardware or physical address of the node. The Ethernet address has only local meaning on the Q-LAN and cannot be used for routing purposes. It does not contain the information on where the node is in the Data Communications Network.

NSAP address

The Network Service Access Point (NSAP) address is used by the network protocol for location information. The NSAP address of a node is its DCN wide identifier which uniquely identifies the node in the network. Although different NSAP formats exist, it is preferable that all nodes in a network should use the same address structure. Complete details concerning the structural formatting of the NSAP address can be found in “NSAP address format” (p. 4-12).
1643 AM or 1643 AMS configuration possibilities

Standard configuration

The 1643 AM or 1643 AMS has standard 16 x 2 Mbit/s connections. This unit is designated tributary slot 1 (TS1), and it is a part of the network element’s main board.

Since the unit in TS1 is a part of the main board, it may not be changed; however, different types of option cards may be placed for use in TS2.

Line interface on TS1

The 1643 AM or 1643 AMS can be equipped with an STM-1 or an STM-4 line interface. A choice is possible between long haul (LH) or short haul (SH).

Option cards in TS2

It is possible to place optional cards in the 1643 AM or 1643 AMS. This tributary port unit will occupy TS2, and it has various possibilities. It may be another card with 16 x 2 Mbit/s interfaces. There are also cards available with 16 x 1.5 Mbit/s (DS1) or 2 x 34 Mbit/s (E3) or 2 x 45 Mbit/s (DS3) or 4 x X.21 interfaces or 2 x STM-1 interfaces (optical) or 2 x STM-1 interfaces (electrical) or the SDSL option card. More information about this card can be found in “Concepts” (p. 9-3). Finally, the TransLAN® Plus optional card has four 10/100 Mbit/s interfaces.

All of these units must be installed by an Alcatel-Lucent technician, as installation requires removal of the locked front panel. Moreover, each optional port unit to be placed in TS2 has its own distinctive front panel.

Potential configurations

The 1643 AM supports these option cards:

<table>
<thead>
<tr>
<th>Option Card</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>X2S11TRIB</td>
<td>2 x optical STM-1 tributary interfaces (short haul)</td>
</tr>
<tr>
<td>X2STM1ETRIB</td>
<td>2 x electrical STM-1 tributary interfaces</td>
</tr>
<tr>
<td>X16E1-V3</td>
<td>16 x E1 interfaces (75/120 Ω)</td>
</tr>
<tr>
<td>x16DS1</td>
<td>16 x DS1 interfaces (100 Ω)</td>
</tr>
<tr>
<td>X2E3-V2</td>
<td>2 x E3 interfaces</td>
</tr>
<tr>
<td>X2DS3-V2</td>
<td>2 x DS3 interfaces</td>
</tr>
<tr>
<td>X4X.21</td>
<td>4 x X.21 interfaces</td>
</tr>
<tr>
<td>X12SHDSL-V2</td>
<td>12 x SHDSL interfaces</td>
</tr>
</tbody>
</table>
The 1643 AMS supports these option cards:

<table>
<thead>
<tr>
<th>Option Card</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>X16E1-V3</td>
<td>16 × E1 interfaces (75/120 Ω)</td>
</tr>
<tr>
<td>X16DS1</td>
<td>16 × DS1 interfaces (100 Ω)</td>
</tr>
<tr>
<td>X2E3-V2</td>
<td>2 × E3 interfaces</td>
</tr>
<tr>
<td>X2DS3-V2</td>
<td>2 × DS3 interfaces</td>
</tr>
<tr>
<td>X4X.21</td>
<td>4 × X.21 interfaces</td>
</tr>
<tr>
<td>X12SHDSL-V2/V3</td>
<td>12 x SHDSL interfaces</td>
</tr>
<tr>
<td>X4IP</td>
<td>4 × 10/100BASE-T Ethernet LAN interfaces (TransLAN®)</td>
</tr>
<tr>
<td>X5IP</td>
<td>3 × 10/100BASE-T, 1 × 10/100/1000BASE-T, and 1 × 1000BASE-X Ethernet LAN interfaces (TransLAN®)</td>
</tr>
<tr>
<td>X8PL</td>
<td>8 × 10/100BASE-T Ethernet LAN interfaces in private line (PL) mode</td>
</tr>
</tbody>
</table>
Node creation

Node

A node is literally “a point at which subsidiary parts originate or center.” So, in other words the NE or the node is the central collection point of its various parts. Creating a node means, then, identifying this central point (the NE name and address) and inputting the exact parts comprising the node. All of this information is compiled and stored in the Management Information Base.

Management information base

The Management Information Base (MIB) is the provisioning information stored in the database of the NE. This includes the configuration of the units within the NE, the name and type of the NE, as well as addressing information and network information necessary for management.

Confirm MIB

Confirming the MIB will send all of the basic NE information that has been entered to the System Controller. This is an essential step in the creation of the NE.

Update MIB

The MIB can be updated rather than confirmed, if the MIB already exists and there have been few changes made. This operation can be advantageous as it takes considerably less time than that of confirming the MIB.

Isolated state

Arriving from the factory, the 1643 AM or 1643 AMS is in an isolated state. This means that communication via DCN is not possible. In other words, no association with the ITM-SC can be established while the network element is in the isolated state.

To enable an association with the ITM-SC the network element must be brought out of the isolated state. To do so, use the ITM CIT to either change or re-select any of the " Provisioned DCN Information" parameters. Once this is done, the network element will be removed from isolation.
Miscellaneous discrete inputs and outputs

MDIs and MDOs

A network element contains Miscellaneous Discrete Inputs (MDI) and Miscellaneous Discrete Outputs (MDO).

- MDIs are inputs to a network element for external equipment. MDIs can be monitored by the management system.
- MDOs are outputs from a network element used to drive external equipment. MDOs can be activated or deactivated by the management system.

Objective

MDIs can be used to collect status information from other transmission equipment or to monitor external events (for example a door contact).

MDOs are used to drive external equipment or to influence the behavior of equipment external to the system.

About

The 1643 AM or 1643 AMS contains four MDIs and four MDOs.

To help with general purpose surveillance, each network element MDI and MDO can be given a unique name, which is stored in the management system. The name can be no longer than 26 characters.

The 1643 AM or 1643 AMS supports a specific alarm supervision via the MDI and MDO contacts which allows to supervise the MDI status of several NEs and signal an alarm condition via the MDO contact of a dedicated 1643 AM or 1643 AMS in a central location without the intervention of a management system.

The user can select between three alarm signaling modes:

- Local Alarms signaling
- Centralized Alarms signaling
- Centralized MDI signaling.

Outcome

With the MDIs, external events are reported to the management system via the alarm representation. If this event occurs an alarm is raised. Also, the severity of these alarms can be set. Once provisioned, MDOs can place external equipment under the system’s control.
Local alarms signaling

Introduction

This is the default mode on the 1643 AM or 1643 AMS.

The MDOs behavior in this mode:

- MDO-2 is active when one or more local alarms (including possible MDI alarms) with severity PROMPT are raised
- MDO-3 is active when one or more local alarms (including possible MDI alarms) with severity DEFERRED are raised
- MDO-4 is active when one or more local alarms (including possible MDI alarms) with severity INFO are raised.

Example

This mode is fine for the following application:
Centralized alarm signaling

Introduction

The NE will drive its MDOs according to alarm information it has centralized from local and remote NEs. A CIT locally connected is used to subscribe or unsubscribe to alarm status reports from remote NEs. However, the NE is able to drive its MDO whether a CIT is locally connected or not.

The MDOs behavior in this mode:

- MDO-2 is active when one or more centralized alarms (including possible MDI alarms) with severity PROMPT are raised
- MDO-3 is active when one or more centralized alarms (including possible MDI alarms) with severity DEFERRED are raised
- MDO-4 is active when one or more centralized alarms (including possible MDI alarms) with severity INFO are raised.

Example

This mode is fine for the following application:
Centralized MDI signaling

Introduction

In this mode, the NE will drive its MDOs according to MDI information it has centralized from local and remote NEs. A CIT locally connected is used to subscribe or unsubscribe to MDI status report from remote NEs. However, the NE will be able to drive its MDO whether a CIT is locally connected or not.

The MDOs behavior in this mode:

- MDO-2 is active when one or more centralized MDI alarms with severity PROMPT are raised
- MDO-3 is active when one or more centralized MDI alarms with severity DEFERRED are raised
- MDO-4 is active when one or more centralized MDI alarms with severity INFO are raised.

Example

This mode is fine for the following application:
Create a node

Overview

Purpose

Creating a node provides the basic information necessary to place an NE into service. As a result the basic provisioning information is correctly provided, and the NE is created.

Contents

<table>
<thead>
<tr>
<th>Creating a node</th>
<th>5-17</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters for creating a node</td>
<td>5-19</td>
</tr>
</tbody>
</table>
Creating a node

When to use
A node should be created when a new network element is available to be placed into service.

Related information
The related procedure is:
- Provision Units
- Confirm the MIB.

Before you begin
Before starting to create a node determine the following:
- the name, address, and location of the node are known.
- the location and type of units physically present in the NE are known.
- the main unit must be assigned before the interfaces associated with this unit can be assigned. For example, a tributary port unit must be assigned before the ports for this unit can be assigned.
- For the 1643 AM and 1643 AMS, the only slot which may be user assigned is TS2.

Any mistake in provisioning the slots will result in a failure when attempting to create the node. When a mistake has been made, after clicking Finish, the error message “Slot configuration conflict” appears. The node creation has failed, and the entire node creation process must be begun a new.
- To create an association with the ITM-SC, the network element cannot be in an isolated state. (As a default condition, the 1643 AM or 1643 AMS arrives from the factory in an isolated state.) To view if the network element is in the isolated state, select Management -> Overlay Comms Network -> DCN. Should the network element be in an isolated state, click Edit. The window Edit Provisioned DCN Information then appears. In this window, change (or reselect) any of the displayed parameters and click OK. Doing so will remove the NE from isolation and association with the ITM-SC will now be possible.

Procedure
Follow these steps to create a network element.

1 Select Management -> Node Creation.
Result: The Node Creation - Parameters window appears.

2 Enter the NE Name and NE Location.

Result: The network element name and location appear, respectively, in the fields NE Name and NE Location.

3 Click Next.

Result: The window Node Creation - Provisioned Slots appears.

4 Complete the procedure “Provision Slots”.

Important! For the 1643 AM or 1643 AMS, the only slot which may be user assigned is TS2.

Result: The slots of the NE are properly assigned.

5 Complete the procedure “Confirm the MIB” (p. 5-25).

Result: The MIB is now confirmed, and after reestablishing the connection between the NE and the ITM-CIT, the MIB status in the window Node Details should be Filled.

6 Complete the procedure “Confirm or Update the MIB”.

Result: The MIB is now confirmed, and after reestablishing the connection between the NE and the ITM CIT, the MIB status in the window Node Details should be Filled.

END OF STEPS
Parameters for creating a node

NE name

The network element’s name is listed. The name must be unique across management domains. If the NE is not managed by the Lucent Optical Network Management System (formerly called WS-NMS), then the name may be up to 20 characters in length. If the NE will be managed by the Lucent Optical Network Management System, then the name must be 3 to 10 characters long with the last three characters a slash and two digits. Only A-Z, 0-9, _, /, and - are permitted for network elements managed by the Lucent Optical Network Management System. An example of a Lucent Optical Network Management System compatible name is LONDON/02.

NE location

The location of the network element is given. The location may have up to 20 uppercase or lowercase characters, digits, and spaces.

Slot

The slot position is given here.

Assigned unit

The type of unit provisioned in the listed slot is shown.

State

Displays the status of the listed slot. The different slot states are given in the table below.

<table>
<thead>
<tr>
<th>Slot State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigned</td>
<td>Slot is assigned.</td>
</tr>
<tr>
<td>Unassigned</td>
<td>Slot is unassigned.</td>
</tr>
<tr>
<td>Auto</td>
<td>Slot is provisioned but waiting for unit. Once the provisioned unit is present, the slot state will automatically change to Assigned.</td>
</tr>
</tbody>
</table>

Operation

When assigning units, an operation must be chosen. The choices are detailed in the following table.

<table>
<thead>
<tr>
<th>Slot State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign</td>
<td>Assigns the unit to the slot.</td>
</tr>
</tbody>
</table>
### Slot State

<table>
<thead>
<tr>
<th>Slot State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unassign</td>
<td>The slot is configured to be empty. The NE will not expect any unit to be present in this slot.</td>
</tr>
<tr>
<td>Auto</td>
<td>Automatically assigns the unit to the slot once the NE establishes the presence of a unit of the correct type. Until this time, the slot acts as unassigned.</td>
</tr>
</tbody>
</table>

### Main unit

The unit provisioned or to be provisioned in the selected slot.

### Upper/lower interface

The interfaces directly associated with the displayed *Main Unit*.

### MIB state

The status of the MIB is indicated. The possible values are given in the table below.

<table>
<thead>
<tr>
<th>MIB State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Empty</td>
<td>An empty system controller (SC) has been inserted or the MIB was cleared after starting an automatic MIB download by the management system. If the MIB State is empty, the management system can proceed with the MIB download.</td>
</tr>
<tr>
<td>Filled</td>
<td>The NE possesses a valid MIB, which has been confirmed.</td>
</tr>
<tr>
<td>Filled Unknown</td>
<td>The NE has a MIB, however, it is of unknown validity. This can occur, for instance, if one SC is replaced by another SC having a MIB.</td>
</tr>
<tr>
<td>Filled Not Confirmed</td>
<td>The NE has a MIB, however, it has not yet been confirmed by the ITM-CIT or ITM-SC. The procedure “Confirm or Update MIB” gives the steps necessary to confirm the MIB. Once confirmed the state will become <em>Filled</em>.</td>
</tr>
<tr>
<td>Waiting for Upload</td>
<td>This state is only possible when the NE is managed by the ITM-SC. After confirmation of the MIB, the NE performs a reset and loses its association with the ITM-SC. When the NE restarts, the MIB State becomes <em>Waiting for Upload</em>. When the ITM-SC reassociates with the NE and detects this MIB state, an MIB upload is performed, and the state will then become <em>Filled</em>.</td>
</tr>
</tbody>
</table>
Provision slots

Overview

Purpose

Use this procedure to provision the slots of a network element.

Contents

<table>
<thead>
<tr>
<th>Provisioning slots</th>
<th>5-22</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters for provisioning slots</td>
<td>5-24</td>
</tr>
</tbody>
</table>
Provisioning slots

When to use

The slot TS2 must be provisioned for a node in the process of creation as well as for already existing network elements.

Related information

The following procedures and information are related:
- Create a Node
- Confirm or Update the MIB
- View NE Slot Information
- View Hardware Inventory - Slots
- “Concepts” (p. 5-4)

Important! For the 1643 AM or 1643 AMS, the only slot which may be user assigned is TS2.

Before you begin

Before performing this procedure make sure:
- Before provisioning the network element slot configuration it is assumed that the new configuration of the NE is known. This includes the exact types of units to be provisioned and the corresponding slot positions for these units.
- The main unit must be assigned before its corresponding interface units are assigned

Procedure

Follow these steps to provision the slots of an NE. This includes both assigning and unassigning units.

1. IF
   provisioning units during node creation (Node Creation - Provisioned Slots is displayed) THEN
   go to.

   the NE already exists
   select Provisioning → Equipment → Provisioned NE Components and go to Step 2
   or select Provisioning → Equipment → Shelf Display and go to Step 3

2. Select the TS2 slot from the list in the window, and click Assign/Unassign.
Result: The Assign NE Units to Slots window appears with information concerning the selected slot and its associated slots.

3 Right-click on a slot or a unit and select Assign/Unassign.

   Result: The Assign NE Units to Slots window appears with information concerning the selected slot and its associated slots.

4 Select the desired operation from the selections at the top of the window.

5 If assigning units, use the pull-down menu for Main Unit and select the correct unit corresponding to the displayed slot.

   Result: The correct unit appears as the new Main Unit/Interface.

6 Click OK.

   Important! When assigning units during node creation, instead of the Provisioned NE Components window, the window Node Creation - Provision Slots will reappear.

   Result: The desired operation for this slot is performed, and the window Provisioned NE Components or Node Creation - Provisioned Slots appears again.

7 If creating a node, then click Finish. Otherwise, click Cancel.

   Result: The window Provisioned NE Components (or in the case of node creation, Node Creation - Provisioned Slots) disappears.

END OF STEPS
Parameters for provisioning slots

Slot
The slot position is given here.

Expected unit
The type of unit provisioned in the listed slot is shown.

State
Displays the status of the listed slot. The different slot states are given in the table below.

<table>
<thead>
<tr>
<th>Slot State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigned</td>
<td>Slot is assigned.</td>
</tr>
<tr>
<td>Unassigned</td>
<td>Slot is unassigned.</td>
</tr>
<tr>
<td>Auto</td>
<td>Slot is provisioned but waiting for unit. Once the provisioned unit is present, the slot state will automatically change to Assigned.</td>
</tr>
</tbody>
</table>

Operation
When provisioning the slots/units, an operation must be chosen. The choices are detailed in the following table.

<table>
<thead>
<tr>
<th>Slot State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign</td>
<td>Assigns the unit to the slot.</td>
</tr>
<tr>
<td>Unassign</td>
<td>The slot is configured to be empty. The NE will not expect any unit to be present in this slot.</td>
</tr>
<tr>
<td>Auto</td>
<td>Automatically assigns the unit to the slot once the NE establishes the presence of a unit of the correct type. Until this time, the slot acts as unassigned.</td>
</tr>
</tbody>
</table>
Confirm the MIB

Overview

Purpose

To make any provisioning changes a part of the Management Information Base (MIB).

Contents

<table>
<thead>
<tr>
<th>Confirming the MIB</th>
<th>5-26</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters for confirming the MIB</td>
<td>5-28</td>
</tr>
</tbody>
</table>
Confirming the MIB

When to use

The purpose of these steps is to confirm the MIB of a network element.

Related information

The following procedures are related.

- Create a Node
- Provision Slots
- “Concepts” (p. 5-4).

Before you begin

No prerequisites are needed.

The following precautions are important to consider:

- Performing an MIB confirm will cause the NE to reset. A new login, after waiting several minutes for the reset to take place, will have to be performed.
- Confirming the MIB for an existing NE can result in traffic disruptions.

Procedure

1. Select Management → Node Details.

   Result: The Node Details window appears. This window allows confirmation or update of a network element MIB.

2. **NOTICE**

   **Service-disruption hazard**

   Confirming the MIB will result in an NE reset. The current login session will be terminated. Also, while overwriting the older MIB, traffic can be affected.

   Click Confirm MIB.

   Result: A confirmation window appears warning that confirming the MIB will result in a system reset and that MIB confirmation can potentially affect traffic.

3. Click Yes.
Result: The operation will be started. Confirming the MIB should take several minutes. During this time, the connection between the ITM-CIT and the NE will be lost. To reestablish this connection, a login must once again be performed after waiting for the operation to complete.

4 Login again.

5 Select Management → Node Details.

Result: The Node Details window appears. In this window, the MIB state can be viewed. It should now be Filled.

6 Click Close.

Result: The Node Details window disappears.

END OF STEPS
Parameters for confirming the MIB

**NE type**

The type of NE is indicated.

**NE location**

The location of the network element is given. The location may have up to 20 uppercase or lowercase characters, digits, and spaces.

**NE name**

The network element’s name is listed. The name must be unique across management domains. If the NE is not managed by the Lucent Optical Network Management System (formerly called WS-NNMS), then the name may be up to 20 characters in length. If the NE will be managed by the Lucent Optical Network Management System, then the name must be 3 to 10 characters long with the last three characters a slash and two digits. Only A-Z, 0-9, _, /, and - are permitted for network elements managed by the Lucent Optical Network Management System. An example of a Lucent Optical Network Management System compatible name is LONDON/02.

**MIB state**

The status of the MIB is indicated. The possible values are given in the table below.

<table>
<thead>
<tr>
<th>MIB State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Empty</td>
<td>An empty system controller (SC) has been inserted or the MIB was cleared after starting an automatic MIB download by the management system. If the MIB State is empty, the management system can proceed with the MIB download.</td>
</tr>
<tr>
<td>Filled</td>
<td>The NE possesses a valid MIB, which has been confirmed.</td>
</tr>
<tr>
<td>Filled Unknown</td>
<td>The NE has a MIB, however, it is of unknown validity. This can occur, for instance, if one SC is replaced by another SC having a MIB.</td>
</tr>
<tr>
<td>Filled Not Confirmed</td>
<td>The NE has a MIB, however, it has not yet been confirmed by the ITM-CIT or ITM-SC. The procedure “Confirm or Update MIB” gives the steps necessary to confirm the MIB. Once confirmed the state will become Filled.</td>
</tr>
</tbody>
</table>
### MIB State Description

<table>
<thead>
<tr>
<th>MIB State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Waiting for Upload</td>
<td>This state is only possible when the NE is managed by the ITM-SC. After confirmation of the MIB, the NE performs a reset and loses its association with the ITM-SC. When the NE restarts, the MIB State becomes <em>Waiting for Upload</em>. When the ITM-SC reassociates with the NE and detects this MIB state, an MIB upload is performed, and the state will then become <em>Filled</em>.</td>
</tr>
</tbody>
</table>

### Management State

The state of the association with the management system is displayed. The possible states are given in the following table.

<table>
<thead>
<tr>
<th>Management State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td><em>Normal</em> will be displayed whenever management operations have been completed. In other words, the management system has completed the MIB upload, MIB download, MIB resynchronization, or reevaluation of fault status. The state can also be <em>Normal</em> when the association between the ITM-SC/ITM-CIT and the NE has been lost.</td>
</tr>
<tr>
<td>Uploading</td>
<td>The management system is performing an MIB upload.</td>
</tr>
<tr>
<td>Resyncing</td>
<td>If the MIB of the NE and the MIB image on the management system are out of synchronization, then the management system invokes a resynchronization. The management state shows the progress of the operation. If executed properly, it should display, in order: <em>Normal</em>, <em>Resyncing</em>, <em>Normal</em>, <em>ReEvaluatingFaultStatus</em>, <em>Normal</em>.</td>
</tr>
<tr>
<td>ReEvaluating FaultStatus</td>
<td>After a resynchronization, the management system initiates a reevaluate fault status operation.</td>
</tr>
<tr>
<td>Downloading</td>
<td>A MIB download has been started by the management system. The management state is set to <em>Normal</em> during the downloading process. If the MIB download is in progress when a loss of association occurs, then the management state will remain <em>Downloading</em>.</td>
</tr>
</tbody>
</table>

### EMS connection state

Indicates whether an active connection (CMISE association) exist to the element manager (ITM-SC).
Retrieve NE slot information

Overview

Purpose

Use this procedure to view how the slots of a provisioned network element are configured.

Contents

| Viewing NE slot information   | 5-31 |
| Parameters for viewing NE slot information | 5-32 |
Viewing NE slot information

When to use

Follow these steps to view the configuration of slots in a provisioned network element.

Related information

The following procedures are related:

- Provision Slots
- “Confirm the MIB” (p. 5-25)
- View Hardware Inventory - Slots
- “Concepts” (p. 5-4)

Before you begin

No prerequisites or precautions are needed.

Procedure

Follow these steps to view the configuration of slots in a provisioned network element.

1. Select Provisioning → Equipment → Provisioned NE Components and select a slot from the list Provisioned Slots in the Provisioned NE Components window or select Provisioning → Equipment → Shelf Display and right-click on a slot.

2. Click Details.
   
   Result: The Provisioned NE Slot Information window appears with the information for the selected slot.

3. Click Close.
   
   Result: The Provisioned NE Slot Information window disappears.

4. Click Close.
   
   Result: The Provisioned NE Components or the Shelf Display window disappear.

End of steps
Parameters for viewing NE slot information

Slot

The slot position is given here.

Actual unit

The unit physically present in the selected slot.

Expected unit

The type of unit provisioned in the listed slot is shown.

Slot state

Displays the status of the listed slot. The different slot states are given in the table below.

<table>
<thead>
<tr>
<th>Slot State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigned</td>
<td>Slot is assigned.</td>
</tr>
<tr>
<td>Unassigned</td>
<td>Slot is unassigned.</td>
</tr>
<tr>
<td>Auto</td>
<td>Slot is provisioned but waiting for unit. Once the provisioned unit is present, the slot state will automatically change to Assigned.</td>
</tr>
</tbody>
</table>

Selected slot

Indicates the slot selected.

Operation

When assigning units, an operation must be chosen. The choices are detailed in the following table.

<table>
<thead>
<tr>
<th>Slot State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign</td>
<td>Assigns the unit to the slot.</td>
</tr>
<tr>
<td>Unassign</td>
<td>The slot is configured to be empty. The NE will not expect any unit to be present in this slot.</td>
</tr>
<tr>
<td>Auto</td>
<td>Automatically assigns the unit to the slot once the NE establishes the presence of a unit of the correct type. Until this time, the slot acts as unassigned.</td>
</tr>
</tbody>
</table>
Retrieve shelf display

Overview

Purpose

Use this procedure to retrieve an overview about shelf and slots by a graphical display.

Contents

| Viewing the shelf display     | 5-34 |
| Parameters for viewing shelf display | 5-35 |
Viewing the shelf display

When to use

Follow these steps to view the shelf display.

Related information

The following procedures are related:

- Provision slots
- Port provisioning

Before you begin

No prerequisites or precautions are needed.

Procedure

Follow these steps to view the configuration of slots in a provisioned network element.

1. Select **Provisioning → Equipment → Shelf Display**.

   **Result:** The **Shelf Display** window appears. It shows a graphical overview of the shelf, the slots, and the units.

2. Right-click on a slot or a unit.

   **Result:** A pop-up menu opens showing the following items:

   - Assign/Unassign
   - Port
   - Protection
   - Details
   - Alarms

3. Select the required item and view the respective parameters.

4. Click **Close**.

   **Result:** The **Shelf display** window disappears.

END OF STEPS
Parameters for viewing shelf display

Report...

Via this button a report is generated which stores all data retrieved for the current shelf display. The data stored includes general information like the NE name and the date and time of the report generation. Furthermore it includes specific data, for example, the equipment configuration.

If you click on Report… you are prompted for a filename.

Update Alarms...

Via this buttons the current alarms are retrieved in order to update the alarm indicators.

Update Shelf...

Via this button the NE is requested for updated information and the shelf display is refreshed.

Alarm

In this group box there are three indicators showing existing alarms for the shelf. The indicators show alarms according to the severity as given in the table below.

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>Prompt</td>
</tr>
<tr>
<td>Red</td>
<td>Deferred</td>
</tr>
<tr>
<td>Yellow</td>
<td>Info</td>
</tr>
</tbody>
</table>

Assign/Unassign...

Via this button the window Assign NE Units to Slots is opened for the selected slot. When assigning units, an operation must be chosen. The choices are detailed in the following table.

<table>
<thead>
<tr>
<th>Slot State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign</td>
<td>Assigns the unit to the slot.</td>
</tr>
<tr>
<td>Unassign</td>
<td>The slot is configured to be empty. The NE will not expect any unit to be present in this slot.</td>
</tr>
<tr>
<td>Auto</td>
<td>Automatically assigns the unit to the slot once the NE establishes the presence of a unit of the correct type. Until this time, the slot acts as unassigned.</td>
</tr>
</tbody>
</table>
For detailed information please refer to chapter “Provisioning slots” (p. 5-22).

**Details…**

Via this button the window **Provisioned NE Slot Information** is opened. For detailed information on this window, please refer to chapter “Parameters for viewing NE slot information” (p. 5-32).

**Alarm**

Via this button the window **Current Alarms** is opened. In this window information on the alarms existing for the selected unit are displayed. For detailed information, please refer to chapter “View current alarms” (p. 6-18).
View hardware inventory

Overview

Purpose

Viewing the hardware inventory allows the user to see all provisioned NE components, along with all of the units’ relevant numeric codes.

Contents

<table>
<thead>
<tr>
<th>Viewing hardware inventory - shelf</th>
<th>5-38</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing hardware inventory - slot</td>
<td>5-39</td>
</tr>
<tr>
<td>Parameters for viewing hardware inventory</td>
<td>5-41</td>
</tr>
</tbody>
</table>
Viewing hardware inventory - shelf

When to use

Viewing the hardware inventory allows the user to see all provisioned NE components, along with all of the units’ relevant numeric codes.

Related information

Related procedures include:
- Provision Slots
- View NE Slot Information
- “Concepts” (p. 5-4)

Before you begin

No prerequisites or precautions are needed.

Procedure

Follow these steps to view the hardware inventory for the shelf of an NE.

1. To view details concerning the shelf, select Provisioning → Equipment → Provisioned NE Components.
   
   **Result:** The Provisioned NE Components window appears.

2. Click HW Inv.
   
   **Result:** The Provisioned NE Hardware Inventory window appears with relevant information concerning the shelf.

3. Click Close.
   
   **Result:** The Provisioned NE Hardware Inventory window disappears.

4. Click Close.
   
   **Result:** The Provisioned NE Components window disappears.

END OF STEPS
Viewing hardware inventory - slot

When to use

The purpose of these steps is to view the hardware inventory for an NE subrack slot.

Related information

Related procedures include:

- Provision Slots
- View NE Slot Information
- “Concepts” (p. 5-4)

Before you begin

No prerequisites or precautions are needed.

Procedure

Follow these steps to view the hardware inventory for an NE subrack slot.

1. To view hardware details concerning a slot, select Provisioning → Equipment → Provisioned NE Components and select a slot from the list Provisioned Slots in the Provisioned NE Components window or select Provisioning → Equipment → Shelf Display and right-click on a slot.

2. Click Details.

   Result: The Provisioned NE Slot Information window appears with the information for the selected slot.

3. Click HW Inv.

   Result: The Provisioned NE Hardware Inventory window appears with relevant information concerning this slot.

4. Click Close.

   Result: The Provisioned NE Hardware Inventory window disappears.

5. Click Close.
Result: The Provisioned NE Components window disappears.

END OF STEPS
Parameters for viewing hardware inventory

Selection

Displays the shelf type. Only displayed when viewing hardware information for a shelf.

Item Code

The special alphanumeric code associated with the desired unit.

COM code

The nine character identifier for the hardware component selected.

IM

Indicates the interchangeability marker. This is a code indicating the ability of a component to function in the place of another, different type of component.

Serial #

Shows the serial number of the displayed component.
View SFP inventory data

Overview

Purpose

The system checks the Alcatel-Lucent specific SFP modules labeling content of all SFPs plugged in and provides a license check if Alcatel-Lucent certified SFPs are used. In case non Alcatel-Lucent certified SFPs are plugged in, the system prohibits the operation of the related ports.

Viewing the SFP inventory data allows you to see the SFPs relevant data like vendor, comcode etc. Therefore you can verify why, for instance, a specific SFP doesn't work.

Contents

| Viewing SFP inventory                          | 5-43 |
| Parameters for viewing SFP inventory data      | 5-44 |
Viewing SFP inventory

When to use

The purpose of these steps is to view the SFP inventory data of a SFP inserted in an NE.

Before you begin

No prerequisites or precautions are needed.

Procedure

1. To view details concerning the shelf, select Provisioning → Transport → Ports or select Provisioning → Equipment → Shelf display and right-click on a shelf or unit and select Port from the pop-up menu.

   **Result:** The Provisioned NE Port Filter window appears.

2. Select the All Ports radio button and click OK.

   **Result:** The Provisioned NE Port Information List window appears.

3. Select a port of type SFP.

4. Click Details.

   **Result:** The Pluggable Module Information window appears with relevant information concerning the SFP.

5. Click DDM Info.

   **Result:** The SFP Digital Diagnostic Monitor Information window appears.

6. Click Close.

   **Result:** The Pluggable Module Information window disappears.

**E N D O F S T E P S**
Parameters for viewing SFP inventory data

Selection

Displays the selected pluggable module.

Administrative State

Displays the administrative state of the pluggable module

The following values are possible:

- module accepted,
- module rejected,
- module allowed,
- module not present

Displayed SFP inventory data

The following inventory data is shown for the displayed component:

<table>
<thead>
<tr>
<th>Information</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Identifier</td>
<td>SFP transceiver or unspecified</td>
</tr>
<tr>
<td>Connector Type</td>
<td>The Connector Type is displayed (Example: LC). If this attribute is not available from the NE, an empty string is displayed.</td>
</tr>
<tr>
<td>Transceiver Code</td>
<td>The Transceiver Code is contained in the EEPROM of the SFP. If this attribute is not available from the NE, an empty string is displayed.</td>
</tr>
<tr>
<td>Link Max Length</td>
<td>Dependent on the value of the Link Type: LENGTH are 1 km, 10 m, 10 m, or 1 m respectively.</td>
</tr>
<tr>
<td>Vendor Name</td>
<td>A 16 byte character string, left aligned and padded on the right with ASCII spaces. An all zero value indicates an unspecified vendor name. Either the vendor name or OUI should be present.</td>
</tr>
<tr>
<td>Vendor OUI</td>
<td>The IEEE Organizationally Unique Identifier (see <a href="http://standards.ieee.org/regauth/oui/index.shtml">http://standards.ieee.org/regauth/oui/index.shtml</a>) of the vendor. An all zero value indicates an unspecified OUI. Either the vendor name or OUI should be present.</td>
</tr>
<tr>
<td>Part Number</td>
<td>A 16 byte character string, left aligned and padded on the right with ASCII spaces. An all zero value indicates an unspecified part-number.</td>
</tr>
<tr>
<td>Information</td>
<td>Meaning</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Revision Number</td>
<td>A 4 byte character string, left aligned and padded on the right with ASCII spaces. If this attribute is not available from the NE, an empty string is displayed.</td>
</tr>
<tr>
<td>Vendor Serial Number</td>
<td>This attribute represents the internal Serial Number of the Vendor, which is not represented on the label of the SFP and not linked to the WES code. If this attribute is not available from the NE, an empty string is displayed.</td>
</tr>
<tr>
<td>Com Code</td>
<td>The Alcatel-Lucent Comcode is suffixed by '000' in case a 9 digit number is used. If this attribute is not available from the NE, an empty string is displayed.</td>
</tr>
</tbody>
</table>
| Lucent Compatibility Byte| The Compatibility byte is a positive integer between 0 and 255 containing a code that represents the Alcatel-Lucent system(s) for which the SFP is intended. Only the number is displayed on the user interface:  
  - 16 or 17 is used for AMS,  
  - 32 or 33 is used for DMX,  
  - 64 or 65 is used for Metropolis ADM (Universal Shelf) and  
  - 128 or 129 is used for Lambda Unite. |
| Lucent Unique ID         | A 4 byte HEX field.                                                                                                                                 |
| SFP Vendor ID            | A 4 byte character string (20HEX). Represents the Manufacture Location Code of the Alcatel-Lucent Serial Number, which is as WES code also represented on the label of the SFP. |
| WES Serial Number        | An 18 byte character string. SFP’s. Represents the Alcatel-Lucent specific Serial Number, which is as WES code (18 Byte) also represented on the label of the SFP. |
| SFP Length               |                                                                                                                                              |
### Information | Meaning
--- | ---
Module Qualifier | Derived from SFP SEEPROM information.  
- 1000BASE-SX  
- 1000BASE-LX  
- I-1  
- S-1.1  
- L-1.1  
- L-1.2  
- L-1.3  
- I-4  
- S-4.1  
- L-4.1  
- L-4.2  
- L-4.3  
- …

Module Type | Derived from SFP SEEPROM information.  
- NOT AVAILABLE  
- STM-1  
- STM-1/STM-4  
- STM-4  
- STM-16  
- GbE  
- UNKNOWN

Apparatus / Item Code | The Apparatus / Item Code is a 12 byte character string.  
Example: OM16CS59

Interchangeability Marker | The Interchangeability Marker is a 6 byte character string, left aligned and padded on the right with ASCII spaces (20HEX)

### Displayed SFP DDM data

The following DDM data is shown for the displayed component:
<table>
<thead>
<tr>
<th>Information</th>
<th>Meaning</th>
</tr>
</thead>
</table>
| SFP Temperature        | Upper alarm threshold = maximum case temperature specified value + accuracy allowance  
                         | Lower alarm threshold = minimum case temperature specified value – accuracy allowance |
| Alarm flag             | Alarm flags indicate conditions likely to be associated with an in-operative link and cause for immediate action. |
| Warning flags          | Warning flags indicate conditions outside the normally guaranteed bounds but not necessarily causes of immediate link failures. |
| Supply voltage         | Upper alarm threshold = maximum supply voltage specified value + accuracy allowance  
                         | Lower alarm threshold = minimum supply voltage specified value - accuracy allowance |
| Optical Transmit Power | Upper alarm threshold = EOL maximum optical output power + accuracy allowance  
                         | Lower alarm threshold = EOL minimum optical output power - accuracy allowance |
| Optical Receive Power  | Upper alarm threshold = EOL maximum optical overload input power + accuracy allowance  
                         | Lower alarm threshold = EOL minimum optical sensitivity input power - accuracy allowance |
| Laser Bias Current     | Upper alarm threshold = 150% of BOL laser bias current                  
                         | Lower alarm threshold = not needed                                      |

**Buttons and Actions**

The following options are available:

<table>
<thead>
<tr>
<th>If you select ...</th>
<th>Then ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unassign</td>
<td>Unassigns the pluggable module.</td>
</tr>
<tr>
<td>Update</td>
<td>Allows you to update the current view or dialog with the most recent information. If a dialog has been open for a while, the data displayed may not still be current. The Update button allows you to obtain the most recent information.</td>
</tr>
<tr>
<td>Close</td>
<td>Closes the window.</td>
</tr>
</tbody>
</table>
View and edit node details

Overview

Purpose

This procedure allows the node details to be viewed, and one element, namely the node location, to be edited.

Contents

| Viewing and editing node details | 5-49 |
| Parameters for viewing or editing node details | 5-51 |
Viewing and editing node details

When to use

The purpose of these steps is to view management information or to change the location of the NE.

Related information

The following procedure is related:

• Create a Node
• “Confirm the MIB” (p. 5-25)

Before you begin

Before performing this procedure make sure:

• Before editing node details, be certain to have the new location for the NE.

The following precaution is important to consider:

• Only one parameter, the location, can be changed by the user. To change other node details, the MIB must be overwritten and a new node created.

Procedure

1 Select Management → Node Details.
   Result: The Node Details window appears.

2 To change the NE Location, click Edit. Otherwise, go to step 5.
   Result: The Edit Node Details window appears.

3 Enter the new NE Location.
   Result: The correct location now appears in the area provided.

4 Click OK.
   Result: The new NE Location is entered, and the window Edit Node Details disappears.

5 Click Close.
Result: The Node Details window disappears.

END OF STEPS
Parameters for viewing or editing node details

NE name

The network element’s name is listed. The name must be unique across management domains. If the NE is not managed by the ITM-NM, then the name may be up to 20 characters in length. If the NE will be managed by the ITM-NM, then the name must be 3 to 10 characters long with the last three characters a slash and two digits. Only A-Z, 0-9, _, /, and - are permitted for network elements managed by the ITM-NM. An example of an ITM-NM compatible name is LONDON/02.

NE location

The location of the network element is given. The location may have up to 20 uppercase or lowercase characters, digits, and spaces.

MIB state

The status of the MIB is indicated. The possible values are given in the table below.

<table>
<thead>
<tr>
<th>MIB State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Empty</td>
<td>An empty system controller (SC) has been inserted or the MIB was cleared after starting an MIB download by the management system. If the MIB State is empty, the management system can proceed with the MIB download.</td>
</tr>
<tr>
<td>Filled</td>
<td>The NE possesses a valid MIB, which has been confirmed.</td>
</tr>
<tr>
<td>Filled Unknown</td>
<td>The NE has a MIB, however, it is of unknown validity. This can occur, for instance, if one SC is replaced by another SC having a MIB.</td>
</tr>
<tr>
<td>Filled Not Confirmed</td>
<td>The NE has a MIB, however, it has not yet been confirmed by the ITM-CIT or ITM-SC. The procedure “Confirm or Update MIB” gives the steps necessary to confirm the MIB. Once confirmed the state will become Filled.</td>
</tr>
<tr>
<td>Waiting for Upload</td>
<td>This state is only possible when the NE is managed by the ITM-SC. After confirmation of the MIB, the NE performs a reset and loses its association with the ITM-SC. when the NE restarts, the MIB State becomes Waiting for Upload. When the ITM-SC reassociates with the NE and detects this MIB state, an MIB upload is performed, and the state will then become Filled.</td>
</tr>
</tbody>
</table>
**Management state**

The state of the association with the management system is displayed. The possible states are given in the following table.

<table>
<thead>
<tr>
<th>Management State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td><em>Normal</em> will be displayed whenever management operations have been completed. In other words, the management system has completed the MIB upload, MIB download, MIB resynchronization, or reevaluation of fault status.</td>
</tr>
<tr>
<td>Uploading</td>
<td>The management system is performing an MIB upload.</td>
</tr>
<tr>
<td>Resyncing</td>
<td>If the MIB of the NE and the MIB image on the management system are out of synchronization, then the management system invokes a resynchronization. The management state shows the progress of the operation. If executed properly, it should display, in order: <em>Normal</em>, <em>Resyncing</em>, <em>Normal</em>, <em>ReEvaluatingFaultStatus</em>, <em>Normal</em>.</td>
</tr>
<tr>
<td>ReEvaluating FaultStatus</td>
<td>After a resynchronization, the management system initiates a reevaluate fault status operation.</td>
</tr>
<tr>
<td>Downloading</td>
<td>A MIB download has been started by the management system. The management state is set to <em>Normal</em> during the downloading process. If the MIB download is in progress when a loss of association occurs, then the management state will remain <em>Downloading</em>.</td>
</tr>
</tbody>
</table>

**EMS connection state**

Indicates whether an active connection (CMISE association) exist to the element manager (ITM-SC).
View and edit MDI information

Overview

Purpose

Use this procedure to view and edit Miscellaneous Discrete Input (MDI) names.

General information

The system provides a number of in- and outputs that can be used to read the status of external alarm points and to drive external devices. Applications could be: door contacts and dedicated station alarm loops. These inputs and outputs are called Miscellaneous Discretes.

The 1643 AM or 1643 AMS is equipped with four Miscellaneous Discrete Inputs (MDIs) and four Miscellaneous Discrete Outputs (MDOs).

The function of the MDIs is to signal external status information. On activation of an MDI an alarm is raised showing the MDI number and name tag.

The MDIs are floating with respect to system ground. Activation of an MDI requires an external voltage in the range of 18-72 V. An MDI is considered active when resistance between the external voltage source and input is less than 10 Ω. An MDI is considered inactive when resistance between the external voltage source and input is more than 500 kΩ.

Contents

| Viewing and editing MDI information | 5-54 |
| Parameters for viewing or editing MDI information | 5-56 |
Viewing and editing MDI information

When to use

The purpose of these steps is to view and edit MDI names.

Related information

The following procedure is related.

- View and Edit MDO Information

Parameters used in this procedure can be found at “Parameters for viewing or editing MDI information” (p. 5-56).

Before you begin

Before performing this procedure make sure that the:

- The miscellaneous discrete input are physically connected to the NE.

The following precaution should be noted.

- The MDI name can be no longer than 26 characters.
- It is only possible to have four MDIs per network element.
- The user should select names for the Miscellaneous Discrete Inputs that are both well-chosen and unique.

Procedure

Follow these steps to view and edit MDI names.

1. Select Provisioning → Equipment → MDI.
   
   **Result:** The Provisioned MDI window appears.

2. Select an MDI from the list under *Id* and *Name*.
   
   **Result:** The appropriate MDI is selected.

3. Click **Edit**.
   
   **Result:** The Edit Provisioned MDI window is displayed. The current name of the selected MDI is displayed on the name line of this window.

4. Enter the *Name* (max. 26 characters).
5 Click **OK**.

**Result:** The new MDI name is entered and the Edit Provisioned MDI window is closed.

6 Click **Close**.

**Result:** The Provisioned MDI window disappears.

**END OF STEPS**
Parameters for viewing or editing MDI information

Id

The number associated with the MDI.

Name

Indicates the name of the MDI.
View or edit MDO information

Overview

Purpose

Use this procedure to view and edit MDO names and statuses.

General information

The system provides a number of in- and outputs that can be used to read the status of external alarm points and to drive external devices. Applications could be: door contacts and dedicated station alarm loops. These inputs and outputs are called Miscellaneous Discretes.

The 1643 AM or 1643 AMS is equipped with four Miscellaneous Discrete Inputs (MDIs) and four Miscellaneous Discrete Outputs (MDOs).

MDOs for the 1643 AM or 1643 AMS have a number of functions:

1. Alarm signaling function:
   This is the so called NE-Controlled state. It is initiated if neither of the MDO’s have a label. In this state the MDOs have the following behavior:
   - MDO 2 is active if one or more local alarms with severity “PROMPT” are raised
   - MDO 3 is active if one or more local alarms with severity “DEFERRED” are raised
   - MDO 4 is active if one or more local alarms with severity “INFO” are raised

2. External driving function:
   From the User Interface (ITM-SC, ITM CIT) each MDO can be activated. When the system is powered, the contact can be set to active (closed) or inactive (opened) under control of the ITM-SC or ITM CIT.

3. Fail-Save Alarming function:
   Dedicated to MDO1. This contact is closed if the system is not powered.

The MDOs are floating with respect to system ground. An active MDO behaves as a voltage free resistance of less than 10 Ω between the output connection and its associated return. It shall be capable of carrying currents of not more than 0.5 A DC. An inactive MDO behaves as a voltage free resistance of more than 500 kΩ between the output connection and its associated return. It is capable of withstanding voltages of not more than 72 V DC.
## Contents

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing or editing MDO information</td>
<td>5-59</td>
</tr>
<tr>
<td>Parameters for viewing or editing MDO information</td>
<td>5-61</td>
</tr>
</tbody>
</table>
Viewing or editing MDO information

When to use

Follow these steps to view and edit MDO names and statuses.

Related information

For related information refer to:

- “View and Edit MDI Information”
- “Parameters for viewing or editing MDO information” (p. 5-61).

Before you begin

Before performing this procedure make sure that:

- the miscellaneous discrete input are physically connected to the NE.

The following precaution should be noted:

- The MDO name can be no longer than 26 characters.
- It is only possible to have four MDOs per network element.
- The user should select names for the Miscellaneous Discrete Outputs that are both well-chosen and unique.

Procedure

Follow these steps to view or edit MDO names and statuses.

1. Select Provisioning → Equipment → MDO.
   
   Result: The Provisioned MDO window appears.

2. Select an MDO from the list under Id and Name.
   
   Result: The appropriate MDO is selected.

3. Click Edit.
   
   Result: The Edit Provisioned MDO window is displayed. The current name of the selected MDO is displayed on the name line of this window.

4. Enter or change the Name (max. 26 characters).
5 Set the **Status** of the MDO to **Active** (closed loop), **Inactive** (open loop).

**Result:** The field **Status** is defined.

6 Click **Select**.

**Result:** The Select Alarm Signalling window appears.

7 Set the **Alarm Signalling Mode** to **Local alarms, Centralized alarms, or Centralized MDI**.

**Result:** The **Alarm Signalling Mode** is defined.

8 Click **OK**.

**Result:** Remote alarming via MDI/MDO is entered, and the Select Alarm Signalling Mode window is closed.

9 Click **Close**.

**Result:** The Provisioned MDO window disappears.

---

**END OF STEPS**
### Parameters for viewing or editing MDO information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Id</strong></td>
<td>The number associated with the MDO.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Indicates the name of the MDO.</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>Indicates the status of the MDO. The possible values are <em>Active, Inactive, and NE Controlled</em>.</td>
</tr>
<tr>
<td><strong>Alarm signaling mode</strong></td>
<td>Indicates how alarms or MDI information will be put through. The possible values are <em>Local alarms, Centralized alarms, or Centralized MDI</em>.</td>
</tr>
</tbody>
</table>
Overview

Purpose

The purpose of port provisioning is to get an overview of all the physical ports of the network element or a specific unit, and to change the settings of these ports.

Contents

<table>
<thead>
<tr>
<th>Provisioning ports</th>
<th>5-63</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters for Port Provisioning</td>
<td>5-65</td>
</tr>
</tbody>
</table>
Provisioning ports

When to use

Use this procedure to:

- know which ports are provisioned in an NE and how they are provisioned
- change the port mode for the alarm handling
- enable or disable test loops

Note: The provisioning ports procedure is also applicable to X5IP. Also note that the type of the port E/FE/GbE LAN refers to 10/100/1000BASE-T(X) Ethernet Interface for the X5IP card.

Related information

Before starting to modify NE ports it is assumed that:

- information about which port on which unit needs to be modified is available.
- there is no traffic on the ports that you want to test with a loopback.
- take care that loopbacks are disabled for normal operations. No normal traffic is possible when a loopback is enabled.

Before you begin

Provisioning of timing ports is described in Chapter 7, “Timing provisioning”.

Procedure

The following procedure describes how a port can be provisioned. Each port type has a different window, but the procedure is the same for all port types.

1. Select Provisioning → Transport → Ports or select Provisioning → Equipment → Shelf display and right-click on a shelf or unit and select Port from the pop-up menu. The Provisioned NE Port Filter is displayed.

   Choose:
   - All Ports to list all available ports -
   - Ports from Slot to restrict the amount of data to be uploaded from the NE. Only the available ports from the selected slot are listed.

2. Click OK.
Result: The Provisioned NE Port Information List window appears with a list of ports.

3 Select one of the ports in the Provisioned NE Port Information List window and click Details.

Result: Depending on the Type of the selected port, a Port Information window appears. There is a separate Port Information window for each port type.

4 Click Edit and the Edit Port Information window appears.

Result: There is also a separate Edit Port Information window for each port type. Refer to “Parameters for Port Provisioning” (p. 5-65).

Note: The Loopback State can be changed in the Edit Port Information window.

5 Change the Port mode, Auto-Negotiation mode and LPT mode to Enabled and click OK.

Result: The edit window closes and the information window appears with the Auto-Negotiation mode enabled and also the LPT Mode enabled.

END OF STEPS
Parameters for Port Provisioning

Introduction

For each port type there is a special window to provision the ports. The 1643 AM or 1643 AMS always has two STM-1 or STM-4 line ports and sixteen 2 Mbit/s ports. If an additional tributary unit is installed, SDSL, 34 Mbit/s, 45 Mbit/s, X.21, or LAN (Ethernet) ports can also be available.

Port types

The following table shows the port types and which parameters are valid for each port.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>1.5 Mbit/s</th>
<th>2 Mbit/s</th>
<th>SDSL</th>
<th>ISDN</th>
<th>34 Mbit/s</th>
<th>45 Mbit/s</th>
<th>X.21</th>
<th>LAN</th>
<th>STM-1 optical or electrical</th>
<th>STM-1 or 4 line</th>
</tr>
</thead>
<tbody>
<tr>
<td>port mode</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>port mode time</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>2 Mbit/s signal mapping</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>loopback state</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>TS0 termination</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>x</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>cable length</td>
<td>x</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>x</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>degraded signal threshold</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>x</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>optical wavelength</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>laser status</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>auto negotiation</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>x</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Ethernet</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>x</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Port

The name of the physical ports consists of two parts separated by a dot. The first part is related to the slot name, the second part is the port number within that slot.

Example: LP2.1, TP1.3, LAN2.1

Type

The Type indicates the type of signal for which the port is an interface point.

Example: 2 Mbit/s, STM-1.

Port mode

The Port Mode controls whether input signals should be monitored or not. The following values can be set.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitored</td>
<td>The port is configured to provide service and the port signal is monitored.</td>
</tr>
<tr>
<td>Auto</td>
<td>The port is configured not to provide service yet. Use this mode when the signal source in the remote NE is not operational yet. As soon as the NE establishes the continuous presence of a fault-free signal for a certain period (Port Mode Time), the port automatically changes to Monitored.</td>
</tr>
<tr>
<td>Not Monitored</td>
<td>The port is configured not to monitor the port signal on the port. No alarms are generated for this port. If there still is a signal present on the not monitored port it is possible to receive a Not Expected Input Signal (NES) alarm. The alarm status of NES must then be provisioned Reported.</td>
</tr>
</tbody>
</table>

Port mode time

The time in minutes during which a fault-free signal must be received continuously before the Port Mode switches from Auto to Monitored. The Port Mode Time can be set from 0-30 minutes and the default is 10 minutes.

2 Mbit/s signal mapping

Signal Mapping indicates the type of mapping used to map the 2 Mbit/s signal into a VC-12. On the 1643 AM or 1643 AMS network element only asynchronous mapping is possible. Asynchronous mapping allows the 2 Mbit/s signal to float within the fixed allocations within the VC-12.
TS0 termination
Displays the TS0 termination mode (Transparent or Double Terminated ISDN in PRI or leased-line modes) of the selected port.

Loopback state
Loopbacks are used to test the physical ports.
- No Loop is set for normal use of the physical port. The port is not looped back for testing.
- An Inloop is a loopback that routes an input signal, received at the physical port, directly back to its corresponding output without altering the signal format. The inloop can be used to test the connectors. Only one inloop can be provisioned at the same time.
- An Outloop is a loopback that routes an output signal, coming from the cross connect, at the physical port back to the corresponding input port. The Output can be used to test how the signal passes through the system.

Cable length
For 1.5 Mbit/s (DS1) and 45 Mbit/s (DS3) signals.
For 1.5 Mbit/s signal a cable length of 0 to 200 metres can be provisioned in steps of 40 metres.
For 45 Mbit/s a cable length can be up to 136 metres (450 feet). Two levels can be provisioned, covering the following cable length:
- 0 - 35 metres (0-120 feet)
- 35 - 136 metres (120 - 450 feet)

Degraded signal threshold
Indicates the number of errors (EB: Errored Blocks) that can occur during the given period. If this number is exceeded and the Port Mode is set to Monitored, a signal degrade alarm is generated. A choice can be made between two thresholds. The section "Provision Degraded Signal Thresholds" describes the setting of these thresholds.

Auto-negotiation
It is possible to enable or disable the Auto-negotiation function at the physical layer of the LAN port by setting the mode to enabled respectively disabled. Setting the mode to disabled will be done when the TransLAN™ board interworks with equipments not supporting the auto-negotiation function. In this case the user can force the port speed (10 Mbit/s or 100 Mbit/s) and select the half duplex or full duplex mode.
Link Pass-through

The Link pass-through mode is only supported on ports that operate on a one-to-one association with a WAN port using GFP encapsulation. Users can enable or disable the Link pass-through mode per port.

Ethernet port parameters

The following Ethernet port parameters can be set when the auto-negotiation is disabled:

- port speed; set to 10 Mbit/s or 100 Mbit/s
- duplex mode; set to half duplex or full duplex
- pause mode; this function can be set to enabled or disabled only when the duplex mode is full duplex.
6 Alarm management

Overview

Purpose

The purpose of alarm management is to monitor the equipment and transmission for events that are raised under the Management System (MS) Supervision and to display the information on the interface of the MS, called the Integrated Transport Manager — Craft Interface Terminal (ITM-CIT).

Objective

The objectives of this chapter are:

- To identify the daily alarm management tasks that can be performed on the ITM-CIT;
- To discuss the alarm management concepts as they apply to the ITM-CIT;
- To identify current and history alarms, and to gather information regarding the location, severity, description, probable cause(s), correlated alarms;
- To locate recommended trouble-clearing actions for current alarms;
- To describe how to apply display filters and sort criteria on the different ITM-CIT alarm lists windows;

Outcome

The expected outcome of alarms management is an interface which alerts maintenance personnel of incoming alarms and their corresponding severity level, as well as relevant detailed information and recommended trouble-clearing procedures.

Intended use

This chapter is intended to maintenance personnel who are responsible to monitor the alarms on a network, using the ITM CIT. It is assumed that some knowledge is available on how to operate the ITM-CIT. For more information, refer to Chapter 2, “Getting Started”.

Scope

The chapter includes procedures to view the alarms, their severity level, the associated probable cause(s), as well Alcatel-Lucent recommended trouble-clearing action(s).

However, specific procedures to restore network nodes to normal operation after system failures are described in the *Alarm Messages and Trouble Clearing Guide* and will not be covered in this chapter.

High level view

Maintenance involves two groups of activities: *preventive* and *corrective*. The ITM-CIT offers a collection of corrective activity features that are described all together as *Event Management*. To accomplish this, the ITM-CIT provides the user with information regarding the event location, nature, probable cause, severity, as well as a recommended trouble-shooting action.

As an example, the table below gives a non-exhaustive list of maintenance activities that can be performed on the management system. Most tasks are correlated to one (or more) ITM-CIT window(s).

<table>
<thead>
<tr>
<th>Maintenance Activities</th>
<th>Using ITM-CIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Identify the alarms: Station Alarms, Bay Alarms, Unit Alarms, ITM-CIT alarms;</td>
<td>Yes (only for CIT alarms)</td>
</tr>
<tr>
<td>2. Evaluate severity of alarm, the correlated alarms, the probable cause(s);</td>
<td>Yes</td>
</tr>
<tr>
<td>3. Identify the alarm source physical location;</td>
<td>Yes</td>
</tr>
<tr>
<td>4. Interpret the information</td>
<td>No</td>
</tr>
<tr>
<td>5. Recommend trouble-clearing action;</td>
<td>Yes</td>
</tr>
<tr>
<td>6. Take action (depending on the alarm)</td>
<td>Yes</td>
</tr>
<tr>
<td>7. Perform preventive maintenance (please refer to Chapter 10, “Performance monitoring”)</td>
<td>Yes</td>
</tr>
</tbody>
</table>

This chapter will describe the relevant windows where the ITM-CIT can be used to complete the above-mentioned job tasks. The first three tasks of the previous table consist in collecting information in order to make a decision concerning the resolution of the alarm. These tasks can be completed by consulting the information available in the relevant ITM-CIT windows.

Contents

<p>| Concepts | 6-4 |</p>
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events origin and flow</td>
<td>6-5</td>
</tr>
<tr>
<td>Event properties</td>
<td>6-8</td>
</tr>
<tr>
<td>Event display</td>
<td>6-12</td>
</tr>
<tr>
<td>Alarm supervision concepts</td>
<td>6-13</td>
</tr>
<tr>
<td>Event history</td>
<td>6-14</td>
</tr>
<tr>
<td><strong>Alarm identification</strong></td>
<td><strong>6-15</strong></td>
</tr>
<tr>
<td>View alarm summary</td>
<td>6-16</td>
</tr>
<tr>
<td>Set up filters</td>
<td>6-17</td>
</tr>
<tr>
<td>View current alarms</td>
<td>6-18</td>
</tr>
<tr>
<td>View alarm details</td>
<td>6-20</td>
</tr>
<tr>
<td>Archive cleared alarms</td>
<td>6-22</td>
</tr>
<tr>
<td>Parameters for identifying the alarms</td>
<td>6-23</td>
</tr>
<tr>
<td><strong>Provision alarm options</strong></td>
<td><strong>6-28</strong></td>
</tr>
<tr>
<td>Setting the alarm options</td>
<td>6-29</td>
</tr>
<tr>
<td>Parameters for setting the alarm options</td>
<td>6-30</td>
</tr>
<tr>
<td><strong>Provision alarm severity assignment profiles (ASAP)</strong></td>
<td><strong>6-32</strong></td>
</tr>
<tr>
<td>Create a new ASAP</td>
<td>6-33</td>
</tr>
<tr>
<td>Modifying an existing ASAP</td>
<td>6-35</td>
</tr>
<tr>
<td>Delete an existing ASAP</td>
<td>6-37</td>
</tr>
<tr>
<td>Retrieve an existing ASAP</td>
<td>6-38</td>
</tr>
<tr>
<td>Assign an ASAP</td>
<td>6-39</td>
</tr>
<tr>
<td>Retrieve an assignment list for a specified ASAP</td>
<td>6-44</td>
</tr>
<tr>
<td>Retrieve assigned ASAPS for a specified managed object</td>
<td>6-45</td>
</tr>
<tr>
<td>Parameters for “ASAP Assignment”</td>
<td>6-46</td>
</tr>
<tr>
<td>Alarm Severity Assignment Profile</td>
<td>6-47</td>
</tr>
<tr>
<td><strong>Alarm supervision</strong></td>
<td><strong>6-64</strong></td>
</tr>
<tr>
<td>Supervise alarms</td>
<td>6-65</td>
</tr>
<tr>
<td>Parameters for supervising alarm</td>
<td>6-72</td>
</tr>
<tr>
<td><strong>View historical data</strong></td>
<td><strong>6-77</strong></td>
</tr>
<tr>
<td>Historical data</td>
<td>6-78</td>
</tr>
<tr>
<td>Retrieving historical data</td>
<td>6-79</td>
</tr>
<tr>
<td>Parameters for retrieving historical data</td>
<td>6-81</td>
</tr>
</tbody>
</table>
Overview

Purpose

The purpose of this section is to present the theoretical concepts related to alarm management and to identify which job tasks can be performed in the relevant ITM-CIT windows by maintenance personnel. The details regarding the procedures to use those windows are treated in upcoming sections of this chapter.

The procedures to use those windows are treated in more detail in this chapter.

Contents

| Events origin and flow | 6-5 |
| Event properties       | 6-8 |
| Event display          | 6-12|
| Alarm supervision concepts | 6-13|
| Event history          | 6-14|
Events origin and flow

Introduction

Events refer to unusual occurrence that happen during transmission and that could potentially, or factually, affect the service. These events are noticed by the management system which displays the information with an associated severity level, according to the way it was configured.

Event types and flow

In fact, a lot of successive events will take place inside the NE or EMS before the user is notified on the EMS interface that a fault has occurred. The following events can be defined:

<table>
<thead>
<tr>
<th>Events</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAULT</td>
<td>The inability for the system to perform a required function. Faults can exist whether detected or not.</td>
</tr>
<tr>
<td>ANOMALY</td>
<td>The smallest observable discrepancy we can observe between the actual and the desired performance of a function. Maintenance actions are not initiated on the single occurrence of anomalies. Anomalies are used as input for defect detections.</td>
</tr>
<tr>
<td>DEFECT</td>
<td>A limited interruption of a system's component ability to perform a required function. An anomaly becomes a defect when it persists for a significant amount of time. A defect may result in consequent actions.</td>
</tr>
<tr>
<td>FAILURE</td>
<td>The termination of a system's ability to perform a required function; therefore it is an event rather than a state. If a fault is present for at least its configured validation time, it then becomes a failure. The failure declaration/clearing is time stamped (raised and cleared time) with an accuracy of 1 second.</td>
</tr>
<tr>
<td>ALARM</td>
<td>A human observable indication that draws the attention to a detected failure. Alarms may be delayed after the detection of failures. They can be divided into unit level alarms: NE level alarms and station alarms.</td>
</tr>
</tbody>
</table>

The table above can be represented with the following event flow chart:
When a **Fault** is detected, it becomes an **Anomaly** after a pre-defined time. If the defect is persistent after an **Alarm Raise Hold Off** period, it becomes a **Defect**. If a **Failure** is detected, it will be notified to the user by generating an **Alarm**. Due to the Alarm, a change of state of the NE can occur, which can generate an **Autonomous Event**. For both Autonomous Events and Alarms, a **Station Alarm** is generated after the **Station Alarm Raise Hold Off** period.

The **Station Alarm Raise Hold Off** period does not necessarily apply to all network elements.
Events displayed

Alarms and autonomous events are the only events visible to the user on the CIT or SC interface. Alarms are part of a category of user's warnings, also referred to as events. Therefore an event can be an alarm or some other type of notification, other than an alarm. Events encompass the following two classes:

- Alarm;
- Autonomous Event.

Alarm

A maintenance warning which indicates a fault on a maintenance entity because the entity has experienced a specific failure. Typically, alarms can be divided into NE alarms and station alarms. A severity level can be assigned to each alarm.

Autonomous events

Any kind of defect, failure, or alarm on Network Elements, lines or paths. An autonomous event may, or may not, have any impact on service. They do not necessarily and obligatorily lead to an alarm, but alarms may be caused by an event.
Event properties

Introduction

In order to bring the event behavior in line with the chosen maintenance philosophy event properties have to be configured. The event properties of the following events can be configured:

- Alarms
- Autonomous Events
- Station Alarm

**Important!** In general we will refer to any of the three above-mentioned, as *event*.

Purpose

The properties of an event will determine:

- *if* an event will appear;
- *when* the event will appear;
- *how* the event will appear;
- *when* the event will disappear when the problem is solved.

Event status

An autonomous event go through a short sequence of statuses before the event is considered solved and therefore, ready to be archived as historical data. Therefore, the event status is the attribute that allows to monitor where in the sequence the event finds itself at any point in time.

The sequence is the following:

- It is raised by the system;
- It gets acknowledged by a maintenance operator;
- The cause of the alarm is attended to, and the problem gets solved.

The table below describes each alarm status:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raised</td>
<td>A valid status when the conditions for alarm detection are TRUE and that the cause has not yet been acknowledged or resolved. The alarm can be reported or not.</td>
</tr>
</tbody>
</table>
### Status Description

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cleared</td>
<td>A valid status when the conditions for the alarm detection are no longer TRUE because the cause(s) of the alarm has been removed. The alarm gets cleared either by the system or by Maintenance personnel. The alarm is then transferred and displayed in the History Alarm list.</td>
</tr>
<tr>
<td>Acknowledged</td>
<td>A valid status when the alarm has been noticed and confirmed by the user but that the causes may not yet have been removed.</td>
</tr>
</tbody>
</table>

Therefore, by looking at an event status on the ITM CIT, one knows if an action has been done on a specific event, and if the cause of the problem has been resolved. Therefore, the status describes the latency or the resolution of the alarm cause(s).

### Reporting state

This is attribute that allows an event/alarm to be displayed on the management system.

There are two possible reporting states:

<table>
<thead>
<tr>
<th>Reporting State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reported</td>
<td>Independently of its severity, the event will appear on the CIT or the SC. The alarm is displayed in the Current Alarm list of the management system and on the NE motherboard as a red flashing LED for transmission alarms, or a static red LED for hardware alarms.</td>
</tr>
<tr>
<td>Not Reported</td>
<td>Independently of its severity, the event will not be displayed on the management system.</td>
</tr>
</tbody>
</table>

Each alarm reporting state can be viewed and modified whenever required. The procedures to do so are described in Chapter 6, “Alarm management”.

### Severity level

The severity is the attribute which attempts to describe the seriousness of the event. The severity level has to be decided by the end-user, and manually assigned to each alarm on the management system, according to your maintenance philosophy. The information is sent to the network element. Once these initial settings are input, the system can start monitoring events and classifying them according to their impact on service (severity).
The three possible severity levels are:

<table>
<thead>
<tr>
<th>Severity</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROMPT</td>
<td>Immediate maintenance action is required because a primary system service is being affected.</td>
</tr>
<tr>
<td>DEFERRED</td>
<td>Maintenance action is required but may be attended to later because no primary system service is being affected.</td>
</tr>
<tr>
<td>INFORMATION</td>
<td>Maintenance information: no maintenance action is required at this node.</td>
</tr>
</tbody>
</table>

**Important!** If you set the alarm reporting status to Not Reported, no attention will be raised to maintenance personal regardless of the alarm severity level.

**Provisioning severity/reporting state**

It is possible to view and to provision a severity and reporting state for each alarm, or for a specific instance on the CIT. An instance is the smallest part on a network element that can generate an alarm. This means that it is possible to modify the severity level of an alarm for a VC12 incoming at a specific port, from a given customer. A similar concept exits on the ITM-SC. For this management system, please refer to *Existing Ressources* feature.

**Alarm control**

When a defect is detected within an NE or management system, the user will be notified of this defect via an alarm after the Raise Hold Off period. This period is used to make sure the defect really exist within the NE or management system. When the defect is solved the alarm will be cleared after the Clear Hold Off period. This period is used to make sure the problem is solved and prevents the alarm reporting to blink on and off repetitively. This will address the *when* question. Please note that it is not possible to set the Raise Hold Off period on the ITM CIT.

**Alarm latching**

When latching is enabled the alarm/autonomous event must be acknowledged before the alarm moves to the history list upon clearance. When alarm latching is not enabled acknowledgment is still possible. But these alarms/autonomous events will go directly to the history list upon clearance whether acknowledged or not. This feature is only available on the ITM-SC.
Clearance acknowledgment

When Clearance Acknowledgement is licensed an alarm or autonomous event, which is initially latched, can only go to the history list after its clearance has been acknowledged. The alarms which have been acknowledged in the raised state remain after clearance in the current alarm list; they only go to the history list when their clearance has been explicitly acknowledged by the user. This feature is only available on the ITM-SC.

Alarms latched on default

All alarms (instantaneous events) are latched on default. This is to make sure the alarm will be notified by the user. So they are moved to the History List only after they have been acknowledged. This feature is only available on the ITM-SC.

Acknowledgments effective only on ITM-SC

Acknowledgments are only effective on the ITM-SC. Interaction with the network element or the NL is not expected or required in order to acknowledge alarms. Acknowledgment of alarms applies to the ITM-SC and NE created alarms. This feature is only available on the ITM-SC.

Maintenance philosophy

Within Event Management many parameters can be customized. It is expected to bring these parameters in line with the maintenance philosophy. Please obtain a consistent implementation of this philosophy in order to avoid confusion about solving problems within the transmission network.
Alarm notifications are issued by the system and displayed on the management system. They are used to inform on the presence of alarms and therefore, allows the operator to monitor and supervise the alarms on a given NE. The alarm notifications contain an array of information such as:

- Time at which the alarm was raised or cleared;
- Location of the alarm;
- Probable causes (alarm types);
- Severity level.

Alarm notifications can be viewed in the various ITM CIT alarm list windows. Each window offers a different type of information regarding the alarms.

<table>
<thead>
<tr>
<th>Alarm Lists</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Alarm</td>
<td>Displays a number of alarms based on your filtering and sorting preferences. Information regarding recommended trouble-shooting actions can also be accessed.</td>
</tr>
<tr>
<td>Alarms Summary</td>
<td>Displays a count of currently raised alarms, for each alarm severity.</td>
</tr>
<tr>
<td>Alarm Details</td>
<td>Displays the specifics for a selected alarm. Alarms details can sometimes be modified from this lists window.</td>
</tr>
</tbody>
</table>
Alarm supervision concepts

Generalities

Alarm supervision is a feature that allows maintenance personnel to monitor currently raised alarms on a local network element, or on several other network elements belonging to the same subnetwork. In order to view the remote network element current alarms list, it is required to have subscribed it to the supervision list.

Subscribing a network element to a supervision list means that the local network element (to which the ITM CIT is connected) is granted access permission to a remote network element, with a specific NSAP address. The access rights is one of “view only”. The list of all subscribed network elements is kept in a register on the network element. This list is called the Supervision Log file. Its path and name can be configured on the ITM CIT. This list modified, reset to default, saved and loaded at a later time from another network element. The details from this list can be viewed on the Supervision List window, on the ITMCIT.

Below is a description of each important windows related to alarm supervision

<table>
<thead>
<tr>
<th>Supervision window</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Alarm Supervision</em></td>
<td>Lists all the network element elements (subscribed and unsubscribed) and displays the current alarm types (red circles). Detailed information can be seen in the Supervision: Current Alarm window. The network element MUST be subscribed in order to see the raised alarms types.</td>
</tr>
<tr>
<td><em>Alarm Subscription</em></td>
<td>Allows to modify the subscription state of a network elements appearing in the Alarm Supervision window.</td>
</tr>
<tr>
<td><em>Supervision: Current Alarm</em></td>
<td>Gives detailed information about all currently raised alarm types for a subscribed network element appearing on the Alarm Supervision window.</td>
</tr>
<tr>
<td><em>Supervision: Add network Element</em></td>
<td>Allows to add a network element on the Alarm Supervision window.</td>
</tr>
<tr>
<td><em>Supervision: Edit network element Information</em></td>
<td>Allows to modify information about a network element that appears on the Alarm Supervision window.</td>
</tr>
<tr>
<td><em>Subscription/Unsubscribing Progress Display</em></td>
<td>Displays the % completion during the subscription or unsubscription process.</td>
</tr>
</tbody>
</table>
Event history

Introduction

Once an alarm has been attended and the cause has been resolved, a change in the alarm status occurs. The alarm status passes from Raised (and/or acknowledged) to Cleared. Once an alarm has a Cleared status, it is transferred to a historical log. The details of this history log can be viewed with the History Alarm List window.
Alarm identification

Overview

Purpose

The purpose of this section is to identify the windows to be used when monitoring the incoming alarms, as well as to describe the procedures to access and configure the display of those windows according to your preference.

Contents

<table>
<thead>
<tr>
<th>View alarm summary</th>
<th>6-16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set up filters</td>
<td>6-17</td>
</tr>
<tr>
<td>View current alarms</td>
<td>6-18</td>
</tr>
<tr>
<td>View alarm details</td>
<td>6-20</td>
</tr>
<tr>
<td>Archive cleared alarms</td>
<td>6-22</td>
</tr>
<tr>
<td>Parameters for identifying the alarms</td>
<td>6-23</td>
</tr>
</tbody>
</table>
View alarm summary

When to use

The procedures of this section can be used to permanently display a summary of all alarms.

Related information

The following items list other relevant information to this procedure:

• There is no related procedure;
• Related concepts are described in the *Concepts of Event Management*.

Before you begin

The items below give information on tasks to perform before beginning the procedure:

• No prerequisite must be met in order to view the alarm lists;
• No precaution are needed when performing this procedure.

View alarm summary

1. Select *Alarms -> Alarm Summary*.

   **Result:** The *Alarm Summary* is active. A total count of currently raised alarms for each severity is permanently displayed on the screen.

2. Select *Alarms -> Alarm Summary* a second time to stop the display.

   **Result:** The *Alarm Summary* disappears from the screen.

**END OF STEPS**
Set up filters

When to use

The procedures of this section can be used to implement display filters for the History Alarm list and Current Alarm list.

Related information

The following items list other relevant information to this procedure:

- There is no related procedure;
- Related concepts are described in the Concepts of Event Management.

Before you begin

The items below gives information on tasks to perform before beginning the procedure:

- No prerequisite must be met in order to view the alarm lists;
- No precaution are needed when performing this procedure.

Set up filters on the current alarm list

1. Select Alarms → Current Alarms or select Provisioning → Equipment → Shelf Display, right-click on a slot or a unit and select Alarms from the pop-up menu.

   **Result:** The Current Alarms window appears.

2. Mark the Filtering check box.

   **Result:** The alarm filtering functionality is enabled.

3. Click Filter...

   **Result:** The Alarm List Filter Configuration window appears.

4. Select your filter options and click OK.

   **Result:** The Alarm List Filter Configuration window disappears. The filters are applied against the display on the Current Alarms window.

**END OF STEPS**
View current alarms

When to use

The procedures of this section can be used to display a list of all current alarms.

Related information

The following items list other relevant information to this procedure:

- There is no related procedure;
- Related concepts are described in the Concepts of Event Management.

Before you begin

The items below gives information on tasks to perform before beginning the procedure:

- No prerequisite must be met in order to view the alarm lists;
- No precaution are needed when performing this procedure.

View the current alarms list

1. Select Alarms → Current Alarms or select Provisioning → Equipment → Shelf Display, right-click on a slot or a unit and select Alarms from the pop-up menu.

   Result: The Current Alarms window appears, showing the currently raised alarms on that NE.

2. Select an alarm from the alarms list.

3. Use the following decision table for your next step.

<table>
<thead>
<tr>
<th>If you wish to...</th>
<th>go to step #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh the list</td>
<td>4</td>
</tr>
<tr>
<td>Have the list automatically updated</td>
<td>5</td>
</tr>
<tr>
<td>Viewing Trouble-clearing Recommendations</td>
<td>6</td>
</tr>
<tr>
<td>Stop the procedure</td>
<td>8</td>
</tr>
</tbody>
</table>

4. Click Update.
The Data retrieval process window appears. The latest information is displayed on screen.

Mark the check box **Automatic Update**.

**Result:** The current alarm list will be automatically and dynamically be refreshed with the latest information.

Select an alarm from the list and click **Help**.

**Result:** The Help—on—alarms file opens and displays information about the recommended trouble-clearing information, possible cause(s) for the alarm, and correlated alarms.

Click **Close**.

**Result:** The Help window disappears.

Click **Close**

**Result:** The Current Alarms window disappears.
View alarm details

When to use

The procedures of this section can be used to view additional information about an alarm.

Related information

The following items list other relevant information to this procedure:

- There is no related procedure;
- Related concepts are described in the *Concepts of Event Management*.

Before you begin

The items below gives information on tasks to perform before beginning the procedure:

- No prerequisite must be met in order to view the alarm lists;
- No precaution are needed when performing this procedure.

View alarm details

1. Select Alarms → Current Alarms or select Provisioning → Equipment → Shelf Display, right-click on a slot or a unit and select Alarms from the pop-up menu.

   **Result:** The Current Alarm window appears.

2. Select an alarm from the list and click Details....

   **Result:** The Current Alarms Details window appears. Full details about the selected alarm is displayed.

3. Click on Previous or Next to see the details of another alarm. Otherwise go to step 4.

   **Result:** The Current Alarm Details presents the results of the navigating through the alarms list, above and below the selected alarm.

4. Click on Close.

   **Result:** Current Alarm Details window closes and the Current Alarms window appears.

5. Click on Close.
Result: The Current Alarms window closes.

END OF STEPS
Archive cleared alarms

When to use

The procedures of this section can be used when you want the cleared alarms to be automatically archived in the history log of a chosen path.

Related information

The following items list other relevant information to this procedure:

- There is no related procedure;
- Related concepts are described in the Concepts of Event Management.

Before you begin

The items below gives information on tasks to perform before beginning the procedure:

- No prerequisite must be met in order to view the alarm lists;
- No precaution are needed when performing this procedure.

Archive cleared alarms

1. Select Alarms → Current Alarms or select Provisioning → Equipment → Shelf Display, right-click on a slot or a unit and select Alarms from the pop-up menu.

   Result: The Current Alarms window appears, showing the currently raised alarms on that NE.

2. Mark the Automatic Update checkbox.

3. Mark the Logging checkbox

   Result: All cleared alarms upon notifications will be logged to a file as defined in the Options (File->Options). From the Options dialog, you can specify the path and filename for the history log file. See Parameters sub-section.

   The Options item is greyed out if Automatic Update is not enabled prior.

4. Click Close

   Result: The Current Alarms disappears.

END OF STEPS
Parameters for identifying the alarms

Introduction

There are four windows that can assist maintenance personnel in identifying alarms within a list, depending on the type of information they wish to gather. Only the ports that you set to monitor will generate an alarm.

The following windows are the alarm lists:

1. **Summary Alarm** window gives a total count of currently raised alarms. This is the ideal tool for an overview of the alarm situation.

2. **Current Alarm** window gives a list of all *reported* current alarms. Details about each alarm are obtained from this screen.

The following windows allow configuration of the alarm lists display

1. **Alarm List Filter Configuration** window allows to set up filters based on a variety of available criteria. It enables the user to restrict the size of the displayed alarm list by selecting appropriate filters.

2. **Alarm List Sorting Configuration** window allows to sort the list based on two available sorting keys.

Abort

This button interrupts data retrieval and closes the *List Retrieval Progress* window. Pressing the **Abort** button cancels the retrieving process and displays a dialog box asking you to confirm your intent to abort the process.

Alarms

Filters the alarms based on alarm types. When **Specific Alarm** radio button is selected, the *source* frame becomes unavailable and the filtering output will depend on the criteria selected in the *Category* frame. Alarms are alphabetically sorted in the *Alarm Type* field. The default is set to *All*

Alarm summary

Groups and summarizes the alarms relative to their severity. A total count, per alarm severity, is kept and reported. The total is displayed as integer 0...9999.

Alarm type

The mnemonic of the fault which is an identifier that uniquely defines the cause of the alarm. It is predefined. The naming convention includes the identification of associated correlated alarms. The fault full description is given in the *Alarm Details* window.
**Automatic update**

The **Automatic Update** check box dynamically refreshes the alarm list. If enabled, the current alarm list is automatically updated when new alarm notifications are received. If disabled, the current alarm list is not automatically updated.

**Category**

Filters the alarms based on the logical location where the alarms occurred, for example **Equipment** filter displays an overview of alarms triggered by a unit failure or a laser fault conditions. The **Transmission** filter displays the alarms that are triggered by faults which are detected in the transmission signal. **Processing** filter displays alarms triggered by inconsistencies during the processing of provisioned data. **Environment** filter displays alarms, triggered by malfunctions in external equipment which is supervised by the system. **Management**, filter displays alarms triggered by malfunctions in the communication between the Management System and the Network Element.

**Class**

For a given class, the classes group a number of alarms generated by an object which can be the node, a shelf, a slot, a termination point, etc.

**Description**

The **Description** field shows the full description of the selected alarm.

**Details**

The **Details**... button displays the details of the selected alarm. Only one alarm can be selected at a time. The button is only selectable when an alarm has been selected from the list.

**Filter**

The **Filter**... button opens the **Alarm List Filter Configuration** window. In this window you can change the filter criteria.

**Filtering**

This check box activates or inactivates the alarm filtering functionality. The alarm filtering is based on the current alarm filters. Whenever the check box is unmarked (inactivated), no filtering occurs.

**Global reported**

The of all alarm instances in the network element. The default sorting order is **Yes, No** and **<empty>**.
Global severity

Settings regarding the urgency of an alarm and which is applicable to all instances of the same kind in the network element. The default sorting order is Prompt, Deferred, and Info.

Help

When an alarm is selected, it is possible to get additional relevant information regarding this alarm, such as probable causes and recommended action for trouble-clearing the alarm.

Instance

Smallest part of the NE that can generate alarms for the selected class. There is no instance available when talking about the Network Element and Shelf classes. There is no sorting default.

Logging

An enabled Logging checkbox allows to archive the information regarding a cleared alarm.

The user's Logging options are:

- Path and Filename referring to where the log file will be archived;
- Append/Overwrite, which allows a user to configure the system to either add the details of a new alarm into an existing log file or alternatively to overwrite the last saved log file.

The Logging check box is only active if the Automatic Update check box is enabled.

Most recent alarm

The most recently raised alarm of the highest severity. So if there are no Prompt alarms, but only Info and Deferred alarms that were raised, the Most Recent Alarm field will the most recent of the Deferred alarms.

NE state

This field displays whether the network element (NE) is a normal state or abnormal. This field is only visible in the NE Current Alarms window. The History Current Alarms window does not display this field.

Probable cause

The Probable Cause field lists all the alarms with their potential causes for the Reporting Class that you selected. The list can be filtered by filling in a reporting class. They are sorted by alarm types.
The Reporting Class refers to a classification which identifies at which SDH level, and/or where on the NE, the alarm is triggered. NE is the default. Once a Reporting Class is selected, the appropriate combo boxes are enabled sequentially. The OK button is available only when all applicable combo boxes for a given Reporting Class have been selected. For example, selecting a VC12 Reporting Class requires to first refer to the appropriate slot, then the port, then the AU4 number containing the so-called VC12, and finally the VC12 number itself.

When the Wan or SDHChannelTTP is selected as the Reporting Class and that a LAN card is selected in the slot combobox, the next combobox (port) will be enabled and populated with only the applicable WAN ports for the 1643 AM or 1643 AMS.

**Reporting state**

An option for the display or incoming alarms. The reporting state can be *Reported* or *Not reported* and be set globally (see) for all alarms or specifically set for some instances (see). Its possible values are *Yes*, for reported and *No*, for non reported. The sorting order is *Yes*, and then *No*. To display an incoming alarm on the ITM CIT, the reporting state must be set to *Reported*.

**Severity**

Classifies the alarm into three priorities, depending on the urgency of the recommended response. The concept chapter describes the three possible severities levels of an alarm.

**Slot select**

Filters the alarms according to the physical location on the NE where the alarm was triggered. The default is set to "All". If a specific slot is selected as filter then the source types NE and Shelf cannot be selected.

**Source**

The location where the alarm was triggered during transmission, for example Network Element (NE), Shelf, Slot, Port, AU, VC, TU, or Timing.

**Specific reported**

The of a specific alarm instance. The default sorting order is *Yes*, *No* and <empty>.

**Specific severity**

Settings regarding the urgency of an alarm and which is applicable to a specific instance in the network element. The default sorting order is *Prompt*, *Deferred*, and *Info*. 
Status

There are two possible status for an alarm: Raised or Cleared. In the Alarm List Filter Configuration window both Raised and Cleared are selected as default.

Suppress

This button suppresses all active (current) alarms so that the next incoming alarm can be seen on the unit LED by the maintenance personnel. When this button is pressed, the alarm is said to “hide”. Consequently, the next alarm is free to be lit on the system controller user panel. The suppressed LED remains lit as long as any of the suppressed alarms is active and not yet trouble-cleared. It is possible to suppress any current alarm on another network element during a remote session.

Suppressed alarms

This field indicates whether some of the listed alarms are suppressed or not. This field will be autonomously updated each time an alarm changes status to “Clear”.

Time raised

The time at which the alarm was raised. The default format is MM/DD/YYYY:00(hr):00(mn):00(s) but can be modified. The displayed time should be the local ITM CIT time, that is the local time zone.

Time cleared

The time at which the alarm was cleared and moved to the History Alarm list. The default format is MM/DD/YYYY:00(hs):00(ms):00(s) but can be modified. The displayed time should be the local ITM CIT time, that is the local time zone.

<—

Removes a specific setting entry from the configured specific settings. The button is enabled only if one alarm type has been selected for which specific settings exist.

-->  

Copies the selected global settings entry onto the specific settings.
Provision alarm options

Overview

Purpose

The purpose of this section is to describe the procedure to make use of an additional alarm feature whenever needed. This option allows to stop the alarms from being presented on the ITM CIT; this is achieved with a functionality called the *Lining Up* mode.

Contents

<table>
<thead>
<tr>
<th>Setting the alarm options</th>
<th>6-29</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters for setting the alarm options</td>
<td>6-30</td>
</tr>
</tbody>
</table>
Setting the alarm options

When to use

Perform these procedures to access the alarm options window and to set/change the alarm options.

Related information

Parameters used in this procedure can be found at “Parameters for setting the alarm options” (p. 6-30)

Before you begin

Before performing these procedures make sure the settings of the alarms are in accordance with the alarm philosophy.

Access the network element alarm control options

Follow this procedure to access the Alarm Control Options window.

1. Select Alarms → NE Alarm Control

   Result: The NE Alarm Control window appears.

2. Click on Edit... to change the lining up mode of the network element.

   Result: The Edit Lining Up Mode window appears.

3. Select the Lining Up mode as Active.

   Result: The next alarms will be blocked and not displayed on the ITM-CIT until the lining up mode is set to inactive.

4. Click on Close button.

   Result: The Edit NE Alarm Control window disappears.

END OF STEPS
Parameters for setting the alarm options

Introduction

The ITM-CIT offers additional alarm control options. You can either stop an alarm from being presented on the ITM-CIT or delay its presentation (or disappearance) from the Current Alarms screen.

An alarm may be stopped by configuring an option called the Lining Up mode.

The other alarm control option allows to set a Raise/Clear delays on the Station Alarm before the alarm indication is raised and/or cleared. Furthermore, it is possible to set its dependency on alarm suppression network element on the ITM-CIT. This is achieved with the Station Alarms Raise/Clear Delays.

It could happen during event monitoring that an alarm disappears from the window, very quickly after being displayed. These alarms are usually due to an event else where in the network and disappears because they are resolved by the system. In order to avoid this “on/off flickering” of alarms, you can set a delay for the raise and clear time of those alarms. In this way, the alarm condition is re-evaluated over the desired time delay and will be presented and/or disappear from the ITM CIT if the condition remains true and that delay time is exceeded.

Lining up mode

When a network element is put in to lining-up mode, no alarms are reported, however any other communication error will still be reported. This prevents the system from becoming cluttered with unnecessary alarms during installation or maintenance actions on the network element. Any existing alarms for the network element are cleared when the manager activates the Lining Up mode. This has the effect of moving all alarms to the history store. The alarm status is re-evaluated by the network element when the lining up is inactivated.

Dependency

Suppress Dependency on Station Alarms. This functionality is used when maintenance personnel wants to be able to decide if the Station Alarms will/or not be suppressed when they are suppressed on the ITM-CIT. The Prompt and Deferred maintenance alarm on the station alarm interface will be unaffected by the suppress button. This option can be activated in run time.

Raise/clear delays

Raise/Clear Delay. This is an additional option allowing to set a time interval before an alarm is raised, or cleared.
It could happen during event monitoring that an alarm disappears from the screen, very quickly after being displayed. These alarms are usually due to an event elsewhere in the network element and disappears because they are resolved by the system. In order to avoid this “on/off flickering” of alarms, you can set a delay for the raise and clear time of those alarms. In this way, the alarm condition is re-evaluated over the desired time delay and will be presented and/or disappear if the condition remains true and that delay time is exceeded.
Overview

Purpose

The purpose of this section is to describe how to provision alarm severity assignment profiles (ASAP).

Contents

| Create a new ASAP                          | 6-33 |
| Modifying an existing ASAP                | 6-35 |
| Delete an existing ASAP                   | 6-37 |
| Retrieve an existing ASAP                 | 6-38 |
| Assign an ASAP                            | 6-39 |
| Retrieve an assignment list for a specified ASAP | 6-44 |
| Retrieve assigned ASAPs for a specified managed object | 6-45 |
| Parameters for “ASAP Assignment”          | 6-46 |
| Alarm Severity Assignment Profile         | 6-47 |
Create a new ASAP

When to use

This procedure is used to create new alarm severity assignment profiles (ASAP).

Related information

For related information, please refer to:

• “Alarm Severity Assignment Profile” (p. 6-47)

Before you begin

Before performing this task, you must have an overview of the network topology.

1. Log into the ITM® CIT, and
2. Connect to the NE.

Required equipment

The following equipment is required to perform this task:

• ITM® CIT

Procedure

Follow this procedure to create a new ASAP:

1. Select Alarms → ASAP List.

   Result: The Alarm Severity Assignment Profiles List window is displayed.

2. Click on Add.

   Result: The Create Alarm Severity Assignment Profile window is displayed.

3. In the field ASAP Name enter the name of the new ASAP to be created.

   Additional information The following provisioning rules apply to the ASAP name:

   1. A user cannot add a new ASAP, using names like “default/Default” (in uppercase
      or lowercase).
   2. The ASAP name is an alphanumeric string of up to 20 characters.
   3. The following characters are permitted in an ASAP name:
      • Upper case letters (A … Z),
      • Lower case letters (a … z),
• Digits (0 … 9),
• Hyphens (-).

4 In the **ASAP Type** select the appropriate ASAP type.

**Reference:** Refer to “ASAP types” (p. 6-48).

5 Click on **Next**.

**Result:** The **Alarm Severity Assignment Profiles Information** window is displayed.

6 Select the ASAP profile and click on **Edit**.

**Result:** The **Edit Alarm Severity Assignment Profile** window is displayed.

7 In the **Severity** field define the appropriate Alarm Severity by selecting the respective radio button.

8 In the **Reporting State** field define the appropriate Reporting State.

9 Click on **OK**.

**END OF STEPS**
Modifying an existing ASAP

When to use

This procedure is used to rename an existing ASAP and/or modify parameter values for an ASAP. Default ASAPS cannot be renamed, but parameter values can be modified.

Related information

For related information, please refer to:

• “Alarm Severity Assignment Profile” (p. 6-47)

Before you begin

Before performing this task, you must have an overview of the network topology.

1. Log into the ITM® CIT, and
2. Connect to the NE.

Required equipment

The following equipment is required to perform this task:

• ITM® CIT

Procedure

Follow this procedure to rename and/or modify parameter values for an ASAP:

1 Select Alarms → ASAP List.
   Result: The Alarm Severity Assignment Profiles List window is displayed.

2 Select the ASAP to be modified in the ASAP List, then click on Details.
   Result: The Alarm Severity Assignment Profile Information window is displayed for the selected ASAP.

3 Click on Edit to modify the severity and the reporting state.
   Result: The Edit Alarm Severity Assignment Profile window is displayed.
   Note: The user can select any alarm to modify and only the selected alarms will be displayed in the edit window.

4 In the field ASAP Name change the name of the ASAP if you want.
Additional information The following provisioning rules apply to the ASAP name:

1. A user cannot add a new ASAP, using names like “default/Default” (in uppercase or lowercase).
2. The ASAP name is an alphanumeric string of up to 20 characters.
3. The following characters are permitted in an ASAP name:
   • Upper case letters (A … Z),
   • Lower case letters (a … z),
   • Digits (0 … 9),
   • Hyphens (-).

5 In the Severity field define the appropriate Alarm Severity by selecting the respective radio button.

6 In the Reporting State field define the appropriate Reporting State.

7 Click on OK.

Result: The Alarm Severity Assignment Profile is modified.
Delete an existing ASAP

When to use

This procedure is used to delete a user-created alarm severity assignment profile (ASAP) that is not currently active. DEFAULT ASAPs cannot be deleted.

Before you begin

Before performing this task, you must have an overview of the network topology.
1. Log into the ITM® CIT, and
2. Connect to the NE.

Required equipment

The following equipment is required to perform this task:
• ITM® CIT

Procedure

Follow this procedure to delete a user-created alarm severity assignment profile (ASAP) that is not currently active.

1 Select Alarms → ASAP List from the main menu.

Result: The Alarm Severity Assignment Profiles List window is displayed.

2 Select the ASAP to be deleted in the ASAP List. Then click on Delete.

Result: A confirmation window appears. Click YES.

The Alarm Severity Assignment Profile is deleted.

END OF STEPS

Retrieve an existing ASAP

When to use

This procedure is used to retrieve information about one or more existing alarm severity assignment profile(s).

Before you begin

Before performing this task, you must have an overview of the network topology.

1. Log into the *ITM® CIT*, and
2. Connect to the NE.

**Required equipment**

The following equipment is required to perform this task:

- *ITM® CIT*

Procedure

Follow this procedure to retrieve parameter values for an ASAP:

1. Select **Alarms → ASAP List**.  
   **Result:** The **Alarm Severity Assignment Profiles List** window is displayed.

2. Select the ASAP to be retrieved in the **ASAP List**, then click on **Details**.  
   **Result:** The **Alarm Severity Assignment Profile Information** window is displayed for the selected ASAP.

3. As an option, you can store or print the currently displayed list:

<table>
<thead>
<tr>
<th>If ...</th>
<th>then ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>you want to store the list as a standard text file (ASCII format)</td>
<td>click the <strong>Report</strong> button and specify a filename and a destination.</td>
</tr>
<tr>
<td>you want to print out the list</td>
<td>click the <strong>Print</strong> button and specify a printer.</td>
</tr>
</tbody>
</table>

4. Click on **Close** to close the window.

END OF STEPS
Assign an ASAP

When to use

This procedure is used to assign an ASAP to one or several manageable object(s).

Related information

For related information, please refer to:
- “Alarm Severity Assignment Profile” (p. 6-47)

Before you begin

Before performing this task, you must have an overview of the network topology.
1. Log into the ITM® CIT, and
2. Connect to the NE.

Required equipment

The following equipment is required to perform this task:
- ITM® CIT

Procedure

Follow this procedure to assign an ASAP to one or several manageable object:

1. Select Alarms → ASAP List.
   
   **Result:** The Alarm Severity Assignment Profiles List window is displayed.

2. Select the ASAP to be assigned to one or several manageable object ins the ASAP List. Then click on Set Assignment....

   **Result:** The ASAP Assignment window is displayed for the selected ASAP.

3. In the left part of the Instance List area of the window you can select the managed object, to which you want to assign the ASAP.

   **Note:** The maximum number of managed object instances that can be retrieved at one time is 100.
**Additional info:** The following table gives a hint how the instance are to be selected. The combo boxes marked with a cross, matching the selected type in the table below, are to be enabled sequentially. When the last combo box is filled, the **OK** button is enabled. Changing one combo box disables and empties all subsequent combo boxes. An empty cell means the combo box is disabled and empty.

**Note:** The managed object instance can have multiple profiles which belong to different profile types, but only one ASAP profile which belongs to one profile type can be assigned to an entity at a time.

<table>
<thead>
<tr>
<th>Combo boxes</th>
<th>Slot</th>
<th>Port</th>
<th>AU</th>
<th>TU/VC12Timing Source</th>
<th>Virtual Switch ID</th>
<th>Service Route ID</th>
<th>Remote Device ID</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Instance Type</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shelf</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Slot</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reg.</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VC4</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VC3</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VC2</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VC12</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VC11</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AU-4-16c</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AU-4-4c</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AU4</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TU3</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TU2</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TU12</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protected MS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RS</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E1 port3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Equipment Protection3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Combo boxes

<table>
<thead>
<tr>
<th>Instance Type</th>
<th>Slot</th>
<th>Port</th>
<th>AU</th>
<th>TU/VC12 Timing Source</th>
<th>Virtual Switch ID</th>
<th>Service Route ID</th>
<th>Remote Device ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS SPRing Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timing Source</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Output Timing Source</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Timing Source</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timing Link Switch</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VCG</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wan</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lan</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dual Stack with Tunneling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SFP Socket</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LAG port</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ethernet Link OAM</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ethernet Service Route</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>LAN CTP Pointer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAN CTP Pointer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Eoc Node</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Remote QD2 SRU</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Remote QD2 NTU</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
## Alarm management

### Provision alarm severity assignment profiles (ASAP)

Assign an ASAP

### Combo boxes

<table>
<thead>
<tr>
<th>Instance Type</th>
<th>Slot</th>
<th>Port</th>
<th>AU</th>
<th>TU/VC12Timing</th>
<th>Virtual Switch</th>
<th>Service Route</th>
<th>Remote Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic SDSL Customer Port</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>SDSL E1 Port</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>SDSL port</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Logical E13</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Remote Logical E13</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Generic P12(Network)4</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Generic P12(Customer)4</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Side Sax P12</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Customer Side Sax P12</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Remote SDSL VCG</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>SDSL VC12</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Remote LAN Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Local SDSL Port</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote LAN CTP</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Remote WAN CTP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Remote PSB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Remote PSB Port</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>LAN Unit Control</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
To put the selected instance to the instance list, click on >.

To select an additional instance, repeat from Step 3.

To assign the selected instances to the ASAP, click on OK.
Retrieve an assignment list for a specified ASAP

When to use

This procedure is used to retrieve an assignment list for a specified ASAP.

Before you begin

Before performing this task, you must have an overview of the network topology.

1. Log into the ITM® CIT, and
2. Connect to the NE.

Required equipment

The following equipment is required to perform this task:

- ITM® CIT

Instructions

Complete the following steps to retrieve an assignment list for a specified ASAP:

1. Select Alarms → ASAP List.
   
   **Result:** The Alarm Severity Assignment Profiles List window is displayed.

2. Select the ASAP to be retrieved in the ASAP List. Click Retrieve assignment....
   
   **Result:** The Retrieve ASAP Assignment window is displayed for the selected ASAP.
   In the Instance List all managed objects to which the ASAP is assigned are listed.

**END OF STEPS**
Retrieve assigned ASAPs for a specified managed object

When to use

This procedure is used to retrieve an ASAP assignment list for a specified managed object.

Before you begin

Before performing this task, you must have an overview of the network topology.

1. Log into the ITM® CIT, and
2. Connect to the NE.

Required equipment

The following equipment is required to perform this task:

- ITM® CIT

Instructions

Complete the following steps to retrieve an ASAP assignment list for a specified managed object:

1. Select Alarms → ASAP List.
   
   Result: The Alarm Severity Assignment Profiles List window is displayed.

2. Click on Retrieve Assignment per Instance.
   
   Result: The ASAP Retrieval per Instance window is displayed.

3. In the Instance List area you can select the managed object, for which you want to display the assigned ASAPs.

END OF STEPS
Parameters for “ASAP Assignment”

Parameters in the ASAP list

The following table shows the data which are shown in the ASAP List part of the window.

<table>
<thead>
<tr>
<th>Information field</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASAP Name</td>
<td>Displays the Alarm Severity Assignment Profiles Name</td>
</tr>
<tr>
<td>ASAP Type</td>
<td>Displays the Alarm Severity Assignment Profiles Type</td>
</tr>
</tbody>
</table>

Fields and parameters in the Instance List

The following table shows the fields which can be used to select manageable objects in the left part of the Instance List area.

<table>
<thead>
<tr>
<th>Information field</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance Type</td>
<td>List the selected Instance Type</td>
</tr>
<tr>
<td>Slot</td>
<td>List the slot</td>
</tr>
<tr>
<td>Port</td>
<td>List the port number of the selected ASAP.</td>
</tr>
<tr>
<td>AU</td>
<td>List the AU4 number of the selected ASAP</td>
</tr>
<tr>
<td>TU</td>
<td>List the TU12 number of the selected ASAP</td>
</tr>
<tr>
<td>Timing Source</td>
<td></td>
</tr>
<tr>
<td>Virtual Switch ID</td>
<td>List the virtual switch ID of the selected Instance</td>
</tr>
<tr>
<td>Service Route ID</td>
<td>The service route ID of the selected Instance.</td>
</tr>
</tbody>
</table>

Buttons and Actions

The following options are available:

<table>
<thead>
<tr>
<th>Button</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;</td>
<td>Adds a completely selected instance to the list in the right part of the Instance List area.</td>
</tr>
<tr>
<td>&gt;</td>
<td>Deletes a selected instance from the list in the right part of the Instance List area.</td>
</tr>
<tr>
<td>OK</td>
<td>The selected ASAP is assigned to the selected Managed Objects.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Closes the window.</td>
</tr>
</tbody>
</table>
Alarm Severity Assignment Profile

Overview

An Alarm Severity Assignment Profile (ASAP) is a list of alarms which can occur in a network element and which each have an alarm severity assigned.

ASAPs can be assigned to 1643 AM and 1643 AMS functional system components (a circuit pack or a specific port for example) during provisioning.

Each ASAP can be uniquely identified by its type and its name.

Concept

ASAP allows the user to control alarm reporting with more flexibility, and to create multiple alarm profiles for each alarm category and to assign these profiles to entities within the system.

The alarms contained in each category are predefined. The categories containing the alarms are referred to as predefined profile types. Each profile type has a default profile and a set of user-created profiles. The user-created profiles and the default profiles within the profile types are referred to as ASAPs. The assigned alarm severity levels refer to each alarm within each ASAP.

Note that predefined or default alarms or profile types cannot be changed or deleted by the user. Only the profiles created by the user can be changed or deleted.

Alarm severities

The alarm severity levels are used in the following description of the ASAP types:

1. Prompt (Urgent alarm that requires immediate (prompt) maintenance action)
2. Deferred (Non-urgent alarm that requires deferred maintenance action)
3. Info (Informational alarm).

Reporting state

Each alarm can be assigned to one of the following reporting states:

<table>
<thead>
<tr>
<th>Reporting state</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reported</td>
<td>The alarm - when raised - will be reported towards the management systems, and displayed on the graphical user interfaces.</td>
</tr>
<tr>
<td>Not Reported</td>
<td>The alarm - when raised - will not be reported.</td>
</tr>
</tbody>
</table>
Please note that changing the alarm reporting state does not affect the display of currently present and history alarms. Especially the display of already present alarms cannot be removed if their reporting state is changed from “Reported” to “Not Reported”.

### ASAP types

The ASAP types, listed in alphabetical order according to their ITM CIT representation, are defined for 1643 AM network elements:

<table>
<thead>
<tr>
<th>ASAP Type</th>
<th>Functional category</th>
</tr>
</thead>
<tbody>
<tr>
<td>dcn</td>
<td>Alarms related to node level DCN (including Q-LAN)</td>
</tr>
<tr>
<td>equipment</td>
<td>Alarms related to equipment (circuit pack and other equipment alarms)</td>
</tr>
<tr>
<td>ethPath</td>
<td>Transmission &amp; TCA causes related to Path for Ethernet</td>
</tr>
<tr>
<td>ethPS</td>
<td>Transmission causes related to Physical Section for Ethernet</td>
</tr>
<tr>
<td>mdi</td>
<td>Alarms related to mdi</td>
</tr>
<tr>
<td>pdhPS</td>
<td>Transmission causes related to Physical Section for PDH (LOS, AIS)</td>
</tr>
<tr>
<td>pdhPath</td>
<td>Transmission &amp; TCA causes related to path for PDH (only supported for E1)</td>
</tr>
<tr>
<td>timing</td>
<td>Alarms related to timing (node, port and timing sources)</td>
</tr>
<tr>
<td>sdhPRS</td>
<td>Transmission &amp; TCA causes related to Physical and Regenerator Section for SDH</td>
</tr>
<tr>
<td>sdhMS</td>
<td>Transmission &amp; TCA causes related to Multiplex Section for SDH</td>
</tr>
<tr>
<td>sdhMSP</td>
<td>Alarms related to 1+1 Multiplex Section Protection for SDH</td>
</tr>
<tr>
<td>sdhHOPath</td>
<td>Transmission &amp; TCA causes related to HO Path for SDH (includes ms/Sm adaptation, Sm NIM, Sm termination and MS-SPRing circuit audit)</td>
</tr>
<tr>
<td>sdhLOPath</td>
<td>Transmission &amp; TCA causes related to LO Path for SDH (includes Sn/Sm adaptation, Sm NIM, Sm termination)</td>
</tr>
<tr>
<td>sdhVCG</td>
<td>Transmission &amp; TCA causes related to Virtual Concatenation (GFP causes should be handled via physical ethernet)</td>
</tr>
<tr>
<td>sdsl</td>
<td>SHDSL related causes</td>
</tr>
</tbody>
</table>

### Default ASAPs

For each of the available ASAP types, there exists a default ASAP. These default ASAPs are named “DEFAULT” for all ASAP types.
In the following, the composition and the alarm severity assignments of the default ASAPs are mentioned as follows:

- “dcn ASAP” (p. 6-49)
- “equipment ASAP” (p. 6-50)
- “mdi ASAP” (p. 6-51)
- “ethPath ASAP” (p. 6-52)
- “pdhPS ASAP” (p. 6-53)
- “ethPS ASAP” (p. 6-53)
- “pdhPath ASAP” (p. 6-54)
- “timing ASAP” (p. 6-55)
- “sdhPRS ASAP” (p. 6-55)
- “sdhMS ASAP” (p. 6-56)
- “sdhMSP ASAP” (p. 6-57)
- “sdhHOPath ASAP” (p. 6-57)
- “sdhLOPath ASAP” (p. 6-57)
- “sdhVCG ASAP” (p. 6-59)
- “sdsl ASAP” (p. 6-60)

**dcn ASAP**

The following table lists the default alarm severity assignments of the “dcn” ASAP.

<table>
<thead>
<tr>
<th>Alarm identifier “Probable cause”</th>
<th>Alarm text</th>
<th>Alarm severity</th>
<th>Reporting state (default setting)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCN-BUcLOST</td>
<td>Mandatory IS-IS parameters missing</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>DCNcCONF</td>
<td>IS-IS configuration error</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>DCNcREPAIR</td>
<td>IS-IS Level-2 Area repair, transmission/configuration error</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>DCNTAPcCONF</td>
<td>DCN-Tunnel auto provisioning configuration error</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>MLQ2</td>
<td>Loss of Q2-communications</td>
<td>Information</td>
<td>Reported</td>
</tr>
<tr>
<td>AITscDCCF</td>
<td>DCC Port - Not available</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>LANcTRM</td>
<td>Q-LAN - Not terminated</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
</tbody>
</table>
The following table lists the default alarm severity assignments of the “equipment” ASAP.

<table>
<thead>
<tr>
<th>Alarm identifier “Probable cause”</th>
<th>Alarm text</th>
<th>Alarm severity</th>
<th>Reporting state (default setting)</th>
</tr>
</thead>
<tbody>
<tr>
<td>E11XcEQF</td>
<td>1.5 Mbit/s extension board (X16DS1) - defective</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>E11XcUNI</td>
<td>1.5 Mbit/s extension board (X16DS1) missing</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>E11XcWUP</td>
<td>Wrong extension board present</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>E11XcUPF</td>
<td>1.5 Mbit/s extension board (X16DS1) - defective</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>E12XcEQF</td>
<td>2 Mbit/s extension board - defective</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>E12XcUNI</td>
<td>2 Mbit/s extension board missing</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>E12XcUPF</td>
<td>2 Mbit/s extension board - defective</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>E31XcEQF</td>
<td>34 Mbit/s extension board (X2E3-V2) - defective</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>E31XcUNI</td>
<td>34 Mbit/s extension board (X2E3-V2) missing</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>E31XcUPF</td>
<td>34 Mbit/s extension board (X2E3-V2) - defective</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>E31XcWUP</td>
<td>Wrong 34 Mbit/s extension board inserted</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>E32XcEQF</td>
<td>45 Mbit/s extension board (X2DS3-V2) - defective</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>E32XcUNI</td>
<td>45 Mbit/s extension board (X2DS3-V2) missing</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>E32XcUPF</td>
<td>45 Mbit/s extension board (X2DS3-V2) - defective</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>E32XcWUP</td>
<td>Wrong 45 Mbit/s extension board inserted</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>IPcEQF</td>
<td>LAN unit failure - protected</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>IPcUNI</td>
<td>LAN unit removed</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>IPcUPF</td>
<td>LAN unit failure</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>IPcWUP</td>
<td>Wrong LAN unit present</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>PMcEQF</td>
<td>Pluggable Module failure</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>PMcUNI</td>
<td>Pluggable Module removed</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>PMcUPF</td>
<td>Unprotected Pluggable Module failure</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>PMcWUP</td>
<td>Wrong Pluggable Module present</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>POWcLSV</td>
<td>Loss of secondary input voltage</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>RPScOVERL</td>
<td>Remote power supply box - load greater than its capacity</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>RPScOPENC</td>
<td>Remote power supply box - No electric current</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>RPScFSD</td>
<td>Remote power supply box - switched off manually</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
</tbody>
</table>
### Alarm management

#### Provision alarm severity assignment profiles (ASAP)

<table>
<thead>
<tr>
<th>Alarm identifier “Probable cause”</th>
<th>Alarm text</th>
<th>Alarm severity</th>
<th>Reporting state (default setting)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPScLEAK</td>
<td>Remote power supply box - defective</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>RPScHVOLT</td>
<td>Remote power supply box - higher voltage</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>RPScPS</td>
<td>Remote power supply box - defective</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>STM1XcEQF</td>
<td>STM-1 interface extension board - Hardware Failure</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>STM1XcUNI</td>
<td>STM-1 interface extension board missing</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>STM1XcUPF</td>
<td>STM-1 interface extension board failure</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>STM1XcWUP</td>
<td>Wrong STM-1 interface extension board inserted</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>UPUS</td>
<td>Unit present in unassigned slot</td>
<td>Information</td>
<td>Reported</td>
</tr>
<tr>
<td>X21XcEQF</td>
<td>X.21 interface extension board - defective</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>X21XcWUP</td>
<td>Wrong X.21 interface extension board inserted</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>X21XcUNI</td>
<td>X.21 interface extension board missing</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>X21XcUPF</td>
<td>X.21 interface extension board - defective</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
</tbody>
</table>

#### Notes:

1. Alarms marked with an asterisk (“*”) in the “Probable cause” column are not supported in the present 1643 AM release. These alarms are prepared for future applications.

### mdi ASAP

The following table lists the default alarm severity assignments of the “mdi” ASAP.

<table>
<thead>
<tr>
<th>Alarm identifier “Probable cause”</th>
<th>Alarm text</th>
<th>Alarm severity</th>
<th>Reporting state (default setting)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MDcIP1</td>
<td>MDI 1: &lt;user entered string&gt;</td>
<td>Information</td>
<td>Reported</td>
</tr>
<tr>
<td>MDcIP2</td>
<td>MDI 2: &lt;user entered string&gt;</td>
<td>Information</td>
<td>Reported</td>
</tr>
<tr>
<td>MDcIP3</td>
<td>MDI 3: &lt;user entered string&gt;</td>
<td>Information</td>
<td>Reported</td>
</tr>
<tr>
<td>MDcIP4</td>
<td>MDI 4: &lt;user entered string&gt;</td>
<td>Information</td>
<td>Reported</td>
</tr>
<tr>
<td>RPSMDcIP1</td>
<td>MDI 1 located on the remote power supply box - indicates an environmental alarm condition</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>RPSMDcIP2</td>
<td>MDI 2 located on the remote power supply box - indicates an environmental alarm condition</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>RPSMDcIP3</td>
<td>MDI located on the remote power supply box - indicates an environmental alarm condition</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
</tbody>
</table>
Notes:
1. In the ITM CIT NE Alarm List, only “MISC” is displayed as the probable cause of an environmental alarm.
2. You can change the alarm text of each individual Miscellaneous Discrete Input (MDI).

**ethPath ASAP**

The following table lists the default alarm severity assignments of the “ethPath” ASAP.

<table>
<thead>
<tr>
<th>Alarm identifier “Probable cause”</th>
<th>Alarm text</th>
<th>Alarm severity</th>
<th>Reporting state (default setting)</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN Dropped packets threshold crossing 15-min</td>
<td>Information</td>
<td>Reported</td>
<td></td>
</tr>
<tr>
<td>LAN Dropped packets threshold crossing 24-hrs</td>
<td>Information</td>
<td>Reported</td>
<td></td>
</tr>
<tr>
<td>LAN Loaded Sec for incoming traffic with class 3 green traffic Thr 15min</td>
<td>Deferred</td>
<td>Reported</td>
<td></td>
</tr>
<tr>
<td>LAN Loaded Sec for incoming traffic with class 3 green traffic Thr 24-hrs</td>
<td>Deferred</td>
<td>Reported</td>
<td></td>
</tr>
<tr>
<td>LAN Loaded Sec for inc Tr with class 3 or 2 green traffic Thr 15min</td>
<td>Deferred</td>
<td>Reported</td>
<td></td>
</tr>
<tr>
<td>LAN Loaded Sec for inc Tr with Cl 3 or 2 green traffic Thr 24-hrs</td>
<td>Deferred</td>
<td>Reported</td>
<td></td>
</tr>
<tr>
<td>LAN Severely Loaded Sec for inc Tr with class 3 green traffic Thr 15min</td>
<td>Deferred</td>
<td>Reported</td>
<td></td>
</tr>
<tr>
<td>LAN Severely Loaded Sec for inc Tr with class 3 green traffic Thr 24-hrs</td>
<td>Deferred</td>
<td>Reported</td>
<td></td>
</tr>
<tr>
<td>MAC address mismatch for LAN/WAN port</td>
<td>Deferred</td>
<td>Reported</td>
<td></td>
</tr>
<tr>
<td>VLAN configuration mismatch</td>
<td>Deferred</td>
<td>Reported</td>
<td></td>
</tr>
<tr>
<td>Maximum number of VLAN instances exceeded</td>
<td>Information</td>
<td>Reported</td>
<td></td>
</tr>
<tr>
<td>Maximum number of VLAN instances exceeded in MIB</td>
<td>Information</td>
<td>Reported</td>
<td></td>
</tr>
<tr>
<td>WAN Dropped packets threshold crossing 15-min</td>
<td>Information</td>
<td>Reported</td>
<td></td>
</tr>
<tr>
<td>WAN Dropped packets threshold crossing 24-hrs</td>
<td>Information</td>
<td>Reported</td>
<td></td>
</tr>
<tr>
<td>WAN Loaded Sec for incoming traffic with class 3 green traffic Thr 15min</td>
<td>Deferred</td>
<td>Reported</td>
<td></td>
</tr>
<tr>
<td>WAN Loaded Sec for incoming traffic with class 3 green traffic Thr 24-hrs</td>
<td>Deferred</td>
<td>Reported</td>
<td></td>
</tr>
</tbody>
</table>
### pdhPS ASAP

The following table lists the default alarm severity assignments of the “pdhPS” ASAP.

<table>
<thead>
<tr>
<th>Alarm identifier “Probable cause”</th>
<th>Alarm text</th>
<th>Alarm severity</th>
<th>Reporting state (default setting)</th>
</tr>
</thead>
<tbody>
<tr>
<td>E11cLOS</td>
<td>1.5 Mbit/s Loss of input signal</td>
<td>Prompt</td>
<td>Not Reported</td>
</tr>
<tr>
<td>E11cNES</td>
<td>1.5 Mbit/s Not expected input signal</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
</tbody>
</table>

### ethPS ASAP

The following table lists the default alarm severity assignments of the “ethPS” ASAP.

<table>
<thead>
<tr>
<th>Alarm identifier “Probable cause”</th>
<th>Alarm text</th>
<th>Alarm severity</th>
<th>Reporting state (default setting)</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMACcLOF</td>
<td>Encapsulated Medium Access Control loss of frame alignment</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>EMACcRCF</td>
<td>GFP Client Signal Fail (CSF) indication</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>LANcANM</td>
<td>Ethernet interface Auto Negotiation Mismatch</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>LANcLOS</td>
<td>Ethernet interface Loss of input signal</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>LANcNES</td>
<td>Ethernet interface Not expected input signal</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>GEcNOSYNC</td>
<td>Loss of Synchronisation</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>X21cLOS</td>
<td>No input signal at the corresponding X.21 port</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>X21cNES</td>
<td>Incoming signal on an X.21 interface port - Not Monitored</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>X21OTMcSW</td>
<td>Output timing mode automatically switched to the self-timed mode</td>
<td>Information</td>
<td>Reported</td>
</tr>
</tbody>
</table>
Notes:
1. Alarms marked with an asterisk (“*”) in the “Probable cause” column are not supported in the present 1643 AM release. These alarms are prepared for future applications.

**pdhPath ASAP**

The following table lists the default alarm severity assignments of the “pdhPath” ASAP.

<table>
<thead>
<tr>
<th>Alarm identifier “Probable cause”</th>
<th>Alarm text</th>
<th>Alarm severity</th>
<th>Reporting state (default setting)</th>
</tr>
</thead>
<tbody>
<tr>
<td>P11OTMcSW</td>
<td>1.5 Mbit/s output timing mode change</td>
<td>Information</td>
<td>Reported</td>
</tr>
<tr>
<td>P12OTMcSW</td>
<td>2 Mbit/s output timing mode change</td>
<td>Information</td>
<td>Reported</td>
</tr>
<tr>
<td>P12ScFEDEG</td>
<td>Degraded signal condition</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>P12ScFELOF</td>
<td>Loss of frame - external NTU modem</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>P12ScSSF</td>
<td>P12s Network connection server signal fail</td>
<td>Information</td>
<td>Reported</td>
</tr>
<tr>
<td>P12SNBBBeTHR15</td>
<td>P12S Near-end background block errors threshold crossing 15-min</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>P12SNBBBeTHR24</td>
<td>P12S Near-end background block errors threshold crossing 24-hrs</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>P12SNEScTHR15</td>
<td>P12S Near-end errored seconds threshold crossing 15-min</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>P12SNEScTHR24</td>
<td>P12S Near-end errored seconds threshold crossing 24-hrs</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>P12SNEScTHR15</td>
<td>P12S Near-end severely ES threshold crossing 15-min</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>P12SNEScTHR24</td>
<td>P12S Near-end severely ES threshold crossing 24-hrs</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>P12SNUAScTHR15</td>
<td>P12S Near-end unavailable seconds threshold crossing 15-min</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>P12SNUAScTHR24</td>
<td>P12S Near-end unavailable seconds threshold crossing 24-hrs</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>FSCcTHR15</td>
<td>configurable 15-minute frame slip/skip count (FSC) threshold - exceeded</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>FSCcTHR24</td>
<td>configurable 24-hour frame slip/skip count (FSC) threshold - exceeded</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>ISDNcLBK</td>
<td>ISDN-PRA Loopback inband activated</td>
<td>Information</td>
<td>Reported</td>
</tr>
<tr>
<td>P12SgcSSF *</td>
<td>P12s Network connection server signal fail egress</td>
<td>Information</td>
<td>Reported</td>
</tr>
<tr>
<td>P12SNBBBegecTHR15 *</td>
<td>P12S Near-end background block errors threshold crossing 15-min egress</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>P12SNBBBegecTHR24 *</td>
<td>P12S Near-end background block errors threshold crossing 24-hrs egress</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>P12SNESgecTHR15 *</td>
<td>P12S Near-end errored seconds threshold crossing 15-min egress</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
</tbody>
</table>
## Alarm management

### Provision alarm severity assignment profiles (ASAP)

### Alarm Severity Assignment Profile

#### timing ASAP

The following table lists the default alarm severity assignments of the “timing” ASAP.

<table>
<thead>
<tr>
<th>Alarm identifier “Probable cause”</th>
<th>Alarm text</th>
<th>Alarm severity</th>
<th>Reporting state (default setting)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBACKcUPM</td>
<td>System timing in backup state</td>
<td>Information</td>
<td>Reported</td>
</tr>
<tr>
<td>TLINKcFLR</td>
<td>Timing link failed</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>TLINKcUNEQ</td>
<td>Timing link unequipped</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>TSCOCcSQ</td>
<td>Station clock output squelched</td>
<td>Information</td>
<td>Reported</td>
</tr>
</tbody>
</table>

#### sdhPRS ASAP

The following table lists the default alarm severity assignments of the “sdhPRS” ASAP.

<table>
<thead>
<tr>
<th>Alarm identifier “Probable cause”</th>
<th>Alarm text</th>
<th>Alarm severity</th>
<th>Reporting state (default setting)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RS1cTIM</td>
<td>STM-1 RS trace identifier mismatch</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>RS4cTIM</td>
<td>STM-4 RS trace identifier mismatch</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>STM1cLOF</td>
<td>STM-1 Loss of frame alignment</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>STM1cLOS</td>
<td>STM-1 Loss of input signal</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>STM1cNES</td>
<td>STM-1 Not expected input signal</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>STM4cLOF</td>
<td>STM-4 Loss of frame alignment</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>STM4cLOS</td>
<td>STM-4 Loss of input signal</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>STM4cNES</td>
<td>STM-4 Not expected input signal</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
</tbody>
</table>
The following table lists the default alarm severity assignments of the “sdhMS” ASAP.

<table>
<thead>
<tr>
<th>Alarm identifier</th>
<th>Alarm text</th>
<th>Alarm severity</th>
<th>Reporting state (default setting)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS1cAIS</td>
<td>STM-1 MS Alarm indication signal received</td>
<td>Information</td>
<td>Reported</td>
</tr>
<tr>
<td>MS1NBBE THR15</td>
<td>STM-1 MS Near-end background block errors threshold crossing 15-min</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>MS1NBBE THR24</td>
<td>STM-1 MS Near-end background block errors threshold crossing 24-hrs</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>MS1NES THR15</td>
<td>STM-1 MS Near-end errored seconds threshold crossing 15-min</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>MS1NES THR24</td>
<td>STM-1 MS Near-end errored seconds threshold crossing 24-hrs</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>MS1NUA THR15</td>
<td>STM-1 MS Near-end unavailable seconds threshold crossing 15-min</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>MS1NUA THR24</td>
<td>STM-1 MS Near-end unavailable seconds threshold crossing 24-hrs</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>MS4cAIS</td>
<td>STM-4 MS Alarm indication signal received</td>
<td>Information</td>
<td>Reported</td>
</tr>
<tr>
<td>MS4NBBE THR15</td>
<td>STM-4 MS Near-end background block errors threshold crossing 15-min</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>MS4NBBE THR24</td>
<td>STM-4 MS Near-end background block errors threshold crossing 24-hrs</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>MS4NES THR15</td>
<td>STM-4 MS Near-end errored seconds threshold crossing 15-min</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>MS4NES THR24</td>
<td>STM-4 MS Near-end errored seconds threshold crossing 24-hrs</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>MS4NUA THR15</td>
<td>STM-4 MS Near-end unavailable seconds threshold crossing 15-min</td>
<td>Information</td>
<td>Reported</td>
</tr>
<tr>
<td>MS4NUA THR24</td>
<td>STM-4 MS Near-end unavailable seconds threshold crossing 24-hrs</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
</tbody>
</table>
The following table lists the default alarm severity assignments of the “sdhMSP” ASAP.

<table>
<thead>
<tr>
<th>Alarm identifier “Probable cause”</th>
<th>Alarm text</th>
<th>Alarm severity</th>
<th>Reporting state (default setting)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS1cFOP</td>
<td>STM-1 MS Protection switching protocol failure</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
</tbody>
</table>

The following table lists the default alarm severity assignments of the “sdhHOPath” ASAP.

<table>
<thead>
<tr>
<th>Alarm identifier “Probable cause”</th>
<th>Alarm text</th>
<th>Alarm severity</th>
<th>Reporting state (default setting)</th>
</tr>
</thead>
<tbody>
<tr>
<td>VC4NBBeTHR15</td>
<td>VC-4 Near-end background block errors threshold crossing 15-min</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC4NBBeTHR24</td>
<td>VC-4 Near-end background block errors threshold crossing 24-hrs</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC4NSeTHR15</td>
<td>VC-4 Near-end errored seconds threshold crossing 15-min</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC4NSeTHR24</td>
<td>VC-4 Near-end errored seconds threshold crossing 24-hrs</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC4NSeSCTR15</td>
<td>VC-4 Near-end severely ES threshold crossing 15-min</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC4NSeSCTR24</td>
<td>VC-4 Near-end severely ES threshold crossing 24-hrs</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC4NUAScTHR15</td>
<td>VC-4 Near-end unavailable seconds threshold crossing 15-min</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC4NUAScTHR24</td>
<td>VC-4 Near-end unavailable seconds threshold crossing 24-hrs</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
</tbody>
</table>

The following table lists the default alarm severity assignments of the “sdhLOPath” ASAP.

<table>
<thead>
<tr>
<th>Alarm identifier “Probable cause”</th>
<th>Alarm text</th>
<th>Alarm severity</th>
<th>Reporting state (default setting)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TU3cAIS</td>
<td>TU-3 Alarm indication signal received</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>TU3cLOP</td>
<td>TU-3 Loss of pointer</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC3NBBeTHR15</td>
<td>VC-3 Near-end background block errors threshold crossing 15-min</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>Alarm identifier &quot;Probable cause&quot;</td>
<td>Alarm text</td>
<td>Alarm severity</td>
<td>Reporting state (default setting)</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------</td>
<td>----------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>VC3NBBEcTHR24</td>
<td>VC-3 Near-end background block errors threshold crossing 24-hrs</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC3NEScTHR15</td>
<td>VC-3 Near-end errored seconds threshold crossing 15-min</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC3NEScTHR24</td>
<td>VC-3 Near-end errored seconds threshold crossing 24-hrs</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC3NSEScTHR15</td>
<td>VC-3 Near-end severely ES threshold crossing 15-min</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC3NSEScTHR24</td>
<td>VC-3 Near-end severely ES threshold crossing 24-hrs</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC3NUAScTHR15</td>
<td>VC-3 Near-end unavailable seconds threshold crossing 15-min</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC3NUAScTHR24</td>
<td>VC-3 Near-end unavailable seconds threshold crossing 24-hrs</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC11cPLM</td>
<td>VC-11 Payload mismatch</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC11cRDI</td>
<td>VC-11 Remote defect indicator</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC11cSSF</td>
<td>VC-11 Network connection server signal fail</td>
<td>Information</td>
<td>Reported</td>
</tr>
<tr>
<td>VC11cTIM</td>
<td>VC-11 Path trace identifier mismatch</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC11cUNEQ</td>
<td>VC-11 Unequipped</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC11NBBEcTHR15</td>
<td>VC-11 Near-end background block errors threshold crossing 15-min</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC11NBBEcTHR24</td>
<td>VC-11 Near-end background block errors threshold crossing 24-hrs</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC11NEScTHR15</td>
<td>VC-11 Near-end errored seconds threshold crossing 15-min</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC11NEScTHR24</td>
<td>VC-11 Near-end errored seconds threshold crossing 24-hrs</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC11NSEScTHR15</td>
<td>VC-11 Near-end severely ES threshold crossing 15-min</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC11NSEScTHR24</td>
<td>VC-11 Near-end severely ES threshold crossing 24-hrs</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC11NUAScTHR15</td>
<td>VC-11 Near-end unavailable seconds threshold crossing 15-min</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC11NUAScTHR24</td>
<td>VC-11 Near-end unavailable seconds threshold crossing 24-hrs</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC12NBBEcTHR15</td>
<td>VC-12 Near-end background block errors threshold crossing 15-min</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC12NBBEcTHR24</td>
<td>VC-12 Near-end background block errors threshold crossing 24-hrs</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC12NEScTHR15</td>
<td>VC-12 Near-end errored seconds threshold crossing 15-min</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
</tbody>
</table>
## Alarm management

**Provision alarm severity assignment profiles (ASAP)**

<table>
<thead>
<tr>
<th>Alarm identifier “Probable cause”</th>
<th>Alarm text</th>
<th>Alarm severity</th>
<th>Reporting state (default setting)</th>
</tr>
</thead>
<tbody>
<tr>
<td>VC12NEScTHR24</td>
<td>VC-12 Near-end errored seconds threshold crossing 24-hrs</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC12NSESscTHR15</td>
<td>VC-12 Near-end severely ES threshold crossing 15-min</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC12NSESscTHR24</td>
<td>VC-12 Near-end severely ES threshold crossing 24-hrs</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC12NUAscTHR15</td>
<td>VC-12 Near-end unavailable seconds threshold crossing 15-min</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>VC12NUAscTHR24</td>
<td>VC-12 Near-end unavailable seconds threshold crossing 24-hrs</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
</tbody>
</table>

### sdhVCG ASAP

The following table lists the default alarm severity assignments of the “sdhVCG” ASAP.

<table>
<thead>
<tr>
<th>Alarm identifier “Probable cause”</th>
<th>Alarm text</th>
<th>Alarm severity</th>
<th>Reporting state (default setting)</th>
</tr>
</thead>
<tbody>
<tr>
<td>VC12VcLOM</td>
<td>VC-12 Virtual concatenated Loss of multiframe</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC12VcSQM</td>
<td>VC-12 Virtual concatenated Sequence mismatch</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC12VcMND</td>
<td>VC-12 virtual concatenated group member differential delay out of range</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>VC12VcVCFAIL</td>
<td>VC-12 member of the VC-12-4v Virtual Concatenation Group (VCG) multiple parallel SHDSL links - failed</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>VC12VcLOA</td>
<td>VC-12 Virtual concatenated Loss of alignment</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC12VcSSF</td>
<td>VC-12 Virtual concatenated server signal fail</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC12VcSSD</td>
<td>VC-12 Virtual concatenated server signal degrade</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>VC12VcPLM</td>
<td>VC-12-Xv Payload mismatch</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC3VcLOA</td>
<td>VC-3 Virtual concatenated Loss of alignment</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC3VcSSF</td>
<td>VC-3 Virtual concatenated server signal fail</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC3VcSSD</td>
<td>VC-3 Virtual concatenated server signal degrade</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>VC3VcPLM</td>
<td>VC-3-Xv Payload mismatch</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC3VcLOM</td>
<td>VC-3 Virtual concatenated Loss of multiframe</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC3VcMND</td>
<td>VC-3 virtual concatenated group member differential delay out of range</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>VC4VcMND</td>
<td>VC-4 virtual concatenated group member differential delay out of range</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>VC3VcSQM</td>
<td>VC-3 Virtual concatenated Sequence mismatch</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC12VcLOPC</td>
<td>VC-12 Virtual concatenated loss of partial capacity</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
</tbody>
</table>
### Alarm management

**Provision alarm severity assignment profiles (ASAP)**

<table>
<thead>
<tr>
<th>Alarm identifier “Probable cause”</th>
<th>Alarm text</th>
<th>Alarm severity</th>
<th>Reporting state (default setting)</th>
</tr>
</thead>
<tbody>
<tr>
<td>VC12VcLOTC</td>
<td>VC-12 Virtual concatenated loss of total capacity</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC12VcFOPR</td>
<td>VC-12 Virtual concatenated failure of protocol received</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC12VcFOPT</td>
<td>VC-12 Virtual concatenated failure of protocol transmitted</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC3VcLOPC</td>
<td>VC-3 Virtual concatenated loss of partial capacity</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC3VcLOTc</td>
<td>VC-3 Virtual concatenated loss of total capacity</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC3VcFOPR</td>
<td>VC-3 Virtual concatenated failure of protocol received</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC3VcFOPT</td>
<td>VC-3 Virtual concatenated failure of protocol transmitted</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC12VcTLCR</td>
<td>Total reception bandwidth lost</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC12VcPLCR</td>
<td>VC-12 Virtual Concatenation Group - partially unavailable</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC12VcTLCT</td>
<td>Total transmission bandwidth lost</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC12VcPLCT</td>
<td>VC-12 Virtual Concatenation Group - partially unavailable</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC3VcTLCR</td>
<td>Total reception bandwidth lost</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC3VcPLCR</td>
<td>VC-3 Virtual Concatenation Group - partially unavailable</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC3VcTLCT</td>
<td>Total transmission bandwidth lost</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>VC3VcPLCT</td>
<td>VC-3 Virtual Concatenation Group - partially unavailable</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
</tbody>
</table>

### sdsI ASAP

The following table lists the default alarm severity assignments of the “sdsI” ASAP.

<table>
<thead>
<tr>
<th>Alarm identifier “Probable cause”</th>
<th>Alarm text</th>
<th>Alarm severity</th>
<th>Reporting state (default setting)</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTUcCNC</td>
<td>SHDSL Network Termination Unit configuration command incomplete</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>NTUcEOCF</td>
<td>SHDSL Network Termination Unit embedded operations channel failure</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>NTUcEQF</td>
<td>SHDSL Network Termination Unit equipment failure</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>NTUcINTB</td>
<td>SHDSL Network Termination Unit minor internal failure</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>NTUcLOSd</td>
<td>Loss of Signal on NTU customer port</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>NTUcNAE</td>
<td>SHDSL Network Termination Unit authentication error</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>Alarm identifier “Probable cause”</td>
<td>Alarm text</td>
<td>Alarm severity</td>
<td>Reporting state (default setting)</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------</td>
<td>----------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>NTUcNDD</td>
<td>SHDSL Network Termination Unit new device detected</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>NTUcPS</td>
<td>SHDSL Network Termination Unit power failure</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>NTUcSWDC</td>
<td>SHDSL Network Termination Unit software download complete</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>NTUcSWDF</td>
<td>SHDSL Network Termination Unit software download failure</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>NTUcSWD</td>
<td>SHDSL Network Termination Unit software download</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>NTUcUMD</td>
<td>SHDSL Network Termination Unit unmanageable device type</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>NTUcUPF</td>
<td>SHDSL Network Termination Unit unprotected failure</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>SDSLN-BBEcTHR15</td>
<td>SHDSL Near-end background block error threshold crossing 15-min</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>SDSLN-BBEcTHR24</td>
<td>SHDSL Near-end background block error threshold crossing 24-hrs</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>SDSLNEscTHR15</td>
<td>SHDSL Near-end errored second threshold crossing 15-min</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>SDSLNEscTHR24</td>
<td>SHDSL Near-end errored second threshold crossing 24-hrs</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>SDSLNS-EScTHR15</td>
<td>SHDSL Near-end severely ES threshold crossing 15-min</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>SDSLNS-EScTHR24</td>
<td>SHDSL Near-end severely ES threshold crossing 24-hrs</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>SDSLNUAScTHR15</td>
<td>SHDSL Near-end unavailable seconds threshold crossing 15-min</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>SDSLNUAScTHR24</td>
<td>SHDSL Near-end unavailable seconds threshold crossing 24-hrs</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>SDSLcBDEG</td>
<td>SDSL Moderate block error rate</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>SDSLcEQF</td>
<td>SDSL unit failure - protected</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>SDSLcDTO</td>
<td>SHDSL discovery time-out</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>SDSLcEXC</td>
<td>SDSL Excessive bit error rate</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>SDSLcLOF</td>
<td>SDSL Loss of frame alignment</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>SDSLcLOS</td>
<td>SDSL Loss of input signal</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>SDSLcNES</td>
<td>SDSL Not expected input signal</td>
<td>Information</td>
<td>Not Reported</td>
</tr>
<tr>
<td>SDSLcSEGD</td>
<td>Failed segment in SHDSL span</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>SDSLcSWE</td>
<td>SHDSL Wiring Error</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>SDSLcUNI</td>
<td>SDSL unit not present</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>SDSLcUPF</td>
<td>SDSL unit failure</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>Alarm identifier</td>
<td>Alarm text</td>
<td>Alarm severity</td>
<td>Reporting state (default setting)</td>
</tr>
<tr>
<td>------------------</td>
<td>------------</td>
<td>----------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>SDSLcWUP</td>
<td>Wrong SDSL unit present</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>SRUcCNC</td>
<td>SHDSL Regenerator Unit configuration command incomplete</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>SRUcEOCF</td>
<td>SHDSL Regenerator Unit embedded operations channel failure</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>SRU1cEOCF</td>
<td>SHDSL Regenerator Unit 1 embedded operations channel failure</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>SRU2cEOCF</td>
<td>SHDSL Regenerator Unit 2 embedded operations channel failure</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>SRUcEQF</td>
<td>SHDSL Regenerator Unit equipment failure</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>SRUcINTB</td>
<td>SHDSL Regenerator Unit minor internal failure</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>SRUcNDD</td>
<td>SHDSL Regenerator Unit new device detected</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
<tr>
<td>SRUcSWDC</td>
<td>SHDSL Regenerator Unit software download complete</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>SRUcSWDF</td>
<td>SHDSL Regenerator Unit software download failure</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>SRUcSWD</td>
<td>SHDSL Regenerator Unit software download</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>SRUcUMD</td>
<td>SHDSL Regenerator Unit unmanageable device type</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>SRU1cUMD</td>
<td>SHDSL Regenerator Unit 1 unmanageable device type</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>SRU2cUMD</td>
<td>SHDSL Regenerator Unit 2 unmanageable device type</td>
<td>Deferred</td>
<td>Reported</td>
</tr>
<tr>
<td>SRUcUPF</td>
<td>SHDSL Regenerator Unit unprotected failure</td>
<td>Prompt</td>
<td>Reported</td>
</tr>
</tbody>
</table>

### ASAP name

The ASAP name is used to distinguish different ASAPs of the same type.

The following provisioning rules apply to the ASAP name:

1. A user cannot add a new ASAP, using names like “default/Default” (in uppercase or lowercase).
2. The ASAP name is an alphanumeric string of up to 20 characters.
3. The following characters are permitted in an ASAP name:
   - Upper case letters (A … Z),
   - Lower case letters (a … z),
   - Digits (0 … 9),
   - Hyphens (-).
Maximum number of ASAPs

The total number of ASAPs is restricted to 64, including the “DEFAULT” ASAPs, and independent from the ASAP type, i.e. beyond the overall maximum number of 64, there is no specific restriction per ASAP type.
Alarm supervision

Overview

Purpose

The purpose of this section is to describe the windows and procedures related to supervision of alarms as well as to describe the mandatory prior subscription of the NE.

Contents

| Supervise alarms                      | 6-65 |
| Parameters for supervising alarm      | 6-72 |
Supervise alarms

When to use

The following procedures cover the range of possible tasks that you may have to perform on the ITM CIT in order to supervise the alarms. In the previous section, we discussed the viewing of the current alarms. This was an operation involving one single NE. In the supervision of alarms, it is possible to view the currently raised alarms of more than one single local NE. Indeed, supervision of alarms on the 1643 AM or 1643 AMS involves the monitoring of alarms on more than one alarm, locally and remotely.

Related information

The items below list other relevant information to this procedure:

- There is no related procedures to the supervision of alarms.
- Concepts of Event Management.

Before you begin

The items below gives information on tasks to perform before beginning the procedure:

- A NE must be listed and subscribed to the Supervision list, in order to see if there is or not presence of raised alarms on that NE.
- No precaution is needed when performing this procedure.

View alarm supervision list

Follow this procedure to view the list of subscribed and unsubscribed NE.

1. Select Alarms-> Alarm Supervision.

   **Result:** The Alarm Supervision window appears.

2. Verify that the desired NE is listed and subscribed.

3. If the network element is

<table>
<thead>
<tr>
<th>Then</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not listed, nor subscribed</td>
</tr>
<tr>
<td>Go to Adding NE to Supervision list, and Subscribing NE to the Supervision list.</td>
</tr>
<tr>
<td>Listed, but not subscribed</td>
</tr>
<tr>
<td>Go to Subscribing NE to the Supervision List.</td>
</tr>
<tr>
<td>Listed and subscribed</td>
</tr>
<tr>
<td>Go to step 5**</td>
</tr>
</tbody>
</table>
4 Click **Close**.

**Result:** The *Supervision: Current Alarms* window closes.

---

### Add a NE to the supervision list

1 Select **Alarms --> Alarm Supervision**.

**Result:** The *Alarm Supervision* window appears.

2 Click **Add**... to add a network element.

**Result:** The *Supervision: Add Network Element* window appears.

3 Select a network element from the proposed list or fill in the “NE name” (p. 6-74), “NSAP” (p. 6-74) and “Comment” (p. 6-72) fields manually.

4 Enter your “Password” (p. 6-74).

5 Confirm your password.

6 Click **OK**.

**Result:** The *Supervision: Add Network Element* window disappears and the ITM CIT attempts to connect and subscribe to the new NE. If any subscription error are detected, a message is displayed. If successful, the NE is showing on the *Alarm Supervision* window, with the **Subscribed** check box ticked.

---

### Delete NE from the supervision list

Follow this procedure in order to take a NE off the Supervision list

1 Select **File --> NE Login --> Alarm Subscription**.
Subscribe an NE to the supervision list

Follow this procedure to subscribe a NE to a list.

1 Select File --> NE Login --> Alarm Subscription.

   Result: The Alarm Subscription window appears.

   When opened for the first time, the list of this window is populated with the local
   network element, the network element area members and the configured nodes list
   (see procedure). For subsequent openings, the list is populated with the most recently
   used information of the Supervision File. On exiting the window, the user shall be
   prompted to save the list if it has been modified.

2 Mark the “Subscribe” (p. 6-75) check box of the desired NE
Result: The network element is selected for the alarm supervision feature.

3 Click **OK**.

**Result:** The subscription process occurs. The *Subscription Progress Display* window appears with the message “Please wait. Currently Subscribing...”. The Bottom caption “Subscribed NEs: 00/00” corresponds to the number of Subscribed/Total #NEs in the list. This figure is automatically updated.

The ITM CIT, logs into each selected NE(s), using the VIEW capability, and activates the alarm supervision function. The network element(s) appear(s) in the *Alarm Subscription* window if there is no password mismatch.

If the subscription process fails due to a wrong password, an error message is displayed, followed by the appearing of the *Supervision: Edit NE Information* window.

4 Click **“Add”** (p. 6-72) and go to procedure *Add a NE to the Supervision List*

5 Click **“Load”** (p. 6-73), if you wish to load a previously saved supervision file (if required)

**Result:** You are prompted to select a previously saved supervision file.

6 Click **Reset** if you wish to re-initialise the supervision file

**Result:** If the list has been changed, you will be prompted to save the changes before re-initialisation. Then, the list shall be emptied and repopulates as it does when it is opennetwork elements for the first time.

7 Click **OK**.

**Result:** The *Save as...* window appears to save the list contents in the supervision log file. Once the save is completed, the ITM CIT starts the subscription process. The *Subscription Progress Display* window appears with the message “Please wait. Currently Subscribing...” The Bottom caption “Subscribed NEs: 00/00” corresponds to the number of Subscribed/Total #NEs in the list. This figure is automatically updated.

The ITM CIT, logs into each selected NE(s), using the VIEW capability, and activates the alarm supervision function. The network element(s) appear(s) in the *Alarm Subscription* window.
All subscription error messages are logged in a log file, and most will not appear on the window. If the passwords are mismatched, login to the network element will fail. An error message is then displayed prompting to check the supervision log file for the reason of the login failure.

END OF STEPS

Supervise current alarms for local NE

Follow this procedure to supervise the currently raised alarms via a local session.

1 Select a NE from the list in the Alarm Supervision window.

2 Click “Alarm list” (p. 6-72)

   Result: The Supervision: Current Alarms window appears listing the raised alarms for the selected NE.

3 Click Close.

   Result: The Supervision: Current Alarms closes.

END OF STEPS

Supervise current alarms for remote NE

Follow this procedure to supervise the currently raised alarms via a remote session.

1 Select Main Menu-> Alarms-> Alarm Supervision.

   Result: The Alarm Supervision window appears.

2 Verify the presence of “Alarm type” (p. 6-72)s.

   Result: Red circles indicate the presence of alarms. Green circles indicate no alarm. These circles are only visible if the network element has the “Status” (p. 6-75) “subscribed”.

3 Select the desired NE.
4 Click “Login” (p. 6-74).

**Result:** The application attempts a remote connection to the selected network element. The application shall use the VIEW capability password stored in the supervision file to login to the selected network element. The remote NE Alarm Supervision window appears.

5 Click on “Alarm list” (p. 6-72)

**Result:** The Supervision: Current Alarms window appears listing the raised alarms for the selected NE.

6 Click Close.

**Result:** The Supervision: Current Alarms closes.

END OF STEPS

Edit the information of an existing NE

Follow this procedure to modify some of the NE information

1 Select Alarms --> Alarm Subscription.

**Result:** The Alarm Subscription window appears.

2 Select a network element from the list.

3 Click “Edit” (p. 6-72).

**Result:** The Supervision: Edit network element Information window appears.

4 Enter your changes to the “NE name” (p. 6-74) and/or “Comment” (p. 6-72).

5 Enter your “Password” (p. 6-74).

6 Confirm your password.
The Password and Confirm Password fields should match since a validation will occur to ensure integrity.

7 Click **OK**

**Result:** You will be prompted to save your changes with the *Save As...* window. These changes are stored into the supervision log file on the system controller of the NE, and on the ITM CIT. The *Supervision: Edit network element Information* window is closed and the originating window is updated.

END OF STEPS
Parameters for supervising alarm

Abort

Stops the subscription and unsubscription process from the Progress Display window. The system prompts for confirmation.

Add

Allows to add a new network element to the Supervision list and to subscribe it simultaneously. Opens the Supervision: Add network element window. Active only if the current session is the local session, else greyed out. When the user clicks OK, the network element is added to the subscription list with the check box ticked.

Alarm list

Allows to access detailed information concerning the alarms listed in the Alarms Supervision list. Only enabled when a subscribed network element has been selected. The ITM CIT opens the Supervision: Current Alarms window for the selected network element in the current local or remote session.

Alarm type

The mnemonic of the fault which is a unique identifier for the cause of the alarm. It is predefined. The naming convention includes the identification of associated correlated alarms. The default sorting order is alphanumerical.

Comment

A comment that was entered during the subscription of the network element. Can be amended from the Edit Network Element Information window.

Confirm password

Allows for password validation. The same characters as the password field should be entered.

Delete

Allows to delete the selected network element from the list. A confirmation message shall be displayed. Only active if a network element has been selected.

Edit

Allows to edit the selected network element information. Opens the Supervision: Edit network element Information window with the fields populated from the selected network element. Only active if a network element has been selected.
Info

Informs you if there is, or not, Info type alarm(s) that were raised. Info alarms, by definition, are maintenance information and no maintenance action is required at this node. Red circle indicates the presence of alarms. Green circle indicates its absence. The circle is empty if the network element has network elementver been subscribed. The status column would then read “-”.

Deferred

Informs you if there is, or not, Deferred—type alarm(s) that were raised. Deferred alarms, by definition, require maintenance action but may be deferred because no primary system service is being affected. Red circle indicates the presence of alarms. Green circle indicates its absence. The circle is empty if the network element has never been subscribed. The status column would then read “-”. The default sorting order is red circle, green circle, <empty>, or reverse.

Failure description

Displays the reason of the subscription process failure for the network element with status “-” (unsubscribed).

Help

The help-on alarms file gives additional information on the alarms and how to deal with the related problem. This help-file contains the same information as present in the “Alarm Messages and Trouble-Clearing Guide”.

Info

Informs you if there is, or not, Information alarm(s) raised on that network element. Red circle indicates the presence of alarms. Green circle indicates its absence. The field is empty if the NE has never been subscribed. The default sorting order is red circle, green circle, <empty>, or reverse.

Load

Allows to open a previously saved supervision file. This button brings up the “Open” window where a previously saved supervision file can be selected from a proposed list. If the list contents had been changed, you will be prompted to save the list before repopulation. Then the list shall then be cleared and repopulate with the new Supervision file data.
Login

Allows to remotely login into the selected network element. This button shall only be sensitive when a network element of the remote login IDs has been selected, and a local session does exist. Otherwise, this button shall be greyed out.

NE name

Shows the name of the network element. This information is kept in the “Supervision Log File” on the system controller of the NE, and on the ITM CIT. The sorting criteria is alphanumerical (or reverse).

NE state

Displays whether the network element is in a Normal state or Abnormal.

NSAP

Services Access Point address of the network element. This is the unique identification number for that network element. It is an end system address of the System Controller according to ISO 8348 AD2. The NSAP can be 16 to 40 Hexadecimal digits. The NSAP format has a distinct structure where the first 13 bytes store the network element Area Address information, the next 6 bytes store the network element unique System Identification, and the last byte stores the NSAP Selector.

The NSAP can be found on the back panel of the network element. It is stored encrypted, along with the network element name and other information, in the “Supervision Log File” on the ITM CIT, as well as on the System Controller.

Password

The login view capability password for that network element. Allows to remotely login into the network element. The system shall accept the following characters for iso8859CharSet: [32–126][161–255]. This includes all printable characters, including space, and only excludes control characters. Displayed as “*” and populated if it is retrieved from a Supervision file.

Prompt

Informs you if there is, or not, Prompt—type alarm(s) that were raised on that network element. Prompt alarms, by definition, require immediate maintenance action because a primary system service is being affected. Red circle indicates the presence of alarms. Green circle indicates its absence. The circle is empty if the network element has network elementver been subscribed. The status column would then read “-“. The default sorting order is red circle, green circle, <empty>, or reverse.
Severity

The classification of alarms depending on their impact on network element service. There are three severity type for alarms as discussed in earlier section of this chapter: Prompt, Deferred, Info.

Source

The source that triggered the alarm.

Status

Shows the network element supervision status. This can be:

- **Subscribed.** The network element is connected and the alarm subscription is operational.
- **Unsubscribed.** The network element has been unsubscribed and disconnected through a manual subscription request.
- **Logged Out.** The network element has been previously connected and subscribed, but a loss of communication has been detected. When the network element is disconnected, a warning message is displayed.
- **“—”**. The network element has been connected and subscribed. Example: Login fails for any reason.

Subscribe

Allows to subscribe and connect a network element in order to be supervised. Active only if the current session is the local session, else greyed out. Only enabled when a network element of which the Status is either “-” or “logged out” or “unsubscribed” has been selected.

Subscribe all

Allows to select all the network element from the subscription list.

Time

This is the local PC time when the supervision alarm message is received from the related network element. The format is MM/DD/YYYY:00:00:00 but can be modified. The most recent alarm is shown on top of the list, by default. The list can be sorted in the opposite order, if preferred.
Unsubscribe

Allows to unsubscribe and disconnect network elements in the network element. A confirmation message shall be displayed. Active only if the current session is the local session, else greyed out. Enabled only when a subscribed network element has been selected. The status shall be changed to *Unsubscribed*.

Unsubscribe all

Allows to deselect all the network elements from the subscription list.
View historical data

Overview

Purpose

The purpose of this section is to describe the windows and procedures to access historical data as well as to describe the procedure to set display filters to the list.

Contents

<table>
<thead>
<tr>
<th>Historical data</th>
<th>6-78</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retrieving historical data</td>
<td>6-79</td>
</tr>
<tr>
<td>Parameters for retrieving historical data</td>
<td>6-81</td>
</tr>
</tbody>
</table>
Historical data

Cleared alarms

The *History Alarms* window lists the cleared alarms and stores the data in the history log for the network element. This path of the history log file is defined in the *File->Options.*
Retrieving historical data

When to use

Follow these steps to view details about alarms that have cleared and moved to the history bin.

Related information

Parameters used in this procedure can be found at “Parameters for retrieving historical data” (p. 6-81).

Before you begin

The items below gives information on tasks to perform before beginning the procedure:

- No prerequisites are needed when performing this procedure.
- No precaution is needed when performing this procedure.

Display the history alarms list

Follow this procedure to display the history of all alarms.

1 Select Alarms -> History Alarms.

Result: History Alarms window appears and displays a list of cleared and raised alarms in the History log of the network element.

2 Select an alarm from the alarms list and click Details...

Result: The History/Current Alarm Details window appears.

3 Click Close to return to the History window.

END OF STEPS

Set up filters

Follow this procedure to implement filters in the History window.

1 Select Alarms -> History Alarms.
**Result:** History Alarms window appears.

2. Mark the **Filtering** checkbox and click **Filter...**

   **Result:** The **Alarm List Filter Configuration** window appears.

3. Select your filter options and click **OK**.

   **Result:** The **Alarm List Filter Configuration** window disappears.

END OF STEPS
Parameters for retrieving historical data

Alarm type

The alarm type is an identifier which uniquely defines the cause of the alarm. It is predefined. The naming convention includes a part which identifies the associated correlated alarms. The default sorting order for this field is alphanumerical.

Category

Filters the alarms based on the location where they occurred. For example Equipment refers to alarms triggered by plug-in units defects such as a unit failure or a laser fault conditions. Processing refers to alarms triggered by inconsistencies during the processing of provisioned data. Environment refers to alarms caused by defects detected in external devices. Management refers to alarms triggered by malfunctions in the communication between the Management System and the Network Element.

Description

The Description field shows the full description of the selected alarm.

Details

The Details... button displays the details of the selected alarm. Only one alarm can be selected at a time. The button is only selectable when an alarm has been selected from the list.

Filter

The Filter... button opens the Alarm List Filter Configuration window. In this window you can change the filter criteria.

Filtering

This check box activates or inactivates the alarm filtering functionality. The alarm filtering is based on the current alarm filters. Whenever the check box is unmarked (inactivated), no filtering occurs. The default is disabled.

Severity

Classifies the alarm into three priorities, depending on the urgency of the recommended response. “Concepts” (p. 6-4) describes the three possible severities levels of an alarm.

Source

The location where the alarm was triggered during transmission, for example Network Element (NE), Shelf, Slot, Port, AU, VC, TU, or Timing.
There are two possible status for an alarm: Raised when it is displayed but not yet attended to and Cleared when it has been raised and attended to.

Time raised

The time at which the alarm was raised. The default format is MM/DD/YYYY:00(hr):00(mn):00(s) but can be modified. The displayed time should be the local ITM-CIT time, that is the local time zone.

Time cleared

The time at which the alarm was cleared and moved to the History Alarm list. The default format is MM/DD/YYYY:00(hs):00(ms):00(s) but can be modified. The displayed time should be the local ITM-CIT time, that is the local time zone.
7 Timing provisioning

Overview

Purpose

The purpose of provisioning timing is to synchronize the network element with a timing reference and to distribute this timing reference to SDH and non-SDH equipment.

Outcome

The outcome of provisioning timing is a synchronized network element working according to the timing network plan.

Recommendations

When provisioning timing, it is recommended to perform the procedures in the order in which they are presented.

Contents

<table>
<thead>
<tr>
<th>Concepts</th>
<th>7-3</th>
</tr>
</thead>
<tbody>
<tr>
<td>NE timing</td>
<td>7-4</td>
</tr>
<tr>
<td>Network synchronization</td>
<td>7-7</td>
</tr>
<tr>
<td>Timing quality levels</td>
<td>7-9</td>
</tr>
<tr>
<td>Priorities</td>
<td>7-11</td>
</tr>
<tr>
<td>Example of network Timing</td>
<td>7-13</td>
</tr>
<tr>
<td>Timing loop</td>
<td>7-14</td>
</tr>
<tr>
<td>Re-timing</td>
<td>7-15</td>
</tr>
<tr>
<td>Timing configuration</td>
<td>7-17</td>
</tr>
<tr>
<td><strong>Provisioning</strong></td>
<td>7-19</td>
</tr>
<tr>
<td>Provisioning timing sources</td>
<td>7-20</td>
</tr>
<tr>
<td>Parameters for provisioning timing sources</td>
<td>7-26</td>
</tr>
<tr>
<td>Provisioning system timing</td>
<td>7-32</td>
</tr>
<tr>
<td>Parameters for provisioning system timing</td>
<td>7-35</td>
</tr>
<tr>
<td>Provisioning station clock output</td>
<td>7-39</td>
</tr>
<tr>
<td>Parameters for provisioning station clock output</td>
<td>7-43</td>
</tr>
<tr>
<td>Provisioning output port timing</td>
<td>7-47</td>
</tr>
<tr>
<td>Parameters for provisioning output port timing</td>
<td>7-50</td>
</tr>
</tbody>
</table>
Concepts

Overview

Purpose

This section explains the concepts of timing in SDH networks.

Features and jargon concerning timing distribution in a network element and a network are treated together with the basic timing architecture of the network element.

Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>NE timing</td>
<td>7-4</td>
</tr>
<tr>
<td>Network synchronization</td>
<td>7-7</td>
</tr>
<tr>
<td>Timing quality levels</td>
<td>7-9</td>
</tr>
<tr>
<td>Priorities</td>
<td>7-11</td>
</tr>
<tr>
<td>Example of network Timing</td>
<td>7-13</td>
</tr>
<tr>
<td>Timing loop</td>
<td>7-14</td>
</tr>
<tr>
<td>Re-timing</td>
<td>7-15</td>
</tr>
<tr>
<td>Timing configuration</td>
<td>7-17</td>
</tr>
</tbody>
</table>
NE timing

Introduction
For telephone exchanges or switches, accurate timing is critical. Therefore switches are synchronized with each other. One way of synchronizing is through the network. In this case all the SDH-network elements in the network are synchronized with one master clock. All the switches in the network can synchronize with the network, and consequently to the master clock.

Timing reference
The timing signal received by a network element is called the timing reference.
The 1643 AM or 1643 AMS can work in two different mode, the STM-1 and the STM-4 mode.
If it is working in the STM-1 mode, the different ports that provide the input signals that are available as timing references are the:
- line port
- tributary port.
If the 1643 AM or 1643 AMS is working in the STM-4 mode and if the STM-1 option board is available, an extra tributary port is present as a timing reference.

Timing output
A network element can provide a synchronization signal to other equipment by sending an output timing signal.
Different output timing sources that can be used are:
- station clock output
- line port
- tributary port.

External clock output
For synchronization of equipment that is not connected to the network element by tributary or line signals, the network element can provide an external clock signal (usually two Mhz). However, this equipment must be in close proximity to the network element as the clock signal can only be carried a few hundred meters.

Timing sources and outputs
A schematic drawing of a network element with the timing sources and output is shown. The dotted arrows indicate outgoing timing signals. The straight arrows indicate the timing inputs on which the internal clock of the network element can be synchronized.
Timing modes

Timing units can be set in different modes:
- free running
- hold over
- locked.

Free running

In the Free running mode, the timing unit generates a clock signal from its own oscillator. No timing signal from other equipment is used for the network element synchronization.

Hold over

The Hold over mode will prevent a frequency step in case of a reference failure. Therefore it uses a frequency memory of the last available frequency.

Locked

In the Locked mode, the timing unit locks the oscillator-frequency to one of the external timing sources.

Schematic view of the timing modes

The next figure gives a schematic view of the three different timing modes.
Timing provisioning concepts

- Hold over mode
- Memory
- Voltage controlled oscillator
- Free running mode
- Feedback loop
- Phase locked loop (PLL)
- Locked mode
- Timing sources

Diagram illustrating the timing concepts with various modes and components.
Network synchronization

Introduction

For telephone exchanges or switches, accurate timing is critical. Therefore switches are synchronized with each other. One way of synchronizing is through the network. In this case all the SDH-network elements in the network are synchronized with one master clock. All the switches in the network can synchronize with the network, and consequently to the master clock.

Timing equipment

A network can use different types of equipment as a timing reference, each having its own, well defined, accuracy.

- Primary Reference Clock (PRC)
- Synchronization Supply Unit-Transit (SSU-T)
- Synchronization Supply Unit-Local (SSU-L)
- SDH Equipment Timingsource (SEC)

PRC

The master clock should be a primary reference clock (PRC), that provides a very accurate network clock (a clock satisfying the ITU-T recommendation G.811). The other network elements in the ring are slaved to this clock. A second clock in the network can be used to act as the backup of the master clock.

The PRC can either be an autonomous clock or it is able to accept synchronization from a radio or satellite signal.

SSU

Noise, called jitter, may accumulate on the signal after passing through many nodes. It therefore becomes necessary at some point to recover and reshape the signal. In this case a synchronization supply unit (SSU) will be used. In addition to recovering and reshaping, the SSU will also be able to run on its own when the reference signal (for instance coming from the PRC) is lost. In this case, the SSU will be able to maintain the quality of the reference signal it produces by means of a holdover mode: the frequency and phase of the reference signal are stored in a memory and used to generate a reference signal locally.

Two kinds of SSUs exist:

- SSU-T: SSU-Transit
- SSU-L: SSU-Local
The functionality of both SSUs is equal, the accuracy of the SSU-T is higher than the accuracy of the SSU-L.

SEC

An SDH network element has its own internal oscillator, called the SDH equipment clock (SEC). The accuracy of a SEC is lower than the accuracy of both the SSU and the PRC.

Network example

The next figure gives an example of a network. Four network elements (NEs) of a large network are drawn, plus a master clock (PRC) and a SSU.
Timing quality levels

Introduction

To choose the most appropriate timing signal from all the incoming timing signals, the quality of the timing signals must be known.

Different quality levels are defined for timing signals. The quality levels specify the quality of the incoming or outgoing timing signal. The quality levels are related to the equipment used to produce the corresponding timing signal.

Accuracy

The accuracy of a timing signal can be given in an accuracy value. Every timing signal will have an average frequency, and a deviation in time from the average frequency value. The deviation from the average frequency, can be represented as a fraction of the average frequency. This fraction is known as the accuracy value.

Example

When a timing reference has an average frequency of 2048 MHz, and varies in time between 2048.01 MHz and 2047.99 MHz, the deviation from the average value is plus or minus 0.01 MHz. This can be expressed in an accuracy value:

Accuracy = \( \frac{0.01}{2048} = 0.0000049 = 4.9 \times 10^{-6} \)

Quality levels

The quality level (QL) values are transported as a synchronization status message in the S1 Byte in the STM-N signal or in the 4th–8th position of the Sa-bit in a framed 2 Mbit/s signal.

<table>
<thead>
<tr>
<th>QL</th>
<th>S1-byte</th>
<th>Accuracy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quality Unknown</td>
<td>S1=0</td>
<td>N/A</td>
<td>No QL information of the signal is available.</td>
</tr>
<tr>
<td>PRC</td>
<td>S1=02</td>
<td>(10^{-11})</td>
<td>Primary Reference Clock indicates that the timing signal is provided by a Primary Reference Clock.</td>
</tr>
<tr>
<td>SSU-T</td>
<td>S1=04</td>
<td>(1.5 \times 10^{-9})</td>
<td>Synchronization Supply Unit-Transit indicates that the timing signal is derived from a Transit SSU</td>
</tr>
<tr>
<td>SSU-L</td>
<td>S1=08</td>
<td>(3 \times 10^{-8})</td>
<td>Synchronization Supply Unit-Local indicates that the timing signal was derived from a Local SSU</td>
</tr>
<tr>
<td>SEC</td>
<td>S1=11</td>
<td>(4.6 \times 10^{-6})</td>
<td>SDH Equipment Clock indicates that the timing signal is provided by an SDH Equipment Clock.</td>
</tr>
</tbody>
</table>
### Timing quality levels

<table>
<thead>
<tr>
<th>QL</th>
<th>S1-byte</th>
<th>Accuracy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNU</td>
<td>S1=15</td>
<td>N/A</td>
<td>Do not use for synchronization indicates that the timing signal should not be used, since it may cause timing loops.</td>
</tr>
</tbody>
</table>
Priorities

Introduction

The timing reference signal is transported through a synchronized network by the network elements. The path this timing signal will follow can be controlled by the network operator.

Description

When only the quality level of the timing reference signal is used, more signals with equal quality level can arrive at a network element. To determine the timing source that the network element will choose in such a case, a priority is assigned to each timing source.

In choosing a timing source, the network element first selects the timing source with the highest quality level. When there are several timing sources available with this highest quality level, the priority is taken into account.

Example

In this figure, notice how the priorities define the timing path when each node receives two signals of PRC quality. The priority in the upper node is disabled since this input signal depends on an output signal of this network element; this could cause a timing loop, as explained in "Timing Loop".
Timing provisioning

Concepts

Priorities

1. Priority = 1
2. Priority = 2
3. Priority = disabled
Example of network Timing

Introduction

Timing in a network can be realized in numerous ways and configurations. The following example shows a timing chain with a regenerator loop and one PRC. The quality levels indicated in the figure represent the information that is carried by the S1 byte of that signal.

Example of a timing chain with a regenerator loop

![Timing Chain Diagram]

This network contains a station clock (PRC quality), a number of network elements and an SSU. A dotted line indicates the outgoing timing signals, a straight arrow inside a network element indicates the timing signal that is used to synchronize with. The connection between the network elements can either be line signals or tributary ports.

Different types of timing

From left to right, the following types of network element timing can be identified:

- station clock timing
- line/tributary timing
- regenerator loop
- line/tributary timing.
Timing loop

Introduction

If a timing plan is not engineered correctly, a timing loop may occur. In a timing loop the timing signal that is received by a network element cannot be traced back to an independent reference. The reference signal that a network element receives in a timing loop, depends on the timing signal that this network element sends out itself. In the figure below an example of a timing loop is given. Both network elements get a timing reference which depends on itself.

Timing loop sketched

In a timing loop the timing reference of a network element is derived from the timing output of the same network element. Due to this, the reference signal becomes very instable. This affects the performance of the network in a negative way.

To prevent timing loops, the quality level and priority for every port must be provisioned correctly. By disabling certain ports timing loops can be avoided.
Re-timing

Introduction

When, for instance, a 2 Mbit/s PDH signal enters an SDH network, it is mapped into a VC-12. This VC-12 itself is aligned to a TU-12 in larger containers (for instance VC-4) and then transported through the network. A pointer is carried along to indicate the position of the VC-12 in the container. During transport through the SDH network, the VC-12 may shift in the TU-12. As a consequence, the pointer will also change, since it dynamically indicates the position of the VC-12.

In other words, the payload can float in the container. Due to this floating, the phase information of the original 2 Mbit/s signal inside the VC-12 can no longer be used.

This problem can be overcome using (2 Mbit/s) retiming. The main idea of retiming is the enforcement of timing integrity at the cost of data integrity.

Re-timing

A phase difference might occur between the tributary signal entering the SDH Network and the network element clock of the node where this signal leaves the SDH network. Even if the whole SDH network is synchronized with one reference clock, this clock can be out of phase with the original clock of the tributary signal. To clock the signal out with the SDH-PRC frequency, the signal is unpacked (from its virtual container) and stored in an elastic buffer. From there it is sent out, and then the retimed signal will carry the SDH-PRC frequency. Now it can be used as a timing reference outside the SDH network.

Retiming is possible on the following tributary interfaces:

- 1.5 Mbit/s interfaces
- 2 Mbit/s interfaces
- X.21 interfaces.

**Important!** Due to the nature of the X.21 protocol, enforcement of timing integrity does not go at the cost of data integrity on this interface.

Self-timed

In the self-timed mode, the timing signal is derived from the bitrate of the, in case of 2 Mbit/s re-timing, VC-12. The bitrate may fluctuate due to pointer adjustments within the SDH network. Therefore the self-timed mode is not suitable for carrying a timing reference through the SDH network.
In the following figure, the dotted lines indicate the timing sources and outputs that are used in the network. The solid lines indicate the data transport. A 2 Mbit/s signal entering an SDH network and leaving it with 2 Mbit/s re-timing.
Timing configuration

Timing functions

Timing functions of the network element can be divided into three main functionalities. These three functionalities correspond to the three main windows for timing management.

To provision the network element timing, all these functionalities must be addressed.

Block functionality

The table below indicates the actions that can be performed in the procedures addressing the three functionalities.

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timing Sources</td>
<td>Input port timing process</td>
</tr>
<tr>
<td></td>
<td>Timing source assignment</td>
</tr>
<tr>
<td></td>
<td>Timing source functions</td>
</tr>
<tr>
<td>System Timing</td>
<td>System timing link switch</td>
</tr>
<tr>
<td></td>
<td>System clock processes</td>
</tr>
<tr>
<td></td>
<td>Output port timing process</td>
</tr>
<tr>
<td>Station Clock Output Timing</td>
<td>Output clock timing link switch</td>
</tr>
<tr>
<td></td>
<td>Station clock output selection</td>
</tr>
<tr>
<td></td>
<td>Station clock output process</td>
</tr>
<tr>
<td></td>
<td>Station clock output distribution functions</td>
</tr>
</tbody>
</table>

Functional diagram

The following diagram indicates the three main functionalities.
Timing provisioning Concepts

Timing configuration

Diagram showing timing reference ports, logical timing sources, and various timing sources and priorities. The diagram illustrates how timing signals to all transmission units are managed, including output timing, system timing, and timing mode selection.
Provisioning

Overview

Purpose

This section provides information on provisioning timing sources, system timing, station clock, and output port timing.

Contents

| Provisioning timing sources                      | 7-20 |
| Parameters for provisioning timing sources      | 7-26 |
| Provisioning system timing                     | 7-32 |
| Parameters for provisioning system timing      | 7-35 |
| Provisioning station clock output              | 7-39 |
| Parameters for provisioning station clock output | 7-43 |
| Provisioning output port timing                | 7-47 |
| Parameters for provisioning output port timing | 7-50 |
Provisioning timing sources

When to use

The purpose of provisioning timing sources is to provide a timing source with a defined quality level (QL), and to assign a valid physical timing reference to the logical timing source used to synchronize the network element.

In the following two cases this procedure must be performed:

- As the first procedure to complete when provisioning the network element timing.
- If the network element system timing will operate in the locked mode.

Related information

Related procedures are:

- “Provisioning system timing” (p. 7-32)
- “Provisioning output port timing” (p. 7-47)
- Provision MSP.

Parameters used in this procedure can be found at “Parameters for provisioning timing sources ” (p. 7-26).

Before you begin

Before starting this procedure, make sure that:

- A network element synchronization plan must be available.

Pay attention to the following item:

- Incorrect settings for worker/protection references and quality level-provisioning can cause a timing loop.

Assign working reference to timing source

To assign a (working) timing reference to a timing source for the 1643 AM or 1643 AMS without STM-1 tributaries, follow this procedure:

1. Select Provisioning --> Timing --> Timing Sources

   Result: The Provisioned NE Timing Source Information window appears.

2. Select a source that must be edited from the list and click Assign.
Assign references to timing sources

To assign a working and protection timing reference to a timing source for the 1643 AM or 1643 AMS working in the STM-4 mode with STM-1 tributaries, follow this procedure:

1. Select Provisioning --> Timing --> Timing Sources

   **Result:** The Provisioned NE Timing Source Information window appears.

2. Select a source that must be edited from the list and click **Assign**.

   **Result:** The Assign Timing Reference to Timing Source window appears.

3. Select a slot (or a "-") from the list under **Working Reference**.
Result: A list of all possible ports (or a "-" ) appears for the selected slot.

4 Select a port (or a "-" ) from the list for the Working Reference.

Result: The Working Reference for the timing source is selected (in case a port is selected) or the Working Reference for the timing source is unassigned (in case "-" is selected).

5 Select a slot (or a "-" ) from the list under Protection Reference.

Result: A list of all possible ports (or a "-" ) appears for the selected slot.

6 Select a port (or a "-" ) from the list for the Protection Reference.

Result: The Protection Reference for the timing source is selected (in case a port is selected) or the Protection Reference for the timing source is unassigned (in case "-" is selected).

7 Click OK to confirm the current settings.

Result: The Assign Timing Reference to Timing Source window is closed and data is sent to the network element.

8 Click Close.

Result: The Provisioned NE Timing Source Information window disappears.

Set QL prov, monitored, switch request, clear wait to restore

To set the quality level for an incoming (SDH) timing reference, set the Monitored state of the timing reference, make a switch request or clear the Global Wait To Restore Time follow this procedure:

1 Select Provisioning --> Timing --> Timing Sources

Result: The Provisioned NE Timing Source Information window appears.

2 Select a source that must be edited from the list and click Edit in the Sources field.
Result: The Edit Provisioned NE Timing Source window appears.

3 Select AUTO or a QL value from the list for QL Provisioned.
   Result: A value is set for QL Provisioned.

4 Select Yes or No for Monitored.
   Result: The monitoring of the reference of the timing source is set.

5 Important! A Switch Request can only be made if a protection reference is assigned. This is only possible if the 1643 AM or 1643 AMS is working in the STM-4 mode and STM-1 tributary units are present.
   Select No Request or a switch request from the list for Switch Request.
   Result: A switch is made.

6 In case the Signal Status of the timing source is Wait To Restore, and it must be reset, click Clear WTR.
   Result: The Signal Status of the timing source changes from Wait to Restore into the actual Signal Status of the timing source.

7 Click OK to confirm the current settings
   Result: The Edit Provisioned NE Timing Source window disappears and data is sent to the network element.

8 Click Close.
   Result: The Provisioned NE Timing Source Information window disappears.

Edit global wait to restore time

To change the Global Wait to Restore Time follow this procedure:

1 Select Provisioning --> Timing --> Timing Sources
Result: The Provisioned NE Timing Source Information window appears.

2 Click **Edit** in the Global Wait To Restore field.

   **Result:** The Edit Global Wait To Restore Time window appears.

3 Set the **Global Wait To Restore Time**.

4 Click **OK** to confirm the current setting.

   **Result:** The global wait to restore time is set for the timing in the network element, and the *Edit Global Wait To Restore Time* window disappears.

5 Click **Close**.

   **Result:** The Provisioned NE Timing Source Information window disappears.

---

**View the timing source status**

To view the status of a timing source follow this procedure:

1 Select **Provisioning --> Timing --> Timing Sources**

   **Result:** The Provisioned NE Timing Source Information window appears.

2 Select a source to be viewed from the list and click **Details**.

   **Result:** The Detailed Timing Sources Information window appears.

3 Click **Update**.

   **Result:** The Detailed Timing Sources Information window is filled with the actual parameter settings for the timing source indicated in the *Source* field.

4 Check the status of the timing source

5 Click **Close** to close the window.
Result: The Detailed Timing Sources Information window disappears.

6 Click Close.

Result: The Provisioned NE Timing Source Information window disappears.

END OF STEPS
Parameters for provisioning timing sources

Introduction

The procedure for provisioning timing sources defines the timing sources for network element synchronization.

The diagram below gives an overview of the relationship between the physical timing references and the logical timing sources.

The physical timing references are indicated on the left side, the logical timing sources on the right side. Physical references can be assigned to the timing sources, therefore parameters are used. The parameters are indicated in the functional diagram. The arrows pointing towards the block indicate the parameters that can be provisioned. The arrows that point away from the block indicate read only parameters. The dotted arrows indicate that arrows apply to more references or sources.

**Important!** The 1643 AM or 1643 AMS can have an optional STM-1 tributary board present when working in the STM-4 mode. In that case some of the screens and parameters are slightly different from the default version. This is because of the possibility to then provision a protection reference.
Active reference

When a protection timing reference is provisioned, the active timing reference can be the working reference or the protection reference. The reference actually being used by the network element is indicated in the Active Reference field.

Clear WTR

The Clear Wait-To-Restore command (Clear WTR) resets the wait to restore timer and the signal status will revert to normal.

Global wait to restore time

In case of a failure the system switches to a valid reference. When the failure is no longer present, the system switches back, after a certain waiting period (the switching is revertive). This waiting period is called the Global Wait to Restore Time. It can range from 0 minutes to 60 minutes. The signal status will become Wait to Restore.
The *Global Wait to Restore Time* setting holds for all the timing in the network element. That is, for the Timing Sources, for the System Timing, and for the Station Clock Output Timing.

**Monitored**

The user can enable or disable the option for monitoring a timing source. If a timing source is monitored, the timing source will forward the *Reference Fail* and *Reference Unequipped* alarms to the management system when applicable.

*Monitored* can have the values Yes or No.

**Protection port/p port**

The protection ports that can be assigned to the timing sources:

<table>
<thead>
<tr>
<th>Timing Sources</th>
<th>Possible Timing References</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRIB-1</td>
<td>TP2.1 to TP2.2</td>
</tr>
<tr>
<td>TRIB-2</td>
<td>TP2.1 to TP2.2</td>
</tr>
</tbody>
</table>

**Protection reference**

The *Protection Reference* indicates the port that is assigned to be the *Protection Port*.

**QL-in**

When the quality level is read from the S1-byte from the timing references, it is reflected in the *QL-in* parameter. This parameter can have all of the defined quality level values. See subsection “Timing Quality Levels”.

**QL-in status**

The user can view the status of the incoming quality level (*QL-in Status*) for each timing source. The possible values are:

<table>
<thead>
<tr>
<th>QL-in status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>The received quality level is in the valid range.</td>
</tr>
<tr>
<td>Invalid</td>
<td>The received quality level falls outside the valid range or is unstable.</td>
</tr>
<tr>
<td>Not Supported</td>
<td>The corresponding input port does not provide S1-byte extraction.</td>
</tr>
<tr>
<td>Not Applicable</td>
<td>No reference is assigned to the timing source, or the assigned signal experiences a reference fail.</td>
</tr>
<tr>
<td>QL-in status</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Unstable</td>
<td>The received quality level is unstable.</td>
</tr>
</tbody>
</table>

**QL-out**

The *QL-out* parameter indicates the actual quality level value of the timing source that is used by the system timing block and the station clock output block. The *QL-out* value is the quality level that enters the system timing and station clock output blocks. When *QL Prov* is *Auto*, *QL-out* equals *QL-in*. When *QL Prov* is not *Auto*, *QL-out* equals *QL Prov*.

**QL prov**

The quality level of timing references can be provisioned by the user. The provisioned quality level is called *QL Prov*. In case of a timing reference without an S1-byte, *QL Prov* allows the user to provision a quality level. When a timing reference does have an S1-byte (*QL-in* can be read by the system), this value can be overruled by *QL Prov*.

**Reference**

*Reference* indicates the actual reference that is used for the selected timing source. This is only applicable if the 1643 AM or 1643 AMS is working in the STM-1 mode or in the STM-4 mode without the optional STM-1 tributary board present.

**Reference fail**

When the incoming signal cannot provide a timing reference, the timing reference is considered to fail. *Reference Fail* can take the values *Yes* or *No*.

**Signal status**

The signal status is received in the timing sources block and forwarded to the system timing block and the station clock output timing block. The possible values are:

<table>
<thead>
<tr>
<th>Signal Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Connected</td>
<td>No reference is assigned to the timing source.</td>
</tr>
<tr>
<td>Failed</td>
<td>A timing link fail is declared for the assigned timing link.</td>
</tr>
<tr>
<td>Wait to Restore</td>
<td>The assigned reference signal will be available again when the Wait to Restore timer has expired.</td>
</tr>
<tr>
<td>Normal</td>
<td>The logical timing source is assigned to a valid timing reference.</td>
</tr>
</tbody>
</table>
Switch requests are shown in the table in order of priority, together with their description.

<table>
<thead>
<tr>
<th>Switch Request</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Request</td>
<td>This is the default value. The system timing is operating under normal conditions.</td>
</tr>
<tr>
<td>Clear</td>
<td>Replaces the status by the normal status (in case of a previous switch).</td>
</tr>
<tr>
<td>Forced</td>
<td>Unconditional switch, issued by the user, even if it is service degrading.</td>
</tr>
<tr>
<td>Manual</td>
<td>A conditional switch, which is issued by the user. The switch will not be performed if it is service degrading.</td>
</tr>
</tbody>
</table>

Switch status

This parameter indicates the latest switch request. When no protection reference is provisioned, this parameter is not available. The possible values of this parameter are listed in the table below:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Request</td>
<td>No switch request has been issued.</td>
</tr>
<tr>
<td>Clear</td>
<td>The former switch request is cleared. Switching will be system controlled after this request.</td>
</tr>
<tr>
<td>Forced Switch</td>
<td>A forced switch has been made to a timing source as indicated by the user.</td>
</tr>
<tr>
<td>Manual Switch</td>
<td>A manual switch has been made to a timing source as indicated by the user.</td>
</tr>
</tbody>
</table>

Timing source

Physical timing references can be assigned to logical timing sources. Once a timing reference is assigned to a timing source, no other reference can be assigned to the same source.

Transmission protected

*Transmission Protected* indicates whether the timing reference is MSP-protected for transmission. The values for *Transmission Protected* are *Yes* and *No*. 
Working port / w port

The working ports that can be assigned to the timing sources:

<table>
<thead>
<tr>
<th>Timing Source</th>
<th>Possible Timing Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line_1</td>
<td>LP1.1, LP2.1</td>
</tr>
<tr>
<td>Line_2</td>
<td>LP1.1, LP2.1</td>
</tr>
<tr>
<td>TRIB_1</td>
<td>TP1.1..TP1.16</td>
</tr>
<tr>
<td></td>
<td>TP2.1..TP2.16, if an optional 2 Mbit/s board is present</td>
</tr>
<tr>
<td></td>
<td>TP2.1..TP2.2, if an optional STM-1 board is present</td>
</tr>
<tr>
<td>TRIB_2</td>
<td>TP1.1..TP1.16</td>
</tr>
<tr>
<td></td>
<td>TP2.1..TP2.2, if an optional STM-1 board is present</td>
</tr>
</tbody>
</table>

Working reference

The *Working Reference* indicates the port that is assigned to be the *Working Port*.

This is only applicable if the 1643 AM or 1643 AMS is working in the STM-4 mode, with the optional STM-1 tributary board present.
Provisioning system timing

When to use

The purpose of "Provision System Timing" is to lock the network element synchronization and outgoing timing signals to a timing source with the highest quality level.

This procedure should be performed in the following cases:

- As the second procedure in network element timing provisioning.
- If the network element system timing is required to operate in the lock out mode.

Pay attention to the following items:

- When used, do not forget to clear the lockout condition after maintenance.

Related information

Related procedures are:

- “Provisioning timing sources” (p. 7-20)
- “Provisioning output port timing” (p. 7-47)

Parameters used in this procedure can be found at “Parameters for provisioning system timing” (p. 7-35)

Before you begin

Before starting this procedure, make sure that:

- The "Provision Timing Sources" procedure is completed.
- The network element synchronization plan must be available.

Set priority and lock out

To set the priority or the lockout for a timing source follow this procedure:

   
   **Result:** The Provisioned NE System Timing Information window appears.

2. Select a source to edit from the list and click **Edit** in the System Timing Sources field.
   
   **Result:** The Edit Automatic Selection Criterions for NE System Timing window appears.

3. Set Priority or Lock Out Request.
Timing provisioning
Provisioning

Important! A lockout request cannot be made if the priority is disabled.

4 Click OK to confirm the current settings.

5 To provision another Timing Source go to step 2, otherwise go to step 6.

6 Click Close
   Result: The Provisioned NE System Timing Information window disappears.

END OF STEPS

Set timing mode and QL mode

To set the Timing Mode and the QL Mode for a timing source follow this procedure:

1 Select Provisioning --> Timing --> System Timing.
   Result: The Provisioned NE System Timing Information window appears.

2 Click Edit in the System QL field.
   Result: The Edit QL Mode window appears.

3 Set the QL Mode to Enabled or Disabled.

4 Click OK to confirm the current settings.
   Result: The Edit QL Mode window disappears.

5 Click Edit in the Timing Mode field.
   Result: The Select Timing Mode window appears.

6 Set the Timing Mode to Free Running, Holdover, or Locked.
7 Click OK to confirm the current settings.

**Result:** The Select Timing Mode window disappears.

8 Click Close

**Result:** The Provisioned NE System Timing Information window disappears.

**END OF STEPS**

### Switch active timing source

To switch the timing source that is used as the active timing source follow this procedure:

1 Select Provisioning --> Timing --> System Timing.

**Result:** The Provisioned NE System Timing Information window appears.

2 Click Switch in the Active System Timing Source field.

**Result:** The Switch Request for NE System Timing window appears.

3 Select a request from the Request list. If a manual switch or a forced switch is required, select also a timing source to switch to from the System Timing Source list.

4 Click OK to confirm the current settings and send the request to the network element.

**Result:** Depending on the System state and the request, the switch will be automatically successful or an error message will be displayed. The Switch Request for NE System Timing window disappears.

5 Click Close

**Result:** The Provisioned NE System Timing Information window disappears.

**END OF STEPS**
Parameters for provisioning system timing

Introduction

The system timing functional block in the network element is responsible for:

- Selecting the timing sources to synchronize the system.
- Selecting the timing mode for the system.
- Translating the quality level into the S1-byte of the outgoing signal.

The different parameters that can be set in the system timing functionality are indicated in the figure below.

Functional diagram

A functional diagram of the System Timing functionality

Active system timing source

The *Active System Timing Source* indicates the timing source currently used to synchronize the system, together with the *Switch Status* of the source and the latest issued *Switch Request*.

Lock out

The user can disable a specific timing source that enters the timing source selection without changing the priority settings. If a timing source is locked out, it will not take part in the timing source selection.
Whether a timing source is locked out is indicated by the Lockout parameter. The possible values for the Lockout parameter are: Yes and No.

**Lock out request**

The Lock out state can be changed with the Lock Out Request parameter. This can be set to Yes or No.

The Lock Out Request is for maintenance purposes. A Timing Source, which has a priority value assigned to it, can be temporarily locked out. When the Timing Source is already disabled, a Lock Out Request is rejected. A Lockout Request is set to No automatically when the Timing Source is disabled.

When Priority = Disabled the Lock Out Request field is greyed out.

**Important!** When a timing source is locked out, the network element is in the Abnormal State.

**Priority**

The priority can be set for each timing source. For a network element with N timing sources provisioned, the priority can have values from 1 to N.

The Priority parameter can also have the value Disabled. A disabled timing source will not be taken into account in the Timing Source Selection for the system timing.

**Important!** Make sure not to provision identical Priority values to multiple timing sources.

**QL**

The quality level of a timing source, that is used for automatic timing mode selection is indicated in the Provisioned NE System Timing Information window. This QL is identical to the QL-out as described in “Parameters to Provision Timing Sources”.

**QL mode**

The QL-mode parameter allows to disable or enable the use of the S1-byte in the algorithm to select the active timing reference. The possible values for QL-mode are Enabled and Disabled.

When QL Mode is enabled, the system will choose the timing source with the best quality level. In case of multiple timing sources with all the best quality level, the timing source with the lowest priority value is selected.
Signal status

The signal status is received in the timing sources block and forwarded to the system timing block and the station clock output timing block. The possible values are:

<table>
<thead>
<tr>
<th>Signal Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Connected</td>
<td>No reference is assigned to the timing source.</td>
</tr>
<tr>
<td>Failed</td>
<td>A timing link fail is declared for the assigned timing link.</td>
</tr>
<tr>
<td>Wait to Restore</td>
<td>The assigned reference signal will be available again when the Wait to Restore timer has expired.</td>
</tr>
<tr>
<td>Normal</td>
<td>The logical timing source is assigned to a valid timing reference.</td>
</tr>
</tbody>
</table>

Switch request

Switch requests are shown in the table in order of priority, together with their description.

<table>
<thead>
<tr>
<th>Switch Request</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Request</td>
<td>This is the default value. The system timing is operating under normal conditions.</td>
</tr>
<tr>
<td>Clear Switch</td>
<td>Replaces the status by the normal status (in case of a previous switch).</td>
</tr>
<tr>
<td>Forced Switch</td>
<td>Unconditional switch, issued by the user, even if it is service degrading.</td>
</tr>
<tr>
<td>Manual Switch</td>
<td>A conditional switch, which is issued by the user. The switch will not be performed if it is service degrading. If $QL=Enabled$, the switch will not be performed if it is service degrading. If $QL=Disabled$, the switch will be performed even if it is service degrading.</td>
</tr>
</tbody>
</table>

Switch status

This parameter indicates the latest switch request. When no protection reference is provisioned, this parameter is not available. The possible values of this parameter are listed in the table below:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Request</td>
<td>No switch request has been issued.</td>
</tr>
</tbody>
</table>
### Value Description

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear</td>
<td>The former switch request is cleared. Switching will be system controlled after this request.</td>
</tr>
<tr>
<td>Forced Switch</td>
<td>A forced switch has been made to a timing source as indicated by the user.</td>
</tr>
<tr>
<td>Manual Switch</td>
<td>A manual switch has been made to a timing source as indicated by the user.</td>
</tr>
</tbody>
</table>

### System QL

This parameter shows the quality level value of the timing signal used to clock the system. Possible values are the quality levels as described in the section “Timing Concepts”.

### Timing mode

This parameter is used to set one of the three timing modes: *Locked*, *Holdover*, and *Free Running*. The nature of the modes is discussed in the Section Concepts

### Timing

If, while operating in the *Locked* mode, the incoming reference becomes unacceptable, the timing mode selector switches to *Holdover*. This is reflected in the *Timing* parameter. When the system stays in the *Locked* mode, the timing status remains *Normal*.

In the *Free Running* mode, the *Timing* parameter always reflects *Normal*. 
Provisioning station clock output

When to use

The purpose of this procedure is to specify the timing source to be used as a reference for the station clock output signals.

The procedure must be executed when:
- A timing reference needs to be provided to external “in station” equipment.
- A regenerator loop is needed.

Related information

Related procedures are:
- “Provisioning timing sources” (p. 7-20)
- “Provisioning system timing” (p. 7-32)
- “Provisioning output port timing” (p. 7-47)

Parameters used in this procedure can be found at “Parameters for provisioning station clock output” (p. 7-43).

Before you begin

Before starting this procedure, make sure that:
- The "Provision Timing Sources" procedure is completed
- The network timing plan is available

Set priority and lock out

To set the priority or the lockout for a timing source follow this procedure:

   
   **Result:** The Provisioned NE Station Clock Output Timing Information window appears.

2. Select a source to edit from the list and click **Edit** in the Station Clock Output Timing Sources field.
   
   **Result:** The Edit Automatic Selection Criterions for NE STCLK Output Timing window appears.

3. Set Priority or Lock Out Request.
Important! Setting the priorities has only effect if Source Selection is set to Independent. This can be done in the procedure "Switch Active Timing Source". Make sure not to use the same priority value for multiple timing sources, unless explicitly required by the timing plan.

4 Click **OK** to confirm the current settings.

**Result:** The *Edit Automatic Selection Criterions for NE STCLK Output Timing* window disappears.

5 To provision another Timing Source go to step 2, otherwise go to step 6.

6 Click **Close**

**Result:** The *Provisioned NE Station Clock Output Timing Information* window disappears.

**END OF STEPS**

### Switch active timing source

To switch the timing source that is used as the active timing source for station clock output timing, follow this procedure:

1 Select **Provisioning --> Timing --> Output Timing**.

**Result:** The *Provisioned NE Station Clock Output Timing Information* window appears.

2 Click **Switch** in the *Active Timing Source* field.

**Result:** The *Switch Request and Source Selection* window appears.

3 Select a request from the *Request* list. If a manual switch or a forced switch is required, select also a timing source to switch to from the *Timing Source* list.

**Important!** A switch request can only be made if the *Source Selection* is set to Independent.

4 Click **OK** to confirm the current settings and send the request to the network element.
Result: Depending on the System state and the request, the switch will be automatically successful or an error message will be displayed. The Switch Request and Source Selection disappears.

5 Click **Close**

Result: The Provisioned NE System Timing Information window disappears.

---

**Set station clock output values**

To enable the use of the Station Clock Output, follow this procedure:

1 Select *Provisioning --> Timing --> Output Timing.*

Result: The Provisioned NE Station Clock Output Timing Information window appears.

2 Click **Edit** in the Output Values field.

Result: The Edit Station Clock Output Values window appears.

3 Select Enabled to enable the use of the station clock output, or select Disabled to disable the use of the station clock output.

**Important!** The 1643 AM or 1643 AMS supports only the 2 MHz station clock output. Other options are greyed out.

4 Click **OK** to confirm the current settings and send the request to the network element.

Result: The Edit Station Clock Output Values disappears.

5 Click **Close**

Result: The Provisioned NE Station Clock Output Timing Information window disappears.

---

END OF STEPS
Edit acceptance QL

When the quality level of the signal for the station clock output falls below the *Acceptance QL*, the station clock output is squelched. To set the *Acceptance QL* follow this procedure:

1. Select **Provisioning --> Timing --> Output Timing**.
   
   **Result:** The **Provisioned NE Station Clock Output Timing Information** window appears.

2. Click **Edit** in the *Acceptance QL* field.
   
   **Result:** The **Edit Acceptance QL for NE STCLK Output Timing** window appears.

3. Select the *Acceptance QL*.

4. Click **OK** to confirm the current settings and send the setting to the network element.
   
   **Result:** The **Edit Acceptance QL for NE STCLK Output Timing** window disappears.

5. Click **Close**
   
   **Result:** The **Provisioned NE Station Clock Output Timing Information** window disappears.

---

**END OF STEPS**
Parameters for provisioning station clock output

Introduction

The station clock output functional block in the network element is responsible for selecting the timing source for the station clock output.

The different parameters in the station clock output timing block are indicated graphically in the figure below.

Functional diagram

A functional diagram of the station clock output functionality

[Diagram showing the functional block diagram with various inputs and outputs, including System Timing, Switch Request, Lockout Request, Priority, Timing Source Selection, STCLK Output, Signal Type, Acceptance QL, Output State, Reports, Switch Status, Output QL, and Locked out.]
Acceptance QL

The user can provision an Acceptance QL, applicable to all station clock output ports (if more than one). This quality level is the minimal quality level value that is accepted by the station clock output process. If the quality level of the signal for the station clock output falls below the Acceptance QL, the network element “squelches” the station clock output signal.

Active system timing source

The Active System Timing Source indicates the timing source currently used to synchronize the system, together with the Switch Status of the source and the latest issued Switch Request.

Lock out

The user can disable a specific timing source that enters the timing source selection without changing the priority settings. If a timing source is locked out, it will not take part in the timing source selection.

Whether a timing source is locked out is indicated by the Lockout parameter. The possible values for the Lockout parameter are: Yes and No.

Lock out request

The Lock out state can be changed with the Lock Out Request parameter. This can be set to Yes or No.

The Lock Out Request is for maintenance purposes. A Timing Source, which has a priority value assigned to it, can be temporarily locked out. When the Timing Source is already disabled, a Lock Out Request is rejected. A Lockout Request is set to No automatically when the Timing Source is disabled.

When Priority = Disabled the Lock Out Request field is greyed out.

Important! When a timing source is locked out, the network element is in the Abnormal State.

Output state

The user can view the Output State of the signal generated by the station clock output(s). Possible values are Normal, Disabled, and Unacceptable.

- Normal: indicates that the output is not disabled and has a quality level equal to or above the Acceptance QL
- Disabled: indicates that the station clock output is disabled
- Unacceptable: indicates a quality level below the Acceptance QL, or a signal status is failed.
Priority

The priority can be set for each timing source. For a network element with N timing sources provisioned, the priority can have values from 1 to N.

The *Priority* parameter can also have the value *Disabled*. A disabled timing source will not be taken into account in the Timing Source Selection for the system timing.

**Important!** Make sure not to provision identical Priority values to multiple timing sources.

Signal type

The *Signal Type* for the station clock outputs is always 2 MHz.

Source selection

The station clock output timing can be derived from one of the system clock processes or from the independent station clock output timing *Source Reference Selector*. This is provisioned by the user. Two options are available:

- *System Timing*
- *Independent Station Clock Timing*.

STCLK output

The user can enable or disable the *Station Clock Output*. If it is disabled it forwards no signal at all and cannot be used.

Switch request

Switch requests are shown in the table in order of priority, together with their description.

<table>
<thead>
<tr>
<th>Switch Request</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Request</td>
<td>This is the default value. The system timing is operating under normal conditions.</td>
</tr>
<tr>
<td>Clear Switch</td>
<td>Replaces the status by the normal status (in case of a previous switch).</td>
</tr>
<tr>
<td>Forced Switch</td>
<td>Unconditional switch, issued by the user, even if it is service degrading.</td>
</tr>
<tr>
<td>Manual Switch</td>
<td>A conditional switch, which is issued by the user. The switch will not be performed if it is service degrading.</td>
</tr>
<tr>
<td></td>
<td>If $QL=Enabled$, the switch will not be performed if it is service degrading.</td>
</tr>
<tr>
<td></td>
<td>If $QL=Disabled$, the switch will be performed even if it is service degrading.</td>
</tr>
</tbody>
</table>
Switch status

This parameter indicates the latest switch request. When no protection reference is provisioned, this parameter is not available. The possible values of this parameter are listed in the table below:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Request</td>
<td>No switch request has been issued.</td>
</tr>
<tr>
<td>Clear</td>
<td>The former switch request is cleared. Switching will be system controlled after this request.</td>
</tr>
<tr>
<td>Forced Switch</td>
<td>A forced switch has been made to a timing source as indicated by the user.</td>
</tr>
<tr>
<td>Manual Switch</td>
<td>A manual switch has been made to a timing source as indicated by the user.</td>
</tr>
</tbody>
</table>
Provisioning output port timing

The purpose of output port timing provisioning is to provision the timing properties for the 1.5 Mbit/s, 2 Mbit/s, and X.21 output ports and the station clock output ports.

When to use

If a 1.5 Mbit/s, 2 Mbit/s or X.21 tributary port has to be used as a timing reference for other equipment. This can be done for both SDH and non-SDH equipment.

Related information

Related procedures are:

- Port Provisioning
- “Provisioning station clock output” (p. 7-39)

Parameters used in this procedure can be found at “Parameters for provisioning output port timing” (p. 7-50).

Before you begin

Pay attention to the following:

- Use of retiming on the 1.5 Mbit/s or 2 Mbit/s tributary ports can affect the data integrity of the signal.
- When quality level information must be sent out on the 2 Mbit/s station clock output ports the Signal Type must be 2 Mbit/s framed.
- The provisioned Signal Type for the station clock output is the same for both station clock output ports.

Provision 1.5 Mbit/s, 2 Mbit/s, or X.21 Output Port Timing

The following procedure is applicable to set the timing parameters for the physical 1.5 Mbit/s, 2 Mbit/s, or X.21 output ports. Since the windows for the different tributaries are the same, < XXX> is used for the different tributaries, instead of repeating the window names for either 1.5 Mbit/s, 2 Mbit/s, or X.21 ports.

1. Select Provisioning --> Transport --> Ports.

   **Result:** The Provisioned NE Port Filter window appears.

2. Select All Ports.
**Provision STM-N Output Port Timing**

To set the parameters for the physical STM-N output ports follow this procedure:

1. Select *Provisioning --> Transport --> Ports.*
Result: The Provisioned NE Port Information List window appears.

2 Select an STM-N port from this list and click Timing.

Result: The Port Timing Information window appears.

3 Click Edit.

Result: The Edit Port Timing Information window appears.

4 Set the Force DNU value.

5 Click OK to confirm the current settings.

Result: Depending on the chosen values a warning message can appear. The Edit Port Timing Information window disappears.

6 Click OK.

Result: The Port Timing Information window disappears.

7 To set another STM-N port go to step 2, else go to step 9.

8 Click Close.

Result: The Provisioned NE Port Information List window disappears.

END OF STEPS
Parameters for provisioning output port timing

Introduction

The 1.5 Mbit/s, 2 Mbit/s and X.21 transmission ports are managed by a number of parameters, which are related to timing. These parameters are shown in the functional diagram below.

Functional diagram

The functional diagram of the Output Port Timing functionality

Acceptance QL

For each individual 1.5 Mbit/s, 2 Mbit/s, or X.21 tributary output port in the Re-Timed mode, an Acceptance QL can be provisioned.

If the System QL (in case of system timing) or the QL-out (in case of independent timing) falls below the Acceptance QL, the timing will go into the Fallback mode.
### Fallback mode

If a 1.5 Mbit/s, 2 Mbit/s, or X.21 port is operating in the Re-timed mode and if the QL Mode is enabled, the output is automatically switched to the provisioned Fallback mode, if the quality level of the system timing drops below the Acceptance QL.

The three Fallback modes are:
- **Re-timed AIS**: A Re-timed AIS is sent out.
- **Self-timed**: The signal is sent out, from the port in the Self-timed mode.
- **None**: No Fallback applies.

### Force DNU

*Force DNU* allows to force an S1 byte value: DNU into an outgoing signal. The Force DNU option can be switched on by selecting *Force*. It can be switched off by selecting *Do Not Force*.

**Important!** When an outgoing signal is forced to carry DNU, this signal cannot be used for synchronization by another network element.

### Outgoing QL

*Outgoing QL* indicates the quality level that is sent out on a given transmission output port which supports S1-byte quality level information carriage.

### SSM out

*SSM Out* displays the quality level corresponding to the current S1-byte value that is sent out from the selected port.

### Timing mode

The timing mode of each individual 1.5 Mbit/s, 2 Mbit/s, and X.21 tributary output port can be set to the Self-Timed or Re-Timed mode:
- In the Self-Timed mode the 2 Mbit/s signal is extracted from the container contents of the VC-12.
- In the Re-Timed mode, the timing of the 2 Mbit/s output signal is derived from the network element system timing; the 2 Mbit/s signal is routed through the elastic buffer.

If the ISDN mode of a 2 Mbit/s ISDN port is set to Leased Line (LL), the default value of the Timing Mode parameter will be Re-Timed.

For more information see the section "Timing Concepts".
Timing alarm reporting

When the Timing State of a 1.5 Mbit/s, 2 Mbit/s, or X.21 tributary output port is Fallback, a defect is declared. The reporting of this Timing Alarm can be Enabled or Disabled for each individual 2 Mbit/s tributary output port. This is done with the Timing Alarm Reporting parameter.

(Port) timing state

The (Port) Timing State of each individual 1.5 Mbit/s, 2 Mbit/s, and X.21 tributary output port can be viewed. The (Port)Timing State can have two values:

- Normal: The port operates as specified in the timing mode
- Fallback: The timing mode has fallen back as specified in the Fallback Mode parameter.
8 Traffic provisioning

Overview

Purpose

Traffic Provisioning (or Transmission Provisioning) sets up the network elements to route the traffic through the network.

Objective

To create transmission paths through the network with or without protection. The protected transmission path can maintain the transmission signal in case of transmission failures.

Outcome

The outcome of traffic provisioning is:
• all traffic can be transported through the network according to the transmission plan
• if protection is used, the traffic that is routed through the network is protected against failures.

Protection types

The following Protection Types can be used:
• SNC: Sub Network Connection protection protects a specific transmission path in a ring.
• MSP: Multiplex Section Protection protects the transmission path in a point-to-point connection.

Intended use

This chapter describes setting up traffic on VC-4, VC-3 and/or VC-12 level in a network with 1643 AM or 1643 AMS network elements.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cross-connection management</strong></td>
<td>8-5</td>
</tr>
<tr>
<td>Transmission Plan</td>
<td>8-6</td>
</tr>
<tr>
<td>Cross Connections</td>
<td>8-8</td>
</tr>
<tr>
<td>VC-3 concatenation</td>
<td>8-10</td>
</tr>
<tr>
<td>VC-12 concatenation</td>
<td>8-11</td>
</tr>
<tr>
<td>SHDSL feature</td>
<td>8-12</td>
</tr>
<tr>
<td><strong>Path protection</strong></td>
<td>8-17</td>
</tr>
<tr>
<td>Sub-Network Connection Protection (SNCP)</td>
<td>8-18</td>
</tr>
<tr>
<td><strong>Line Protection</strong></td>
<td>8-20</td>
</tr>
<tr>
<td>Multiplexer Section Protection</td>
<td>8-21</td>
</tr>
<tr>
<td><strong>Ethernet concepts</strong></td>
<td>8-23</td>
</tr>
<tr>
<td>Ethernet over SDH</td>
<td>8-24</td>
</tr>
<tr>
<td>Virtual concatenation</td>
<td>8-41</td>
</tr>
<tr>
<td>Spanning tree protocol (STP)</td>
<td>8-47</td>
</tr>
<tr>
<td>GARP VLAN Registration Protocol (GVRP)</td>
<td>8-54</td>
</tr>
<tr>
<td>Ethernet over SDH applications</td>
<td>8-56</td>
</tr>
<tr>
<td>Operational modes</td>
<td>8-64</td>
</tr>
<tr>
<td>Tagging modes</td>
<td>8-75</td>
</tr>
<tr>
<td>Ethernet mapping schemes</td>
<td>8-81</td>
</tr>
<tr>
<td><strong>Ethernet engineering rules and guidelines</strong></td>
<td>8-83</td>
</tr>
<tr>
<td>Port provisioning</td>
<td>8-84</td>
</tr>
<tr>
<td>Quality of Service (QoS) overview</td>
<td>8-90</td>
</tr>
<tr>
<td>Classification, queueing, and scheduling</td>
<td>8-94</td>
</tr>
<tr>
<td>Quality of Service provisioning</td>
<td>8-103</td>
</tr>
<tr>
<td>Performance monitoring</td>
<td>8-105</td>
</tr>
<tr>
<td><strong>Provision Ethernet over SDH</strong></td>
<td>8-106</td>
</tr>
<tr>
<td>Provisioning Ethernet services</td>
<td>8-107</td>
</tr>
<tr>
<td>Parameters of the window “View SDH Channel / VCG Information”</td>
<td>8-112</td>
</tr>
<tr>
<td>Provisioning a virtual switch in repeater (promiscuous) mode</td>
<td>8-113</td>
</tr>
<tr>
<td>Provisioning a virtual switch in LAN interconnect mode</td>
<td>8-116</td>
</tr>
<tr>
<td>Provisioning a virtual switch in MLAN (VPN) mode</td>
<td>8-119</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Provisioning a virtual switch in MLAN (VPN) mode with QoS</td>
<td>8-123</td>
</tr>
<tr>
<td>Provisioning a virtual switch in spanning tree mode</td>
<td>8-132</td>
</tr>
<tr>
<td>Parameters for provisioning a LAN unit in repeater mode</td>
<td>8-143</td>
</tr>
<tr>
<td>Parameters for provisioning LAN unit in spanning tree mode</td>
<td>8-147</td>
</tr>
<tr>
<td><strong>Provision MAC address tables</strong></td>
<td>8-153</td>
</tr>
<tr>
<td>Provision static MAC address table</td>
<td>8-154</td>
</tr>
<tr>
<td>Provision the MAC address learning mode</td>
<td>8-157</td>
</tr>
<tr>
<td>Provision the MAC address aging pass timer</td>
<td>8-159</td>
</tr>
<tr>
<td><strong>Provision Quality of Service (QoS)</strong></td>
<td>8-160</td>
</tr>
<tr>
<td>Provision the QoS profile definitions</td>
<td>8-161</td>
</tr>
<tr>
<td>Parameters for provisioning a QoS profile</td>
<td>8-162</td>
</tr>
<tr>
<td>View QoS profile information</td>
<td>8-165</td>
</tr>
<tr>
<td>View the details of a LAN/WAN port QoS parameters</td>
<td>8-166</td>
</tr>
<tr>
<td>Edit QoS mode</td>
<td>8-167</td>
</tr>
<tr>
<td>Provision QoS Flow Identification Table</td>
<td>8-169</td>
</tr>
<tr>
<td>Parameters for provisioning Flow Identification Tables</td>
<td>8-172</td>
</tr>
<tr>
<td>Edit the QoS egress details</td>
<td>8-177</td>
</tr>
<tr>
<td>Ingress rate control</td>
<td>8-178</td>
</tr>
<tr>
<td><strong>Provision cross connections without protection</strong></td>
<td>8-179</td>
</tr>
<tr>
<td>Creating cross connections without protection</td>
<td>8-180</td>
</tr>
<tr>
<td>Deleting cross connections</td>
<td>8-182</td>
</tr>
<tr>
<td>Parameters for provisioning cross connections without protection</td>
<td>8-183</td>
</tr>
<tr>
<td><strong>Provision cross connections with SNC protection</strong></td>
<td>8-184</td>
</tr>
<tr>
<td>Add SNC/N protection to an unprotected cross-connection</td>
<td>8-185</td>
</tr>
<tr>
<td>Remove protection from an SNC/N protected cross-connection</td>
<td>8-187</td>
</tr>
<tr>
<td>Delete an existing cross-connection</td>
<td>8-189</td>
</tr>
<tr>
<td>Parameters for provisioning a cross-connection with SNC protection</td>
<td>8-191</td>
</tr>
<tr>
<td><strong>View or Edit the LTU information</strong></td>
<td>8-192</td>
</tr>
<tr>
<td>View the LTU information</td>
<td>8-193</td>
</tr>
<tr>
<td>Edit the LTU Information</td>
<td>8-194</td>
</tr>
<tr>
<td>Parameters for viewing or editing LTU information</td>
<td>8-195</td>
</tr>
<tr>
<td><strong>View or Edit the SHDSL connection information</strong></td>
<td>8-196</td>
</tr>
<tr>
<td>View the SHDSL connections</td>
<td>8-197</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>-------</td>
<td>------</td>
</tr>
<tr>
<td>Update the SHDSL connection list</td>
<td>8-198</td>
</tr>
<tr>
<td>Details of the SHDSL Connection List</td>
<td>8-199</td>
</tr>
<tr>
<td>Parameters for viewing or editing the SHDSL connections list</td>
<td>8-200</td>
</tr>
<tr>
<td><strong>View or Edit the NTU information</strong></td>
<td><strong>8-201</strong></td>
</tr>
<tr>
<td>Update the NTU information</td>
<td>8-202</td>
</tr>
<tr>
<td>View the NTU information</td>
<td>8-203</td>
</tr>
<tr>
<td>Edit the NTU information</td>
<td>8-204</td>
</tr>
<tr>
<td>View or Edit NTU's General Configuration</td>
<td>8-205</td>
</tr>
<tr>
<td>Remote SHDSL Power Supply (RPS)</td>
<td>8-207</td>
</tr>
<tr>
<td>VC 12 termination point information</td>
<td>8-208</td>
</tr>
<tr>
<td>Update the VC 12 termination point information window</td>
<td>8-209</td>
</tr>
<tr>
<td>Report the VC 12 termination point information list</td>
<td>8-210</td>
</tr>
<tr>
<td>Edit the VC 12 termination point information list</td>
<td>8-211</td>
</tr>
<tr>
<td>Parameters for viewing or editing NTU information and VC 12 termination point information</td>
<td>8-213</td>
</tr>
<tr>
<td>Provisioning the SHDSL on the NT10ETH modem</td>
<td>8-215</td>
</tr>
<tr>
<td><strong>View SNC protection</strong></td>
<td><strong>8-216</strong></td>
</tr>
<tr>
<td>Viewing SNC protection</td>
<td>8-217</td>
</tr>
<tr>
<td>Parameters for viewing SNC protection</td>
<td>8-218</td>
</tr>
<tr>
<td><strong>Edit SNC protection</strong></td>
<td><strong>8-219</strong></td>
</tr>
<tr>
<td>Editing a SNC protection</td>
<td>8-220</td>
</tr>
<tr>
<td>Parameters for editing SNC protection</td>
<td>8-221</td>
</tr>
<tr>
<td><strong>View MSP protection</strong></td>
<td><strong>8-222</strong></td>
</tr>
<tr>
<td>Viewing MSP protection</td>
<td>8-223</td>
</tr>
<tr>
<td>Parameters for viewing MSP protection</td>
<td>8-224</td>
</tr>
<tr>
<td><strong>Edit MSP protection</strong></td>
<td><strong>8-225</strong></td>
</tr>
<tr>
<td>Editing MSP protection</td>
<td>8-226</td>
</tr>
<tr>
<td>Parameters for editing MSP protection</td>
<td>8-228</td>
</tr>
<tr>
<td><strong>Add MSP protection</strong></td>
<td><strong>8-230</strong></td>
</tr>
<tr>
<td>Adding MSP protection</td>
<td>8-231</td>
</tr>
<tr>
<td>Parameters for adding MSP protection</td>
<td>8-233</td>
</tr>
</tbody>
</table>
Cross-connection management

Overview

Purpose

The following section illustrates the cross-connection management of 1643 AM.

Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmission Plan</td>
<td>8-6</td>
</tr>
<tr>
<td>Cross Connections</td>
<td>8-8</td>
</tr>
<tr>
<td>VC-3 concatenation</td>
<td>8-10</td>
</tr>
<tr>
<td>VC-12 concatenation</td>
<td>8-11</td>
</tr>
<tr>
<td>SHDSL feature</td>
<td>8-12</td>
</tr>
</tbody>
</table>
Transmission Plan

Introduction

A network element can be an Add Drop Multiplexer (ADM) or a Terminal Multiplexer (TM). An ADM can be part of a ring, a TM is part of a point to point connection. The transmission plan shows an overview of the network and the traffic. To provide traffic in the network, cross connections are made in each separate network element.

Design Transmission Plan

Transmission provisioning is based on a transmission plan, which must be available when the separate network elements are configured. The transmission plan shows:

- the parameters needed for making the cross connections
- which ports are terminating ports

The following hints can be used to set up a transmission plan:

- Make a drawing of the current network configuration (for example a ring) in which to provision a transmission path. It is important to make clear in this drawing how the network elements are connected to each other.

Example: LB-side of network element A connected to LA-side of network element B.
• Identify path channels within the line connections between network elements: first check which channels are available.

Example: Between network elements A and B: #1.153, between network elements B and C: #1.111 etc. (#1 is AU-4 number 1). A ring with 1643 AM or 1643 AMS network elements is only possible on STM-1 level, therefore only #1 is available

• Identify network elements in which add-drop cross connections should be established. These are the terminating network elements of the transmission path.

• Identify terminating ports. First check which ports are available.

Example: TP2.1 in network element A and TP1.2 in network element D.

• Identify the network elements in which through connections should be established (in between terminating network elements).

Example: network element C.

LA: Line Port A  LB: Line Port B
Cross Connections

A cross-connection is made to create a path from one point to another point in the network. A transmission plan is made to provision paths in a network and according to this plan cross connections can be made in each network element involved in the path.

The Cross Connect Unit connects the signals at VC-4, VC-3, or VC-12 level between the termination points of the line ports or tributary ports.

Cross connect units

The 1643 AM or 1643 AMS network element is an Add Drop Multiplexer. Cross connections can be made between the two line ports and between a line port and a tributary port. It is also possible to make a cross-connection with SNC/N protection.

Diagram

The following diagrams show the transmission architecture for the 1643 AM or 1643 AMS network element for STM-1 interfaces. The 1643 AM or 1643 AMS network element supports STM-4 interfaces as well.
Connection points

A cross-connection is made between termination points (TP). On the tributary units a VC-12 termination point is selected. On the line units, the TU number inside the VC-4 must be selected. The TU number consists of three numbers:

- k: the number of the TUG-3 inside the VC-4
- l: the number of the TUG-2 inside the TUG-3
- m: the TU-12 number inside the TUG-2.

Example:

```
TP1.1,1.112
```

The following table shows the names of the termination points.

<table>
<thead>
<tr>
<th>Unit</th>
<th>TP Type</th>
<th>TP name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line 1 and Line 2 (STM-1 or STM-4)</td>
<td>TU-12/TU-3</td>
<td>LP1.1,1.[klm] and LP2.1,1.[klm]</td>
</tr>
<tr>
<td>Tributary 1 (2 Mbit/s)</td>
<td>VC-12</td>
<td>TP1.1 — TP1.16</td>
</tr>
<tr>
<td>Tributary 2 (1.5 Mbit/s)</td>
<td>VC-11</td>
<td>TP2.1 — TP2.16</td>
</tr>
<tr>
<td>Tributary 2 (2 Mbit/s)</td>
<td>VC-12</td>
<td>TP2.1 — TP2.16</td>
</tr>
<tr>
<td>Tributary 2 (34/45 Mbit/s)</td>
<td>VC-3</td>
<td>TP2.1 — TP2.2</td>
</tr>
<tr>
<td>Tributary 2 (X.21)</td>
<td>VC-12</td>
<td>TP2.1 ... TP2.4</td>
</tr>
<tr>
<td>Tributary 2 (Ethernet)</td>
<td>VC-12/VC3</td>
<td>LAN2.1 ... LAN2.4</td>
</tr>
<tr>
<td>Tributary 2 (STM-1)</td>
<td>VC-4</td>
<td>TP2.1 — TP2.2</td>
</tr>
</tbody>
</table>

Alarms

The cross connections can only be created at one network element at the same time. If the termination points are monitored this will cause the following alarms: VC-4/VC3/VC12 unequipped and TU3/TU12 Loss Of Pointer. Therefore first provision the complete transmission path and then set the ports and termination points to monitored.
VC-3 concatenation

Introduction

The concatenation of two VC-3s provides a mechanism to transport payloads greater than the capacity of a single VC-3, for example to transport Ethernet data in SDH networks. This feature is for the LAN tributary only.

A concatenated VC-3 group is indicated as VC-3-2v. V means virtual concatenation.

Virtual concatenation

Virtual concatenation allows the transport of a single VC-3-2v structure in two individual TU-3 without the use of any concatenation indication in the pointer bytes (which is the case for contiguous concatenation). It only requires the path termination function to provide concatenation functionality, hence guaranteeing interworking with other standard low order connection functions.

Termination

VC-3 concatenation is only supported without termination. This means that only VC-3 level cross connections can be made.

A VC-3-2v signal is handled like two individual VC-3 signals. The same alarms and performance values are supported as for VC-3. The result of the VC-3-2v supervision is copied into the two VC-3s.

- An alarm in an VC-3-2v group is displayed as one alarm for the entire group.
- Two VC-3s can have different path and path trace.
VC-12 concatenation

Introduction

The concatenation of two VC-12s provides a mechanism to transport payloads greater than the capacity of a single VC-12, for example to transport Ethernet data in SDH networks. This feature is for the LAN tributary only.

A concatenated VC-12 group is indicated as VC-12-Xv. V means virtual concatenation X can be 2,3,4,5.

Virtual concatenation

Virtual concatenation allows the transport of a single VC-12-xv structure in x individual TU-12 without the use of any concatenation indication in the pointer bytes (which is the case for contiguous concatenation). It only requires the path termination function to provide concatenation functionality, hence guaranteeing interworking with other standard low order connection functions.

Termination

VC-12 concatenation is only supported without termination. This means that only VC-12 level cross connections can be made.

A VC-12-xv signal is handled like X individual VC-12 signals. The same alarms and performance values are supported as for VC-12. The result of the VC-12-xv supervision is copied into the X VC-12s.

- An alarm in an VC-12-xv group is displayed as one alarm for the entire group.
- X VC-12s can have different path and path trace.
**SHDSL feature**

**SHDSL option card**

The SHDSL feature is used to transport 2 Mbit/s signals over copper lines in cases where no fiber is available for transportation.

This option card can be used for the following applications:
- to connect UMTS base stations to the SDH network when only copper lines are available
- to deliver ISDN PRI to customers over copper lines.

In the first application an n* 2 M bit/s connection to a UMTS base station is provided over copper pairs (max. 3.5 km). In the base station, the termination of the SHDSL signal (the NTU function) can be done by off-the-shelf modems. It is expected that each UMTS service provider is expected will need four 2 M bit/s links; a base station will be used by at most three providers. Another application consists of the delivery of an ISDN 2 Mbit service over SHDSL.

The following figure shows an application with UMTS base station and NTU modems

The WaveStar® ITM-SC supports this option board on the 1643 AM or 1643 AMS.

The SHDSL option board can be added to the 1643 AM or 1643 AMS to provide capabilities in addition to those that are provided by the main board: the option board provides 12 Symmetrical single-pair high-bitrate Digital-Subscriber Line (SHDSL) interfaces.

The SHDSL option card supports outloop loopbacks on all ports.
Applications

There are two application possibilities for the SHDSL feature:

- End-user access for E1 via an E1 NTU (NT2M modem)
- End-user access for Ethernet using a 10Base-T or a 100-Base-TX interface via an Ethernet NTU (NT10ETH modem). Each NT10ETH modem has 1 or 2 Ethernet ports towards the end-user

The 1643 AM and 1643 AMS has to be equipped with an X12SHDSL-V2/V3 option card and is then operating as LTU (Line Termination unit). All ports of the X12SHDSL-V2/V3 option card operate either in the E1/SHDSL mode or in the TU12/SHDSL mode.

An E1 modem provides one E1 user interface and one single SHDSL link. This means a one-to-one correspondence between an LTU SHDSL port, the NT2M, and the E1 end-user interface.

An NT10ETH modem has two 10/100BASE-T(X) interfaces and can have one to four parallel SHDSL links, that are all connected to the same X12SHDSL-V2/V3 option card.

Each SHDSL link can have up to two SHDSL Regenerator Units (SRUs) depending on the span connected to the LTU port. Each SRU supports one SHDSL link.

Remote management of SHDSL devices

The LTU maintains an information database of all attached NTUs and SRUs for the purpose of configuration, performance, and fault information retrieval or control by network management. All elements attached to an SHDSL span have to respond to queries made to them from other elements. The database in the LTU is considered the “master database”. Conflicts between the entities in the SHDSL span are resolved in favour of the LTU. For 1643 AM and 1643 AMS only communication initiated by the LTU is supported.

The alarm status of the SHDSL devices (NTU and SRUs) that are attached to an SHDSL port on the LTU is polled by the LTU in regular intervals. Polling is realized by means of EOC messages or by a combination of EOC and EOC-ext. messages.
The following sections describe Ethernet NTU support features for SHDSL configurations.

NTUs Bridge Mode Provisioning

The 1643 AM/AMS supports bridge mode provisioning to the Ethernet NTU.

The following bridge modes are supported. They are:

- Self learning bridge (IEEE 802.1D)
- V-LAN bridge (IEEE 802.1Q)
- Provider bridge (IEEE 802.1ad)

NTU V-LAN functionality (Bridge Mode) Support

The 1643 AM/AMS provides enhanced PM support for third party NTUs. It supports a two port Ethernet SHDSL modem (NTU) which is connected via 1 to 4 parallel TU-12s over SHDSL mapped links. The Enhanced NTU ETH LAN port PM counters are available via the QD2-Lite extension. The Ethernet traffic bandwidth is optimized by GFP-F encapsulation and VC-12-Xv virtual concatenation using LCAS.

When an NTU works in V-LAN bridge mode (IEEE802.1Q), the NTU's V-LAN table is used to assign the VID to ETH ports and WAN ports. The QD2-Lite message is only used to write to the table; a readout of the existing entries is not provided. The network element is the configuration master and retains a V-LAN table of its own. It ensures by corresponding commands that the V-LAN table in the NTU matches the V-LAN table in the AM.

Using the V-LAN Entry command, individual entries in the table can be added, modified or deleted. This command is used when individual V-LAN entries are changed by the EMS.

A table entry for a VID is deleted by a V-LAN Table Entry command in which all WAN(x) bits and LAN(x) bits are set to "0". The V-LAN Table command can be used to copy the entire V-LAN table from the AM to the NT10ETH. The entire V-LAN table is deleted by an "empty" V-LAN Table command that contains no table entry. The length of such a message is L=2.

After the restoration of an SDSL link, the NE (AM) must refresh the entire V-LAN table with the V-LAN Table command. Refreshing the V-LAN table with the V-LAN Table command is not allowed to result in the interruption of individual or of all V-LANs.

NTU LPT functionality Support

The 1643 AM/AMS supports Link Pass Through (LPT) functionality via EOC commands.
Users can enable or disable LPT using the following parameters.

- CA-CSF: GFP Client Signal Fail Signalling
- CA-SSF: Disabling LAN interfaces during WAN connection failure

**NTU Ethernet QoS support**

The 1643 AM/AMS provides enhanced PM support for third party NTUs. It supports a two port Ethernet SHDSL modem (NTU) which is connected via 1 to 4 parallel TU-12s over SHDSL mapped links. The Enhanced NTU ETH LAN port PM counters are available via the QD2-Lite extension. The Ethernet traffic bandwidth is optimized by GFP-F encapsulation and VC-12-Xv virtual concatenation using LCAS.

The 1643 AM/AMS supports the following NTU Ethernet QoS functions.

- PriorityMode
- IngressRateControl
- CIRAverageBitRate
- CIRMaxBurstSize
- PortPriority

**NTU web interface**

The NMS of the 1643 AM/AMS can be used to set user passwords for the NTU web interface.

**NTU general configuration support**

The 1643 AM/AMS provides enhanced PM support for third party NTUs. It supports a two port Ethernet SHDSL modem (NTU) which is connected via 1 to 4 parallel TU-12s over SHDSL mapped links. The Enhanced NTU ETH LAN port PM counters are available via the QD2-Lite extension. The Ethernet traffic bandwidth is optimized by GFP-F encapsulation and VC-12-Xv virtual concatenation using LCAS.

The 1643 AM/AMS supports the following enhanced NTU configuration.

1. Enhanced NTU SDH port configuration
2. Enhanced NTU Ethernet port configuration
3. Enhanced NTU Ethernet WAN port configuration
4. NTU Ethernet Bridging Configuration

**NTU General Alarms and Status Report**

The 1643 AM/AMS provides enhanced PM support for third party NTUs. It supports a two port Ethernet SHDSL modem (NTU) which is connected via 1 to 4 parallel TU-12s over SHDSL mapped links. The Enhanced NTU ETH LAN port PM counters are available via the QD2-Lite extension. The Ethernet traffic bandwidth is optimized by GFP-F encapsulation and VC-12-Xv virtual concatenation using LCAS.
The 1643 AM/AMS supports the following enhanced NTU alarms and status reports.

- SDH port status
- Ethernet port status
- Updated Encaps and VCG status: TLCR, PLCR, FOPR, TLCT, PLCT, FOPT, LOA

**Remote SHDSL Power Supply (RPS) Support**

The 1643 AM/AMS manages an external Remote SHDSL Power Supply (RPS) box via the MDI/MDO interfaces. Note that remote power supply must be set to 'managed mode' by the DIP switch=ON in the power box.

The 1643 AM management system can also be set to 'managed mode' for the remote power supply.

The 1643 AM/AMS supports the following remote power supply provisioning functions.

- **Restart_cmd**: Restarts the RPS module after forced shutdown
- Enable/Disable RPS related alarms (per port and not per alarm). This provisioning is used to suppress alarms generated by the RPS module.

The 1643 AM/AMS remote power supply module supports the following alarms.

- RPS power failure (per box)
- Overl: Overload (per port)
- OpenC: Open circuit (per port)
- FSD: Forced shut down (per port)
- Leak: Leakage asymmetrical (per port)
- HVolt: Overvoltage alarm (per port)

Note that the MDI interfaces 1...4 and MDO interfaces 1...4 will not function as normal when the RPS is set to managed mode.
Path protection

Overview

Purpose

The principle of a path protection is based on the duplication of the signals to be transmitted and the selection of the best signal available at the path connection termination. The two (identical) signals are routed over two different path segments, one of which is defined as the main path and the other as standby path. The same applies to the opposite direction. The system only switches to the standby path if the main path is faulty.

Contents

| Sub-Network Connection Protection (SNCP) | 8-18 |
Sub-Network Connection Protection (SNCP)

Introduction

SubNetwork Connection (SNC) protection is used to protect the traffic for a pre-selected path (path protection). This type of path protection can be used for VC-4, VC-3 and VC-12 level.

SNC protection is characterized by sending the signal in both directions. When a fault condition occurs the receive NE switches to the protecting line. The capacity for protection cannot be used for any other traffic.

To be able to protect every provisioned path on an individual basis within a subnetwork.

A provisioned subnetwork containing individually paths that are 1+1 protected against service failures.

Principle

SubNetwork Connection (SNC) protection switching deals with protection against transmission failures in and between Ring Add/Drop NEs. One leg is selected as a designated worker and the other leg as a designated protecting. This means that the capacity is used for protection even if the normal route is available. A trail continues to use the working route until a fault condition occurs or an external switch request is issued to switch to the protecting route. This type of protection is non revertive. This means that when a traffic failure in the working route has been cleared, traffic will remain on the protection route until a manual or forced switch is applied, or when a failure occurs on the protection line. This behavior is irrespective of any service restoration in the working route.
SNC/N

Sub Network Connection Non-intrusive protection or SNC/N monitoring. The switching criteria for SNC/N are based on both signal failures and signal degrade. Signal failures that cause SNC/N protection switch are the same as for SNC/I: AIS (Alarm Indication Signal), UNEQ (unequipped VC), TIM (Trace Identifier Mismatch), TU-AIS and TU-LOP (Loss of Pointer). Signal degrades that cause SNC/N protection switching are based on the number of Errored Blocks detected during a certain period. The Threshold that defines when a signal is declared degraded can be set by the user.

SNC/I

Sub Network Connection Inherent protection or SNC/I monitoring. The switching criteria for SNC/I are based on signal failures.

Signal failures that cause SNC/I protection switch are:
- AIS (Alarm Indication Signal),
- UNEQ (unequipped VC),
- TIM (Trace Identifier Mismatch),
- TU-AIS
- TU-LOP (Trail Signal Failure, TSF).
Line Protection

Overview

Purpose

In line protection switching, the complete (physical) transmission path between two multiplexers is duplicated. This means that a separate Optical Interface Unit is connected in each multiplexer for the main (working) and standby (protection) section.

MSP

The SDH multiplex section protection scheme complies with the ITU-T G.841.

Contents

| Multiplexer Section Protection | 8-21 |
Multiplexer Section Protection

Multiplex Section Protection (MSP) is used to protect the traffic in a point-to-point connection. A requirement for this kind of protection is that the transmission units and lines are doubled.

Multiplex Section Protection is only applicable for 1643 AM or 1643 AMS network element configurations with STM-1 interfaces.

MSP provides the capability for switching the transmission path from the working section to the protection section in a point-to-point connection. The protection line cannot be used for carrying low priority traffic.

To protect a multiplexer section in a point-to-point connection.

A protection setting to protect the transmission path against transmission failures in a point-to-point connection (MS-AIS, LOF, MS-DEG) and port equipment failures.

Principle

In a point-to-point connection between network elements, protected by MSP, the lines and units must be doubled. One pair is selected as a designated worker and the other pair is designated protecting. The capacity in the protection or stand-by section must be reserved and is not available for traffic.

Simply put, the protection or stand-by section carries the same traffic as the worker section and it cannot be used for carrying any other kind of traffic.

A trail continues to use the working route until a fault condition occurs or an external switch request is issued to switch to the protecting route.

Example of MSP protection.

Revertive

In the case of failure when in the Revertive mode the traffic switches to the protecting line and switches back when the failure is solved.
Non-Revertive

In the Non-Revertive mode the traffic switches to the protecting line and remains on the protected line even when the failure is solved.

Uni-directional

In the case of failure in the Unidirectional mode only the receive side switches.

Bi-directional

In the case of failure in the Bidirectional mode both sides, the transmit and receive, are switched.
Ethernet concepts

Overview

Purpose

This section describes the 1643 AM Ethernet feature.

References

For more specific information refer to the TransLAN® Ethernet SDH Transport Solution Applications and Planning Guide.

The TransLAN® Ethernet SDH Transport Solution – Applications and Planning Guide presents a detailed overview of the TransLAN® Ethernet SDH Transport Solution, it describes its applications, gives planning information, engineering rules, and technical specifications. Additionally it provides some Ethernet background information.

The TransLAN® Ethernet SDH Transport Solution – Applications and Planning Guide can be ordered at or downloaded from the Customer Information Center (CIC) at http://www.cic.lucent.com/, or via your Local Customer Support.

Contents

| Ethernet over SDH                    | 8-24 |
| Virtual concatenation               | 8-41 |
| Spanning tree protocol (STP)        | 8-47 |
| GARP VLAN Registration Protocol (GVRP) | 8-54 |
| Ethernet over SDH applications      | 8-56 |
| Operational modes                  | 8-64 |
| Tagging modes                       | 8-75 |
| Ethernet mapping schemes           | 8-81 |
Ethernet over SDH

Introduction

To connect remote PC LAN network sites via an SDH network without the need for intermediate bridges or routers, the 1643 AM or 1643 AMS network element is equipped with the Ethernet Interface extension card.

The following figure visualizes the basic design of a TransLAN® card (for example, X4IP):

Legend:

A The external interfaces, to which the end-customer's Ethernet LANs are physically connected.
B The interface between the Ethernet physical interface port and the Ethernet switch. The internal interfaces of the Ethernet switch towards the Ethernet physical interface port are referred to as “LAN ports”. Note that two types of LAN ports can be differentiated according to their port role: “customer LAN ports” and “network LAN ports” (cf. “Port provisioning” (p. 8-84)).

C The internal interface between the Ethernet switch and the encapsulation and mapping function. The internal interfaces of the Ethernet switch towards the encapsulation and mapping function are referred to as “WAN ports”. Note that two types of WAN ports can be differentiated according to their port role: “network WAN ports” and “customer WAN ports” (cf. “Port provisioning” (p. 8-84)).

D The interface between the encapsulation and mapping function and the cross-connect function of the network element. This is where the virtually concatenated payload is cross-connected to be transported over the SDH network.

**X4IP-V2 option card (TransLAN®)**

The TransLAN® implementations use standardized protocols to transport Ethernet frames over the SDH network. The Ethernet over SDH (EoS) method and the generic framing procedure (GFP) are used to encapsulate the Ethernet frames into the SDH transmission payload. Virtual concatenation and LCAS are used to allocate a flexible amount of WAN bandwidth for the transport of Ethernet frames as needed for the end-user's application.

The Ethernet Interface extension card contains four 10/100BaseT Ethernet ports (LAN ports). The LAN ports automatically determine the speed of the network, whether it is 10BaseT or 100BaseT.

The physical L2 switch that is present on an Ethernet Interface extension card can be split into several logical or virtual switches. A Virtual Switch is a set of LAN/WAN ports on an Ethernet Interface extension card that are used by different VLAN's which can share the common WAN bandwidth. Each of the virtual switches can operate in a specific Virtual Switch mode depending on the VLAN tagging scheme.

First the VLAN tagging mode has to be specified on Ethernet Interface extension card level, this can be either IEEE 802.1Q VLAN tagging or VPN-tagging (Transparent). In VPN tagging (Transparent) mode, the end-user 802.1Q VLAN tags that optionally may appear in the end user traffic are ignored in the forwarding process. These VLAN tags are carried transparently through the SDH network. In IEEE 802.1Q VLAN-tagging mode, the VLAN tags are also carried transparently, but the VLAN ID in the VLAN tags is used in the forwarding decision. Therefore end user VLAN IDs must be unique per physical switch.
X8PL option card

The X8PL option card provides eight Ethernet interfaces in Private Line mode for the 1643 AM and 1643 AMS. The Private Line mode enables traffic to be mapped from each Ethernet port one-to-one into an SDH container. Thus a private connection from an Ethernet port through an SDH network to another Ethernet port at the remote end of the link is possible.

The X8PL option card supports a flexible allocation of SDH bandwidth to LAN ports by making use of the Link Capacity Adjustment Scheme (LCAS, see “Link Capacity Adjustment Scheme (LCAS)” (p. 8-43)). All LAN ports have the same capabilities. Each WAN port supports VC-12-Xv (X = 1...63) or VC-3-Xv (X = 1...3).

The VC-12s that form one VCG can be chosen from any TUG-3, in any time slot order. However, it is recommended to select the VC-12s in sequential order, preferably in one TUG-3. In this way the end-to-end network design can be kept simple and easy to maintain.

Physical interfaces

The physical interface function provides the connection to the Ethernet network of the end-customer. It performs autonegotiation, and carries out flow control.

The following physical interfaces are enabled on Alcatel-Lucent TransLAN® cards:

- 10BASE-T
- 100BASE-TX
- 1000BASE-SX
- 1000BASE-LX

The supported LAN interfaces for Ethernet and Fast Ethernet applications are 10BASE-T and 100BASE-TX. The numbers “10” and “100” indicate the bitrate of the LAN, 10 Mbit/s (Ethernet) and 100 Mbit/s (Fast Ethernet) respectively. The “T” or “TX” indicates the wiring and the connector type: Twisted pair wiring with RJ-45 connectors.

The supported LAN interfaces for Gigabit Ethernet applications are 1000BASE-SX, 1000BASE-LX, and 1000BASE-ZX. Again, the number indicates the bitrate of the LAN, 1 Gbit/s (Gigabit Ethernet). “SX” indicates a short-haul interface, “LX” and “ZX” indicate a long-haul interface.

Ethernet switch

The Ethernet switch connects the LAN ports with the WAN ports. It performs learning, filtering, and forwarding according to the IEEE 802.1D standard.

The physical Ethernet switch can be logically split in multiple, independent switches or port groups, called “virtual switch”. In the transparent tagging modes (LAN interconnect or LAN-VPN), also the name “LAN group” is used instead of “virtual switch”.
The following applies to port groups or virtual switches, respectively:

- A virtual switch defines a spanning tree domain, and can be assigned a mode of operation (LAN interconnect, LAN-VPN, IEEE 802.1Q, IEEE 802.1ad (PBM) or LAN-VPN with QoS).
- A virtual switch includes any number (at least 2) of external Ethernet LAN ports and/or internal WAN ports associated with a VC-n-Xv payload.
- Per data pack a VLAN ID can only be used in one virtual switch. This means that a VLAN must have all its port members inside one single virtual switch. Learning the same VLAN dynamically via GVRP on another virtual switch of this data pack should be prevented by network design.
- Traffic between virtual switches of the same physical switch is not possible.
- Each port can be a member of only one virtual switch at a time.

In the following example, a virtual switch is provisioned that connects 2 LAN ports with 1 WAN port:

![Diagram of virtual switch connecting LAN and WAN ports]

**Supported frame sizes**

The 1643 AM support Ethernet frames of up to 1650 bytes. The X8PL card of the 1643 AM supports Ethernet frames of up to 1600 bytes.

**Ethernet encapsulation with GFP**

The generic framing procedure (GFP) is used to adapt the asynchronous Ethernet payload to the synchronous SDH server layer.

A GFP-header (eight octets) is prepended to each Ethernet frame to indicate frame length and payload type. Gaps between Ethernet frames are filled with “IDLE” frames (four octets each).
GFP, standardized by the ITU-T in the recommendations G.7041 and Y.1303, is a very efficient encapsulation protocol because it has a fixed and small overhead per packet.

In earlier versions (prior to the Garnet network release of June 2002) of the TransLAN® equipment, the Ethernet over SDH (EoS) encapsulation and mapping method is used for VC-12 and/or VC-3 based designs (10/100BASE-T Ethernet / Fast Ethernet cards). EoS is a proprietary encapsulation protocol, based on the ANSI T1X1.5/99-268r1 standard, and can be regarded as a precursor of GFP. EoS and GFP are both length-based encapsulation methods. EoS is similar to GFP in terms of frame delineation and mapping (incl. scrambling); differences between the two encapsulation methods lie in the size and interpretation of the EoS/GFP encapsulation core headers, as well as the length of the Idle frames.

The generic framing procedure, framed mode (GFP-F) compliant to the ITU-T Rec. G.7041 is available on all TransLAN® products since the Garnet Maintenance / Mercury network release of January 2003.

The following GFP encapsulation are possible:
- Mapping of Ethernet MAC frames into Lower Order SDH VC12–Xv
- Mapping of Ethernet MAC frames into Lower Order SDH VC3–Xv
- Mapping of Ethernet MAC frames into Higher Order SDH VC4–Xv.

Virtual concatenation

The virtual concatenation function arranges the Ethernet frames into the right SDH virtual container. It is possible to map the client's data signal over a number of grouped virtual containers.

Related information

Please refer to “Virtual concatenation” (p. 8-41) for more detailed information.

VC12–Xv virtual concatenation

The 1643 AM supports virtual concatenation of Lower Order SDH VC-12 as inverse multiplexing technique to size the bandwidth of a single internal WAN port for transport of encapsulated Ethernet and Fast Ethernet packets over the SDH/SONET network. This is noted VC12-Xv, where X = 1...5. Usage is in conformance with ITU-T G.707 Clause 11 (2000 Edition) and G.783 Clause 12.5 (2000).
This feature implies specific processing of some overhead bytes:

- **Source direction:** Each individual VC-12 (from the VC12-Xv group) K4-byte (bit 1-2 multiframed) will be written to indicate the values of the multi-frame indicator (timestamping), as well as the sequence indicator (individual VC-12 position inside a VC12-Xv)
- **Sink direction:** Each individual VC-12 (from the VC12-Xv group) K4-byte (bit 1-2 multiframed) multi-framing indicator and sequence indicator is used to check that the differential delay between the individual VC-12s of the VC12-Xv remains within implementation limits.

Additionally, the use of G.707 Extended Signal Label is supported using V5 (bits 5-7) field, in which the “101” value is written, which points to the appropriate bits of K4 (bit 1) multiframe for writing in the Extended Signal Label value.

**VC3-Xv virtual concatenation**

The 1643 AM supports virtual concatenation of Lower Order SDH VC-3 as inverse multiplexing technique to size the bandwidth of a single internal WAN port for transport of encapsulated Ethernet and Fast Ethernet packets over the SDH/SONET network. This is noted VC3–Xv, where X = 1,2 (SDH). Usage is in conformance with ITU-T G.707 Clause 11 (2000 Edition) and G.783 Clause 12.5 (2000) and T1X1 T1.105 Clause 7.3.2 (2001 Edition).

This feature implies specific processing of some overhead bytes:

- **Source direction:** each individual VC-3 (from the VC3–Xv group) H4-byte will be written to indicate the values of the two-stage multi-frame indicator (timestamping), as well as the sequence indicator (individual VC-3 position inside a VC3–Xv)
- **Sink direction:** each individual VC-3 (from the VC3–Xv group) H4-byte two-stage-multi-framing indicator and sequence indicator is used to check that the differential delay between the individual VC-3 of the VC3–Xv remains within implementation limits.

**VC4-Xv virtual concatenation**

The 1643 AM supports virtual concatenation of Higher Order SDH VC-4 as inverse multiplexing technique to size the bandwidth of a single internal WAN port for transport of encapsulated Gigabit Ethernet packets over the SDH/SONET network. This is noted VC4/STS3c-Xv, where X = 1...4.

This feature implies specific processing of some overhead bytes:

- **Source direction;** each individual VC-4 (from the VC4–Xv/STS3c-Xv group) H4-byte will be written to indicate the values of the two-stage multiframe indicator (timestamping), as well as the sequence indicator (individual VC-4 position inside a VC4/STS3x-Xv group).

- **Sink direction;** each individual VC-4 (from the VC4/STS3c-Xv group) H4-byte two-stage-multi-framing indicator and sequence indicator is used to check that the differential delay between the individual VC-4 of the VC-4/STS3c-Xv remains within implementation limits.

**LAN interfaces**

1643 AM and 1643 AMS support up to four 10/100BASE-T LAN interfaces, as part of the *TransLAN®* Ethernet SDH Transport Solution, when the X4IP-V2 option card is used.

1643 AM and 1643 AMS support up to eight Ethernet interfaces in Private Line mode, when the X8PL option card is used. The X8PL board is a point-to-point Ethernet solution without any switching capabilities. The Ethernet ports are directly connected to the virtual concatenation groups (VCGs of flexible SDH Channel TTPs).

**Main features of the X4IP-V2 and X8PL options cards**

The following table lists the main features and differences of the two option cards X4IP-V2 and X8PL which can be used for Ethernet applications:

<table>
<thead>
<tr>
<th></th>
<th>X4IP-V2</th>
<th>X8PL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports</td>
<td>4 ports</td>
<td>8 ports</td>
</tr>
<tr>
<td>Provides a Layer 2 switch</td>
<td>no switch</td>
<td>cost optimized option card for point-to-point applications</td>
</tr>
<tr>
<td>Supports advanced networking applications like ring connections or point-to-multi-point connections</td>
<td>supports the LCAS (Link Capacity Adjustment Scheme) protocol (please refer to “Link Capacity Adjustment Scheme (LCAS)” (p. 8-43))</td>
<td></td>
</tr>
<tr>
<td>No LCAS (Link capacity adjustment scheme) support</td>
<td>supports the LCAS (Link Capacity Adjustment Scheme) protocol (please refer to “Link Capacity Adjustment Scheme (LCAS)” (p. 8-43))</td>
<td></td>
</tr>
<tr>
<td>EoS (Ethernet over SDH) mapping or GFP (Generic Framing Procedure)</td>
<td>GFP or LAPS (Link Access Procedure SDH) (please refer to “Ethernet mapping schemes” (p. 8-81))</td>
<td></td>
</tr>
</tbody>
</table>
X5IP Option card

The X5IP option card (item code X5IP) will combine X4IP and X8PL capabilities in the following aspects, as compared to X4IP and X8PL card:

- **GE ports support**
  - 10/100/1000 BASE-T GE port (1 E)
  - 1000BASE-X GE (1 O)
- **3 10/100 FE ports support**
- **Full flexible mapping low order VC12/VC3 termination**
- **LCAS for V12 (VC12-1v to VC12-63v) and VC3 (VC3-1v to VC3-3v)**
- **High number of WAN ports (up to 8)**
- **LPT supported on all ports**

The following table list the main features and differences of the two option cards X4IP and X5IP:

<table>
<thead>
<tr>
<th>Feature List</th>
<th>X4IP</th>
<th>X5IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN Port</td>
<td>fix vc channel mapping(4)</td>
<td>flexible vc channel mapping(8)</td>
</tr>
<tr>
<td>LCAS</td>
<td>Dsabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>SDH TP</td>
<td>VC12 VC3 TP function</td>
<td>VC12 VC3 TP function</td>
</tr>
<tr>
<td>ether Encapsulation</td>
<td>EOS/GFP</td>
<td>GFP</td>
</tr>
<tr>
<td>LAN Port</td>
<td>10/100M FE port (4 E)</td>
<td>10/100/1000M GE port</td>
</tr>
<tr>
<td>SFP</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>L2 switch</td>
<td>VPN/IEEE(1q and 1ad)</td>
<td>IEEE(1q and 1ad)</td>
</tr>
<tr>
<td>STP/GVRP/IRUP/SVDP</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>QOS</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Mac prov</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>RTD</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>LPT</td>
<td>No</td>
<td>Yes (for all ports)</td>
</tr>
<tr>
<td>PM per port</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PM per flow</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PM per TC</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>increase vlan support</td>
<td>64 static/64 dynamic</td>
<td>64 static/64 dynamic</td>
</tr>
<tr>
<td>LED test</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Ethernet Interfaces

On the faceplate, the X5IP option card provides the following interfaces.

- **10/100/1000BASE-T(X)** electrical Ethernet interface using RJ-45 connectors supports 10BASE-T, 100BASE-T(X), or 1000BASE-T specifications.
- **10/100BASE-T(X)** electrical Ethernet interface using RJ-45 connectors supports 10BASE-T and 100BASE-TX specifications.
- **1000BASE-SX** optical Ethernet interface, covers a distance of 550 m over 50 μm MMF with an operating wavelength of 770-860 nm.
- **1000BASE-LX** optical Ethernet interface, covers a distance of 5 km over 10 μm SMF with an operating wavelength of 1310 nm.
- **1000BASE-ZX** optical Gigabit Ethernet interface in single fiber mode, covers a distance of 70 km with an operating wavelength of 1550 nm for long haul transmission.

Configurable Auto-negotiation

The X5IP option card supports configurable Auto-negotiation for 1000BASE-X PHYs, 10/100/1000BASE-T(X), and 10/100BASE-T(X) rates.

**1000BASE-X PHYs**

1000BASE-X Ethernet PHYs support Auto-negotiation for Duplexity (Full/Half Duplex) and pause operations (none, Rx only, Tx only or both directions). The X5IP option card only supports the Full-Duplex mode. Pause operations can only be enabled or disabled by provisioning point-to-point Ethernet services.

**10/100/1000BASE-T(X)**

Triple rate electrical Ethernet PHYs (10/100/1000BASE-T(X)) support Auto-negotiation for Duplexity (Full/Half Duplex), Port Rate (10/100/1000 Mbit/s), and Pause operation (None, Rx only, Tx only or both directions).

**10/100BASE-T(X)**

The Lucent NMS and the ITM-CIT can be used to manually override the Auto-negotiation function. If this function is disabled, users can select a specific operational mode such as port speed, Half/Full Duplex, and Flow Control.

Ethernet Mapping

The following sections describe the mapping schemes for VC3-Xv and VC12-Xv Ethernet frames.

**Mapping Ethernet frames into VC3-Xv: GFP Encapsulation**

The X5IP option card supports the following mapping scheme for Ethernet frames.

- **AU4 < - > VC4 < - > m**
- **TUG3 < - > X**
The GFP encapsulation scheme follows the ITU-T G.7041 standard.

**Mapping Ethernet frames into VC12-Xv: GFP Encapsulation**

The X5IP option card supports the following mapping scheme for Ethernet frames.

- AU4 < - > VC4 < - > m *
- TUG3 < - > n *
- TUG2 < - > X*TU12 < - > X*VC12 < - > VC12-Xv < - > GFP < - > 802.3

**Flexible Bandwidth Assignment**

The X5IP option card supports flexible assignment of VC capacity to create various size VCGs. The available capacity of one VC4 can be divided in three TUG3s. Each TUG3 can be used a single VC3 or as 21 VC12s.

These VC3 and VC12 containers can be assigned to a maximum number of eight VCGs. For each VCG, users can choose between VC12-Xv (X=1-63) and VC3-Xv (X=1-3), based on the total number of containers that are available for each container type.

**Link Capacity Adjustment Scheme (LCAS)**

The 1643 AM/AMS supports the LCAS function for VC3-Xv concatenated signals on the X5IP option card. According to ITU-T G.7042/Y.1305 standard, this function is implemented using H4[1,4] bits of multiframe positions 2, 3, 8, 9, and 10.

The 1643 AM/AMS also supports the LCAS function for VC12-Xv concatenated signals on the X5IP option card. According to ITU-T G.7042/Y.1305 standard, this function is implemented using K4[2] multiframe bits 12 through 32.

The X5IP option card supports the latest LCAS standards as per ITU-Ts G.806 at 2006.3 and G.7042 at 2005.5 recommendations. The following enhancements are implemented.

- G.806 at 2006.3: modified defect and alarm correlation process; hold-off timer is now part of the defect-alarm process
- G.7042 at 2005.5: error corrections implemented.

**LAN modes**

The X5IP option card supports the following LAN modes.

- LAN bridge mode
- LAN promiscuous mode
**Bridge mode**

According to the IEEE802.1D standard, the Ethernet bridge provides the following functions.

- Point-to-point LAN bridge
- Multiport bridge for ten ports
- MAC address filtering via self learning protocol (up to 8k MAC addresses)
- Spanning-tree algorithm
- Transparency to VLAN tagged packets from end customers
- Broadcasting, including end user BPDUs

All L2 switching relations can process packets at wire speed. In case of congestion on a specific port, packets will be arbitrarily dropped from the tail.

**Promiscuous mode**

In addition to the L2 switching capabilities of the LAN bridge mode, the X5IP option card supports operations in promiscuous mode. In this mode, the L2 switching function forwards all Ethernet packets that are received without address filtering. This function is only supported for a point-to-point switching relation.

**VLAN tagging - IEEE 802.1Q**

The X5IP option card supports an IEEE 802.1Q compliant VLAN tagging, classification, and filtering standard on all of its external Ethernet LAN ports or internal WAN ports.

The Ethernet packets are processed as follows:

A customer's VLAN tagged packets are VLAN classified according to the VLAN ID contained in the VLAN tag. The system performs VLAN ingress filtering based on the port membership of the receiving port for a specific VLAN.

A customer's untagged and priority-tagged packets are VLAN classified according to a default port VLAN ID that is assigned to the receiving port. The system inserts the PVID in the VLAN tag. A unique VLAN ID can be provided to customers.

**E/FE/GbE VLAN trunking**

The X5IP option card aggregates E/FE/GbE traffic of multiple end-users over a single external Ethernet or Fast Ethernet or Gigabit Ethernet port. A VLAN trunk port is a shared member of multiple VLANs from different end-users.

**GARP VLAN Registration Protocol (GVRP)**

The 1643 AM/AMS supports the GARP VLAN Registration Protocol (GVRP) on the X5IP option card. This protocol is used to maintain VLAN identification consistency and connectivity throughout the switched WAN network.
For more information about GVRP, see “GARP VLAN Registration Protocol (GVRP)” (p. 8-54).

Rapid spanning tree protocol (rSTP)

The 1643 AM/AMS supports the Rapid Spanning Tree Protocol for each virtual switch on the X5IP option card based on the IEEE 802.1D standard.

For more information about the Rapid Spanning Tree Protocol, see “Rapid spanning tree protocol (rSTP)” (p. 8-53).

Overlength Ethernet Frames

The X5IP option card supports forwarding, encapsulation, and mapping of Ethernet frames with lengths up to 1650 octets/bytes.

Enhanced Flow Classification

The X5IP option card supports Enhanced Flow Classification - 802.1Q mode and 801.2ad mode. Network traffic from end users can be classified into flow categories on the edge ports of a TransLAN® domain. As a result, ports can be provisioned as “Edge” or “Interior” ports. Edge ports are either Customer Role ports (UNI) or “Virtual ports” on a Trunk port (E-NNI). A virtual port is the traffic over a trunk port belonging to a single end-user and is characterized by an S-VID tag.

The QoS edge ports support up to seven provisionable flows of 1k per unit and can be defined with a combination of the following criteria:

- flow = port
- flow = C-Tag (C-VID, C-UP) previously known as: VID, UP
- flow = IP-TOS field (DSCP)
- flow = Destination address mask (for broadcast/multicast and for customer control traffic)

Additionally, a default flow for each user is already present. When ports are designated as “Interior”, the flow classification is completely based on the S-UPT bits. There is no rate control and the S-UPT bits are transparently transported through the device. Virtual ports on a trunk port can be provisioned to behave as "Interior" ports, i.e. to use the S-UPT bits for classification instead of the freely provisionable flow. By provisioning a (virtual) port as an "Interior" port, the flow definition is fixed.

Enhanced Flow Properties

The 1643 AM/AMS supports enhanced flow classification properties that can be provisioned for each flow. Users can provision the properties of each flow by assigning a traffic class and provisioning the threshold rate. For example, immediate dropping (strict
policing: CIR=PIR) or marking with high dropping precedence (over-subscription: CIR<= PIR<= MAX). The assigned traffic class and dropping precedence are coded into the S-UPT bits of the frame on the egress side.

The X5IP option card supports Committed Burst Size (CBS) and Peak Burst Size (PBS) provisioning. Users can provision the CBS and PBS parameters to QoS profiles for IEEE 802.1Q and IEEE 802.1ad modes.

**QoS provisioning in Provider Bridge Mode (PBM)**

The X5IP option card supports Flow Classification of ingress traffic into the L2 switch based on the IEEE 802.1Q tagging mode. For every Flow Classification, users can assign a Flow Profile containing the QoS parameters that are to be applied to the flow.

A Flow Profile can be labeled and pre-provisioned. It can be assigned to multiple flows and contains the following parameters:

- Traffic conditioning parameters such as TransLAN® ingress rate control parameters including dropping precedence marking.
  
  Frames below CIR are classified as "green" (low dropping precedence). Frames between CIR and PIR are classified as "yellow" (high dropping precedence). Frames above PIR are classified as "red" and are dropped. The high or low dropping precedence is encoded in the LSB of the user_priority field of the S-TAG.

- Traffic class flow assignment including traffic class marking indicating a certain service level.
  
  Users can assign a traffic class for each flow which determines the value of the 2 MSB user_priority bits in the S-TAG of the frames that are classified to the flow. The relation between the assigned traffic class and the 2 MSB user_priority bits is fixed. Based on the traffic class, the frame will be assigned to a certain queue by a fixed traffic class to queue mapping function that is present in each switch.

**Q-tagging mode**

The X5IP option card supports Flow Classification in the IEEE 802.1Q tagging mode. Users can assign a similar flow profile as described above for the IEEE 802.1ad tagging mode. Note that the QoS classification operations will only modify the end-user priority (UP) bits.

**CQS - Provider Bridge Mode (PBM) and Q-tagging mode**

The X5IP option card supports classification, queuing, and scheduling functions for four traffic classes, associated with three queues in the Provider Bridge Mode and Q-tagging mode.

Note: In the Q-tagging mode, this function is a non-standard conformance operation mode in which the customer's user priority (UP) bits will be modified.
**Ingress rate control in Provider Bridge Mode (PBM) and Q-tagging mode**

The X5IP option card supports ingress rate control values through rate policing per flow at customer role ports in provider bridge mode and Q-tagging mode. This function is based on 'Strict policing' values where (PIR=CIR) and 'Oversubscription' values where (PIR>CIR).

Note: In the Q-tagging mode, this function is a non-standard conformance operation mode in which the third user priority (UP) bit of the customer tag will be modified.

**LAN port provisioning**

The following sections describe LAN port provisioning capabilities that are supported by the X5IP option card.

**LAN port as network port or customer port**

The X5IP option card can be used to operate a LAN port as a network port or customer port. Based on the IEEE 802.1Q and IEEE 802.1ad modes, the 1643 AM/AMS supports a flexible operational port role assignment per LAN port. During port provisioning, a LAN port can be set to a 'network' role.

The following properties are applicable to a port in a 'network' port role:

- No V-LAN tagging operations
- Provider based Spanning Tree Protocol (provisionable, default=enabled)
- GVRP operations (provisionable, default=enabled)

The following properties are applicable to a port in a 'customer' port role:

- V-LAN tagging operations
- No provider based Spanning Tree Protocol
- No GVRP operations

**WAN port as network port or customer port**

In IEEE 802.1Q and IEEE 802.1ad modes, the Network Element supports a flexible operational port role assignment per WAN port. Next to the default "network" port role, a WAN port can be set to "customer" role.

The following properties apply to a port in "network" port role:

- No VLAN tag/untag operation
- Provider Spanning Tree Protocol (provisionable, default is enabled)
- GVRP operation (provisionable, default is enabled)

The following properties apply to a port in "customer" port role:

- VLAN tag/untag operation
- No provider Spanning Tree Protocol
- No GVRP operation
**Link Pass-through**

The Fast Ethernet electrical interface and Gigabit Ethernet electrical and optical interfaces on the X5IP option card support Link Pass-through modes.

The Ethernet port transmitter is shutdown in the upstream network due to the following failures.

- loss of signal reported on a remote TransLAN Ethernet option card due to Ethernet cable or fiber failure
- SDH/SONET network failure
- upstream equipment failure

Remote failures are reported in-band through the GFP-Client Signal Fail message. The Link pass-through mode is only supported on ports that operate on a one-to-one association with a WAN port using GFP encapsulation. Users can enable or disable the Link pass-through mode per port.

**LAN and WAN ports and VLAN**

A VLAN can contain multiple LAN ports and multiple WAN ports.

Multiple LAN ports can be assigned to different VLANs, also mentioned as Virtual LAN’s. This keeps the traffic on each VLAN totally separate. VLAN groups are used to connect LAN ports and WAN ports. The LAN ports are the physical 10BaseT or 100BaseT or gigabit Ethernet ports on the NE. All valid Ethernet packets are accepted (both Ethernet 2 and IEEE 802.3). The WAN ports are the logical connection points to the SDH channels. The LAN port is the interface between the customers Ethernet LAN and the Ethernet switch on the LAN unit. The WAN port is the internal port between the Ethernet switch and the part of the LAN unit where the Ethernet frame is mapped into or de-mapped from SDH payloads.
VLAN trunking

VLAN trunks carry the traffic of multiple VLANs over one single Ethernet link and allow handling off aggregated LAN traffic from multiple end users via one single high capacity Ethernet link (Fast Ethernet or Giga Ethernet) to data equipment in a Central Office or an IP Edge Router, IP Service Switch, or an ATM Switch. The main benefit of VLAN trunking is that TransLAN cards can hand off end user LAN traffic via one high capacity LAN port instead of multiple low speed LAN ports.

Advantages of VLAN trunking are:
- it does not require the assignment of CID tags
- it permits different 802.1 tagged frames to share the same physical LAN port
- it gives additional flexibility for egress logical WAN port assignment
- it permits successfully routing via an aggregation function.

Learning bridges

To increases the efficiency of the network, it can be separated into segments. A bridge, which may have several parts, passes packets between multiple network segments. By noting at which port an Ethernet packet with a certain source address arrives, the bridge learns to which ports a packet with a certain destination address must be sent. If the port does not know the destination address, then it will send it to all the ports except the port where it comes from. The tables which the learning bridge uses to pass the Ethernet packets to its ports are not shown to the user by the management systems.

MAC-Bridges perform automatic address learning based on the source MAC-address present in each frame.
- In this process an unknown SA of a frame is stored together with the port number over which the frame entered the Bridge to be used when frames with that DA need to be forwarded
- Addresses that are not refreshed (relearned) within the so-called MAC address ageing time, are removed.
- The MAC address table has a size of 8k or 64k in our implementations.

In case more different source address than there is memory space are passing in a specific interval, the MAC address ageing time, addresses are prematurely flushed and possibly need to be re-learned.

The MAC address ageing time is not stable. Ageing time can vary between 240s up to 420s.

This causes some excess traffic as unlearned traffic is broadcasted. Too much unlearned traffic can also affect the learned traffic (because of the broadcasting).
Example

After the bridge has received a packet from station C it knows that station C is attached to port 2. When the bridge knows to which ports a station is attached, it will send packets with destination addresses of these stations only to the port the station is attached to (for example, a packet from station B to station C is only forwarded to port 2). When a destination address of a packet is of a station in its own segment, the packet is not forwarded by the bridge (for example, a packet from station D to station E).

Quality of service

Refer to “Quality of Service (QoS) overview” (p. 8-90).
Virtual concatenation

The SDH granularity problem

The virtual containers of the SDH have fixed sizes. These virtual containers are important for the transport of Ethernet frames over the SDH network:

- VC-12: 2 Mbit/s
- VC-3: 50 Mbit/s
- VC-4: 150 Mbit/s

It is difficult to fit the Ethernet traffic into one of these virtual containers. For many applications the containers, or contiguously concatenated virtual containers, such as VC-4-4C (600 Mbit/s) for example, are either too small or too big. This is known as the granularity problem.

Virtual concatenation is a mechanism by which a number of independent VCs can be used to carry a single payload. This way, the granularity problem is solved.

The following table shows the possible payload sizes, and the virtual containers that are used for the transport.

<table>
<thead>
<tr>
<th>Payload</th>
<th>Virtual containers</th>
<th>Concatenation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 Mbit/s</td>
<td>1 × VC-12</td>
<td>VC-12</td>
</tr>
<tr>
<td>4 Mbit/s</td>
<td>2 × VC-12</td>
<td>VC-12-2v</td>
</tr>
<tr>
<td>6 Mbit/s</td>
<td>3 × VC-12</td>
<td>VC-12-3v</td>
</tr>
<tr>
<td>8 Mbit/s</td>
<td>4 × VC-12</td>
<td>VC-12-4v</td>
</tr>
<tr>
<td>10 Mbit/s</td>
<td>5 × VC-12</td>
<td>VC-12-5v</td>
</tr>
<tr>
<td>50 Mbit/s</td>
<td>1 × VC-3</td>
<td>VC-3</td>
</tr>
<tr>
<td>100 Mbit/s</td>
<td>2 × VC-3</td>
<td>VC-3-2v</td>
</tr>
<tr>
<td>150 Mbit/s</td>
<td>1 × VC-4</td>
<td>VC-4</td>
</tr>
<tr>
<td>300 Mbit/s</td>
<td>2 × VC-4</td>
<td>VC-4-2v</td>
</tr>
<tr>
<td>450 Mbit/s</td>
<td>3 × VC-4</td>
<td>VC-4-3v</td>
</tr>
<tr>
<td>600 Mbit/s</td>
<td>4 × VC-4</td>
<td>VC-4-4v</td>
</tr>
<tr>
<td>750 Mbit/s</td>
<td>5 × VC-4</td>
<td>VC-4-5v</td>
</tr>
<tr>
<td>900 Mbit/s</td>
<td>6 × VC-4</td>
<td>VC-4-6v</td>
</tr>
<tr>
<td>1 Gbit/s</td>
<td>7 × VC-4</td>
<td>VC-4-7v</td>
</tr>
</tbody>
</table>

Virtual concatenation

Virtual concatenation can be used for the transport of payloads that do not fit efficiently into the standard set of virtual containers (VCs).
Virtual concatenation splits the contiguous bandwidth into individual VCs, transports these VCs separately over the SDH network, and recombines them to a contiguous signal at the path termination. An important aspect of virtual concatenation is that it *only needs to be supported at the end nodes* (i.e. at the TransLAN® cards that interface with the end-customer's LAN). The rest of the network simply transports the separate channels.

**Example 1**

As an example, the following figure shows the virtual concatenation of $5 \times VC-12$:

![Virtual Concatenation Diagram](https://via.placeholder.com/150)

The 10 Mbit/s payload is put into a VC-12–5v, i.e. into a virtual concatenation group (VCG) consisting of five virtually concatenated VC-12s. These VC-12s can travel the network independently, and do not have to follow the same route. At the endpoint, the VC-12–5v is reassembled, and the payload is extracted.
Example 2

The second example shows the principle of virtual concatenation in a Gigabit Ethernet (GbE) network application. Protection of the virtually concatenated payload is possible via standard SDH transmission protection schemes.

Differential delay

Due to the different propagation delay of the VCs a differential delay occurs between the individual VCs. This differential delay has to be compensated and the individual VCs have to be re-aligned for access to the contiguous payload area.

The TransLAN® re-alignment process covers at least a differential delay of 32 ms.

Link Capacity Adjustment Scheme (LCAS)

LCAS is an extension of virtual concatenation that allows dynamic changes in the number of channels in a connection. In case channels are added or removed by management actions this will happen without losing any customer traffic.

LCAS allows a bandwidth service with scalable throughput in normal operation mode. In case of failure the connection will not be dropped completely but only the affected channel(s). The remaining channels will continue carrying traffic. LCAS provides automatic decrease of bandwidth in case of link failure and re-establishment after link recovery.

In case only one end supports (or has turned on) the LCAS protocol, the side that does support LCAS adapts automatically to the restrictions that are dictated by the non-supporting end, i.e. the entire link behaves as a link that does not support in-service bandwidth adaptations.

Bandwidth allocation (GbE)

Unlike the TransLAN+ and M-LAN cards the GbE unit has a fully flexible internal cross connect. This means that it is impossible to simply request bandwidth. For the GbE card the user selects which VCs to add to the SDH Channel/VCG. In addition the user has the option of substructuring the VC4s into VC3s thus giving additional flexibility as in the
other Ethernet cards the substructuring was fixed. The user may select from the following SDH Rates: VC3, VC3-2v, VC4-1v, VC4-2v, VC4-3v, and VC4-4v. This gives a range from 50 Mbps to 600 Mbps.

**Dynamic bandwidth adjustment (GbE)**

One of the major problems with using Virtual Concatenation is that if one of the VCs has a fault and fails the whole signal fails. This means that if a single VC fails the entire SDH Channel/VCG is lost. The GbE card for the 1643 AM network element supports the Link Capacity Adjustment Scheme (LCAS). This LCAS allows dynamic bandwidth increase or decrease without loss of signal. Furthermore, if the signal of one or more of the components becomes degraded then LCAS will autonomously remove those VCs from the group. When the failure is repaired LCAS will automatically return those component VCs to the SDH Channel/VCG.

The following table indicates the effect LCAS has on the transmission capacity:

<table>
<thead>
<tr>
<th>Enabling/disabling LCAS</th>
<th>Capacity no VC-n failures</th>
<th>One or more (but not all) VC-ns failures</th>
<th>All VC-ns fail</th>
</tr>
</thead>
<tbody>
<tr>
<td>LCAS disabled</td>
<td>Working Capacity = Provisioned Capacity</td>
<td>Working Capacity = 0</td>
<td>Working Capacity = 0</td>
</tr>
<tr>
<td>LCAS enabled</td>
<td>Working Capacity = Provisioned Capacity</td>
<td>Working Capacity is reduced by amount of failed VC-ns service degraded.</td>
<td>Working Capacity = 0</td>
</tr>
</tbody>
</table>

With the introduction of LCAS for VC4-Xv an additional attribute “SDHWorkingCapacity” is needed. The working capacity shows the value of the actual capacity available, this allows the operator to see when service is degraded. The working capacity will also be displayed for non-LCAS, showing a zero if the signal is degraded on any VC-n. When LCAS is enabled Working Capacity show a zero only when the signal is fully degraded. The next three figures depict the effect of LCAS.
Non-degraded service

Non LCAS causing degraded service

Single failure causes total signal loss.
With LCAS enabled only signal degradation is caused

**Single failure only causes signal degradation.**

**VC allocation (GbE)**

There are 4 x VC-4 TTPs on the GbE card. Each of these can be substructured to VC-3 TTPs or used as VC-4 TTPs. When the operator requests an SDH Channel/VCG it has a choice of various capacities from a single VC-3 (50 Mbit/s) up to VC-4-4v (600 Mbit/s). If the operator requires a bandwidth of say 100 Mbit/s, one of the VC-4 TTPs must be adapted into VC-3 TTPs, and two of these will be virtually concatenated as a VC-3-2v. For the next SDH Channel/VCG the operator will then only have a maximum bandwidth of 450 Mbit/s (VC-4-3v) as this is what is still available.
Spanning tree protocol (STP)

Overview

The spanning tree protocol (STP) is a standard Ethernet method for eliminating loops and providing alternate routes for service protection. Standard STP depends on information sharing among Ethernet switches/bridges to reconfigure the spanning tree in the event of a failure. The STP algorithm calculates the best loop-free path throughout the network.

STP defines a tree that spans all switches in the network; it for example, uses the capacity of available bandwidth on a link (path cost) to find the optimum tree. It forces redundant links into a standby (blocked) state. If a link fails or if a STP path cost changes the STP algorithm reconfigures the spanning tree topology and may reestablish previously blocked links. The STP also determines one switch that will be the root switch; all leaves in the spanning tree extend from the root switch.

Maximum bridge diameter

The maximum bridge diameter is the maximum number of bridges between any two hosts on the bridged LAN for any spanning tree configuration.

For TransLAN® applications the maximum bridge diameter is 25 nodes.

Spanning tree example

The following example network serves to illustrate the principle how a spanning tree is constructed.
**Determination of the root**

For every switch a priority can be configured. The switch priority is a number between 0 (highest priority) and 61440 (lowest priority) in steps of 4096. The switch with the highest priority will become root.

If there are two or more switches with the same highest priority, then the switch with the lowest number for the MAC address will become root. This rule ensures that there is always exactly one root, as MAC addresses are unique.
Determination of the root ports

Root ports are those ports that will be used to reach the root. For each switch the port with the lowest root path cost is chosen, where the root path cost is determined by adding the path costs to the root. In the example port 2b and 3b are root ports.
For every port a path cost value can be configured. For E/FE TransLAN® cards, the default value of the path cost is determined by dividing 20,000,000,000 by the bandwidth in kbit/s. For GbE TransLAN® cards, the path cost is a means to influence the active network topology.

**Determination of the designated and blocked ports**

The designated port is the one port that is going to be used for a certain LAN. In the example, there are six LANs.

The designated ports for LAN 1, LAN 2 and LAN 3 are the ports 1a, 2a and 3a respectively, because these LANs have only one connection to a switch. If there are more connections to a switch, then the port with the lowest root path cost is chosen. Thus the designated ports for LAN 4, LAN 5 and LAN 6 are the ports 1b, 1c and 3c respectively.

Ports that are neither root ports nor designated ports are blocked. In the example port 2c is a blocked port.

Thus the loop free spanning tree is constructed.

**Spanning tree protocol (STP)**

If more than one bridge is used between segments of the network a bridging loops occur, which cause packets to circulate forever. The spanning tree algorithm avoids the occurrence of these bridging loops. The spanning tree algorithm elects a root node and makes sure that each bridge blocks its ports in such a manner that there is only one path from any given point on the network to the root. In this way a mesh network is reduced to...
A tree which spans every node. The WAN part of the network formed by the NEs maintains its own spanning tree, independent of the spanning tree maintained on the customer's LANs. Thus the spanning tree protocol behavior is different on the LAN side and the WAN side of an NE.

Due to the spanning tree algorithm meshed configurations can be made to enhance availability (alternative channels if one fails). If multiple VC-n paths are provisioned between two nodes, the spanning tree algorithm closes down SDH channels to avoid loops. Thus the increase of bandwidth for payload due to multiple VC-n paths may not be as expected. So, to increase the capacity of the path use virtual concatenated VC-4s, VC-3s or VC-12s in stead of multiple VC-4, VC-3, or VC-12 paths.

The figure below illustrates an example of SDH ports that are switched off due to the spanning tree algorithm.

**STP per virtual switch per operation mode**

The *TransLAN*® board supports a single STP (Spanning Tree Protocol) per Virtual Switch under LAN-interconnect mode and a single STP per VPN under the VPN mode.

In the STP Virtual Switch mode, the *TransLAN*® board supports a single STP per Virtual Switch. When operating in the Repeater mode, the Ethernet virtual bridge (an instance of the TransLAN Ethernet bridging function) must not participate in a STP.

**STP status parameters**

In the STP Virtual Switch mode, a number of STP status parameters per Port/Virtual Switch are retrievable/editable. The most important ones are the support of Port State retrieval and the support of Bridge/Port Priority provisioning.
The Port state can have one of the following values:

- Disabled; the port is disabled completely.
- Blocking; BPDUs and normal frames are discarded.
- Listening; BPDUs are processed, but normal frames are discarded. The Filtering Database is not updated.
- Learning; BPDUs are processed, but normal frames are discarded received.
- Forwarding; BPDUs are processed and normal frames are forwarded.

Path cost provisioning

The system sets a default STP path cost for each link which is inverse proportional to the speed (2, 4, 6, 8, 10, 50 and 100 Mbit/s). BPDUs are capable of carrying 32 bits of Path Cost information; however, IEEE Std. 802.1D, 1998 edition, and earlier revisions of this standard limited the range of the Path Cost parameter to a 16-bit unsigned integer value.

The recommended values in IEEE Std. 802.1t-2001, make use of the full 32 bit range available in BPDUs in order to extend the range of link speeds supported by the protocol. In LAN's where bridges that use the recommended values defined in the IEEE Std. 802.1D, 1998 edition and bridges that use the recommended values in IEEE Std. 802.1t-2001 are required to inter-operate, either the older Bridges or the new Bridges need to be reconfigured to make Path Cost values compatible. However, this situation is not likely to occur since the first release of STP in IEEE 802.1Q tagging will support the values recommended in IEEE Std. 802.1t-2001.

Bridge priority provisioning

Ranges and granularities for Port priority defined in IEEE Std. 802.1D, 1998 edition have been modified in IEEE Std. 802.1t, 2001 edition: value range should now be expressed in steps of 4096 instead of 1. The step values chosen ensure that the low-order bits that have been re-assigned cannot be modified (Bridge priority 12 low-order bits have become a 12-bit system ID extension for Multiple Spanning Trees).

The magnitude of the priority values can be directly compared with those based on previous versions of the standard, which ensures full interoperability. Although the NE and management systems support a granularity of 1, it is advised to provision a Port Priority with the new granularity of 4096 in order to ensure interoperability.

Port priority provisioning

Ranges and granularities for Port Priority defined in IEEE Std. 802.1D, 1998 edition have been modified in IEEE Std. 802.1t, 2001 edition: value range should now be expressed in steps of 16 instead of 1. The step values chosen ensure that the low-order bits that have been re-assigned cannot be modified (Port priority 4 low-order bits are now considered to be part of the Port Number). The magnitude of the priority values can be directly compared with those based on previous versions of the standard, which ensures full
interoperability. Although the NE and management systems support a granularity of 1, it is advised to provision a Port Priority with the new granularity of 16 in order to ensure interoperability.

Rapid spanning tree protocol (rSTP)

The rapid spanning tree protocol reduces the time that the standard spanning tree protocol needs to reconfigure after network failures. Instead of several tens of seconds, rSTP can reconfigure in less than a second. The actual reconfiguration time depends on several parameters, the two most prominent are the network size and complexity. IEEE802.1w describes the standard implementation for rSTP.

Specific attributes for TransLAN® STP enhancements:

- Failure Detection - Use SDH-layer failure detection to trigger STP reconfiguration.
- Convergence Time - Key aspects of the message-based IEEE 802.1w/D10 (rSTP) protocol instead of timer-based 802.1D (STP) protocol.
- Support larger network diameter by adjusting the “Maximum Age Timer” parameter and enhanced STP configuration controls and reports.
- Automatic mode detection - The rSTP is supported as an enhancement to STP, it cannot be enabled explicitly. It rather will operate by default and will fall back to STP as soon as it finds peer nodes that do not support rSTP. The STP mode that the bridge elected can be retrieved per port.
GARP VLAN Registration Protocol (GVRP)

Automatic configuration of VLANs

The GARP VLAN Registration Protocol (GVRP) is a protocol that simplifies VLAN assignment on network-role ports and ensures consistency among switches in a network. GVRP is supported only in the IEEE 802.1Q / IEEE 802.1ad VLAN tagging modes. In the transparent tagging modes (VPN tagging modes), a similar protocol, the proprietary spanning tree with VPN registration protocol (STVRP) is supported. STVRP is enabled per default and cannot be disabled.

By using GVRP, VLAN identifiers (VLAN IDs) only need to be provisioned on customer-role ports of access nodes. VLAN IDs on network-role ports of intermediate and access nodes are automatically configured by means of GVRP. The provisioned VLAN IDs on customer-role ports are called static VLAN entries; the VLANs assigned by GVRP are called dynamic VLAN entries. In addition, GVRP prevents unnecessary broadcasting of Ethernet frames by forwarding VLAN frames only to those parts of the network that have customer-role ports with that VLAN ID. Thus, the traffic of a VLAN is limited to the STP branches that are actually connecting the VLAN members.

Legend:

1. Static VLAN IDs need to be entered manually at customer-role ports.
2. Dynamic VLAN IDs of intermediate and access nodes are automatically configured.
3. No automatic configuration of VLAN IDs on ports towards those access nodes where the respective VLAN ID is not provisioned, i.e. no unnecessary broadcasting of Ethernet frames by forwarding VLAN frames only to those parts of the network that have customer-role ports with that VLAN ID.
Note that GVRP and the spanning tree protocol (STP) interact with each other. After a stable spanning tree is determined (at initialization or after a reconfiguration due to a failure) the GVRP protocol recomputes the best VLAN assignments on all network-role ports, given the new spanning tree topology.

GVRP can be enabled (default setting) or disabled per virtual switch. However, all virtual switches on an Ethernet network need to be in the same GVRP mode. For interworking flexibility one can optionally disable STP per network-role port; implicitly GVRP is then disabled as well on that port. GVRP must be disabled in order to interwork with nodes that do not support GVRP.

Max. number of VLANs

The maximum supported number of active VLANs (VLAN identifiers) is limited for reasons of controller performance, and varies depending on product, tagging mode and GVRP activation status. The following table shows the applicable values. Note that even if the maximum number of active VLANs is limited to 64, 247, or 1024, VLAN identifiers out of the full range of VLAN identifiers (0 … 4093) can be used for tagging purposes.

<table>
<thead>
<tr>
<th>Product</th>
<th>Transparent tagging (VPN tagging) mode</th>
<th>IEEE 802.1Q / IEEE 802.1ad tagging mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>GVRP enabled</td>
<td>GVRP disabled</td>
</tr>
<tr>
<td>1643 AM / 1643 AMS²</td>
<td>64 VLANs per card</td>
<td>64 VLANs per card</td>
</tr>
</tbody>
</table>

Notes:

1. No distinction is made with respect to the STVRP activation status, because STVRP is enabled per default and cannot be disabled.

2. An alarm (MACcVLANOVFW – Maximum number of VLAN instances exceeded) will be reported when the max. number of active VLANs per TransLAN® card is exceeded.

3. The LambdaUnite® MSS transparent tagging mode rather compares to the provider bridge tagging mode (see “IEEE 802.1ad VLAN tagging” (p. 8-77)) than to this transparent tagging (VPN tagging) mode.

A maximum of 5000 VLAN/port associations is supported per network element, except for the 1643 AM/1643 AMS, where the maximum number of VLAN/port associations is 2000. An alarm (MIBcVLANOVFW – Maximum number of VLAN instances exceeded in MIB) will be reported when the max. number of VLAN/port associations per network element is exceeded.
Ethernet over SDH applications

Purpose

This section gives an introduction to the possible TransLAN® Ethernet over SDH applications.

Types of applications

Layer-2 switching allows different types of applications, including:

- Ethernet point-to-point transport
- Ethernet point-to-point transport in buffered repeater mode
- Ethernet multipoint transport (dedicated bandwidth)
- Ethernet multipoint transport (shared bandwidth)
- Ethernet multiplexing (VLAN trunking)

TransLAN® supports all Ethernet transport solutions. Specific system configuration is required for each network application.

Direct interconnection of two LANs - Ethernet point-to-point transport

The most straight-forward Ethernet application on the TransLAN® equipment is a leased line type of service with dedicated bandwidth to interconnect two LAN segments which are at a distance that cannot be bridged by using a simple Ethernet repeater, because the collision domain size rules would be violated.

The two interconnected LANs need not be of the same speed; it is possible to interconnect a 10BASE-T and a 100BASE-T LAN this way for example.
Mode of operation

Ethernet point-to-point transport can be realized by using any of the TransLAN® operational modes. However, the preferred mode of operation for the direct interconnection of two LANs is the repeater mode.

Related information

Please also refer to “Repeater mode” (p. 8-66).
Ethernet multipoint transport with dedicated bandwidth

The following figure shows a network example of a multipoint Ethernet over SDH network with dedicated bandwidth:

This multipoint network is dedicated to a single user.

Mode of operation

Ethernet multi-point transport with dedicated bandwidth can be realized by using any of the following TransLAN® operational modes:

- LAN interconnect mode
- LAN-VPN mode
- LAN-VPN with QoS mode
- STP virtual switch mode compliant with IEEE 802.1Q
- STP virtual switch mode compliant with IEEE 802.1ad (provider bridge mode)
Related information

Please also refer to:

- “LAN-interconnect mode” (p. 8-68)
- “LAN-VPN (M-LAN) mode” (p. 8-70)
- “IEEE 802.1Q STP virtual switch mode” (p. 8-72)
- “Provider bridge mode” (p. 8-74)

Ethernet multipoint transport with shared bandwidth

The following figure shows a network example of a multipoint Ethernet over SDH network with shared bandwidth:

![Diagram of Ethernet multipoint transport with shared bandwidth](image-url)
The SDH capacity is shared among more than one customer in this multipoint network. This allows customer A to use the complete SDH bandwidth at the moment that customer B is inactive, and vice versa. As Ethernet traffic is inherently bursty, sharing bandwidth can increase the efficiency of the network usage.

Isolation of the traffic of different end-users can be accomplished by using transparent tagging or VLAN tagging (see “Tagging modes” (p. 8-75)), depending on the desired mode of operation.

**Mode of operation**

Ethernet multi-point transport with shared bandwidth can be realized by using any of the following TransLAN® operational modes:

- LAN-VPN mode
- LAN-VPN with QoS mode
- STP virtual switch mode compliant with IEEE 802.1Q
- STP virtual switch mode compliant with IEEE 802.1ad (provider bridge mode)

**Related information**

Please also refer to:

- “LAN-VPN (M-LAN) mode” (p. 8-70)
- “IEEE 802.1Q STP virtual switch mode” (p. 8-72)
- “Provider bridge mode” (p. 8-74)

**VLAN trunking**

Trunking applications are a special case of Ethernet multipoint transport, either with dedicated or shared bandwidth.

Trunking applications are those applications where traffic of multiple end-users is handed-off via a single physical Ethernet interface to a router or switch for further processing. This scenario is also called “back-hauling”, since all traffic is transported to a central location, for example, a point-of-presence (PoP) of a service provider.

Trunking applications can be classified into two topology types:

- Trunking in the hub-node
- Distributed aggregation in the access network

Common to both topology types is that the Ethernet traffic of multiple LANs is aggregated on one or a few well filled Ethernet interfaces, the trunking LAN interface(s). Thus, the Ethernet traffic of multiple end-users can be made available to a service provider at a central location via a limited number of physical connections. Without VLAN trunking, each end-user would need to be connected to the service provider equipment via his own Ethernet interface.
Trunking applications include the aggregation of Ethernet traffic of a single end-user as well as the aggregation of Ethernet traffic of multiple different end-users. Isolation of the traffic of different end-users can be accomplished by using transparent tagging or VLAN tagging (see “Tagging modes” (p. 8-75)), depending on the desired mode of operation.

A typical TransLAN® trunking application would be a configuration where many E/FE access nodes are combined with a trunking GbE hub node (cf. “Distributed aggregation in the access network” (p. 8-62)).

**Trunking in the hub node**

This figure shows an example of VLAN trunking in the hub node:

Each access node is individually connected to the hub node over a single SDH connection (or even one SDH connection per LAN port). The trunking LAN interface is a network-role LAN port. The VLAN tags in the Ethernet frames are preserved, i.e. made available to the service provider, and can thus be used for further processing.

A high WAN port density is required in the hub-node.

Averaging of the peak traffic loads of each access node (or LAN port) is not used. Each SDH link bandwidth has to be engineered for the corresponding amount of peak traffic.
Distributed aggregation in the access network

This figure shows an example of distributed aggregation in the access network:

The SDH bandwidth can be shared by many end-users, which allows to gain from the statistical effects in the traffic offered by each end-user (“statistical multiplexing”). Thus, the distributed aggregation in the access network configuration is more bandwidth efficient than the trunking in the hub node topology.

Another difference is that in the trunking in the hub-node topology, the hub node has to support many WAN ports, which is not the case in the distributed aggregation in the access network configuration.

A certain bandwidth allocation fairness can be guaranteed by applying ingress rate control in the access nodes. Please note that ingress rate control is not supported on GbE TransLAN® cards but only on E/FE TransLAN® cards.
Mode of operation

Trunking applications can be realized by using any of the following TransLAN® operational modes:

- LAN interconnect mode (dedicated bandwidth only)
- LAN-VPN mode
- LAN-VPN with QoS mode
- STP virtual switch mode compliant with IEEE 802.1Q
- STP virtual switch mode compliant with IEEE 802.1ad (provider bridge mode)

Related information

Please also refer to:

- “LAN-interconnect mode” (p. 8-68)
- “LAN-VPN (M-LAN) mode” (p. 8-70)
- “IEEE 802.1Q STP virtual switch mode” (p. 8-72)
- “Provider bridge mode” (p. 8-74)
Operational modes

Overview of operational modes

These TransLAN® operational modes exist:

- Repeater mode
- Proprietary VPN modes:
  - LAN interconnect mode
  - Multipoint LAN bridging mode ("LAN-VPN mode", "MLAN mode")
  - Multipoint LAN bridging mode enhanced with IEEE 802.1p QoS functions ("LAN-VPN with QoS", "MLAN_QoS mode")
- Standard compliant IEEE modes:
  - STP virtual switch mode compliant with IEEE 802.1Q
  - STP virtual switch mode compliant with IEEE 802.1ad ("Provider bridge mode")

Virtual Switch operation mode

When the transparent tagging mode has been selected on the Ethernet Interface extension card (LAN unit) level, a different Virtual Switch operational mode must be chosen per Virtual Switch. The Virtual Switch can be configured in the following operation modes:

- Repeater
- LAN-interconnect
- LAN-VPN (MLAN)
- LAN-VPN (MLAN) with QoS.

When the IEE802.1Q/IEEE 802.1a tagging mode has been selected, the operation mode of the Virtual Switch is always Spanning Tree.

The physical Layer 2 (L2) switch that is present on an Ethernet LAN tributary board can be split into several logical or virtual switches. A Virtual Switch is a set of LAN/WAN ports on an Ethernet LAN tributary board that are used by different VLAN's which can share the common WAN bandwidth. Each of the virtual switches can operate in a specific Virtual Switch mode depending on the VLAN tagging scheme, and each Virtual Switch mode allows specific LAN-WAN port associations as explained in the following paragraphs.

First the VLAN tagging mode has to be specified on LAN unit level, this can be either IEEE 802.1Q/IEEE 802.1ad VLAN tagging or VPN (transparent) tagging. In VPN tagging mode, end-user VLAN tags that optionally may appear in the end user traffic are ignored in the forwarding process. These VLAN tags are carried transparently through the "TransLAN Network". In VLAN-tagging mode, the VLAN tags are also carried
transparency, but the VLAN ID in the VLAN tags is used in the forwarding decision. Therefore customers' VLAN IDs may not overlap on a physical Ethernet switch, the VLAN IDs must be unique per switch pack. (FEP 1_188_14221)

After having provisioned the tagging mode, per virtual switch a different Virtual Switch operational mode may be chosen. The Ethernet LAN tributary board supports either the Repeater mode, LAN-Interconnect, LAN-VPN, and Spanning Tree Protocol Virtual Switch mode of operation. IEEE 802.1D MAC forwarding and address filtering, multi-point bridging, and spanning tree protocol (STP) are supported under all modes of operation, except the Repeater mode.

The following table gives an overview of the different modes and a list of the corresponding supported functionality:

<table>
<thead>
<tr>
<th>VLAN Tagging Mode</th>
<th>Virtual Switch Mode</th>
<th>Ethertype/TPID</th>
<th>QoS_CQs (Quality of Service - Classification Queueing Scheduling)</th>
<th>Dynamic VLAN Registration Protocol</th>
<th>Spanning Tree Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN Tagging</td>
<td>Repeater</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>No STP</td>
</tr>
<tr>
<td></td>
<td>LAN Interconnect (Dedicated Bandwidth)</td>
<td>N/A</td>
<td>N/A</td>
<td>STVRP</td>
<td>Multiple STP</td>
</tr>
<tr>
<td></td>
<td>LAN-VPN (Shared Bandwidth)</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEEE 802.1Q/IEEE 802.1ad VLAN tagging</td>
<td>Spanning Tree Switched Network</td>
<td>600 ... FFFF, except for 8100 enabled</td>
<td>disabled GVRP</td>
<td>Single STP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Repeater</td>
<td>600 ... FFFF, except for 8100 enabled</td>
<td>N/A</td>
<td>No STP</td>
<td></td>
</tr>
</tbody>
</table>

Interoperability of operational modes

Virtual Switches that are configured in the same operational mode can interwork. Virtual Switches not configured in the same operational mode do not interwork in all cases. If a Virtual Switch is configured in the “Repeater” mode or the “STP Switch” mode, it can only interwork with Virtual Switches that are configured in the same mode.

Interworking between a remote LAN-interconnect virtual switch and a VPN virtual switch is not prohibited, because the LAN-interconnect mode can be seen as a special case of the VPN mode.
VPN tagging mode

VPN tagging is used to identify user frames in the LAN interconnect, LAN-VPN or LAN-VPN with QoS mode of operation. VPN tagging is often also referred to as “transparent tagging”.

VPN tagging is characterized as follows:

- Selecting the VPN tagging mode implies that the port role of the ports is fixed. LAN ports are always customer role ports, and WAN ports are always network role ports (see “Flexible port role assignment” (p. 8-85)).
- VPN tagging is a double tagging mode. This means that a customer identifier (CID tag) is inserted into each frame at each network ingress LAN port. User frames that are already tagged become double tagged. The CID tag is removed from the frame at each network egress LAN port.
- Ports forward only those frames that have a CID tag which “belongs” to that port (i.e. which has previously been provisioned on that port).

In the VPN tagging mode, the term “LAN group” is synonymously used to the term “virtual switch”.

Configuration rules and guidelines

Please observe these configuration rules and guidelines:

- Be aware that the port role of the LAN and WAN ports is fixed (see above):
  - LAN ports are always customer role ports.
  - WAN ports are always network role ports.
- On LAN ports the CID needs to be provisioned *manually*.
- The CID provisioned on each LAN port must be *unique* within a shared WAN to create a fully independent VPN.

The VPN provisioning on the WAN ports is done automatically by means of the proprietary spanning tree with VPN registration protocol (STVRP).

Repeater mode

A virtual switch in repeater mode consists of exactly one LAN port and one WAN port in a fix 1:1 relationship. All Ethernet frames entering the virtual switch at a LAN port are transparently forwarded to the corresponding WAN port and transported over the network with the specific limitation for X4IP described in chapter “Provisioning a virtual switch in repeater (promiscuous) mode” (p. 8-113). None of the standard IEEE Std 802.1D/Q processes (MAC address learning, MAC frames forwarding, and filtering, VLAN classification, and filtering) applies. Received frames are relayed to the other port of the virtual switch, irrespective of their format or contents.
The WAN port that supports the Repeater mode requires the provisioning of the following parameters:

- WAN port capacity (require manual provisioning) at 2, 4, 6, 8, 10, 50 or 100 Mbit/s
- association of the WAN port to a LAN port
- create cross-connections between VC-X and TU-X (where X=12 or 3).

The following figure shows the network element configured in the Repeater operation mode.

A virtual switch in repeater mode emulates an Ethernet repeater except that it
- breaks-up the collision domains,
- removes the length limitation of CSMA/CD LANs, and
- also works in full-duplex mode.

**Synonyms**

The TransLAN® repeater mode of operation is often also referred to as “promiscuous mode” or “buffered repeater mode”.

**Intended use**

The repeater mode is only intended to be used in point-to-point configurations to offer a leased-lines type of service. The repeater mode is supported by E/FE as well as GbE TransLAN® cards.
**Configuration rules and guidelines**

Please observe these configuration rules and guidelines:

- The use of the repeater mode is limited to virtual switches consisting of exactly *one customer LAN port* and *one network WAN port*. Only point-to-point connections are supported.
- *No* customer identifier (CID) can be configured.
- It is *not* possible to provision QoS functions.
- Flow control can be enabled or disabled per LAN port.
- *No* WAN port configurations are possible.
- When a virtual switch is switched from any of the other operational modes into repeater mode, then all VLAN and QoS configuration information will be reset. When the virtual switch is switched back again into the previous mode, then these configuration settings will *not* become operational again but must be provisioned again.

The Ethernet packets are carried across the SDH network in a channel. Each channel comprises up to 63 VC12 or up to 2 VC3 concatenated. These VC12s and VC3s behave in the same way as normal SDH VC12s from an E1 port or SDH VC3s from an E3 port. There is some buffering in the NE, but it is still possible to lose packets because the channel bandwidth can be less than the Ethernet traffic rate.

**LAN-interconnect mode**

The LAN-interconnect mode of operation offers dedicated WAN bandwidth to a single end-user. Under the LAN-interconnect mode of operation, a Virtual Switch must only contain LAN ports with the same CID (Customer ID) to ensure the entire WAN port bandwidth allocated for the group is dedicated to a single end-user. Any combination of LAN- and WAN-ports is allowed, but with a minimum of two ports to be meaningful.
The following figure shows the network element configured in the LAN-interconnect operation mode.
The Ethernet packets are carried across the SDH network in a channel. Each channel comprises up to 63 VC12 or up to 2 VC3 concatenated. These VC12s or VC3s behave in the same way as normal SDH VC12s from an E1 port respectively normal SDH VC3s from an E3 port.

This operation mode supports the following features:

- Learning bridges
- Spanning tree
- Additional SDH bandwidth
- Virtual Switch and
- CID (Customer Identifier).

**Special case of the LAN-VPN mode**

The LAN interconnect mode of operation is a special case of the LAN-VPN operation. In the LAN interconnect mode a virtual switch may contain LAN and WAN ports of a single user only.

The TransLAN® cards can support both modes of operation simultaneously as long as the corresponding virtual switches do not include the same WAN ports.

**Configuration rules and guidelines**

Please observe these configuration rules and guidelines:

- On LAN ports the CID needs to be provisioned manually.
  
  The permitted CID value range is [0 … 4093]. However, note that only values out of the value range [1 … 4093] can be used to identify a user while the value “0” cannot. The corresponding LAN port is disabled if the CID is set to “0”.

- In the LAN interconnect mode, the virtual switch is dedicated to a single customer. Therefore, all LAN ports of a virtual switch must have the same customer identifier (CID).

- In the LAN interconnect mode, LAN ports are always customer-role ports, and WAN ports are always network-role ports (see “Port provisioning” (p. 8-84)).

**LAN-VPN (M-LAN) mode**

Under the LAN-VPN (Virtual Private Network) operation mode, a number of LAN- and WAN ports are grouped together to form one virtual switch. The Virtual Switch contains LAN ports of multiple end-users sharing the same WAN port(s) bandwidth. To safeguard each individual end-user's data flow and to identify an end-user's VPN from the shared WAN, the Ethernet Interface card assigns a CID to each LAN port within a Virtual Switch. The CID of each end-user (or LAN port) must be unique within a shared WAN port to create a fully independent VPN. The VPN provisioning on the WAN ports on the access and intermediate nodes is done automatically by the proprietary protocol STVRP (Spanning Tree with VPN Registration Protocol) that runs without operator intervention.
The end-users are assigned bandwidth by the operator. It allows multiple end-users to share the same SDH WAN bandwidth with each end-user being allocated a sub-VC-12-Xv (X= 1, 2, 3, 4, 5) or sub-VC-3-Xv (X=1, 2) rate of bandwidth when using the Fast Ethernet card and sub-VC-4-Xv (X=1, 2,...7) or sub-VC-3-Xv (X=1, 2) when using the Gigabit Ethernet card. The combined end-user bandwidth is then mapped to the SDH time-slots and transported in the SDH network as a single data load. The minimum rate that can be configured per end-user at a LAN port is 150 kbit/s. The operator also specifies a traffic policy for each end-user.

The LAN-VPN operation mode controls the shared bandwidth by making use of the following features:

- Learning bridges
- Spanning tree
- V-LAN (Virtual-LAN)
- CID (Customer Identifier)
- Assigned bandwidth policy (CIR = Committed Information Rate and PIR = Peak Information Rate)
- Additional SDH bandwidth and SDH WAN bandwidth sharing
- Traffic policy (Strict policing/Oversubscription).

The following figure shows the network element configured in the LAN-VPN operation mode.
IEEE 802.1Q STP virtual switch mode

The IEEE 802.1Q/IEEE 802.1ad VLAN tagging scheme can be seen as an extension of the LAN-VPN mode, providing more flexibility in defining the VPN’s and in general leading to a more efficient use of bandwidth. In IEEE 802.1Q VLAN tagging mode, a virtual switch is formed by a combination of LAN- and WAN ports on a physical switch that is used by different VLAN’s which can share the common WAN bandwidth. Each port can be part of only one virtual switch, but a certain port may be associated with more than one VLAN. The ports that are associated with a certain VLAN ID form the VLAN Port Member Set.

On ingress, each packet is filtered on its VLAN ID. If the receiving port is a member of the VLAN to which a received MAC frame is classified, then the frame is forwarded. The user can provision whether untagged packets are dropped, or tagged with a PVID (Port VLAN ID), via the acceptable frame type parameter.

Example VLAN trunking

The VLAN trunking example shown in the next figure is one of the possible applications in this operation mode.
VLAN IDs assigned to LAN Ports should not overlap in case the operator wants to ensure Layer-2 security between those LAN Ports (in many applications, LAN Ports are likely to be dedicated to one customer). It is the responsibility of the operator to define appropriately non-overlapping VLAN IDs on all the created virtual switches.

Also the provisioned PVID, with which untagged incoming frames are tagged, should not overlap with any VLAN ID on the virtual switch of which the customers’ port is part (again, this is the responsibility of the operator). Manual provisioning of intermediate nodes can be cumbersome and difficult. Therefore it is recommended to use the auto-provisioning mode for VLAN ID's on the intermediate nodes. A protocol named GVRP (GARP VLAN Registration Protocol) provides this functionality. GVRP is an application of the Generic Attribute Registration Protocol (GARP) application, which runs on top of the active spanning tree topology.

IEEE 802.1Q defines two kinds of VLAN registration entries in the Bridge Filtering Database: static and dynamic entries. In the TransLAN® implementation, static entries need to be provisioned on access node LAN ports only. GVRP will take care of configuring dynamic entries on the WAN ports of intermediate and access nodes.

A spanning tree per virtual switch is implemented. If the user wants the traffic to be protected by the spanning tree protocol and uses the manual-provisioning mode, he must make sure that the WAN ports in the alternative path also will have the corresponding VLAN IDs assigned. E.g. in a ring topology, all NE's in the ring must be provisioned with this VLAN ID. In automatic mode, the GVRP protocol will take care of the dynamic VLAN ID provisioning. The user has the possibility to flush dynamic VLAN's, thus remove dynamic VLAN's that are no longer used.

Only independent VLAN learning is supported. This means, if a given MAC address is learned in a VLAN, the learned information is used in forwarding decisions taken for that address only relative to that VLAN.

For the IEEE 802.1Q VLAN tagging mode, the oversubscription mode is not supported (cf. “Quality of Service (QoS) overview” (p. 8-90)).

**Configurable spanning tree parameters**

Even though the management system is an SDH network element manager, the data networking problems still need to be addressed when managing network elements carrying Ethernet traffic. As such the following parameters are visible/provisionable per virtual switch.

- bridge address
- bridge priority
- root cost
- root port
- port priority
- bridge priority
Provider bridge mode

The provider bridge mode, a double tagging mode with provisionable TPID ("Ethertype"), is— from a functional point of view— comparable to the LAN-VPN mode with the chief difference that the provider bridge mode is compliant to the IEEE 802.1ad standard while the VPN modes are Alcatel-Lucent proprietary modes, and that the provider bridge mode supports Quality of Service features while the LAN-VPN mode does not.

Traffic is forwarded based on the destination MAC address and the outer VLAN tag (S-tag).

As in the IEEE 802.1Q STP virtual switch mode, a virtual switch in the provider bridge mode is a set of LAN/WAN ports on a physical switch that are used by different VLANs which can share the common WAN bandwidth. VLANs in the same virtual switch are defined by their VLAN port member set. An instance of the spanning tree protocol runs on the WAN ports for each virtual switch.

The LAN ports and WAN ports can be configured to be customer-role or network-role ports (see “Flexible port role assignment” (p. 8-85)).

In the provider bridge mode, the IEEE 802.1ad VLAN tagging mode is used (see “IEEE 802.1ad VLAN tagging” (p. 8-77)).
Tagging modes

Overview

Sharing transport channels between multiple users requires the identification of MAC frames. Tagging is the process of attaching an identifier, a “tag”, to a MAC frame in order to identify the user to which the frame pertains.

These tagging modes are supported:

- **Transparent** tagging ("VPN tagging")
- **IEEE 802.1Q/IEEE 802.1ad VLAN tagging**
  - VLAN tagging compliant with IEEE 802.1Q-1998 ("IEEE 802.1Q VLAN tagging")
  - VLAN tagging compliant with IEEE 802.1ad ("IEEE 802.1ad VLAN tagging", "Provider bridge tagging mode")

The different tagging modes are explained later-on in this section.

**Important!** Note that it is not possible to use different tagging modes at the same time on the same TransLAN® card.

However, within the transparent tagging mode there can be virtual switches in the repeater mode, LAN interconnect mode, or LAN-VPN mode (with or without IEEE 802.1p QoS) at the same time on the same physical switch.

**Transparent tagging**

Transparent tagging (or “VPN tagging”) is a double tagging mode used to identify end-user frames in the LAN interconnect, LAN-VPN or LAN-VPN with QoS mode of operation.

Selecting the transparent tagging mode implicitly means that the port role of the ports is fixed. LAN ports are always customer-role ports, and WAN ports are always network-role ports (see “Flexible port role assignment” (p. 8-85)).

To enable bandwidth sharing, a customer identification (CID) is associated with every LAN port. This CID is inserted into incoming Ethernet frames, in an extra tag. MAC address filtering and learning is done independently for every CID.

Ethernet frames that are already tagged become double tagged. Already present end-user VLAN tags remain unused in the transparent tagging mode, i.e. every VLAN tag is transmitted transparently through the SDH network.

Outgoing frames are only transmitted on LAN ports which have the respective CID associated. The extra tag is removed before the Ethernet frames are forwarded to an external LAN.
Note that in the VPN tagging mode the term “LAN group” is synonymously used to the term “virtual switch”.

### Configuration rules and guidelines

Please observe these configuration rules and guidelines:

- The port role of the LAN and WAN ports is fixed in the operational modes that make use of the VPN tagging mode (see above):
  - LAN ports are always customer role ports.
  - WAN ports are always network role ports.
- On LAN ports the CID needs to be provisioned *manually*.
- The CID provisioned on each LAN port must be *unique* within a shared WAN to create a fully independent VPN.

The VPN provisioning on the WAN ports is done automatically by means of the proprietary spanning tree with VPN registration protocol (STVRP).

**Important!** Changing the tagging mode from transparent tagging to IEEE 802.1Q/IEEE 802.1ad VLAN tagging or vice versa is traffic affecting! Furthermore, most objects provisioned in one mode will be deleted or reset to default - except the LAN group / virtual switch infrastructure - when switching to the other mode.

### IEEE 802.1Q VLAN tagging

IEEE 802.1Q VLAN tagging is used to identify end-user frames in the STP virtual switch mode compliant with IEEE 802.1Q.

These are the IEEE 802.1Q VLAN tagging rules:

- On end-user LAN interfaces:
  - At each network ingress port, untagged user frames are tagged with a default identifier, the port VLAN identifier (PVID) which is removed from the frame at the network egress port.
    
    Already tagged frames are forwarded if their VLAN identifier is in the port's static or dynamic list of VLAN IDs, i.e. if the port belongs to the configured port member set for that VLAN ID. The static VLAN ID list is configurable. The dynamic VLAN ID list is automatically generated by making use of the GARP VLAN Registration Protocol (GVRP).
  - At each network egress port, the port VLAN identifier (PVID) is removed from previously untagged frames that were tagged with the PVID at the ingress port. VLAN tagged frames are forwarded if the port belongs to the configured port member set for the respective VLAN ID.

- On trunking LAN interfaces, *all* tagged frames are forwarded in both directions. Untagged frames are discarded (dropped).
- The end-customer VLAN tag sets have to be disjunct.
IEEE 802.1ad VLAN tagging

The IEEE 802.1ad VLAN tagging mode (“provider bridge tagging mode”) is a double tagging mode with provisionable Ethertype (TPID), used to identify end-user frames in the STP virtual switch mode compliant with IEEE 802.1ad (“provider bridge mode”).

At each customer role port, a provider bridge tag carrying a customer identifier (CID) is inserted into each Ethernet frame in the ingress direction, and removed from the frame in the reverse direction. Frames that are already tagged become double tagged. The IEEE 802.1ad VLAN tagging mechanism is transparent to the end-customer. VPNs on transit nodes (no customer LAN port) are automatically instantiated by means of the standard GVRP protocol which optionally can be disabled.

The value of the Ethertype (TPID) can be flexibly chosen. However, some values are reserved for specific purposes, for example:

- 0x0800 for IP
- 0x0806 for ARP
- 0x8847 for MPLS
- 0x8100 is not selectable because this is the default value for the STP virtual switch mode compliant with IEEE 802.1Q.

The recommended value for the Ethertype in the provider bridge tagging mode is 0x9100.

Configuration rules and guidelines

Please observe these configuration rules and guidelines:

- The provider bridge mode can be configured by selecting the IEEE 802.1Q / IEEE 802.1ad tagging mode in combination with provisioning an Ethertype in the range 0x0601 ... 0xFFFF, but unequal to 0x8100. Provisioning the value 0x8100 for the Ethertype results in the selection of the STP virtual switch mode compliant with IEEE 802.1Q.

  The recommended value for the Ethertype in the provider bridge tagging mode is 0x9100. Please also observe the reserved values as given above.

- The customer identification (CID) can be configured in the range [1 … 4093].

  Important! Changing the tagging mode is traffic affecting!

Furthermore, most objects provisioned in one mode will be deleted or reset to default - except the LAN group / virtual switch infrastructure - when switching to a different mode.
Tagged MAC frame

The following figure illustrates the structure of the MAC frame in different tagging modes as well as the structure of the respective tags.

IEEE 802.1Q VLAN tagging mode

- Destination address: 6 bytes
- Source address: 6 bytes
- VLAN tag (C-tag): 4 bytes
- Length/Type: 2 bytes
- Payload: 46-1500 bytes
- FCS: 4 bytes

VPN tagging mode / IEEE 802.1ad VLAN tagging mode

- Destination address: 6 bytes
- Source address: 6 bytes
- CID-tag (S-tag): 4 bytes
- VLAN tag (C-tag): 4 bytes
- Length/Type: 2 bytes
- Payload: 46-1500 bytes
- FCS: 4 bytes
Legend:

TPID  Tag protocol identifier ("Ethertype") - indicates the presence of a VLAN tag (or CID tag, respectively). Furthermore, it indicates that the length/type field can be found at a different position in the frame (moved by 4 bytes).

UP (3 bits)  User priority - “0” (low priority) … “7” (high priority).

CFI (1 bit)  Canonical Format Identifier - indicates the presence or absence of routing information.

ID (12 bits)  Identification - customer identification which can be configured in the range [0 … 4093].

Concerning their structure there is no difference between a VLAN tag (C-tag) and a CID tag (S-tag). A distinction between both types of tags can be made by means of the value in the TPID field, the “Ethertype”. In the IEEE 802.1ad VLAN tagging mode (provider bridge tagging mode), the Ethertype can be provisioned per virtual switch.

The value of the Ethertype depends on the mode of operation:

- In the transparent tagging modes (VPN tagging modes), the value of the Ethertype is 0xFFFF, and cannot be changed.
- In the IEEE 802.1Q VLAN tagging mode, the value of the Ethertype is 0x8100, and cannot be changed.
- In the IEEE 802.1ad VLAN tagging mode (provider bridge tagging mode), the value of the Ethertype can be flexibly chosen in the range 0x0601 … 0xFFFF, but unequal to 0x8100. The recommended value for the Ethertype in the provider bridge tagging mode is 0x9100.
Comparison of different tagging schemes

The next figure summarizes the possible tagging schemes:

- No tagging
- Single tagging (IEEE 802.1Q VLAN tagging)
- Double tagging (VPN tagging, IEEE 802.1ad VLAN tagging)
**Ethernet mapping schemes**

**Introduction**

1643 AM and 1643 AMS support the following schemes for the mapping of Ethernet packets into SDH frames:

- Link Access Procedure SDH (LAPS encapsulation)
- Ethernet over SDH (EoS encapsulation)
- Generic Framing Procedure (GFP encapsulation)

**LAPS encapsulation**

LAPS encapsulation is implemented according to ITU-T X.86. It is supported when using the option card X8PL.

**EoS encapsulation**

EoS encapsulation is implemented according to T1X1.5/99-268. It is supported when using the option card X4IP-V2 or X5IP.

**GFP encapsulation**

GFP encapsulation is implemented according to T1X1.5/2000-147. It is supported when using the option cards X8PL or X4IP-V2 or X5IP.

GFP provides a generic mechanism to adapt traffic from higher-layer client signals over a transport network.

The following GFP encapsulation are possible:

- Mapping of Ethernet MAC frames into Lower Order SDH VC12–Xv
- Mapping of Ethernet MAC frames into Lower Order SDH VC3–Xv

**TUG structure**

For X8PL, it is possible to set the TUG structure of the VC4 that runs to the option board. The TUG structure determines what VC12s/VC3s are available for assignment to a VCG. The method of setting the bandwidth of a VCG has also been modified. For X8PL it is not possible to modify the bandwidth parameter of a VCG. Instead VC12s/VC3 have to be allocated to a certain VCG, the total combined bandwidth of the allocated VCs is reflected in the bandwidth parameter of the VCG.

The TUG structure of the VC4 running to the option board also determines the possible cross-connections to the X8PL unit.
**VC12-Xv GFP encapsulation**

The 1643 AM and 1643 AMS support virtual concatenation of Lower Order SDH VC-12 as inverse multiplexing technique to size the bandwidth of a single internal WAN port for transport of encapsulated Ethernet and Fast Ethernet packets over the SDH/SONET network. This is noted VC12-Xv, where X = 1...5 when using the X4IP-V2 option card and X = 1...63 when using the X8PL option card. Usage is in conformance with ITU-T G.707 Clause 11 (2000 Edition) and G.783 Clause 12.5 (2000).

Additionally, the use of G.707 Extended Signal Label is supported using V5 (bits 5-7) field.

**VC3-Xv GFP encapsulation**

The 1643 AM and 1643 AMS support virtual concatenation of Lower Order SDH VC-3 as inverse multiplexing technique to size the bandwidth of a single internal WAN port for transport of encapsulated Ethernet and Fast Ethernet packets over the SDH/SONET network. This is noted VC3–Xv, where X = 1,2 (SDH). *For X8PL also VC3-3v is supported.* Usage is in conformance with ITU-T G.707 Clause 11 (2000 Edition) and G.783 Clause 12.5 (2000) and T1X1 T1.105 Clause 7.3.2 (2001 Edition).
Overview

Purpose

This chapter contains provisioning information as well as specific engineering rules and guidelines.

Contents

<table>
<thead>
<tr>
<th>Port provisioning</th>
<th>8-84</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quality of Service (QoS) overview</td>
<td>8-90</td>
</tr>
<tr>
<td>Classification, queueing, and scheduling</td>
<td>8-94</td>
</tr>
<tr>
<td>Quality of Service provisioning</td>
<td>8-103</td>
</tr>
<tr>
<td>Performance monitoring</td>
<td>8-105</td>
</tr>
</tbody>
</table>
Port provisioning

**Customer-role and network-role ports**

The user can assign a so-called “port role” to WAN ports as well as to LAN ports. In this way it is possible to forward VLAN tags, especially in double-tagging mode, also via LAN ports. Additionally it is possible to run the STP and GVRP protocols on physical LAN ports, too.

Each LAN port or WAN port can have one of the following port roles:

<table>
<thead>
<tr>
<th>Port role</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Customer role** | Customer-role ports are usually located at the edge of the switched TransLAN® network boundary, providing the Ethernet interface to the end-customer. Ethernet frames may be but need not necessarily to be tagged.  

In the majority of cases, LAN ports are customer-role ports. However, two LAN ports connected via an Ethernet LAN link would be an example of network-role LAN ports. Another example would be a trunking LAN port connected via an Ethernet LAN link to an ISP router (where VLAN tags are needed for further processing). |
| **Network role** | Network-role ports usually interconnect the nodes that make up the TransLAN® network. Ethernet frames need to be tagged.  

In the majority of cases, WAN ports are network-role ports. However, a WAN port which is connected to an Ethernet private line unit (EPL unit), thus extending the switched TransLAN® network boundary, would be an example of a customer-role WAN port. |
The following figure serves to visualize the concept of customer-role and network-role ports.

Flexible port role assignment

In most cases physical LAN ports have the customer role and physical WAN ports have the network role, but there may be exceptions in some applications. In the following figure the WAN port connects an EPL link and is therefore at the edge of the TransLAN® network. Thus it has the customer role in this case.
In the example in the figure below the VLAN tags have to be forwarded to a router. The router uses the tagging information for its switch decisions. Additionally the LAN port must fulfill a network role. In this case it behaves like a node of the TransLAN® network. It could also participate in the STP in order to avoid loops, if there was another link from a Router LAN interface to a second node within the TransLAN® network.

A LAN port which operates in the “network role” behaves like a WAN port in terms of VLAN tagging, STP, and GVRP.

The default settings are shown in the following table

<table>
<thead>
<tr>
<th>Port role</th>
<th>LAN port</th>
<th>WAN port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer role</td>
<td>default</td>
<td></td>
</tr>
<tr>
<td>Network role</td>
<td>default</td>
<td></td>
</tr>
</tbody>
</table>

In the IEEE 802.1Q STP virtual switch mode and in the provider bridge mode, the port role of each LAN and WAN port can be flexibly assigned. Each LAN or WAN port can be configured to be either a customer-role or network-role port.
These are the characteristics of customer-role and network-role ports:

<table>
<thead>
<tr>
<th>Customer-role port</th>
<th>Network-role port</th>
</tr>
</thead>
<tbody>
<tr>
<td>In the IEEE 802.1Q STP virtual switch mode:</td>
<td>No tagging or untagging operations are performed.</td>
</tr>
<tr>
<td>In the ingress direction, untagged Ethernet frames are tagged with a default identifier, the port VLAN identifier (PVID). The PVID is removed from each frame at each network egress port. See also: “IEEE 802.1Q VLAN tagging” (p. 8-76)</td>
<td></td>
</tr>
<tr>
<td>In the provider bridge mode:</td>
<td>The spanning tree protocol (STP) can be enabled (default setting) or disabled.</td>
</tr>
<tr>
<td>A provider bridge tag carrying a customer identifier (CID) is inserted into each Ethernet frame in the ingress direction, and removed from the frame in the reverse direction. Frames that are already tagged become double tagged. See also: “IEEE 802.1ad VLAN tagging” (p. 8-77)</td>
<td>GVRP can be enabled (default setting) or disabled. Dynamic VLAN IDs or CIDs of intermediate and access nodes are automatically configured if GVRP is enabled.</td>
</tr>
<tr>
<td>The spanning tree protocol (STP) is not supported.</td>
<td>GVRP is not supported. VLAN IDs or CIDs need to be configured manually.</td>
</tr>
<tr>
<td>Ingress rate control exists at “UNI” and “E-NNI” ports only (see “Quality of Service (QoS) overview” (p. 8-90)).</td>
<td>Ingress rate control exists at “UNI” and “E-NNI” ports only (see “Quality of Service (QoS) overview” (p. 8-90)).</td>
</tr>
<tr>
<td></td>
<td>There is no rate control on “I-NNI” ports. The traffic class encoded in the p1 and p2 bits of the incoming frames is evaluated and transparently passed through.</td>
</tr>
</tbody>
</table>

**Fix port-role assignment in the VPN tagging modes**

In all the operational modes relying on the VPN tagging mode (see “Transparent tagging” (p. 8-75)) the port role is fixed:

- LAN ports are *always* customer role ports.
- WAN ports are *always* network role ports.

*This port-role assignment in the VPN tagging modes cannot be changed.* Corresponding provisioning options that might be available on the graphical user interfaces of the management systems do not apply to the VPN tagging modes and are blocked.
Repeater mode

In the repeater mode, there is no necessity to distinguish between customer-role and network-role ports, because the repeater mode can only be used in point-to-point configurations, and there is:

- no tagging mechanism,
- no spanning tree, and
- no GVRP or STVRP.

In the repeater mode, there is simply a LAN port and a WAN port. The LAN port provides the connection to the end-customer LAN, and the WAN port provides the connection to the SDH transport network (see “Repeater mode” (p. 8-66)).

Example

As an example, the following figure shows a possible network application:

Legend:

- UNI port  User-Network-Interface (always a customer-role port)
- I-NNI port  Internal Network-Network Interface (always a network-role port)
E-NNI port  External Network-Network Interface (here a trunking network-role port)
Quality of Service (QoS) overview

Introduction

Quality of service (QoS) control allows to differentiate between Ethernet frames with different priorities. If traffic with a high priority and traffic with a low priority compete for SDH capacity, the traffic with the high priority should be served first. This can be realized through quality of service control.

QoS control is supported on the E/FE and Gigabit Ethernet cards, in the IEEE 802.1Q VLAN tagging mode and the IEEE 802.1ad VLAN tagging mode (provider bridge mode). QoS control is implemented as a DiffServ architecture applied to layer 2 (in accordance with IETF recommendations on Differentiated Services, cf. www.ietf.org).
Flow classification, queueing, and scheduling

The following figure provides an overview of the QoS control:

### Quality of Service configuration options

The following table gives an overview of the QoS provisioning options depending on the configured mode of operation.
### Mode of operation

<table>
<thead>
<tr>
<th>Mode of operation</th>
<th>Ethertype (hex. value)</th>
<th>QoS CQS</th>
<th>QoS_osub</th>
<th>Ingress rate control</th>
<th>HoL blocking prevention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repeater mode</td>
<td>–</td>
<td>[disabled]</td>
<td>[disabled]</td>
<td>[none]</td>
<td>[disabled]</td>
</tr>
<tr>
<td>VPN mode</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LAN interconnect</td>
<td>0xFFFF</td>
<td>[disabled]</td>
<td>[disabled]</td>
<td>[none]</td>
<td>[disabled]</td>
</tr>
<tr>
<td>LAN-VPN</td>
<td>0xFFFF</td>
<td>[disabled]</td>
<td>[enabled]</td>
<td>strict policing</td>
<td>[enabled]</td>
</tr>
<tr>
<td>LAN-VPN with QoS</td>
<td>This mode of operation was supported in previous releases. However, it is no longer supported in the 1643 AM Release 1.0 through 7.2</td>
<td></td>
<td></td>
<td>oversubscription</td>
<td></td>
</tr>
<tr>
<td>IEEE mode</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>STP virtual switch mode compliant with IEEE 802.1Q</td>
<td>0x8100</td>
<td>[enabled]</td>
<td>disabled</td>
<td>strict policing</td>
<td>[enabled]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>strict policing, oversubscription</td>
<td>[enabled]</td>
</tr>
<tr>
<td>STP virtual switch mode compliant with IEEE 802.1ad (Provider bridge mode)</td>
<td>0x0601 ... 0xFFFF (≠ 0x8100)</td>
<td>[enabled]</td>
<td>enabled</td>
<td>strict policing, oversubscription</td>
<td>[enabled]</td>
</tr>
</tbody>
</table>

### Notes:

1. **QoS CQS:** Quality of Service - Classification, Queueing, and Scheduling

2. “QoS_osub” represents a configuration parameter which determines if the encoding and evaluation of the dropping precedence is supported (supported if QoS_osub is enabled).

3. Entries in square brackets indicate an implicit selection. If in the “QoS CQS” column for example the entry is “[disabled]”, then the preceding selection of tagging and operation mode implies that Quality of Service - Classification, Queueing, and Scheduling (QoS CQS) is not available. It is implicitly disabled, and cannot be enabled.

4. The Ethertype can be set per virtual switch. However, as all virtual switches of a *TransLAN®* card are switched in common, it is effectively set per *TransLAN®* card.

5. The distinction between the STP virtual switch mode compliant with IEEE 802.1Q and the STP virtual switch mode compliant with IEEE 802.1ad (provider bridge mode) can be realized by provisioning the Ethertype. In the STP virtual switch mode compliant with IEEE 802.1Q, the Ethertype is fix preset to 0x8100. In the provider bridge mode, the Ethertype can be provisioned in the range 0x0600 ... 0xFFFF, but unequal to 0x8100.

6. If “HoL blocking prevention” is enabled then frames that are destined for an uncongested port will not be discarded as a result of head-of-line blocking.

### Ingress rate control provisioning method

If Quality of Service - Classification, Queueing, and Scheduling (QoS CQS) is enabled, then ingress rate control can be provisioned per flow by using QoS profiles (see “Quality of Service provisioning” (p. 8-103)). Otherwise, ingress rate control can only be provisioned per port.
Service level agreements

On the 1643 AM the responsibility for admission control is left to the operator. This means there is no check that the Service Level Agreements on already existing connections can be fulfilled, when a new user starts sending data from node A to B.

In this respect the notion of over-subscription factor is important. This is the factor by which the calculated bandwidth, based on for example, the traffic matrices of the operators sharing a link, exceeds the physically available bandwidth. Although theoretically the bandwidth can only be guaranteed for an over-subscription factor ≤ 1, in practice an over-subscription factor of 5-10 can be used without giving problems. Due to the effects of statistical multiplexing it is safe to “sell the bandwidth more than once”. The burstiness of the traffic from individual customers that share a common link makes this possible. The Service Level Agreements give a quantification for the “statistics” of the multiplexing.

Provisioning LAN and WAN ports details

The provisioning of the classifier and rate controller per flow is done only on the ingress customer-role port (LAN port). On the network ports (WAN port), only the scheduler for the egress queues is provisioningable.

It is important that some of the QoS settings are provisioned consistently on all ports throughout the whole customer's VPN domain. In the LAN-VPN (M-LAN) operation mode, the rate controller mode (none, strict policing, oversubscription) must be provisioned consistently (per virtual switch). The latter applies to the only. For the scheduler, for each egress queue the mode = strict_priority/weighted_bandwidth and corresponding weights (per virtual switch) must be provisioned consistently. This is ensured by a background aging function of the system. The parameter will be enforced to be set equally.
Classification, queueing, and scheduling

Flow classification

The flow classifier determines into which flow each incoming packet is mapped. On customer-role ingress ports, a number of flows can be defined, based on port, user priority, VLAN ID, IP-ToS field, and Destination MAC Address. For each flow a rate controller can be specified (CIR/PIR value).

Apart from these flows based on input criteria, a default flow is defined for packets that do not fulfill any of the specified criteria for the flows, for example, untagged packets that have no user priority field. Thus, untagged traffic is classified per port. All traffic on a certain port is treated equally and attached a configurable default port user priority value to map the traffic on the appropriate queues.

A default user priority can be specified on port level to be added to each packet in the default flow (see “Default user priority” (p. 8-98)). Furthermore, the rate controller behavior for the default flow can be specified. The same fixed mapping table from user priority to traffic class to egress queue is applied to packets in the default flow as to packets in the specified flows.

Provided that Quality of Service - Classification, Queueing and Scheduling (QoS CQS, cf. “Quality of Service configuration options” (p. 8-91)) is enabled, each flow can be assigned a traffic class by using QoS profiles (see “Quality of Service provisioning” (p. 8-103)).

Each traffic class is associated with a certain egress queue (see “Traffic class to queue assignment” (p. 8-99)).

Ingress rate control

Ingress rate control is a means to limit the users access to the network, in case the available bandwidth is too small to handle all offered ingress packets.

A rate controller has two parameters, a provisionable committed information rate (CIR, see below), and a committed burst size (CBS). The committed burst size is the committed information rate multiplied by 0.11 seconds. (CBS = 0.11 seconds × CIR).

Rate control is supported for every ingress flow on every customer-role port. There is one rate controller per flow. A “color unaware one-rate two-color marker” is supported, which can be seen as a degenerate case of the two-rate three-color marker. “Color unaware” means that the rate controller ignores and overwrites any dropping precedence given by an upstream network element (network-role ports with DiffServEdge function (E-NNI) only).

The rate controller measurement accuracy is optimized for long frame traffic. Shorter frames are underestimated. Thus, it is recommended to dimension the transporting network to have always a headroom of at least 10% bandwidth compared to the
committed rate (CIR) provisioned. For example: when a flow needs to be limited to 10 Mbps, it is recommended to configure approx. 9 Mbps at an LKA4 / X4IP customer-role port.

A two-rate three-color marker is defined by three colors, specifying the dropping precedence, and two rates as delimiter between the colors. The marker will mark each packet with a certain color, depending on the rate of arriving packets, and the amount of credits in the token bucket. The size of the token bucket will determine how long and far a data burst may be surpassed before the packets are marked with a higher dropping precedence.

The three colors indicate:

- **Green**: Low dropping precedence.
- **Yellow**: Higher dropping precedence.
- **Red**: The packet will be dropped.

The two rates mean:

| **Committed Information Rate (CIR)** | The committed information rate is the delimiter between green and yellow packets.
|--------------------------------------|---|
| **Peak Information Rate (PIR)**     | The peak information rate is the delimiter between yellow and red packets.

If the information rate is less than the committed information rate, all frames will be admitted to the egress queues. These frames will be marked “green”, and have a low probability to be dropped at the egress queues.

If the information rate is greater than the PIR, the frames will be marked “red” and dropped immediately.

For the IEEE 802.1Q STP virtual switch mode and the provider bridge mode the relationship is as specified in the assigned QoS profile. Note that on the LKA4X4IP unit, any PIR is interpreted as infinite (if not: CIR=0, or CIR=PIR).

**Important!** Provisioning of rate controllers does not apply to “I-NNI” ports (see “Quality of Service (QoS) overview” (p. 8-90)).
In general, the behavior of the rate controller is characterized as follows:

- All packets below CIR are marked green.
- All packets between CIR and PIR are marked yellow.
- All packets above PIR are marked red and dropped.

In case oversubscription support is disabled (QoS_osub = disabled), then the provisioning of the PIR is ignored and system-externally the value of the CIR is taken instead. This leads to a strict policing of all flows entering at a customer-role port of this VS.

Rate control modes

The rate controller can operate in two different modes:

1. **Strict policing mode (CIR = PIR)**

   The strict policing mode allows each user to subscribe to a minimum committed SDH WAN bandwidth, or CIR (committed information rate). This mode will guarantee the bandwidth up to CIR but will drop any additional incoming frames at the ingress LAN port that would exceed the CIR.

   All packets below CIR are marked green; all packets above PIR (= CIR) are marked red and dropped.

   ![CIR = PIR ≤ MAX Diagram](image1)

2. **Oversubscription mode (CIR < PIR)**

   The oversubscription mode allows users to burst their data flow to a maximum available WAN bandwidth at a given instance. When PIR is set equal to the maximum of the physical network port bandwidth, then a user is allowed to send more data than the specified CIR. The additional data flow above CIR has a higher dropping probability.

   The following two cases can be differentiated in oversubscription mode.

   ![0 < CIR < PIR = MAX Diagram](image2)
Provisioning the rate control mode

The desired rate control mode can be chosen by enabling/disabling oversubscription support (QoS_osub = enabled/disabled), and by setting the CIR and PIR values. CIR and PIR values can be set by means of QoS profiles (see “Quality of Service provisioning” (p. 8-103)).

The setting of the QoS_osub configuration parameter in combination with the relationship between CIR and PIR determines which rate control mode becomes effective. If, for example, oversubscription support is enabled, and the relationship between CIR and PIR is CIR = PIR ≤ MAX, then the rate controller is operated in strict policing mode.

Important!

1. Which of the rate control modes can actually be configured depends on the mode of operation (see “Quality of Service configuration options” (p. 8-91)).
2. As a general rule it is recommended to use the oversubscription mode for TCP/IP applications, especially in case of meshed or ring network topologies where multiple end-users share the available bandwidth.

Dropper / Marker

Based on the indication of the rate controller, and the rate control mode for the flow, the dropper/marker will do the following:

<table>
<thead>
<tr>
<th></th>
<th>No rate control</th>
<th>Oversubscription mode</th>
<th>Strict policing mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming rate &lt; CIR</td>
<td>mark “green”</td>
<td>mark “green”</td>
<td>mark “green”</td>
</tr>
<tr>
<td>Incoming rate &gt; CIR</td>
<td>mark “green”</td>
<td>mark “yellow”</td>
<td>drop</td>
</tr>
</tbody>
</table>

In the dropper function a decision is made whether to drop or forward a packet. On a TransLAN® card a deterministic dropping from tail when the queue is full is implemented. Packets that are marked red are always dropped. If WAN Ethernet link congestion occurs, frames are dropped. Yellow packets are always dropped before any of the green packets are dropped. This is the only dependency on queue occupation and packet color that is currently present in the dropper function. No provisioning is needed.
Default user priority

A default user priority can be configured for each customer-role port. Possible values are 0 (lowest priority) … 7 (highest priority) in steps of 1. The default setting is 0.

Provisioning of the default user priority does not apply to network-role ports.

The default user priority is treated differently depending on the tagging mode:

- **LAN-VPN (M-LAN) mode**
  
  Incoming frames without a user priority encoding (untagged frames) are treated as if they had the default user priority.

- **IEEE 802.1Q VLAN tagging mode and provider bridge mode**
  
  Incoming frames without a user priority encoding (untagged frames) get a default user priority assigned. This C-UP may be further on equal to a user priority given by one of the provisioned flow descriptors. The subsequent traffic class assignment for this flow, however, will overwrite this C-UP bits again.

Traffic classes

At each ingress port, the traffic class (TC) for each frame is determined. At customer-role ports, this is done via the flow identification and the related provisioned traffic class. At network-role ports, the traffic class is directly derived from the p-bits of the outermost VLAN tag.

Depending on the operation mode, these traffic classes exist:

<table>
<thead>
<tr>
<th>Provider bridge mode and IEEE 802.1Q VLAN tagging mode with encoding of the dropping precedence</th>
<th>The traffic class is encoded in the user priority bits using p2 and p1. Thus, four traffic classes are defined: 0, 1, 2, 3.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.1Q VLAN tagging mode without encoding of the dropping precedence</td>
<td>The traffic class is encoded in the user priority bits using p2, p1, and p0. Thus, eight traffic classes are defined: 0, 0-, 1, 1-, 2, 2-, 3, 3-. The “n” traffic classes differ from the “n-” traffic classes in the value of the p0 bit.</td>
</tr>
</tbody>
</table>

Notes:

1. The support of dropping precedence encoding and evaluation can be enabled or disabled per virtual switch by means of the QoS_osub configuration parameter (QoS_osub = enabled/disabled). All virtual switches belonging to the same TransLAN® network must be provisioned equally for their TPID and this QoS_osub configuration parameter.
These tables show the traffic class encoding in the user priority bits:

<table>
<thead>
<tr>
<th>Traffic class</th>
<th>p2</th>
<th>p1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Traffic class</th>
<th>p2</th>
<th>p1</th>
<th>p0</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1-</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2-</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3-</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

For the IEEE 802.1Q VLAN tagging mode with oversubscription support (QoS›_osub = enabled) it is recommended not to use the n- classes, otherwise all frames will always be marked yellow (i.e. they will have a higher dropping precedence; p0 = 0). In the provider bridge mode, any assignment of an n- class will be recognized as the related n class (tolerant system behavior for inconsistent provisioning).

**Traffic class to queue assignment**

The assignment of the traffic classes to the egress queues is as follows:

<table>
<thead>
<tr>
<th>Transparent tagging</th>
<th>IEEE 802.1Q VLAN tagging and IEEE 802.1ad VLAN tagging (provider bridge mode)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic class</td>
<td>Queue</td>
</tr>
<tr>
<td>3, and Internal use</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
Notes:

1. “Internal use” means that the queue is used for network management traffic (spanning tree BPDU's or GVRP PDU's, for example).

Queueing

The egress treatment is the same for customer-role and network-role ports.

Every port has four associated egress queues. The queues 1 and 2 are to be used for delay-insensitive traffic (for instance file transfer); the queues 3 and 4 are to be used for delay-sensitive traffic (for instance voice or video).

Please refer to “Traffic class to queue assignment” (p. 8-99) for the assignment of the traffic classes to the egress queues.

Repeater mode

In the repeater mode, there is no queuing process as described above. All frames go through the same queue.

Scheduler

The preceding functional blocks assure that all packets are mapped into one of the egress queues, and that no further packets need to be dropped.

The scheduler determines the order, in which packets from the four queues are forwarded. The scheduler on each of the four queues can be in one of two operational modes, strict priority or weighted bandwidth. Any combination of queues in either of the two modes is allowed. When exactly one queue is in weighted bandwidth mode, it is interpreted as a strict priority queue with the lowest priority.

Provided that Quality of Service - Classification, Queueing, and Scheduling (QoS CQS, cf. “Quality of Service configuration options” (p. 8-91)) is enabled, the queue scheduling method can be configured as follows:

<table>
<thead>
<tr>
<th>Queue scheduling method</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strict priority</strong></td>
</tr>
<tr>
<td>The packets in strict priority queues are forwarded strictly according to the queue ranking. The queue with the highest ranking will be served first. A queue with a certain ranking will only be served when the queues with a higher ranking are empty. The strict priority queues are always served before the weighted bandwidth queues.</td>
</tr>
<tr>
<td><strong>Weighted bandwidth</strong></td>
</tr>
<tr>
<td>The weights of the weighted bandwidth queues will be summed up; each queue gets a portion relative to its weight divided by this summed weight, the so-called normalized weight. The packets in the weighted bandwidth queues are handled in a Round-Robin order according to their normalized weight.</td>
</tr>
</tbody>
</table>
Each of the two modes has his well-known advantages and drawbacks. Strict priority queues will always be served before weighted bandwidth queues. So with strict priority, starvation of the lower priority queues cannot be excluded. Starvation should be avoided by assuring that upstream policing is configured such that the queue is only allowed to occupy some fraction of the output link's capacity. This can be done by setting the strict policing rate control mode for the flows that map into this queue, and specifying an appropriate value for the CIR. The strict priority scheme can be used for low-latency traffic such as Voice over IP and protocol data such as spanning tree BPDU’s or GVRP PDU’s.

Weighted bandwidth queues are useful to assign a guaranteed bandwidth to each of the queues. The bandwidth can of course only be guaranteed if concurrent strict priority queues are appropriately rate-limited.

Usually the queue with the lowest number also has the lowest ranking order, but the ranking order of the strict priority queues can be redefined.

Important! It is recommended not to change the mode and ranking of the queue which is used by protocol packets like spanning tree BPDU's and GVRP PDU's (queue 3 or queue 4, respectively; cf. “Traffic class to queue assignment” (p. 8-99)).

Weight

A weight can be assigned to each port’s egress queue in order to define the ranking of the queue.

The weight of a strict priority queue has a significance compared to the weight of other strict priority queues only.

The weight of a weighted bandwidth queue has a significance compared to the weight of other weighted bandwidth queues only.

The weights of the weighted bandwidth queues are normalized to 100%, whereas the normalized weights of the strict priority queues indicate just ordering.

Example

The following table shows an example of a scheduler table:

<table>
<thead>
<tr>
<th>Queue</th>
<th>Queue scheduling method</th>
<th>Priority/Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Strict priority</td>
<td>13</td>
</tr>
<tr>
<td>3</td>
<td>Strict priority</td>
<td>12</td>
</tr>
<tr>
<td>2</td>
<td>Weighted bandwidth</td>
<td>60</td>
</tr>
<tr>
<td>1</td>
<td>Weighted bandwidth</td>
<td>30</td>
</tr>
</tbody>
</table>

The strict priority queues are served before the weighted bandwidth queues. The strict priority queue with the highest weight is served first, queue 4 in this example.
In this example, the queue 1 will be served \( \frac{30}{30+60} \) of the time and queue 2 will be served \( \frac{60}{30+60} \) of the time which is left over from the strict priority queues. In case frames get queued into strict priority queues, then the queue 4 gets priority over frames of queue 3.

Depending on the mode of operation, queue 3 or queue 4 is used for network management traffic, for instance for the spanning tree protocol (see “Traffic class to queue assignment” (p. 8-99)). Hindering this traffic can influence Ethernet network stability.

**Default settings**

These are the default settings of the queue scheduling method and weight:

<table>
<thead>
<tr>
<th>Queue</th>
<th>Queue scheduling method</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Strict priority</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Strict priority</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>Strict priority</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>Strict priority</td>
<td>239</td>
</tr>
</tbody>
</table>
Quality of Service provisioning

QoS provisioning concept

A 3-stage provisioning concept is used for QoS provisioning. This concept can easily be adapted to different provisioning needs in different network applications.
The basic QoS provisioning concept consists of the following stages:

1. For each port one or more customized flow identification tables (FIT) can be assigned.

   An FIT can be assigned either to an entire physical port, or to a fraction of a physical port, i.e. to a so-called “virtual port”. Only E-NNI trunk ports can be split into virtual ports each having an FIT assigned. A virtual port can be defined by means of a virtual port descriptor (VPD).

   In case more than one FIT is assigned, each FIT is related to usually one virtual port. Each FIT may also be related to several virtual ports, provided they are identified by the same virtual port descriptor (VPD).

2. The flow identification tables contain the identification criteria for the flows (for example the values of the C-VID and/or C-UP). Furthermore, the flow identification tables contain a reference identifying the assigned QoS profile.

   Up to 2000 flow identification tables are supported per network element.

3. The QoS profiles contain the provisioning parameters (CIR, PIR, traffic class).

   Using this method of QoS provisioning via QoS profiles can be enabled or disabled on a per-NE basis.

   On a per-port basis you can decide to only use default QoS profiles, or to define your own QoS profiles in order to accomplish flow configuration.

**Provisioning defaults**

The parameter settings in the default QoS profiles for customer-role and network-role ports are:

<table>
<thead>
<tr>
<th>Port role</th>
<th>CIR</th>
<th>PIR</th>
<th>TC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer-role</td>
<td>MAX</td>
<td>MAX</td>
<td>0</td>
</tr>
<tr>
<td>Network-role</td>
<td>MAX</td>
<td>MAX</td>
<td>T</td>
</tr>
</tbody>
</table>

The traffic class “T” is the so-called “transparent traffic class”. The p-bits of the outermost tag (S-UP of the S-tag, or UP of the VLAN tag) remain unchanged, i.e. keep their value which has been assigned by a data unit anywhere upstream.

Explicit provisioning of the flow identification at network-role ports is only intended in the case of so called external network-network interfaces (E-NNIs) connecting to the network of other operators, or to trunking routers, respectively.
Performance monitoring

Performance counters

On the VC-12, VC-3, or VC-4 termination points connected to a WAN port, standard SDH performance monitoring can be activated. The same counters that apply for VC-12, VC-3, or VC-4 termination points on any other port also apply to the VC-12, VC-3, or VC-4 termination points on a WAN port.

Apart from this standard SDH performance monitoring, a limited amount of counters that are dedicated to LAN/WAN ports are defined. Activation of these counters can be established by setting:

- the LAN/WAN port mode to monitored
- selecting a LAN port or WAN port as active PM point
- setting the PM point type to LAN or WAN.

The supported counters are:

- \( CbS \) (total number of bytes sent)
- \( CbR \) (total number of bytes received)
- \( pDe \) (total number of errored packets dropped)

Note that \( CbS \) and \( CbR \) are rather traffic monitoring counters than performance monitoring counters, as they give insight in the traffic load in all places in the network. \( pDe \) is a real performance monitoring counter as it gives an indication about the performance of the network. Only unidirectional PM is supported for these parameters.

See the following figure for the location of the measurements. Note that because of the difference in units, bytes versus packets, the counters cannot be correlated with each other. Also the counter for dropped packets considers only packets dropped due to errors, and does not include packets dropped due to congestion.
Provision Ethernet over SDH

Overview

Purpose

To connect remote PC LAN network sites via an SDH network without the need for intermediate bridges or routers and enable the transport of Ethernet packets across the SDH network.

Contents

| Provisioning Ethernet services                      | 8-107 |
| Parameters of the window “View SDH Channel / VCG Information” | 8-112 |
| Provisioning a virtual switch in repeater (promiscuous) mode | 8-113 |
| Provisioning a virtual switch in LAN interconnect mode | 8-116 |
| Provisioning a virtual switch in MLAN (VPN) mode      | 8-119 |
| Provisioning a virtual switch in MLAN (VPN) mode with QoS | 8-123 |
| Provisioning a virtual switch in spanning tree mode  | 8-132 |
| Parameters for provisioning a LAN unit in repeater mode | 8-143 |
| Parameters for provisioning LAN unit in spanning tree mode | 8-147 |
Provisioning Ethernet services

When to use

Use this procedure to provision Ethernet services.

Note: The Provisioning Ethernet services procedure is also applicable to X51P.

Related information

For related information, see:

- “LAN interfaces” (p. 8-30)
- “Ethernet mapping schemes” (p. 8-81)
- “Ethernet over SDH” (p. 8-24)

Before you begin

You must be logged into the ITMCIT and the respective network element.

Required equipment

The following equipment is required to perform this task:

- ITMCIT

Provisioning the basic Ethernet parameters

Proceed as follows to provision the basic Ethernet parameters:

1. From the ITMCIT main menu, select Provisioning → Equipment → Prov NE Components

   Result: The Provisioned NE Components window opens.

2. Select the slot where the Ethernet card is located.

   Click on Assign/Unassign.

   Result: The Assign NE Units to Slots window appears.

3. Depending if the Ethernet card is already inserted in the shelf either select the radio button Assign or Auto (for preprovisioning, if no board is inserted in the respective board).

4. To assign a unit, use the pull-down menu for Main Unit and select the correct unit corresponding to the displayed slot.
5 Click on OK.

Result: The desired operation for this slot is performed, and the window Provisioned NE Components appears again.

6 Click Close.

Result: The window Provisioned NE Components disappears.

7 From the ITM CIT main menu, select Provisioning → LAN Management → LAN Unit

Result: The LAN Unit Information window opens.

8 Using the Slot drop-down list box select the respective Ethernet card and click on Apply.

Result: The LAN Unit Information window is now populated with information for this unit.

9 To select the tagging mode to be used for this unit click on Edit
Result: The Edit LAN Unit Information window is opened.

10 NOTICE

Uncareful Change of TransLAN application mode can result in undefined operation. In a specific case, switching from IEEE tagging mode (Spanning Tree Switch) to VPN mode (double tagging/transparent), this can result in a crash of the pack.

A 'graceful shutdown' of the configuration of the TransLAN network is then required to ensure proper operation:

1. Remove cross-connection for all affected TransLAN NEs
2. Remove VCGs
3. Delete virtual switches
4. Change mode
5. Create virtual switches
6. Create VCGs and WAN ports
7. Provision VLANs, PVIDs, CID, assign ports etc.
8. Re-create cross-connection.

In the Edit Lan Unit Information window select either:

- the Transparent radio button, if you want to run the unit in transparent tagging mode, also known as double tagging or VPN tagging.
  
  **Note:** X5IP does not support Transparent tagging mode.

- the IEEE 802.1Q / IEEE 802.1ad radio button, if you want to run the unit in standard VLAN tagging mode.

The usage of the tagging modes is described in “Virtual Switch operation mode ” (p. 8-64).

Click OK.

Result: The LAN Unit Information window is now populated with new information for this unit.

11 Click on Close

Result: The LAN Unit Information window is closed.

12 From the ITM CIT main menu, select Provisioning → LAN Management → VCG
**Result:** The SDH channel / VCG List window opens.

13 In the SDH channel / VCG List window select the respective port and click on Details.

**Result:** The SDH channel / VCG Information window is now populated with information for this port.

Refer to “Parameters of the window “View SDH Channel / VCG Information”” (p. 8-112).

14 For provisioning the basic Ethernet and VCG port parameters to be used for this port click on Edit.

**Result:** The Edit SDH Channel / VCG Information window is opened.

15 Set the
- **Encapsulation Mode** to Generic Framing Procedure
- **LCAS Mode** to Enabled or Disabled
- **TP Mode** to Monitored or Not Monitored and
- **VC Type** to VC3 or VC12

from the drop down list and then click **Ok**.

**Result:** The Edit SDH Channel / VCG Information window is closed.

16

<table>
<thead>
<tr>
<th>IF</th>
<th>THEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>you want to provision a virtual switch in spanning tree mode (provided that the tagging mode was set to standard VLAN tagging in Step 9 of this procedure)</td>
<td>continue with “Provisioning a virtual switch in spanning tree mode” (p. 8-132)</td>
</tr>
<tr>
<td>you want to provision a virtual switch in repeater mode (provided that the tagging mode was set to transparent tagging, also known as double tagging or VPN tagging, in Step 9 of this procedure)</td>
<td>continue with “Provisioning a virtual switch in repeater (promiscuous) mode ” (p. 8-113)</td>
</tr>
<tr>
<td>IF</td>
<td>THEN</td>
</tr>
<tr>
<td>-------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>you want to provision a virtual switch in provider bridge mode,</td>
<td>continue with “Provisioning a virtual switch in spanning tree mode” (p. 8-132)</td>
</tr>
<tr>
<td>(provided that the tagging mode was set to IEEE 802.1ad, in Step 9 of this procedure)</td>
<td></td>
</tr>
</tbody>
</table>

**END OF STEPS**
### Fields and parameters

The following table shows the status data which are shown in the **View SDH Channel / VCG Information** window.

<table>
<thead>
<tr>
<th>Information field</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Switch</td>
<td>Displays the physical switch.</td>
</tr>
<tr>
<td>SDH Channel / VCG</td>
<td>Displays the name of the SDH channel termination point</td>
</tr>
<tr>
<td>TP mode</td>
<td>Displays the current SDH Channel Monitoring mode of each Termination Point individually.</td>
</tr>
<tr>
<td>Encapsulation Mode</td>
<td>Displays the encapsulation mode</td>
</tr>
<tr>
<td>LCAS Mode</td>
<td>Displays if LCAS is either enabled or disabled.</td>
</tr>
<tr>
<td>Hold Off Time (s)</td>
<td>Displays the hold off timer</td>
</tr>
<tr>
<td>WtR Time (min)</td>
<td>Displays the global WtR timer for LCAS</td>
</tr>
<tr>
<td>Capacity</td>
<td></td>
</tr>
<tr>
<td>Provisioned (Source)</td>
<td>Displays the provisioned source WAN port capacity</td>
</tr>
<tr>
<td>Provisioned (Sink)</td>
<td>Displays the provisioned sink WAN port capacity</td>
</tr>
<tr>
<td>Working (Source)</td>
<td>Displays the source working capacity</td>
</tr>
<tr>
<td>Working (Sink)</td>
<td>Displays the sink working capacity</td>
</tr>
<tr>
<td>Associated VC (Display VC information in the VCG)</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Displays the name of the VC TP</td>
</tr>
<tr>
<td>VC Type</td>
<td>Displays the type of the VC resource</td>
</tr>
<tr>
<td>Source Status</td>
<td>Displays the status of the VC resource</td>
</tr>
<tr>
<td>Sink Status</td>
<td>Displays the status of the VC resource</td>
</tr>
<tr>
<td>Relative Differential Delay (ms)</td>
<td>Shows the relative differential delay of the VCG Tribs in ms. The fastest trib has a delay of 0 ms. The delay of the other trib is relative to the fastest one. Refer also to “Differential delay” (p. 8-43)</td>
</tr>
</tbody>
</table>
Provisioning a virtual switch in repeater (promiscuous) mode

When to use

To route Ethernet packets from one customer being able to use one LAN or WAN port
The Provisioning a virtual switch in repeater (promiscuous) mode procedure is applicable to X4IP and X5IP.

Related information

Related procedures and information are:
- “Provisioning Ethernet services” (p. 8-107).
- “Parameters for provisioning a LAN unit in repeater mode” (p. 8-143)
- “Ethernet over SDH” (p. 8-24).

Before you begin

Before provisioning a virtual switch determine and check the following:
- the tagging mode of the LAN unit is set to Transparent or IEEE 802.1ad
- the virtual switch name and label
- the LAN port label
- the WAN port capacity
- deleting a virtual switch will detach the associated LAN ports or WAN ports. If these ports carry traffic, this traffic will be lost
- detaching a LAN port or a WAN port can disrupt traffic over these ports

For provisioning a virtual switch in repeater mode the following procedures must be performed:
- create a virtual switch and assign a LAN port and WAN ports to the virtual switch
- provision the TUG structure and create cross connections between the WAN port <-> CC <-> line port
- fill in LAN port label
- select the WAN capacity
The limitation of X4IP card:

1. The bridge in repeater mode is not transparent for end-user frames that use a TPID field that equals to the Ethertype that is used in the temporary VLAN tag between the local bridge ingress and egress ports. A repeater link can be used to interconnect TransLAN parts (through LAN ports in NR) or other provider equipment or networks. In that case select another TPID for the repeater. TPID can be provisioned only equally for all virtual switches of a data unit.

2. If the data unit has only virtual switches in repeater mode provisioned, then the TPID is not accessible.

Workaround: Create another virtual switch in switched mode, change the TPID to a value different to 8100 and different to the TPID of the NEs with the NR ports to be interconnected, and delete the virtual switch again.

Create a virtual switch

1. Select Provisioning → LAN Management → Virtual Switch.
   
   Result: The Virtual Switch List window appears

2. Click Add.

   Result: The Add Virtual Switch window appears.

3. Enter a name of maximum 20 characters in the Virtual Switch Label field (for example Sales).

4. Select Repeater in the Operation mode area.

5. In the group box Available Port List select one LAN port.
   Click on the < button to attach the selected LAN port(s) to the virtual switch.

   Result: The selected LAN port appears in the Selected Port Membership group box.

6. In the group box Available Port List select one WAN port.
   Click on the < button to attach the selected WAN port to the virtual switch.

   Result: The selected WAN port appears in the Selected Port Membership group box.

7. Click OK
Result: A new Virtual Switch has been created.

The Virtual Switch Information window is updated displaying the created Virtual Switch.

8 Click OK.

Result: The Virtual Switch Information window is closed.

END OF STEPS

Provision WAN port configuration details

No procedures have to be performed to provision the WAN port configuration details when the operation mode of the Virtual Switch is configured in the Repeater mode.

Provision TUG structure and cross connections

For provisioning the TUG structure and Cross Connections reference is made to:

- “Provision cross connections without protection” (p. 8-179)
Provisioning a virtual switch in LAN interconnect mode

When to use

To route Ethernet packets from one customer, being able to use more than one physical LAN port to more than one WAN ports.

Related information

Related procedures and information are:

- “Provisioning Ethernet services” (p. 8-107).
- “Parameters for provisioning a LAN unit in repeater mode” (p. 8-143)
- “Ethernet over SDH” (p. 8-24).

Before you begin

Before provisioning a virtual switch determine and check the following:

- the tagging mode of the LAN unit is set to Transparent
- the virtual switch name and label
- the WAN port capacity
- deleting a virtual switch will detach all the associated LAN ports or WAN ports. If these ports carry traffic, this traffic will be lost
- detaching a LAN port or a WAN port can disrupt traffic over these ports.

For provisioning a virtual switch in repeater mode the following procedures must be performed:

- create a virtual switch and assign a LAN port and WAN ports to the virtual switch
- provision the TUG structure and create cross connections between the WAN port <-> CC <-> line port.
- select the WAN capacity
- fill in the LAN port label and the customer ID (CID)

Create a virtual switch

1. Select Provisioning → LAN Management → Virtual Switch.

   **Result:** The Virtual Switch List window appears.

2. Click Add.
Result: The Virtual Switch Information window appears.

3 Enter a name of maximum 20 characters in the Virtual Switch Label field (for example Sales).

4 Select LAN interconnect in the Operation Mode area.

5 In the group box Port Membership select the LAN Ports tab.
Attach one or more LAN port(s) to the virtual switch by clicking the appropriate checkbox.

6 Fill in the Customer ID (CID) of the selected LAN port.

7 In the group box Port Membership select the WAN Ports tab.
Attach one or more WAN port(s) to the virtual switch by clicking the appropriate checkbox.

8 Fill in the Customer ID (CID) of the selected WAN port.

9 Click Apply

   Result: A new Virtual Switch has been created.

   The Virtual Switch Information window is updated displaying the created Virtual Switch.

10 Click OK.

   Result: The Virtual Switch Information window is closed.

END OF STEPS

Provision WAN port configuration details

No procedures have to be performed to provision the WAN port configuration details when the operation mode of the Virtual Switch is configured in the LAN interconnect mode.
Provision LAN port configuration details

1 Select **Provisioning → LAN Management → LAN Port**
   
   **Result:** The *LAN Port Information List* window appears displaying the information of the LAN ports belonging to the selected physical switch.

2 Select the *LAN port* from the list and click **Details**.
   
   **Result:** The *LAN Port Configuration Details* window appears.

3 Click **Edit**.
   
   **Result:** The *Edit LAN Port Configuration Details* window appears.

4 Fill in the *Label* and the *Customer ID (CID)* of the selected port.

5 Click **OK**.
   
   **Result:** The *LAN Port Configuration Details* window reappears displaying the updated LAN port configuration information.

6 Click **Close** to exit.

---

Provision TUG structure and cross connections

For provisioning the TUG structure and Cross Connections reference is made to:

- “Provision cross connections without protection” (p. 8-179)
Provisioning a virtual switch in MLAN (VPN) mode

When to use

To route Ethernet packets from different customers which are using different physical LAN ports in one Virtual Switch and share the bandwidth of the WAN ports.

Configuration rules and guidelines

Please observe these configuration rules and guidelines:

- Be aware that the port role of the LAN and WAN ports is fixed (see “Flexible port role assignment” (p. 8-85)):
  - LAN ports are always customer role ports.
  - WAN ports are always network role ports.
- On LAN ports the CID needs to be provisioned manually.
- The CID provisioned on each LAN port must be unique within a shared WAN to create a fully independent VPN.

The VPN provisioning on the WAN ports is done automatically by means of the proprietary spanning tree with VPN registration protocol (STVRP).

Related information

Related procedures and information are:

- “Provisioning Ethernet services” (p. 8-107).
- “Parameters for provisioning a LAN unit in repeater mode” (p. 8-143)
- “Ethernet over SDH” (p. 8-24).

Before you begin

Before provisioning a Virtual Switch determine and check the following:

- the tagging mode of the LAN unit is set to Transparent
- the Virtual Switch name and label
- the WAN port capacity
- deleting a virtual switch will detach all the associated LAN ports or WAN ports. If these ports carry traffic, this traffic will be lost
- detaching a LAN port or a WAN port can disrupt traffic over these ports.

For provisioning a virtual switch in MLAN (VPN) mode the following procedures must be performed:

- create a virtual switch and assign a LAN port and WAN ports to the virtual switch
- provision the TUG structure and create cross connections between the WAN port <-> CC <-> line port.
Provisioning a virtual switch in MLAN (VPN) mode

- select the WAN capacity
- fill in the LAN port label, the customer ID, and the CIR value and the PIR mode (strict policy or oversubscription)
- set the TP mode to be monitored or not

Create a virtual switch

1. Select **Provisioning → LAN Management → Virtual Switch.**
   
   **Result:** The Virtual Switch List window appears

2. Click **Add.**
   
   **Result:** The Virtual Switch Information window appears.

3. Enter a name of maximum 20 characters in the Virtual Switch Label field (for example Sales).

4. Select **MLAN (VPN)** in the Operation Mode area.

5. In the group box Port Membership select the LAN Ports tab.
Attach one or more LAN port(s) to the virtual switch by clicking the appropriate checkbox.

6 Fill in the Customer ID (CID) of the selected LAN port.

7 In the group box Port Membership select the WAN Ports tab.
Attach one or more WAN port(s) to the virtual switch by clicking the appropriate checkbox.

8 Fill in the Customer ID (CID) of the selected LAN port.

9 Set the Default Flow CIR and the Default Flow CIR for the selected port(s).

10 Click Apply
   
   **Result:** A new Virtual Switch has been created.
   
   The Virtual Switch Information window is updated displaying the created Virtual Switch.

11 Click OK.
   
   **Result:** The Virtual Switch Information window is closed.

END OF STEPS

Provision LAN port configuration details

1 Select Provisioning → LAN Management → LAN Port
   
   **Result:** The LAN Port Information List window appears.

2 Select the LAN port from the list and click Details.
   
   **Result:** The LAN Port Configuration Details window appears.

3 Click Edit.
Result: The Edit LAN Port Configuration Details window appears.

4 Fill in the Label, the Customer ID (CID) and the CIR and select the PIR mode of the selected port and click OK.

Result: The LAN Port Configuration Details window reappears displaying the updated LAN port configuration information.

5 Click Close to exit.

END OF STEPS

Provision TUG structure and cross connections

For provisioning the TUG structure and Cross Connections reference is made to:

- “Provision cross connections without protection” (p. 8-179)
Provisioning a virtual switch in MLAN (VPN) mode with QoS

When to use

To route Ethernet packets from different customers which are using the same physical LAN port to more than one WAN port.

Configuration rules and guidelines

Please observe these configuration rules and guidelines:

- Be aware that the port role of the LAN and WAN ports is fixed (see “Flexible port role assignment” (p. 8-85)):
  - LAN ports are always customer role ports.
  - WAN ports are always network role ports.
- On LAN ports the CID needs to be provisioned manually.
- The CID provisioned on each LAN port must be unique within a shared WAN to create a fully independent VPN.

The VPN provisioning on the WAN ports is done automatically by means of the proprietary spanning tree with VPN registration protocol (STVRP).

Related information

Related procedures and information are:

- “Provisioning Ethernet services” (p. 8-107).
- “Parameters for provisioning a LAN unit in repeater mode” (p. 8-143)
- “Ethernet over SDH” (p. 8-24).

Before you begin

Before provisioning a Virtual Switch determine and check the following:

- the tagging mode of the LAN unit is set to Transparent
- the Virtual Switch name and label
- the LAN port name, label and members
- the WAN port label and members
- the LAN and WAN port details information
• the Rate control mode of the Virtual Switch and the CIR value
• for QoS provisioning on the ingress side of the Virtual Switch (only LAN port) the traffic class assignment, the operation mode (strict policy or oversubscription and the CIR value.
• for QoS provisioning on the egress side of the Virtual Switch (LAN and WAN port), the scheduler method and weight.
• deleting a virtual switch will detach all the associated LAN ports or WAN ports. If these ports carry traffic, this traffic will be lost
• detaching a LAN port or a WAN port can disrupt traffic over these ports

For provisioning a virtual switch in MLAN (VPN) mode with QoS the following procedures must be performed:

• create a virtual switch and assign a LAN port and WAN ports to the virtual switch
• provision the TUG structure and create cross connections between the WAN ports <-> CC <-> line ports
• provision LAN and WAN port details, the WAN port capacity and the monitoring mode of the VCG
• provision the Quality of Service (QoS) on the ingress side of the Virtual Switch (LAN port)
• provision the Quality of Service (QoS) on the egress side of the Virtual Switch (LAN port)
• provision the Quality of Service (QoS) on the egress side of the Virtual Switch (WAN port)

Create a virtual switch

1 Select Provisioning → LAN Management → Virtual Switch.

   Result: The Virtual Switch List window appears

2 Click Add.

   Result: The Virtual Switch Information window appears.

3 Enter a name of maximum 20 characters in the Virtual Switch Label field (for example Sales).

4 Select MLAN (VPN) with QoS in the Operation Mode area.
5 In the group box Port Membership select the LAN Ports tab. 
Attach one or more LAN port(s) to the virtual switch by clicking the appropriate checkbox.

6 Fill in the Customer ID (CID) of the selected LAN port. 
Select the Acceptable Frame Type and the Ingress Filtering permission.

7 In the group box Port Membership select the WAN Ports tab. 
Attach one or more WAN port(s) to the virtual switch by clicking the appropriate checkbox.

8 In the group box Qos - Ingress Flow select the Traffic Class Assignment method applicable for incoming packets.

9 In the group box Qos - Ingress Flow in the right flow mapping table several parameters can be set for specific flow by first selecting a specific flow.
Fill in the CIR value and select the PIR mode from the pull down list.

Now the provision process starts for the selected flows. If the initial state of the Traffic Class Assignment method is Default Overriding, then starts the provision process with the Mapping Table method setting. The hourglass shall be shown during the provision process.

10 In the group box QoS - Ingress Flow select the Default User Priority applicable for incoming packets.

11 In the group box QoS - Ingress Flow select the Default Flow CIR (Committed Information Rate) value applicable for incoming packets.

12 In the group box QoS - Ingress Flow select the Default Flow PIR Mode (Peak Information Rate) applicable for incoming packets.
In the group box QoS - Egress Queue the Egress QoS Information can be set for specific queues on a LAN port.
1. Select the LAN Port tab.
2. Select a Queue.
3. Select the Type.
4. Fill in the Weight.
5. Select a Queue.

**Result:** For each edited queue the **Normalized Weight** is recalculate according the edited Queue Type and Weight.

In the group box QoS - Egress Queue the Egress QoS Information can be set for specific queues on a WAN port.
1. Select the WAN Port tab.
2. Select a Queue.
3. Select the Type.
4. Fill in the Weight.
5. Select a Queue.

**Result:** For each edited queue the **Normalized Weight** is recalculate according the edited Queue Type and Weight.

Click **Apply**

**Result:** A new Virtual Switch has been created.

The Virtual Switch Information window is updated displaying the created Virtual Switch.

Click **OK**.

**Result:** The Virtual Switch Information window is closed.

**End of Steps**
Result: The **LAN Port Information List** window appears.

2 Select a *LAN port* from the list and click *Details*.

**Result:** The **LAN Port Configuration Details (IEEE 802.1Q)** window appears.

3 Click *Ingress*.

**Result:** The *Ingress QoS Information* window appears displaying the QoS on the ingress side of the Virtual Switch.

4 Click *Edit*.

**Result:** The *Edit Ingress QoS Information* window appears.

5 Select the *Traffic Class Assignment* method applicable for incoming packets.

6 Fill in the *CIR* value and select the *PIR* mode from the pull down list and click *OK*.

Now the provision process starts for the selected flows. If the initial state of the Traffic Class Assignment method is Default Overriding, then starts the provision process with the Mapping Table method setting. The hourglass shall be shown during the provision process.

7 Select the *User Priority*, fill in the *Flow CIR* value and select the *PIR Mode* for the default flow.

8 Click *OK*.

**Result:** The updated *Ingress QoS Information* window reappears.

9 Click *Close*.

**Result:** The **LAN Port Configuration Details** window appears.

10 Click *Close* to exit.

END OF STEPS
Provisioning a virtual switch in MLAN (VPN) mode with QoS

Provision QoS egress side Virtual Switch (LAN port)

1. Select **Provisioning → LAN Management → LAN Port**.
   
   **Result:** The *LAN Port Information List* window appears.

2. Select a *LAN port* from the list and click *Details*.
   
   **Result:** The *LAN Port Configuration Details (IEEE802.1Q)* window appears.

3. Click *Egress*.
   
   **Result:** The *Egress QoS Information* window appears displaying the QoS on the egress side of the selected LAN port.

4. Select a *Queue* and click *Edit*.
   
   **Result:** The *Edit Egress QoS Information* window appears.

5. Select the *Type* and fill in the *Weight*.

6. Click the arrow button to recalculate the Normalized Weight according the edited Queue Type and Weight and Click *OK*.
   
   **Result:** The updated Egress QoS Information window reappears.

7. Click *Close*.
   
   **Result:** The *Egress QoS Information* window disappears.

8. Click *Close*.
   
   **Result:** The *LAN Port configuration details* window disappears.

9. Click *Close*.
Result: The LAN Port Information list window disappears.

10 Click Close to exit.

END OF STEPS

View WAN to TP mapping details and set the SDH channel mode

1 From the ITM CIT main menu, select Provisioning → LAN Management → VCG
   Result: The SDH channel / VCG Filter window opens.

2 In the SDH channel / VCG Filter window select the respective port and click on OK.
   Result: The SDH channel / VCG Information window is now populated with information for this port.

3 For provisioning the basic Ethernet and VCG port parameters to be used for this port click on Edit.
   Result: The Edit SDH Channel / VCG Information window is opened.

4 By means of the respective Enable and Disable radio buttons enable or disable the LCAS Mode.

   The LCAS protocol provides a synchronisation and a “handshake” mechanism between the concatenation source and sink functions to allow a change in the group size without transmission hits. Another function of the LCAS protocol is to autonomously remove VCG members that experience transmission failures or degraded transmission performance.

5 If the LCAS protocol is enabled, then define the WTR Time (wait-to-restore time, possible values are 0 ... 60min, in steps of 1 min) and the Hold-Off Time (possible values 0 ... 10s, in steps of 0.1s)

6 Set the TP Mode to Monitored or Not Monitored.

7 Set the VC Type and the Encapsulation Mode to be used.
8 In the source group box select a VC from the Available field click on the > button.

9 Select the Same Settings for Source and Sink radio button.

10 Click on OK.

**Result:** The Edit SDH Channel / VCG Information window is closed.

---

Provision QoS egress side Virtual Switch (WAN port)

1 Select **Provisioning → LAN Management → WAN Port**.

**Result:** The **WAN Port Information List** window appears.

2 Select a **WAN port** from the list and click **WAN Port Configuration Details**.

**Result:** The **WAN Port Configuration Details (IEEE802.1Q)** window appears.

3 Click **Egress**.

**Result:** The **Egress QoS Information** window appears displaying the QoS on the egress side of the selected WAN port.

4 Select a **Queue** and click **Edit**.

**Result:** The **Edit Egress QoS Information** window appears.

5 Select the **Type** and fill in the **Weight**.

6 Click the arrow button to recalculate the Normalized Weight according the edited Queue Type and Weight and Click **OK**.

**Result:** The updated Egress QoS Information window reappears.

7 Click **Close**.
Result: The Egress QoS Information window disappears.

8 Click Close.

Result: The WAN Port Information list window disappears.

9 Click Close to exit.

END OF STEPS

Provision TUG structure and cross connections

For provisioning the TUG structure and Cross Connections reference is made to:

- “Provision cross connections without protection” (p. 8-179)
Provisioning a virtual switch in spanning tree mode

When to use

To route Ethernet packets from different customers which are using the same physical LAN port to more than one WAN port.

The Provisioning a virtual switch in spanning tree mode procedure is also applicable to X5IP.

Related information

Related procedures and information are:

- “Provisioning Ethernet services” (p. 8-107).
- “Parameters for provisioning a LAN unit in repeater mode” (p. 8-143)
- “Ethernet over SDH” (p. 8-24).

Before you begin

Before provisioning a virtual switch determine and check the following:

- the tagging mode of the LAN unit is set to IEEE802.1Q / IEEE 802.1ad
- the virtual switch name and label
- the LAN port name, label and members
- the WAN port label and members
- the LAN and WAN port details information
- the Rate Control of the Virtual Switch (QoS Oversubscription enable or disable)
- for QoS provisioning of the LAN port, the traffic class assignment, the operation mode (strict policy or over subscription, the CIR, the scheduler method and weight.
- for QoS provisioning of the WAN port, the traffic class assignment, the scheduler method and weight.
- deleting a virtual switch will detach all the associated LAN ports or WAN ports. If these ports carry traffic, this traffic will be lost
- the Traffic Class Assignment and LAN and WAN port number
- for QoS provisioning of the LAN port, the Traffic Class Assignment, the Forwarding Class and CIR
- for QoS provisioning of the WAN port, the type of policy for the selected queue and weight.
- detaching a LAN port or a WAN port can disrupt traffic over these ports
For provisioning a virtual switch in the Spanning Tree mode the following must be performed:

- create a virtual switch
- provision LAN and WAN port details
- provision the TUG structure and create cross connections between the WAN ports <-> CC <-> line ports
- provision the WAN port capacity and the monitoring mode of the SDH channel
- create a VLAN
- provision the Quality of Service (QoS) on the LAN and WAN ports.

For provisioning a virtual switch in the Provider Bridge Mode PBM the CID (PVID) must be provisioned twice:

- once for the CID (PVID) entry (in “Create a virtual switch” (p. 8-133))
- once for the VLAN filter (tagged/untagged port lists) (in “Create a VLAN on a virtual switch” (p. 8-141))
  - enter the CID (PVID) for a certain customer role port (as usual)
  - enter the port number into the 'untagged membership list' for this CID
  - don't put this port number into any other VLAN list
  - put only network role ports into the 'tagged membership list' for this CID (only needed if this is not done by GVRP)

**Important!** TransLAN always advertises to transport untagged traffic in IEEE802.1D/Q mode, for preservance of e.g. end customer Bridge PDU traffic. For this purpose, the TransLAN network will assign a default VLAN id (PVID) that is used only internally to securely transport untagged customer traffic. This PVID is attached at the ingress port, and removed at egress. Therefore it is not allowed to send traffic to the TransLAN network that is already tagged with the same VLAN as the default PVID used in the TransLAN network for this end customer. This traffic will inevitably be untagged, and might not be useable anymore for the end customer.

Create a virtual switch

1. Select **Provisioning → LAN Management → Virtual Switch**.
   
   **Result:** The *Virtual Switch List* window appears

2. Click **Add**.
Result: The Add Virtual Switch window appears.

3 Enter a name of maximum 20 characters in the Virtual Switch Label field (for example Sales).

4 Select Spanning Tree in the Operation Mode area.

5 Select TPID value in the Ether Type area.
   It is recommended only to provide one of the following two values:
   - 0x8100
     for IEE802.1Q STP
   - 0x9100
     for IEE802.1ad STP (provider bridge mode)

6 Select the virtual switch and click Details.
   Result: The Virtual Switch List Information window appears.

7 Click Edit.

8 Select if QoS oversubscription is either Enabled or Disabled if Ether Type is 8100.

9 Select if Dynamic VLAN registration is either Enabled or Disabled.

10 Attach one or more LAN port(s) to the virtual switch by selecting them in the Available Port List and shifting them to the group box Selected Port Membership by clicking on the left arrow button.

11 Attach one or more WAN port(s) to the virtual switch by selecting them in the Available Port List and shifting them to the group box Selected Port Membership by clicking on the left arrow button.

12 Click OK.
Result: The Virtual Switch List window appears

13 Select the newly created virtual switch and click Details.

Result: The Virtual Switch List Information window appears.

If tagging mode has been changed from transparent to IEEE, it can take up to 30 seconds until the Virtual Switch List Information window appears. The reason is that after a tagging mode switch, the LAN image is restarted. So you should wait until the LAN image start up has finished, before starting any operation.

14 Click Edit.

15 Fill in the Virtual Switch Label and the PVID.

Additional info If the LAN port should be configured for untagged traffic, a PVID must be set. Additionally a VLAN-ID with the same value of the PVID must be configured otherwise it is not known in the GVRP protocol.

16 Click OK.

Result: The Virtual Switch List Information window appears

17 Provision LAN port parameters.

Reference: Refer to “Configuring LAN port parameters on a virtual switch” (p. 8-137).

18 Provision WAN port parameters.

Reference: Refer to “Configuring WAN port parameters on a virtual switch” (p. 8-140).

19 Fill in the Spanning Tree Path Cost and the Priority, select the required Flow Type. Therfore proceed as follows:

1. Click STP info ...button.
2. In the opened Spanning Tree Protocol Information screen click on Edit.
3. In the opened Edit Spanning Tree Protocol Information screen you can select the Bridge Priority, Spanning Tree Path Cost and the Priority.
4. Click on OK to close the Edit Spanning Tree Protocol Information screen.
5. Click on Close to close the Edit Spanning Tree Protocol Information screen.

20 In the group box QoS - Ingress Flow select the Traffic Class Assignment method applicable for incoming packets.

Additional info: Refere to “Quality of Service (QoS) overview” (p. 8-90).

21 In the group box QoS - Ingress Flow in the right flow mapping table several parameters can be set for specific flow by first selecting a specific flow.

Fill in the CIR value and select the PIR mode from the pull down list.

Additional info

Now the provision process starts for the selected flows. If the initial state of the Traffic Class Assignment method is Default Overriding, then starts the provision process with the Mapping Table method setting. The hourglass shall be shown during the provision process.

22 In the group box Qos - Ingress Flow select the Default User Priority applicable for incoming packets.

23 In the group box Qos - Ingress Flow select the Default Flow CIR (Committed Information Rate) value applicable for incoming packets.

24 In the group box Qos - Ingress Flow select the Default Flow PIR Mode (Peak Information Rate) applicable for incoming packets.

25 In the group box Qos - Egress Queue the Egress QoS Information can be set for specific queues on a LAN port.
1. Select the LAN Port tab.
2. Select a Queue.
3. Select the Type.
4. Fill in the Weight.
5. Select a Queue.
Result: For each edited queue the **Normalized Weight** is re-calculate according the edited Queue Type and Weight.

26 In the group box **Qos - Egress Queue** the Egress QoS Information can be set for specific queues on a WAN port.

1. Select the **WAN Port** tab.
2. Select a **Queue**.
3. Select the **Type**.
4. Fill in the **Weight**.
5. Select a **Queue**.

Result: For each edited queue the **Normalized Weight** is recalculate according the edited Queue Type and Weight.

27 Click **Apply**

Result: A new Virtual Switch has been created.

The **Virtual Switch Information** window is updated displaying the created Virtual Switch.

28 Click **Close**.

Result: The **Virtual Switch Information** window is closed.

**END OF STEPS**

Configuring LAN port parameters on a virtual switch

1 Select **Provisioning → LAN Management → Virtual Switch**

Result: The **Virtual Switches List** window is displayed.

2 Select the respective virtual switch and click **Details**.

Result: The **Virtual Switch List Information** window appears.

3 Select the LAN/WAN port in the **Port Membership** field and click on **Port Details**.
Result: The Select Port Role screen is displayed.

4 Select the Port Role to be used for the LAN port.

Reference: Refer to “Flexible port role assignment” (p. 8-85).

Result: The Customer/Network Port Information (depending on the selected port role) window is displayed.

5 Select the required PVID and the required Acceptable Frame Type.

Rules for PVID and VLAN configuration: For PVID and VLAN configuration follow the following rules:

1. Unused/unconnected port (i.e. not in a Spanning Tree Mode VS)
   - default VLAN Id (/PVID) = 4093
   - Acceptable Frame Type (default value as already specified)
     Customer Port: Accept All Frames
     Network Port: Only VLAN-Tagged

2. Customer Port in Virtual Switch spanning Tree Mode with EtherType/TPID = 8100 (i.e. IEEE 802.1Q mode)
   - default VLAN Id (/PVID) = 4093 allowed
   - if default VLAN Id (/PVID) = 1..4093 then
     a untagged VLAN Id = default VLAN Id is associated with that port

3. Network Port in Virtual Switch spanning Tree Mode with EtherType/TPID = 8100 (i.e. IEEE 802.1Q mode)
   - default VLAN Id (/PVID) = 4093
   - no untag VLAN Ids associated with port (i.e. untagged port member set must be empty)
   - any number of tagged VLAN Ids associated with the port are allowed

4. Customer Port in Virtual Switch spanning Tree Mode with EtherType/TPID 8100 (i.e. IEEE 802.1ad mode):
   - default VLAN Id (/PVID) = 4093 allowed
   - if default VLAN Id (/PVID) = 1..4093 then
     there is one untagged VLAN Id = default VLAN Id associated with that port 3 (for the VLAN Id = PVID, the customer role port is always in the Untagged Port Member set)
     there are no other VLAN Id (tagged or untagged) associated with that port
5. Network Port in Virtual Switch Spanning Tree Mode with EtherType/TPID 8100 (i.e. IEEE 802.1ad mode):
   - default VLAN Id (/PVID) = 4093
   - no untagged VLAN Ids associated with port (i.e. untagged port member set must be empty)
   - any number of tagged VLAN Ids associated with the port are allowed

6. Select the Default User Priority applicable for incoming packets.

7. If
   - the chosen Port Role is Customer Port, continue with Step 11.
   - the chosen Port Role is Network Port, continue with Step 8.

8. In the Virtual Switch Information window, select Network Port and click Port Details.
   **Result:** The Network Port Information window appears.
   Refer to “GARP VLAN Registration Protocol (GVRP)” (p. 8-54).

9. Click Edit, select Network Port in Select Port Role window and then click Next.
   **Result:** The Edit Network Port Information window appears.

10. Select enabled or disabled for GVRP and select enabled or disabled for STP Protocol from the drop down list and click Ok.

11. Select the QoS mode. Either Default Profile or Flow Configuration are possible.
    **Additional info** When QoS mode of a port is set to Default Profile, no rate control is executed for the flows coming into this port.
    Setting QoS mode to Default Profile allows you to set-up your flow Pool configuration (several steps needed) and then switch to this pool configuration with changing the QoS mode to Flow Configuration.
    **Related information** For provisioning QoS refer to “Provision QoS Flow Identification Table” (p. 8-169).

12. Click on OK.
Configuring WAN port parameters on a virtual switch

1. Select **Provisioning → LAN Management → Virtual Switch**
   
   Result: The **Virtual Switches List** window is displayed.

2. Select the respective virtual switch and click **Details**.
   
   Result: The **Virtual Switch List Information** window appears

3. Select the WAN port in the **Port Membership** field and click on **Port Details**.
   
   Result: The **Select Port Role** screen is displayed.

4. Select the **Port Role** to be used for the WAN port.
   
   Reference: Refer to “Flexible port role assignment” (p. 8-85).

   Result: The **Customer/Network Port Information** (depending on the selected port role) window is displayed.

5. Select the required **PVID** and the required **Acceptable Frame Type**.

6. Select the **Default User Priority** applicable for incoming packets.

7. If

<table>
<thead>
<tr>
<th>If</th>
<th>Then</th>
</tr>
</thead>
<tbody>
<tr>
<td>the chosen Port Role is Customer Port,</td>
<td>continue with <strong>Step 11</strong>.</td>
</tr>
<tr>
<td>the chosen Port Role is Network Port,</td>
<td>continue with <strong>Step 8</strong>.</td>
</tr>
</tbody>
</table>

8. In the **Virtual Switch Information** window, select Network Port and click **Port Details**.
Result: The Network Port Information window appears.

9 Click **Edit**, select **Network Port** in Select Port Role window and then click **Next**.

Result: The Edit Network Port Information window appears.

10 Select enabled or disabled for **GVRP** and select enabled or disabled for **STP Protocol** from the drop down list and click **Ok**.

11 Select the **QoS mode**. Either **Default Profile** or **Flow Configuration** are possible.

Additional info When **QoS mode** of a port is set to **Default Profile**, no rate control is executed for the flows coming into this port.

Setting QoS mode to **Default Profile** allows you to set-up your flow Pool configuration (several steps needed) and then switch to this pool configuration with changing the **QoS mode** to **Flow Configuration**.

Related information For provisioning QoS refer to “Provision QoS Flow Identification Table ” (p. 8-169).

12 Click on **OK**.

Result: The Customer/Network Port Information window is displayed.

**END OF STEPS**

Create a VLAN on a virtual switch

1 Select **Provisioning → LAN Management → Virtual Switch**.

Result: The **Virtual Switch List** window appears and displays all virtual switches on the selected physical switch.

2 Select a virtual switch from the list and click **Details**.

Result: The **Virtual Switch Information** window appears.

3 To create a new VLAN click **Add** in the **VLAN** field and continue with step 7.
**Result:** The *Add Static VLAN Entry* window appears.

4 To edit an existing VLAN select a *VLAN* from the list and click *Details*.

**Result:** The *VLAN Information* window appears.

5 Click *Edit*.

**Result:** The *Edit Static VLAN Entry* window appears.

6 Fill in the *VLAN ID* and the *VLAN Label*.

**Additional info** Each VLAN id must be unique once per pack.

<table>
<thead>
<tr>
<th>To</th>
<th>Then</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add LAN/WAN port(s) into the tagged member of the VLAN</td>
<td>Select the port(s) from the Port List and add it to the Tagged Member list by using the →arrow button.</td>
</tr>
<tr>
<td>Remove LAN/WAN port(s) from the tagged member of the VLAN</td>
<td>Select the port(s) from the Untagged Member list and remove it by using the &lt;-arrow button.</td>
</tr>
<tr>
<td>Add LAN/WAN port(s) into the untagged member of the VLAN</td>
<td>Select the port(s) from the Port List and add it to the Untagged Member list by using the →arrow button.</td>
</tr>
<tr>
<td>Remove LAN/WAN port(s) from the untagged member of the VLAN</td>
<td>Select the port(s) from the Untagged Member list and remove it by using the &lt;-arrow button.</td>
</tr>
</tbody>
</table>

8 Click *Apply* and *OK*.

**Result:** The *VLAN Information* window reappears.

9 Click *Close* to exit.

**End of steps**

**Provision TUG structure and cross connections**

For provisioning the TUG structure and Cross Connections reference is made to:
- “Provision cross connections without protection” (p. 8-179)
Parameters for provisioning a LAN unit in repeater mode

Customer Identity (CID)
Customer Identity for a LAN port within virtual switch. This is an integer between 0 and 4093. The Customer Identifier separates the end users. For all switch modes other than repeater, if CID is 0 the system implicitly disables the functions of the corresponding LAN port. (i.e. for those switch modes only the values between 1 and 4093 are used to identify a customer in a network).

CIR
Committed Information Rate. CIR can be configured for each flow (default flow and user priorities)

LAN port
A LAN port is the physical port on the NE.

LAN port label
The label given to the LAN Port by the user. The label is a character string up to 20 characters long.

LAN members
LAN ports associated with the selected Virtual Switch.

LAN port ingress QoS
The following parameters for LAN port ingress QoS can be set:
- Traffic Class Assignment (mapping table or default over riding)
- CIR
- Mode of Operation (strict policing or over subscription)

LAN port egress QoS
The following parameters for LAN port Ingress QoS can be set:
- Scheduler Method (weighted bandwidth or strict priority)
- Weight
Port VLAN Identifier (PVID)

Incoming VLAN-untagged frames are tagged with a Port VLAN Identifier, which can be provisioned. The VLAN ID in the VLAN tags is used for the forwarding decision. Possible values are an integer in the range [1 .. 4093], or No PVID (no default value is to be used).

Rate control mode

The Rate Control Mode is displayed. The value will be the current mode of an existing Virtual Switch or to None for a new virtual switch.

Tagging mode

The tagging mode of the LAN unit configured as Repeater, LAN interconnect, MLAN (VPN) or MLAN (VPN) with QoS is transparent.

Virtual switch

A Virtual Switch is a set of LAN/WAN ports on a TransLAN® option board that are used by different VLANs which can share the common WAN bandwidth.

Virtual switch name

The name of the Virtual Switch as described in the port naming scheme document.

Virtual switch label

The label given to the Virtual Switch by the user when the Virtual Switch was created via the “Create/Edit Virtual Switch” screen. The label is a character string up to 20 characters long (for example Sales).

VCG name

The name of the VCG associated with the WAN port is fixed: VCG2.x, where VCG2 refers to the slot and x is the number of the VCG. This is the same number as the WAN port associated to the VCG1.

WAN port name

The WAN Port name is a fixed name: WAN2.x, where WAN2 refers to the slot and x is the number of the WAN port. The number of the WAN Port can be 1 up to 4.

WAN port members

WAN ports associated with the selected Virtual Switch.
WAN port egress QoS

The following parameters for LAN port egress QoS can be set:
- Scheduler Method (weighted bandwidth or strict priority)
- Weight

LAN port information details

This table gives an overview of the LAN port information details which, depending on the Virtual Switch mode, must be provisioned.

<table>
<thead>
<tr>
<th></th>
<th>Repeater</th>
<th>LAN Interconnect</th>
<th>LAN VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Label</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>CID</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>CIR</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Default User Priority</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Mode</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

WAN port information details

This table gives an overview of the WAN port information details which, depending on the Virtual Switch mode, must be provisioned.

<table>
<thead>
<tr>
<th></th>
<th>Repeater</th>
<th>LAN Interconnect</th>
<th>LAN VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Channel (VCG)</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

Virtual switch operation modes

The virtual mode can be set to:
- Point to point LAN. In this mode the Ethernet interfaces are connected in a point-to-point manner across the SDH network. The Virtual switch supports 1 LAN port and 1 WAN port. The principle of the TransLAN is described in “Concepts” (p. 9-3).
- LAN-Interconnect. In this mode a LAN group contains multiple LAN ports and multiple WAN ports. Only one end user is connected to one or up to four LAN port(s). The NE functions as a learning bridge; Spanning Tree algorithms are supported. The principle of the TransLAN+ type is described in “Concepts” (p. 9-3).
- LAN VPN (Virtual Private Network), also mentioned as M-LAN. In this mode a LAN group contains multiple LAN ports and multiple WAN ports. The LAN port(s) can be shared by multiple end users. The NE functions as a learning bridge; Spanning Tree algorithms are supported. The principle of the M-LAN type is described in “Concepts” (p. 9-3).

- LAN VPN with QoS (Virtual Private Network), also mentioned as M-LAN. In this mode a LAN group contains multiple LAN ports and multiple WAN ports. The LAN port(s) can be shared by multiple end users. On the LAN and WAN ports the Quality of Service parameters can be set. The NE functions as a learning bridge; Spanning Tree algorithms are supported. The principle of the M-LAN type is described in “Concepts” (p. 9-3).

### WAN port capacity

On the 1643 AM or 1643 AMS network element, there are 4 WAN ports totally in a LAN unit. The mode of the WAN ports 1~4 is given in the table below. Each mode stands for a type of the capacity combination of the WAN ports. Any other combination is not allowable currently. Each of the factors Xa, Xb, Xc, andXd can be range from 1 to 5 respectively.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Capacity WAN port 1</th>
<th>Capacity WAN port 2</th>
<th>Capacity WAN port 3</th>
<th>Capacity WAN port 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100 Mbit/s</td>
<td>Xb * 2 Mbit/s</td>
<td>Xc * 2 Mbit/s</td>
<td>Xd * 2 Mbit/s</td>
</tr>
<tr>
<td>2</td>
<td>50 Mbit/s</td>
<td>50 Mbit/s</td>
<td>Xc * 2 Mbit/s</td>
<td>Xd * 2 Mbit/s</td>
</tr>
<tr>
<td>3</td>
<td>50 Mbit/s</td>
<td>Xb * 2 Mbit/s</td>
<td>Xc * 2 Mbit/s</td>
<td>Xd * 2 Mbit/s</td>
</tr>
<tr>
<td>4</td>
<td>Xa * 2 Mbit/s</td>
<td>50 Mbit/s</td>
<td>Xc * 2 Mbit/s</td>
<td>Xd * 2 Mbit/s</td>
</tr>
</tbody>
</table>
Parameters for provisioning LAN unit in spanning tree mode

ALAF

The NE Automatic Learning and Forwarding Status [Enabled, Disabled].

Acceptable frame type (LAN port)

The Acceptable Frame Type mode of the LAN Port shall be displayed and shall be either: ‘All Frames’ or ‘VLAN Tagged’.

Acceptable frame type (WAN port)

The Acceptable Frame Type mode of the WAN Port shall be displayed and shall be either: ‘All Frames’ or ‘VLAN Tagged’.

Bridge address

The MAC address of the Virtual Switch.

Create time

The Creation Time of the Virtual Switch.

CIR

Committed Information Rate.

Ether type

Ethernet type

It is recommended only to provide one of the following two values:

- 0x8100
  for IEE802.1Q STP
- 0x9100
  for IEEE802.1ad STP

Flow type

The flow type can be set to Port/Userpriority/VLAN or Port/Userpriority.

GVRP

Dynamic VLAN Registration Protocol
QOS_CQS - LAN port ingress QoS

The following parameters for LAN port ingress QoS can be set:

- Traffic Class Assignment (mapping table or default over riding)
- CIR
- Mode of Operation (strict policing or over subscription)

QOS_CQS - LAN port egress QoS

The following parameters for LAN port egress QoS can be set:

- Scheduler Method (weighted bandwidth or strict priority)
- Weight

LAN port label

The label given to the LAN Port by the user. The label is a character string up to 20 characters long.

LAN members

LAN Ports associated with the selected Virtual Switch.

PVID

The Default VLAN number used for untagged packets.

PVID (WAN port)

Displays the port VLAN ID of the selected WAN port. PVID = 1...4093. The default VLAN number used for untagged packets (= 4094).

Rate control mode

The Rate Control Mode is displayed. The value will be the current mode of an existing Virtual Switch or to None for a new virtual switch.

STP

Spanning Tree Protocol Parameter.

STP bridge priority

The bridge priority of the Virtual Switch, the Virtual switch with the lowest value is elected the ‘root bridge’. An integer 0...65535.

STP root bridge address

The MAC address of the Virtual Switch which is the Root Bridge.
STP root bridge priority

The Virtual switch with the lowest bridge priority value is elected the ‘root bridge’. An integer 0...65535.

STP root cost

Indicates the cost of the path to the root as seen from the Virtual Switch. This will be displayed in s/20 Tb.

STP root port

The root port used for spanning tree algorithm.

Tagging mode

The tagging mode of the LAN unit configured as Repeater, LAN interconnect, MLAN (VPN) or MLAN (VPN) with QoS is transparent. The tagging mode of the LAN unit configured as Spanning Tree is IEEE802.1Q.

VCG name

The name of the VCG associated with the WAN port is fixed: VCG2.x, where VCG2 refers to the slot and x is the number of the VCG1. This is the same number as the WAN port associated to the VCG.

Virtual switch

A Virtual Switch is a set of LAN/WAN ports on a TransLAN® option board that are used by different VLANs which can share the common WAN bandwidth.

Virtual switch name

The name of the Virtual Switch as described in the port naming scheme document.

Virtual switch label

The label given to the Virtual Switch by the user when the Virtual Switch was created via the “Create/Edit Virtual Switch” screen. The label is a character string up to 20 characters long.

VLAN version number

The VLAN Version Number this only has one possible value ‘IEEE Std 802.1Q - 1998 Edition’.
VLAN ID max

On each unit (pack), the MAX VLAN number is 64 (GVRP enabled) or 100 (GVRP disabled) with 2000 VLAN associated ports. Given that the X4IP unit can support VLANs of at most 8 ports, the worst case upper limit for the 1643 AM/1643 AMS is 2000/8 = 250 VLANs.

VLAN ID

The unique ID for the VLAN. The ID is an integer between 1 and 4093.

VLAN label

The label given to the VLAN by the user. The label is a character string up to 32 characters long.

VLAN tagged (Tagging Mode)

The tagging status of this port in this VLAN. i802.1Q or Transparent.

VLAN status

The Status of the VLAN shall be ‘Static’ in the case of a user created VLAN and ‘Dynamic’ when created by ALAF. In the case of a VLAN with both dynamic and static sections the Status shall be ‘Composite’.

WAN port name

The WAN Port name is a fixed name: WAN2.x, where WAN2 refers to the slot and x is the number of the WAN port. The number of the WAN Port can be 1 up to 4.

WAN members

WAN Ports associated with the selected Virtual Switch.

WAN port ingress QoS

The following parameters for WAN port ingress QoS can be set:

- Traffic Class Assignment (mapping table or default over riding)

WAN port egress QoS

The following parameters for LAN port egress QoS can be set:

- Scheduler Method (weighted bandwidth or strict priority)
- Weight
LAN port information details

This table gives an overview of the LAN port information details which, depending on the Virtual Switch mode, must be provisioned.

<table>
<thead>
<tr>
<th></th>
<th>Repeater</th>
<th>Spanning Tree</th>
<th>LAN VPN</th>
<th>LAN Interconnect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Label</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>CID</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>CIR</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>PVID</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Default User Priority</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Acceptable Frame Type</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Ingress Filter</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

WAN port information details

This table gives an overview of the WAN port information details which, depending on the Virtual Switch mode, must be provisioned.

<table>
<thead>
<tr>
<th></th>
<th>Repeater</th>
<th>Spanning Tree</th>
<th>LAN VPN</th>
<th>LAN Interconnect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Channel</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Ingress Filter</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Acceptable Frame Type</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default User Priority</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>PVID</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>STP Port State</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>STP Port Priority</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>STP Port Path Cost</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>
WAN port capacity

On the 1643 AM or 1643 AMS network element, there are 4 WAN ports totally in a LAN unit. The mode of the WAN ports 1~4 is given in the table below. Each mode stands for a type of the capacity combination of the WAN ports. Any other combination is not allowable currently. Each of the factors Xa, Xb, Xc andXd can be range from 1 to 5 respectively.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Capacity WAN port 1</th>
<th>Capacity WAN port 2</th>
<th>Capacity WAN port 3</th>
<th>Capacity WAN port 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100 Mbit/s</td>
<td>Xb * 2 Mbit/s</td>
<td>Xc * 2 Mbit/s</td>
<td>Xd * 2 Mbit/s</td>
</tr>
<tr>
<td>2</td>
<td>50 Mbit/s</td>
<td>50 Mbit/s</td>
<td>Xc * 2 Mbit/s</td>
<td>Xd * 2 Mbit/s</td>
</tr>
<tr>
<td>3</td>
<td>50 Mbit/s</td>
<td>Xb * 2 Mbit/s</td>
<td>Xc * 2 Mbit/s</td>
<td>Xd * 2 Mbit/s</td>
</tr>
<tr>
<td>4</td>
<td>Xa * 2 Mbit/s</td>
<td>50 Mbit/s</td>
<td>Xc * 2 Mbit/s</td>
<td>Xd * 2 Mbit/s</td>
</tr>
</tbody>
</table>
Overview

Purpose

The switches on the data packs operate in self-learning mode, i.e. the source addresses (SA) of received frames are stored in a MAC address table and the destination addresses (DA) of received frames will be compared to those in the table to find the right egress port. Packets whose DA is not found in the table will be broadcasted to all relevant ports. The dynamic MAC address table entries age out after a while (300s) to make room for new entries.

The “Static MAC Address Provisioning” feature allows the user to make manual entries into the MAC address table. These entries are called static entries and are not subject to address aging. In case of unicast addresses a single egress port can be provisioned. In case of multicast addresses a list of egress ports can be provisioned.

The X4IP-V2 option card supports addition of static MAC address entries into the filtering database. These entries are not submitted to the ageing time process. Conversely, users can delete MAC address entries from the filtering database using configuration commands.

The X4IP-V2 option card supports static MAC address table management. Users can set a maximum limit for the number of MAC address entries that can be learned per V-LAN.

The 1643 AM/AMS supports the filtering database flushing function using configuration commands.

The X4IP-V2 option card supports the programmable ageing pass time feature. To learn the MAC address entries automatically, the ageing pass timer can be provisioned for a duration between 10 seconds to 630 seconds in steps of 10 seconds for the whole filtering database. The default value is 300 seconds. The X4IP-V2 option card supports queries for whole and static MAC address entries and dynamic MAC address entries by specifying the MAC address and V-LAN tag.

Contents

| Provision static MAC address table | 8-154 |
| Provision the MAC address learning mode | 8-157 |
| Provision the MAC address aging pass timer | 8-159 |
Provision static MAC address table

When to use

This procedure is used to provision the static MAC address table.

**Note:** The Provision static MAC address table procedure is also applicable to X5IP.

Before you begin

The items below gives information on tasks to perform before beginning the procedure:

- “Provisioning a virtual switch in spanning tree mode” (p. 8-132)
- Cross connection should be enabled “Provision cross connections without protection” (p. 8-179) and VCG should be set to monitored.

Provisioning the static MAC address table

1. Select **Provisioning → LAN Management → Virtual Switch**.
   
   **Result:** The *Virtual Switch List* window appears.

2. Select the **Physical Switch** and *Virtual Switch*.

3. Click **Static MAC Table**.
   
   **Result:** The *Static MAC Address Table* appears.

   In the *Static MAC Address List* the following is displayed for each list entry:

   - The *MAC Address*
   - The *VLAN ID*
   - The *Multicast Group ID*
   - The *Out Port.*

4. The following actions can only be performed when the static MAC address table is activated.

<table>
<thead>
<tr>
<th>If you want to</th>
<th>THEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>activate the static MAC address table,</td>
<td>click <strong>Enable</strong>.</td>
</tr>
<tr>
<td>If you want to</td>
<td>THEN</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>deactivate the static MAC address table,</td>
<td>click <strong>Disable</strong>.</td>
</tr>
<tr>
<td></td>
<td>When deactivating a static MAC address table, a warning screen is</td>
</tr>
<tr>
<td></td>
<td>displayed, indicating that all manual provisioned functions and all</td>
</tr>
<tr>
<td></td>
<td>related configurations will be lost.</td>
</tr>
</tbody>
</table>

5

<table>
<thead>
<tr>
<th>If you want to</th>
<th>Then</th>
</tr>
</thead>
<tbody>
<tr>
<td>add a static MAC address to the list,</td>
<td>click <strong>Add</strong>. The <em>Add Static MAC Address</em> window appears.</td>
</tr>
<tr>
<td></td>
<td>Goto Step 6</td>
</tr>
<tr>
<td>modify a static MAC address</td>
<td>select one entry in the list and click <strong>Edit</strong>. The *Edit Static</td>
</tr>
<tr>
<td></td>
<td><em>MAC Address</em> window appears. Goto Step 7</td>
</tr>
<tr>
<td>remove one element from the list.</td>
<td>select one entry in the list and click <strong>Remove</strong>.</td>
</tr>
<tr>
<td></td>
<td>Goto Step 9</td>
</tr>
</tbody>
</table>

6

In the field **VLAN ID** enter the ID you want to specify for the new static MAC address list entry.

In the field **MAC Address** enter the new MAC address.

**Result:** In the *Port List* field all ethernet port belonging to the respective virtual switch are displayed.

The *Out Port List* shows the selected ethernet ports, to which ethernet frames, with matching MAC address and VLAN ID, are to be forwarded to.

**Note:** For *Multicast MAC address* the *Out Port List* can consists of the *Port List* instead of a single destination port.

7

To add a port to the *Out Port List* select it in the *Port List* and click → button.

To remove a port from the *Out Port List* select it in the *Port List* and click ← button.

8

Click **Ok**.
Result: The MAC address is added to the Static MAC Address list in the Static MAC Address Table window.

9 Click Close.

Result: The Static MAC Address Table window is closed.

10 Click Retrieve MAC Address.

Result: The Retrieve MAC Address window appears.

11 In the Out Port List enter the MAC Address, VLAN ID and click Retrieve.

12 Click Flush MAC Address or Flush MAC Address Table.

Result: The Flush MAC Address window appears.

13 In the Flush MAC Address enter the MAC Address and VLAN ID and click Ok.

Result: The Flush MAC Address Table deletes all the entries at once whereas Flush MAC Address deletes one entry at a time.
Provision the MAC address learning mode

When to use

This procedure is used to provision the MAC address learning mode.

Note: The Provision the MAC address learning mode procedure is also applicable to X5IP.

Before you begin

The items below gives information on tasks to perform before beginning the procedure:

- “Provisioning a virtual switch in spanning tree mode” (p. 8-132)

Provisioning the static MAC address table

1. Select Provisioning → LAN Management → Virtual Switch.
   
   Result: The Virtual Switch List window appears.

2. Select the Physical Switch and Virtual Switch.

3. Click Details.
   
   Result: The Virtual Switch Information window appears.

4. Select one port of the Virtual Switch.
   
   Result: The MAC Address Control button is activated.

5. Click MAC Address Control.
   
   Result: The MAC Address Control window appears.

6. Click Edit.
The MAC Address Learning Mode can be used to define the learning and forwarding method for received ethernet frames.

- **automaticModeOn**: The source address of the frame will be automatically learned (i.e. dynamic MAC address entry is created or updated within the forwarding table). If there exists already a dynamic or static MAC address matching the destination address and vlanId of the frame, it will be forwarded according to the table entry; otherwise the frame will be forwarded to all output ports of the Virtual Switch, except the port where the frame was received.

- **automaticModeOff**: Received frames are not treated as input of the automatic learning process.

The packets will be handled in the following way:

- If there exists not a dynamic or static MAC address matching the source address and vlanId of the frame, the frame will be dropped and trapped into the CPU. A trap control reduces the traffic to the CPU to one MAC Address per second, which will be displayed in the Mismatched MAC Address List.

- If there exists a dynamic or static MAC address matching the destination address and vlanId of the frame, it will be forwarded according to the table entry.

Click Ok.

Result: The Edit MAC Address Control is closed.

Click Close.

Result: The MAC Address Control window is closed.

END OF STEPS
Provision the MAC address aging pass timer

When to use

This procedure is used to provision the MAC address aging pass timer.

Note: The Provision the MAC address aging pass timer procedure is also applicable to X5IP.

Before you begin

The items below gives information on tasks to perform before beginning the procedure:

- “Provisioning a virtual switch in spanning tree mode” (p. 8-132)

Provisioning the static MAC address table

1 Select Provisioning → LAN Management → LAN Unit.

   Result: The LAN Unit Information window appears.

2 In the Slot from the drop-down list box, select the respective card from the LAN Unit Information window.

   Result: The LAN Unit Information window is populated with information for this unit.

3 Click Edit.

   Result: The Edit LAN Unit Information window appears.

4 The aging time can be increased or decreased by changing the value in the Dynamic MAC Table Aging Pass Time (s) and click ok.

   Result: The Aging Pass Time is changed and displayed in the LAN Unit Information window.

5 Click Close.

END OF STEPS
Provision Quality of Service (QoS)

Overview

Purpose

Quality of Service is supported on the TransLAN® tributary board and the Gigabit Ethernet card. It is implemented as a DiffServ architecture applied to layer 2.

QoS control allows to differentiate between Ethernet frames with different priorities. If traffic with a high priority and traffic with a low priority compete for SDH capacity, the traffic with the high priority should be served first. This can be realized through QoS control.

References

“Quality of Service (QoS) overview” (p. 8-90)

Contents

| Provision the QoS profile definitions | 8-161 |
| Parameters for provisioning a QoS profile | 8-162 |
| View QoS profile information | 8-165 |
| View the details of a LAN/WAN port QoS parameters | 8-166 |
| Edit QoS mode | 8-167 |
| Provision QoS Flow Identification Table | 8-169 |
| Parameters for provisioning Flow Identification Tables | 8-172 |
| Edit the QoS egress details | 8-177 |
| Ingress rate control | 8-178 |
Provision the QoS profile definitions

When to use

Provision of the QoS Profile definitions is possible only if the QoS configuration capacity is set to Enable (see previous procedure).

Procedure

Complete the following steps to provision the QoS profile definitions:

1. Select Provisioning → LAN Management → QoS Profile
   
   Result: The NE LAN QoS Profile List window appears.

2. To add a QoS profile proceed with Step 3, to modify a QoS profile proceed with Step 4 and to delete a QoS profile proceed with Step 6.

3. Select Add Profile, fill the fields in the Add QoS Profile and click OK.
   
   Result: The new QoS profile is displayed in the NE LAN QoS Profile List list.

4. Select the corresponding profile and click Edit.
   
   Result: The parameter of the selected profile is displayed in the Edit QoS Profile screen.

5. Change the definition and click OK.
   
   Additional The parameters to be defined are described in “Parameters for provisioning a QoS profile” (p. 8-162).
   
   Result: The QoS profile is displayed in the NE LAN QoS Profile List list showing the changed parameters.

6. Select the corresponding profile and click on Delete.
   
   Result: The QoS profile is removed from the list.

END OF STEPS
Parameters for provisioning a QoS profile

Overview

The system allows you to create, edit, and delete QoS Profiles, however it is not possible to delete any “default QoS Profile”.

Profile-ID

Each profile has a unique Profile ID for future use (PM point identification).

Name

For any QoS Profile, including the default profiles, the system allows you to assign a name.

PrintableString SIZE: 1 .. 20

Default values:
- For default profiles assigned to NR ports: NR default profile’,
- For default profiles assigned to CR ports: ’CR default profile
- For other profiles: < no default >

A QoS Profile Name must be unique within the NE

Committed Information Rate (CIR)

For any QoS Profile, except the default profiles, the system allows you to assign a Committed Information Rate (CIR) (unit: kbit/s).

Values: [ 0, 150, 151, .... 1000, 1010, .... 10000, 10100, .... 100000, 101000, .... MAX ]

Default Value: 0

If other values as the defined are entered, the system rounds the value to the next allowed value.

For default QoS Profiles the CIR is only retrievable.

Peak Information Rate (PIR)

For any QoS Profile, except the default profiles, the system allows you to assign a Peak Information Rate (PIR) (unit: kbit/s).

Values: 0, 150, 151, .... 1000, 1010, .... 10000, 10100, .... 100000, 101000, .... MAX ]

Default value: 0

If other values as the defined are entered, the system rounds the value to the next allowed value.
From rate controller perspective 0 stops the whole traffic of this flow,
The PIR shall not be lower than the CIR.
For default QoS Profiles the PIR is only retrievable.

**Traffic Class**

For any QoS Profile, except the default profiles, the system allows you to assign a Traffic Class (TC).

Values: 0, 1, 2, 3, 0-, 1-, 2-, 3-, T
The system allows to assign Traffic Class T only to NR ports (with QoS mode = Default Profile), never to CR ports.
In case of Provider Bridge Mode (IEEE 802.1ad) the TC='1' is reserved for future use. Please do not use it in any QoS Profile.

**Committed Burst Size (CBS)**

For any QoS Profile, except the default profiles, the system allows you to assign a Committed Burst Size (CIR) (unit: kbit/s).

The following value range is supported for the attribute committed Burst Size (CBS):
- 0: only allowed if ethernetQoSProfileFlowCIR equals 0.
- 12 Kbyte, 13 Kbyte .. 100 Kbyte (i.e. in step of 1 Kbyte)
- 100 Kbyte, 110 Kbyte, .. 1000 Kbyte (i.e. in step of 10 Kbyte)
- 1000 Kbyte, 1100 Kbyte, .. 1300 Kbyte (i.e. in step of 100 Kbyte)
- 1400 Kbyte (this value is the maximal value for CBS called maxCBS)

**Important!** The following constraint must be met: PBS CBS

**CBS mode**

Determines whether the CBS value is derived from the attribute value ethernet QoS Profile Flow CIR or directly provisioned by the manager.

The following values are supported:
- Specified value: Committed Burst Size (CBS) is directly set as provisioned by the manager.
- Small bucket size:
  The value for the Committed Burst Size (CBS) is calculated in the following way:
  - CBS = 0.010 * (ethernetQoSProfileFlowCIR / 8)
  - if CBS == 0 then burstSizeValue = 0
If $0 < \text{CBS} \leq \text{maxCBS}$ then burstSizeValue will be set to the next greater or equal value from the allowed value range

- If CBS > maxCBS then burstSizeValue = maxCBS

**Large bucket size:**

The value for the Committed Burst Size (CBS) is calculated in the following way:

- CBS = 0.110 * (ethernetQoSProfileFlowPIR / 8)
- the burstSizeValue will be determined based on calculated CBS value.

**Peak Burst Size (PBS)**

For any QoS Profile, except the default profiles, the system allows you to assign a Peak Burst Size (PBS) (CIR) (unit: kbit/s).

**PBS mode**

Determines whether the PBS value is derived from the attribute value ethernet QoS Profile Flow PIR or directly provisioned.

The following values are supported:

- **Specified value:** Peak Burst Size (PBS) is directly set as provisioned by the manager.
- **Small bucket size:**
  
  The value for the Peak Burst Size (PBS) is calculated in the following way:
  
  - PBS = 0.010 * (ethernetQoSProfileFlowPIR / 8)
  - if PBS \(\text{== 0} \) then burstSizeValue = 0 (not consistent with rule CBS/PBS \(\geq 2\) kB. MR planned)
  - If $0 < \text{PBS} \leq \text{maxPBS}$ then burstSizeValue will be set to the next greater or equal value from the allowed value range
  - If PBS > maxPBS then burstSizeValue = maxPBS

- **Large bucket size:**
  
  The value for the Peak Burst Size (PBS) is calculated in the following way:
  
  - PBS = 0.110 * (ethernetQoSProfileFlowPIR / 8)
  - the burstSizeValue will be determined based on calculated PBS value.
View QoS profile information

When to use

To view the user details of the QoS profiles used in flow groups (Flow Identification Table = FIT).

Related information

Related information can be found in concept section “Quality of Service provisioning” (p. 8-103).

Procedure

Complete the following steps to display the details of the QoS profiles:

1. Select Provisioning → LAN Management → QoS Profile

   Result: The NE LAN QoS Profile List window appears.

2. Click on Close to exit the window.

   END OF STEPS
View the details of a LAN/WAN port QoS parameters

When to use

To allow the user to view the details of a LAN or WAN port's QoS parameters. LAN or WAN is used in the windows title as appropriate.

Procedure

Complete the following steps to provision the QoS profile definitions:

1. Select **Provisioning → LAN Management → Virtual Switch**
   
   **Result:** The Virtual Switches List window is displayed.

2. Select the respective virtual switch and click **Details**.
   
   **Result:** The Virtual Switch List Information window appears

3. Select the LAN/WAN port in the Port Membership field and click on **Port Details**.
   
   **Result:** The Customer/Network Port Information window is displayed.

**END OF STEPS**
Edit QoS mode

When to use

To allow the user to manage the configured flow profiles or to use the default flow profile.

Note: The Edit QoS mode procedure is also applicable to X5IP.

Procedure

Complete the following steps to edit the QoS mode:

1. Select **Provisioning → LAN Management → Virtual Switch**
   
   Result: The **Virtual Switch List** window is displayed.

2. Select the respective virtual switch and click **Details**.
   
   Result: The **Virtual Switch List Information** window appears

3. Click **Edit** and in the **Edit Virtual Switch** window select **TPID value** in the **Ether Type** area.
   
   It is recommended only to provide one of the following two values:
   
   - **0x8100**
     
     for IEE802.1Q STP
   
   - **0x9100**
     
     for IEEE802.1ad STP (provider bridge mode)

4. Select the LAN/WAN port in the **Port Membership** field and click on **Port Details**.
   
   Result: The **Port Information** window is displayed.

5. Click on **Edit**.
Result: The Customer/Network Port Information window is displayed.

6 In the field QoS Mode select the appropriate mode:
   - **Flow Configuration**: the Flow Profile definitions in the Virtual Port Descriptor (QoS Flow Tables) (refer to “Provision QoS Flow Identification Table” (p. 8-169)) are used for this port.
   - **Default Profile**: the default profile definitions are used for this port.

END OF STEPS
Provision QoS Flow Identification Table

When to use
To allow the user to edit the details of the LAN/WAN port QoS flow groups.

Note: The Provision QoS Flow Identification Table procedure is also applicable to X5IP.

Related information
Refer to “Quality of Service provisioning” (p. 8-103).

Procedure
Complete the following steps to edit the Flow Identification Table:

1. Select Provisioning → LAN Management → Virtual Switch
   Result: The Virtual Switches List window is displayed.

2. Select the respective virtual switch and click Details.
   Result: The Virtual Switch List Information window appears

3. Select a LAN/WAN port in the Port Membership field and click on Port Details.
   Result: The Customer/Network Port Information window is displayed.

4. **IF you want to**
   **THEN continue with**
   
<table>
<thead>
<tr>
<th>IF you want to</th>
<th>THEN continue with</th>
</tr>
</thead>
<tbody>
<tr>
<td>add a new Flow Table</td>
<td>Step 5</td>
</tr>
<tr>
<td>insert a Flow Group</td>
<td>Step 7</td>
</tr>
<tr>
<td>edit a Flow Group</td>
<td>Step 11</td>
</tr>
<tr>
<td>delete a Flow Group</td>
<td>Step 14</td>
</tr>
<tr>
<td>delete a Flow Table</td>
<td>Step 16</td>
</tr>
</tbody>
</table>

5. Click on Add Flow Table.
   Result: The Add Flow Table window is displayed.

6. In the Descriptor field enter none.
Result The two default Flow Descriptors none and other are created.

7 Select a flow descriptor other than the flow table none.

Result: The fieldInsert Flow Groupis applicable.

8 Click on Insert Flow Group.

Result: The Insert Flow Group screen is displayed.

9 In the Descriptor field enter an appropriate descriptor and in the Profile ID field enter the ID of the QoS profile to be used.

Additional info Refer to “Parameters for provisioning Flow Identification Tables” (p. 8-172).

10 Continue with Step 18.

11 Choose the Flow Group in the list and click on Edit Flow Group.

Result: The Edit Flow Group screen is displayed.

12 In the Descriptor field enter an appropriate descriptor and in the Profile ID field enter the ID of the QoS profile to be used.

Additional info Refer to “Parameters for provisioning Flow Identification Tables” (p. 8-172).

13 Continue with Step 18.

14 Select the Flow Group in the list and click on Delete Flow Group.

Result: The selected Flow Group is deleted.

15 Continue with Step 18.

16 Select the respective entry (with the descriptor none) in the list and click on Delete Flow Table.
Result: The selected Flow Table is deleted.

17 Continue with Step 18.

18 Click on OK for confirmation.

19 Click on Close to exit the window.

END OF STEPS
Parameters for provisioning Flow Identification Tables

Overview

The system allows you to create, edit, and delete FITs per port. The concept of the Flow Identification Tables is described in “Quality of Service provisioning” (p. 8-103).

The FIT contains a restricted number of lines. Each line can contain a pair of one Flow Descriptor (FD) and 1 QoS_Profile (refer to “Parameters for provisioning a QoS profile” (p. 8-162)).

Example:

Insert Flow Group screen

The Flow Descriptor (FD) and QoS_Profile are created, edited via specific screens, the Insert Flow Group screen and the Edit Flow Group screen.
Virtual Port Descriptor (VPD) / Flow Identification Table

The major identifier of a FIT is the Virtual port descriptor (VPD). For each FIT assigned to a port, the system allows you to provision exactly one virtual port descriptor (VPD).

The VPD consists of S-VID and S-UP, which will be entered as follows:

\[
\text{SVID} = \text{<value>} \& \& \text{SUP} = \text{<value>}
\]

**S-VID**

S-VID is the VLAN ID of a S-tag. S-tag is the server tag (tag used by the provider only).

For any S-VID defining a virtual port, the system allows you to provision the following:
- Possible values: 1, 2, 3, ..., 4093, RANGE(), ENUMERATION(), all

**S-UP**

S-UP is the user priority of the server tag S-tag.

Possible values: 0, 1, 2, 3, 4, 5, 6, 7, MASKx2x1x0, all ]

Default value: all

**Provisioning constraints**

The following constraints apply:
- Allowed values for a FIT assigned to a customer role port: *no Virtual port descriptor (VPD)*
- Allowed values for a FIT assigned to a network role port: S-Tag (S-VID; S-UP)
- Default values for a FIT assigned to a customer role port: none
- Default values for a FIT assigned to a network role port: no default value
- Customer role ports with 'QoS_portmode = Flow_Configuration' have exactly one VPD assigned.
- Network role ports with 'QoS_portmode = Flow_Configuration' have one or more VPDs assigned.
- None of them shall be 'VPD = no_virtual_port'.

The port is converted from a DiffServInt port to a DiffServEdge port at the moment when the QOS_portmode is set to 'Flow_Configuration'.

Be aware that all VPDs of a physical network role port need not cover all possible S-VID / S-UP combinations.
- Be aware that all defined S-VID / S-UP combinations shall be unique.
- The number of ports having 'VPD = S-Tag()' shall be restricted to max. 4, if the number is not otherwise even more restricted.
Flow Descriptor (FD)

For each customer role port one Flow Identification Table (FIT) can be assigned. For each virtual port one Flow Identification Table (FIT) can be assigned. A FIT is structured in lines. Each line allows to enter a Flow Descriptor.

For any FIT, the system shall allow the user to add or delete the last-but-1’th Flow Descriptor.

Possible values:
- C-Tag(C-VID; C-UP)
  
  Example: CVID=128&CUP=2
- IPTOScTagged (TOSbyte),
- IPTOSuntagged (TOSbyte),
- DA (MACaddress; MACmask)

  Example: DA=<MAC address>

C-VID

C-VID is the VLAN ID of a c-tag. C-tag is the customer tag.

For any C-VID defining a virtual port, the system allows you to provision the following

- Possible values: [1, 2, 3, ..... 4093, MASKx_{11}x_{10}x_{9}x_{8}x_{7}x_{6}x_{5}x_{4}x_{3}x_{2}x_{1}x_{0}, ANY_C-VID ]
  
  ANY_C-VID is a ‘don’t care’ - criteria for the C-VID,
  
  xi = { 0, 1, X}, X is a don’t care for this bit position

- Default: no default value

C-UP

C-UP is the user priority of the customer tag c-tag.

Possible values: 0, 1, 2, 3, 4, 5, 6, 7, MASKx_{2}x_{1}x_{0}, all ]

Default value: all

TOSbyte

For any IPTOScTagged (TOSbyte) or IPTOSuntagged (TOSbyte), the system allows you to provision the following:

- Possible values: [MASKx_{7}x_{6}x_{5}x_{4}x_{3}x_{2}x_{1}x_{0}]
  
  xi = { 0, 1, X}, X is a don’t care for this bit position

- Possible parameters: ITT and ITU.
Syntax for IPTOScTagged (TOSbyte)

- **ITT=VALUE** - VALUE is an Integer with range 0 ... 255, representing the decimal value of a byte.
- **ITT&VALUE** - VALUE is an 8 bit word, where a "1" and a "0" represents the actual value of the range and position, and an "x" represents a don’t care condition.

**Note: ITT stands for IP TOS Tagged:** The IP-TOS value of the IP payload of the tagged frame is taken as a flow descriptor. To be able to filter on the IP-TOS information in the IP payload the switch needs to know whether the Ethernet frame is VLAN tagged or untagged. IP-TOS stands for Internet Protocol - Type Of Service.

Syntax for IPTOSuntagged (TOSbyte)

- **ITU=VALUE** - VALUE is an Integer with range 0 ... 255, representing the decimal value of a byte.
- **ITU&VALUE** - VALUE is an 8 bit word, where a "1" and a "0" represents the actual value of the range and position, and an "x" represents a don’t care condition. The combined mask value is “xxxx1xxx” and the “1” stands for the actual value to be selected on in the TOS byte bit position for the Max Throughput.

**Note:** To discriminate on untagged frames with the Max Throughput bit set the following flow Descriptor needs to be determined as follows. The discriminative bit is the 4th bit of the TOS byte with the value “1”. This needs to be determined on untagged (customer) frames.

**Note: ITU stands for IP TOS Untagged:** The IP-TOS value of the IP payload of the untagged frame is taken as a flow descriptor. To be able to filter on the IP-TOS information in the IP payload the switch needs to know whether the Ethernet frame is VLAN tagged or untagged. IP-TOS stands for Internet Protocol - Type Of Service.

**DA**

The DA flow descriptor is used to either enter

- the MAC address or
  
  Each byte can range from 00, 01, 02, ..., to ... FD, FE, FF.

- the MAC mask
  
  Each byte can range from 00, 01, 02, ..., to ... FD, FE, FF. In the binary presentation of each BYTE each - binary 0 indicates a don’t care for the related bit, binary 1 indicates a significant related bit in the binary presentation of the related BYTE of the MAC address.

**Provisioning constraints**

The last Flow Descriptor entry in a FIT is always: OTHERS,
Only one value is allowed per line of a FIT, the parameter of this `Value`, however, may be composed of several instances of for example, C-VIDs by using the terms as defined in the following requirements, for example, by MASKS:

- In IEEE single tagging mode C-VID must be element of S-VID, C-UP must be element of S-UP, otherwise an empty flow is defined.
- Because in case of IEEE single tagging mode the C-tag and the S-tag are identical, at a network role port only those C-VID values will be matched which are also defined as a value to the S-VID of the VPD.
- In general, in PBM it is needed to define as a precondition for classifying according the IP-TOS byte whether the frames received at the CR port are expected to have a C-tag or not (except an automatic is build in the HW)
- For a Galnet data unit it is needed in IEEE single tagging mode to define as a precondition for the FD, if the received frames are expected to have a C-tag or not.
- Uniqueness of the flows defined by a Flow Descriptor in comparison to other Flow Descriptors is not needed.
Edit the QoS egress details

Related information

Refer to “Classification, queueing, and scheduling” (p. 8-94).

Procedure

Complete the following steps to edit the details of a LAN / WAN port egress QoS

1. Select **Provisioning → LAN Management → Virtual Switch**
   
   Result: The Virtual Switch Information window is displayed.
   
   The information regarding QoS Egress is displayed in the QoS **Egress Queue** information field.

2. Select one egress queue and click on **Edit...**
   
   Result: The Edit Egress Queue Information window is displayed.

3. Use the radio buttons (Weighted Bandwidth and Strict Priority) to select the scheduler method and click on **OK**.

4. To modify the value for the modified weight enter the desired value in the field on the left bottom of the screen and then click on the button with the > (right arrow) symbol.

5. Click on **OK**.
   
   Result: A Service affecting Warning Screen is displayed.

6. Click on **Yes**.
   
   Result: The Virtual Switch Information window is displayed again.

END OF STEPS
Ingress rate control

When to use

The following procedure is performed in order to find the Ingress rate control.

Before you begin

The items below gives information on tasks to perform before beginning the procedure:

- Proper LAN card must be installed in TS2.

Ingress rate

Follow this procedure in order to view the Ingress rate control:

   Result: The NE LAN QoS Profile List window appears.

2. Select a profile from the Profile List and click Edit.
   Result: The Edit QoS Profile window appears.

3. In the Edit QoS Profile window select the CBS, PBS modes and Traffic class from the drop down list and CIR, PIR, and CBS, PBS size should be provisioned and then click Ok.
   Result: The window is populated with the new information.

END OF STEPS
Provision cross connections without protection

Overview

Purpose

To provide traffic over the network all cross connections must be provisioned. The cross-connection settings can be modified if the traffic demand changes. The following changes can be made:

- add a new cross-connection or add a leg to an existing cross-connection
- delete a cross-connection.

Contents

| Creating cross connections without protection | 8-180 |
| Deleting cross connections | 8-182 |
| Parameters for provisioning cross connections without protection | 8-183 |
Creating cross connections without protection

When to use

When a new traffic plan is implemented or the existing traffic plan is changed.

Related information

The following procedures are used for test and maintenance of the provisioned path. These procedures are described in Chapter 9, “Traffic maintenance”.

- port provisioning.
- provisioning termination points
- path trace provisioning
- for theoretical information see section Traffic Maintenance Concepts.

Before you begin

To make a cross-connection first determine the following

- What is the capacity of the cross-connection? VC-12, VC-3 or VC-4
- Will the cross connection be used as a loopback for maintenance purposes
- Does the cross connection require SNC protection or is it unprotected (Standard)
- Between which termination points (TP) is the cross connection made
- Before adding a cross connection and, if desired its protection, be sure to have information regarding the design of the transmission path
- Before deleting a cross connection or part of a cross connection be sure to know whether the cross connection to be removed still carries traffic? If yes this traffic will be lost after removing the cross-connection
- Deleting or changing a cross-connection is traffic affecting if the current existing cross-connection is carrying traffic.

Procedure

Use the following procedure to add a cross-connection in the 1643 AM or 1643 AMS network element.

1 Select Provisioning - Transport - Cross Connection.  
   **Result:** The Cross Connection Filter window appears.

2 Select the Cross Connection Type, Capacity, Directionality, TP, Slot, Port, and the AU4 number in the Cross Connection Filter window and select OK.
Result: All available cross connections that meet the selected filter criteria are listed in the Cross Connection Selection List window. The filter criteria are displayed in the filter area.

3 Select Add in the CC area.

Result: The Add Cross Connection window appears.

4 Select the Capacity and set the Cross Connection Type to Standard. Select the Slot and Port and click select for each termination point in the From and To fields.

Result: A list of available termination points appears for each termination point.

5 Select one TP in each field and select Apply. Select OK if no other cross connections are to be made.

Result: The TPs appear in the Selection boxes. The cross-connection between the selected TPs is made. If OK was selected the Add Cross Connection window closes and the new cross connections appear in the list of the Cross Connection List window.

END OF STEPS
Deleting cross connections

When to use

When a new traffic plan is implemented or the existing traffic plan is changed use this procedure to delete cross connections.

Related information

Precautions:

- Before deleting a cross-connection or part of a cross-connection be sure to know whether the cross-connection to be removed still carries traffic? If yes this traffic will be lost after removing the cross-connection
- Deleting or changing a cross-connection is traffic affecting if the current existing cross-connection is carrying traffic

Procedures

Use the following procedure to delete an existing cross-connection. This procedure can be used to delete any cross connections.

1. Select Provisioning -> Transport -> Cross Connection.
   
   Result: The Cross Connection Filter window appears.

2. Select the filter Cross Connection Type, Capacity, Directionality, TP, Slot, Port, and the AU4 number and select OK.
   
   Result: The Cross Connection Selection List window appears with all available cross connections that meet the selected filter criteria. The filter criteria are displayed in the filter area of the Cross Connection Selection List window.

3. Select the cross-connection to be deleted from the list and select Delete in the CC area.
   
   Result: A confirmation window appears.

4. Click Yes to confirm the removal of the cross-connection.
   
   Result: The cross-connection is removed. The cross-connection disappears from the list in the Cross Connection List window.
Parameters for provisioning cross connections without protection

The following parameters are used to provision cross connections without protection.

Capacity

The capacity of the cross-connection: This can be VC-4, VC-3, or VC-12.

Cross Connection type

The following types of cross connections are possible:

- **Standard**: this is a cross-connection without protection.
- **SNC**: a cross-connection with SNC protection.

Directionality

*Uni*: unidirectional or *Bi*: bidirectional

**Important!** The 1643 AM or 1643 AMS only supports unidirectional and bi-directional cross-connects.

Termination Points (TP)

The cross connections are made between termination points. The *From*, *To* and *Protection* columns are used to select these termination points. The *Protection* area is greyed out if *standard* is selected as *Cross Connection Type*.

For unprotected cross connections it makes no difference which TP is selected in the From and which TP is selected in the To list.

For a loopback connection, the direction is always unidirectional and the termination points in the From and To list are the same.

The termination point is selected by the *Slot* and *Port* where the termination point belongs to. The *AU4#* is 1 for STM-1 ports. AU# can be 1, 2, 3 or 4 for STM-4 ports. Example:
Provision cross connections with SNC protection

Overview

Purpose

To provide traffic over the network, cross connections must be provisioned in the network elements. The cross-connection settings can be modified if the traffic demands changes. The following changes can be made:

- add a cross-connection
- add protection to or remove protection from an existing cross-connection
- delete a cross-connection.

Contents

<table>
<thead>
<tr>
<th>Add SNC/N protection to an unprotected cross-connection</th>
<th>8-185</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove protection from an SNC/N protected cross-connection</td>
<td>8-187</td>
</tr>
<tr>
<td>Delete an existing cross-connection</td>
<td>8-189</td>
</tr>
<tr>
<td>Parameters for provisioning a cross-connection with SNC protection</td>
<td>8-191</td>
</tr>
</tbody>
</table>
Add SNC/N protection to an unprotected cross-connection

When to use

When a new traffic plan is implemented or the existing traffic plan is changed.

Related information

This section describes the provisioning of protected transmission paths. The provisioning of paths with no protection is described in previous section “Provision Cross Connections without Protection”

The following procedures are used for test and maintenance of the provisioned path. These procedures are described in Chapter 9, “Traffic maintenance”.

• port provisioning.
• provisioning termination points
• path trace provisioning
• for theoretical information see “Concepts” (p. 9-3).

Before you begin

To add protection to an unprotected cross-connection first determine the following:

• What is the capacity of the cross-connection? VC-12, VC-3, or VC-4?
• Does the cross-connection require SNC protection
• Between which termination points (TP) is used for the SNC protection path
• Before adding the protection, be sure to have information regarding the design of the transmission path

Procedure

1. Select Provisioning -> Transport -> Cross Connection.
   
   Result: The Cross Connection Filter window appears.

2. Select the Cross Connection type, Capacity, Directionality, TP, Slot, Port, and the AU-4 number and select OK.
   
   Result: The Cross Connection Selection List window appears with all available cross connections that meet the selected filter criteria. The filter criteria are displayed in the filter area of the Cross Connection Selection List window.

3. Select the unprotected cross-connection from the list and select Edit in the CC area.
Result: The Edit Cross Connection window appears. The From and To fields are filled in according to the selected cross-connection.

4 Change Cross Connection Type from Standard to SNC and select the Slot and the Port in the protection area. Click select.

Result: A list of available termination points appears, including the termination points of the selected cross-connection.

5 Select a TP.

Result: The TP appears in the selection box.

6 Select OK.

Result: The cross-connection between the selected TPs is made. The Edit Cross Connection window closes and the modified cross-connection appears in the list of the Cross Connection List window.

END OF STEPS
Remove protection from an SNC/N protected cross-connection

When to use

When a new traffic plan is implemented or the existing traffic plan is changed.

Related information

This section describes the provisioning of protected transmission paths. The provisioning of paths with no protection is described in previous section “Provision Cross Connections without Protection”

The following procedures are used for test and maintenance of the provisioned path. These procedures are described in Chapter 9, “Traffic maintenance”.

- port provisioning.
- provisioning termination points
- path trace provisioning
- For theoretical information see section Traffic Provisioning Concepts.

Before you begin

To remove the protection from a protected cross-connection first determine the following:

- What is the capacity of the cross-connection? VC-12, VC-3, or VC-4?
- Does the cross-connection require to be unprotected (Standard)?
- Which termination points are used for the SNC protection path
- Removing the protection of the cross-connection degrades the transmission path. The transmission path is no longer protected. A failure in the signal results in loss of traffic.

Procedure

1. Select Provisioning -> Transport -> Cross Connection.

   **Result:** The Cross Connection Filter window appears.

2. Select the Cross Connection type, Capacity, Directionality, TP, Slot, Port, and the AU-4 number and select OK.
Result: The Cross Connection Selection List window appears with all available cross connections that meet the selected filter criteria. The filter criteria are displayed in the filter area of the Cross Connection Selection List window.

3 Select the protected cross-connection from the list and select Edit in the CC area.

Result: The Edit Cross Connection window appears. The From and To and Protection fields are filled in according to the selected cross-connection.

4 Change Cross Connection Type from SNC to Standard and click OK.

Result: The protection leg is removed. An unprotected cross-connection remains. The Edit Cross Connection window closes and the modified cross-connection appears in the list of the Cross Connection List window.

END OF STEPS
Delete an existing cross-connection

When to use

When a new traffic plan is implemented or the existing traffic plan is changed.

Related information

This section describes the provisioning of protected transmission paths. The provisioning of paths with no protection is described in previous section “Provision Cross Connections without Protection”

The following procedures are used for test and maintenance of the provisioned path. These procedures are described in Chapter 9, “Traffic maintenance”.

• port provisioning.
• provisioning termination points
• path trace provisioning
• for theoretical information see “Concepts” (p. 9-3).

Before you begin

To delete a cross-connection first determine the following:

• What is the capacity of the cross-connection? VC-12, VC-3, or VC-4?
• Does the cross-connection have SNC protection or is it unprotected (Standard)?
• Between which termination points (TP) is the cross-connection made
• Does the cross-connection to be removed still carry traffic?

Procedure

1 Select Provisioning -> Transport -> Cross Connection.
   Result: The Cross Connection Filter window appears.

2 Select the Cross Connection type, Capacity, Directionality, TP, Slot, Port, and the AU-4 number and select OK.
   Result: The Cross Connection Selection List window appears with all available cross connections that meet the selected filter criteria. The filter criteria are displayed in the filter area of the Cross Connection Selection List window.

3 Select the cross-connection to be deleted from the list and click Delete in the CC area.
Result: A confirmation window appears.

4 Click **Yes** to confirm the removal of the cross-connection.

**Result:** The cross-connection is removed. The cross-connection disappears from the list in the *Cross Connection List* window.

**END OF STEPS**
Parameters for provisioning a cross-connection with SNC protection

The following parameters are used to provision cross connections without protection.

**Capacity**

The capacity of the cross-connection: This can be VC-4, VC-3, or VC-12.

**Cross Connection type**

The following types of cross connections are possible:

- *Standard*: this is a cross-connection without protection.
- *SNC*: a cross-connection with SNC protection.

**Directionality**

*Uni*: unidirectional or *Bi*: bidirectional

**Important!** The 1643 AM or 1643 AMS only supports unidirectional cross-connects.

**Termination Points (TP)**

The cross connections are made between termination points. The *From, To* and *Protection* columns are used to select these termination points. The *Protection* area is greyed out if *standard* is selected as *Cross Connection Type*.

For unprotected cross connections it makes no difference which TP is selected in the From and which TP is selected in the To list.

For a loopback connection, the direction is always unidirectional and the termination points in the From and To list are the same.

The termination point is selected by the *Slot* and *Port* where the termination point belongs to. The *AU4#* is 1 for STM-1 ports. AU# can be 1, 2, 3 or 4 for STM-4 ports. Example:

```
LP1.1,1
```

**Existence**

A *Virtual* termination point is a point which is not connected to a physical unit. These points are used to implement cascaded cross connections. All other termination points are *Real*
View or Edit the LTU information

Overview

Purpose

To view or edit card level transport parameters for the SHDSL option card on the 1643 AM or 1643 AMS LTU.

Contents

| View the LTU information                  | 8-193 |
| Edit the LTU Information                  | 8-194 |
| Parameters for viewing or editing LTU information | 8-195 |
View the LTU information

When to use
To view or edit the card level transport parameters for the SHDSL option card on the 1643 AM or 1643 AMS LTU.

Related information
No related information is available.

Before you begin
No prerequisites or precautions are needed when performing this procedure.

Procedure

1 Select Provisioning —> SHDSL —> LTU
   Result: The LTU Information window is displayed. Displayed is information about the selected LTU device.

2 Click Close to exit this window
   Result: The window closes.

END OF STEPS
Edit the LTU Information

When to use

When a new traffic plan is implemented or the existing traffic plan is changed.

Related information

No related information is available.

Before you begin

No prerequisites or precautions are needed when performing this procedure.

Procedure

1. Select “Edit” on view LTU Information
   
   Result: The Edit LTU Information window is displayed.

2. Select the SHDSL Transport Mode E1 or TU12.

3. Click OK the screen closes if the job completes successfully.

END OF STEPS
Parameters for viewing or editing LTU information

Selection

Display the slot name of the LTU device (read only).

SHDSL Transport Mode

Displays the transport mode as “E1” or “TU12”. The available choices are populated dynamically by receiving the available values from the MIB image.
View or Edit the SHDSL connection information

Overview

Purpose

To view information about the connection between SHDSL local ports and SHDSL remote ports

Contents

<table>
<thead>
<tr>
<th>Content</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>View the SHDSL connections</td>
<td>8-197</td>
</tr>
<tr>
<td>Update the SHDSL connection list</td>
<td>8-198</td>
</tr>
<tr>
<td>Details of the SHDSL Connection List</td>
<td>8-199</td>
</tr>
<tr>
<td>Parameters for viewing or editing the SHDSL connections list</td>
<td>8-200</td>
</tr>
</tbody>
</table>
View the SHDSL connections

When to use

To view the SHDSL connections between local ports and remote ports. The SHDSL connection information can be used to check the SHDSL capacity.

Related information

No related information is available.

Before you begin

No prerequisites or precautions are needed when performing this procedure.

Procedure

1. Select Provisioning —> SHDSL —> Connection/NTU
   
   **Result:** The SHDSL Connection List window is displayed.

2. Click Close to exit this window
   
   **Result:** The window closes.

_End of steps_
Update the SHDSL connection list

When to use

To update the window with the most recent information. If the window is open for some time the data displayed may not be current anymore. The update button allows the user to obtain the most recent information.

Related information

No related information is available.

Before you begin

No prerequisites or precautions are needed when performing this procedure.

Procedure

1. Select Provisioning —> SHDSL —> Connection/NTU
   
   **Result:** The SHDSL Connection List window is displayed.

2. Select Update
   
   **Result:** The window is updated with the most recent SHDSL connection information.

3. Click Close to exit this window.
   
   **Result:** The SHDSL Connection List window closes.

END OF STEPS
Details of the SHDSL Connection List

When to use

To view or to edit the selected NTU.

Related information

No related information is available.

Before you begin

No prerequisites or precautions are needed when performing this procedure.

Procedure

1. Select Provisioning —> SHDSL —> Connection/NTU
   
   **Result:** The SHDSL Connection List window is displayed.

2. Select one SHDSL connection from the list.

3. Click NTU Details
   
   **Result:** The NTU Information window is displayed.

END OF STEPS
Parameters for viewing or editing the SHDSL connections list

LTU Port
Displays in alphabetical order the name of the SHDSL local port.

NTU/SRU port
Displays in alphabetical order the name of the SHDSL remote port.

Alias ID
Displays in numerical order the alias ID of the NTU device.

Location
Displays in alphabetical order the name of the NTU device.

Node Name
Displays in alphabetical order the name of the node.
View or Edit the NTU information

Overview

Purpose

To view or to edit information about modems connected to the selected LTU.

Contents

| Update the NTU information                  | 8-202 |
| View the NTU information                    | 8-203 |
| Edit the NTU information                    | 8-204 |
| View or Edit NTU's General Configuration    | 8-205 |
| Remote SHDSL Power Supply (RPS)             | 8-207 |
| VC 12 termination point information         | 8-208 |
| Update the VC 12 termination point information window | 8-209 |
| Report the VC 12 termination point information list | 8-210 |
| Edit the VC 12 termination point information list | 8-211 |
| Parameters for viewing or editing NTU information and VC 12 termination point information | 8-213 |
| Provisioning the SHDSL on the NT10ETH modem | 8-215 |
Update the NTU information

When to use

To update the window with the most recent information. If the window is open for some time the data displayed may not be current anymore. The update button allows the user to obtain the most recent information.

Related information

No related information is available.

Before you begin

No prerequisites or precautions are needed when performing this procedure.

Procedure

1. Select Provisioning —> SHDSL —> Connection/NTU
   
   **Result:** The SHDSL Connection List window is displayed.

2. Select one SHDSL connection from the list.

3. Select NTU Details
   
   **Result:** The NTU information window is displayed.

4. Click Update
   
   **Result:** The window is updated with the most recent LTU modem information.

5. Click Close to exit this window.
   
   **Result:** The window closes.

END OF STEPS
View the NTU information

When to use
To view information about modems connected to the selected LTU.

Related information
No related information is available.

Before you begin
No prerequisites or precautions are needed when performing this procedure.

Procedure

1. Select Provisioning —> SHDSL —> Connection/NTU
   Result: The SHDSL Connection List window is displayed.

2. Select one SHDSL connection from the list.

3. Click NTU Details
   Result: The NTU Information window is displayed.

4. Click Close to exit this window
   Result: The window closes.

End of steps
Edit the NTU information

When to use

To display and set the name and alias ID of the NTU device.

Related information

No related information is available.

Before you begin

No prerequisites or precautions are needed when performing this procedure.

Procedure

1. Select Provisioning —> SHDSL —> Connection/NTU.
   
   **Result:** The SHDSL Connection List window is displayed.

2. Select one SHDSL connection from the list.

3. Click NTU Details.
   
   **Result:** The NTU Information window is displayed.

4. Click Edit
   
   **Result:** The **Edit Remote Node** Information window is displayed.

5. Set the name and location of the NTU device and type the password and confirm the web access password.

6. Click OK to commit changes to the NE and close the window.

**END OF STEPS**
View or Edit NTU's General Configuration

When to use
To view the NTU's Bridge mode, VLAN, and QoS functionality support

Before you begin
No prerequisites or precautions are needed when performing this procedure.

Procedure

1. Select Provisioning —> SHDSL —> Connection/NTU.
   Result: The SHDSL Connection List window is displayed.

2. Select one SHDSL connection from the list.

3. Click Virtual Switch .
   Result: The Remote Virtual Switch Information window appears.

4. Click Edit.
   Result: The Edit Remote Virtual Switch Information window appears.

5. In the Remote Virtual Switch Mode, select the appropriate mode and from the drop down list select None or Strict Policy for Remote Ingress Rate Control and click Ok.
   The Virtual switch modes are:
   • Self Learning Bridge
   • Vlan Bridge
   • Provider Bridge
   Result: The window is populated with the new information.

6. In Remote Virtual Switch Information window select the port and click on Port Details.
   Result: The Remote LAN CTP Information window appears.

7. Click Edit and provision the CIR, CBS and Default Vlan ID values and click Ok.
8 If the **Remote Virtual Switch Mode** is *Vlan Bridge* then click **Add**.

**Result:** The **Add Static VLAN Entry** window appears.

9 Fill in the ID, Label, and select the Ports and Click **Ok**.

10 Click **Details** or **Delete** to view the details of the VLAN or to delete the VLAN entry.

11 Click **VCG** from the main window.

**Result:** The **Remote VCG Information** window appears.

12 Click **Edit**.

**Result:** The **Edit Remote VCG** window appears.

13 Select *Enabled* or *Disabled* for the **LCAS Mode**, **CA-CSF** and **CA-SSF** and click **Ok**.

**Result:** The window is populated with the new information.

---

**END OF STEPS**
Remote SHDSL Power Supply (RPS)

When to use

To view or to edit the information on Remote Power Supply.

Before you begin

No prerequisites or precautions are needed when performing this procedure.

Procedure

1. Select **Provisioning → Equipment → RPS**.
   
   **Result:** The **Remote Power Supply Box Information** window appears.

2. Click **Edit**.
   
   **Result:** The **Edit RPS Box Information** window appears.

3. Select **Managed** or **Unmanaged** radio button and click **Ok**.

4. If the **RPS Management Mode** is Managed, the window will be populated with **RPS MDI**, **RPS MDO** and **RPS Port** information.

5. Click **Edit** and set the name and also set the status to **Active** or **Inactive** in the **Edit RPS MDO Information** window.

6. Set the **Alarm Suppressed** to **True** or **False** from the **Edit RPS Port Information** window and click **Ok**.
   
   **Result:** The window is populated with new information.
VC 12 termination point information

When to use

To view or edit the VC 12 termination point information of the SHDSL application.

Related information

No related information is available.

Before you begin

No prerequisites or precautions are needed when performing this procedure.

Procedure

1. Select Provisioning —> SHDSL —> Connection/NTU
   
   Result: The SHDSL Connection List window is displayed.

2. Select one SHDSL connection from the list.

3. Click VC12 Termination
   
   Important! The VC12 Termination button is active only when the selected LTU/NTU connection is in TU12 mode.
   
   Result: The VC12 Termination Point Information window is displayed.

4. Click Close to exit this window
   
   Result: The window closes.

End of steps
Update the VC 12 termination point information window

When to use

To update the window with the most recent information. If the window is open for some time the data displayed may not be current anymore. The update button allows the user to obtain the most recent information.

Related information

No related information is available.

Before you begin

No prerequisites or precautions are needed when performing this procedure.

Procedure

1. Select Provisioning —> SHDSL —> Connection/NTU
   
   Result: The SHDSL Connection List window is displayed.

2. Select one SHDSL connection from the list.

3. Click VC12 Termination
   
   Result: The VC12 Termination Point Information window is displayed.

4. Update the VC12 Termination Point Information window.
   
   Result: The window is updated with the most recent VC12 termination point information.

5. Click Close to exit this window
   
   Result: The window closes.

END OF STEPS
Report the VC 12 termination point information list

When to use
To write a report of the VC 12 termination information list on your computer.

Related information
No related information is available.

Before you begin
No prerequisites or precautions are needed when performing this procedure.

Procedure

1. Select Provisioning —> SHDSL —> Connection/NTU
   **Result:** The SHDSL Connection List window is displayed.

2. Select one SHDSL connection from the list.

3. Click VC12 Termination
   **Result:** The VC12 Termination Point Information window is displayed.

4. Click Report
   **Result:** The system prompts the user for a filename to which the system shall store all data from the current view or dialog in ASCII format. The data stored includes general information like the NE name and the date/time of the report generation. Furthermore it includes specific data that is visible on the screen and data that is invisible such as data assessable via a scroll bar. Examples of reports are lists of current cross connections, current alarms, equipment configuration, etc. & c.

5. Click Close.
   **Result:** The window closes.

END OF STEPS
Edit the VC 12 termination point information list

When to use
To edit the VC 12 termination point information for the SHDSL

Related information
No related information is available.

Before you begin
No prerequisites or precautions are needed when performing this procedure.

Procedure

1. Select Provisioning —> SHDSL —> Connection/NTU
   Result: The SHDSL Connection List window is displayed.

2. Select one SHDSL connection from the list.

3. Click VC12 Termination
   Result: The VC12 Termination Point Information window is displayed.

4. Click Edit.
   Result: The Edit VC12 Termination Point Information window is displayed.

5. Select the TI mode.

6. Set the API which to be expected.

7. Select the API display mode

8. Select the TIM detection

9. Click OK to commit changes to the NE and close the window.
Result: The window closes.
Parameters for viewing or editing NTU information and VC 12 termination point information

Accepted TSL (Hex, Description)
The received SL. Hex, Value, and Description (read only). Greyed out and empty when the accepted TSL does not have the value “Normal”.

Accepted TSL Value Status
Shows the accepted TTI Value Status (read only).

Accepted TTI Value Status
Shows the accepted TTI value status (read only).

AIS on PLM
When checked the AIS insertion on PLM detection is enabled (editable).

AIS on TIM
When checked the AIS insertion on TIM detection is enabled (editable).

API
The API which is inserted in the transmit direction. Greyed out and empty if the TI mode is set to the non-specific byte mode (editable).

API Display Mode
Greyed out if the corresponding “API” field is greyed out.

LTU port
Displays the port name of the connected LTU port (read only).

NTU port
Displays the port name of the connected NTU port (read only).

Issue Number
Displays the vendor issue number of the NTU device (read only).

Node Name
Displays the name of the NTU device (editable).
Serial Number
Displays the vendor serial number of the NTU device (read only)

Selection
Displays the TP address (read only).

Software Version
Displays the software of the NTU device (read only).

TI Mode
When the TI mode is changed to the byte mode, the default value (0x00 or 0x01) will be shown (editable).
When the TI mode is changed to specific string mode the corresponding API will be reset to its default value (15 times 0x00 or 15 times 0x01). Auto CRC-7 checkbox will be unchecked and the CRC-7 will be filled in with the same default value (1 time 0x00 or 1 time 0x01). In case of the 16 times 0x01 default, the API display mode will be set to Hex.

TIM Detection
When checked the TIM detection is enabled (editable).

Transmitted TSL (Hex, Description)
The SL which is inserted in transmit direction. Hex, Value, and Description (read only).

Unit ID
Displays the unit identification code of the NTU device (read only).

Vendor Model
Displays the vendor model of the NTU device (read only).

Vendor ID
Displays in the vendor ID of the NTU device (read only).
Provisioning the SHDSL on the NT10ETH modem

When to use

The following procedure is performed to provision the SHDSL on the NT10ETH card.

Related information

No related information is available.

Before you begin

Always use the TUG 12 mode.

Procedure

1. Select Provisioning —> SHDSL —> Connection/NTU
   
   **Result:** The SDSL Connections window is displayed.

2. Select one SHDSL connection from the list.

3. Click VC12.
   
   **Result:** The SDSL VC12 TP List window is displayed.

4. Select one of the Termination Points from the list.
   
   **Result:** The VC12 Termination Point Information window is displayed.
View SNC protection

Overview

Purpose

To view the SNC connectivity Information in the selected network.

Contents

<table>
<thead>
<tr>
<th>Viewing SNC protection</th>
<th>8-217</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters for viewing SNC protection</td>
<td>8-218</td>
</tr>
</tbody>
</table>
Viewing SNC protection

When to use

The SNC connectivity information can be used to check line capacity in the ring and to determine if existing SNC protection is provisioned correctly.

Procedure

1. Select Protection -> Transmission -> SNC.
   Result: The SNC Protected TP Filter window is displayed.

2. Make a selection and click OK.
   Result: The Provisioned NE SNC Protection Information window is displayed.

3. Make a selection from the list and click Details.
   Result: The Details Provisioned NE SNC Protection Information window is displayed.

4. Click Close to exit.
   Result: The window closes.
Parameters for viewing SNC protection

Capacity box

This selection allows the user to filter on particular cross connect capacities. Values are: All, VC-4, VC-3, and VC-12.

Slot

Selection of the applicable card types. For VC-12 level the value is fixed to slot TS1.

Port

To select one of the available ports. Values are 1..4 or All.

AU4#

To select one of the AU-4s.

Protected cross connections

List of TPs and their capacity of selected pairs from working TP, protecting TP, and active TP.

Selected pair

List of TPs of selected pairs from working, protecting, and active reference.
Edit SNC protection

Overview

Purpose

To change the hold off time for individual SNC Protection on VC-4, VC-3 or VC-12 level.

Contents

| Editing a SNC protection                  | 8-220 |
| Parameters for editing SNC protection     | 8-221 |
Editing a SNC protection

When to use

When a specific SNC Protection has been chosen to be changed.

Before you begin

An SNC path should have been provisioned.

Procedures

1. Select Protection -> Transmission -> SNC.
   Result: The SNC Protected TP Filter window is displayed.

2. Make a selection and click OK.
   Result: The Provisioned NE SNC Protection Information window is displayed.

3. Make a selection from the list and click Details.
   Result: The Details Provisioned NE SNC Protection Information window is displayed.

4. Click Edit.
   Result: The Edit Provisioned NE SNC Protection Information window is displayed.

5. Make a selection for the Hold off Time with usage of the above parameter information and click OK.
   Result: The switch window closes and the information window is re-displayed.

6. Click Close to exit.
   Result: The window closes.

END OF STEPS
Parameters for editing SNC protection

Hold off time

Provides the delay between the moment that the signal fail or degrade condition is set, and the start of the execution of the switch-over. The default value is 0.0 seconds. Values are 0.0 ... 10.
View MSP protection

Overview

Purpose

To view the MSP connectivity Information for established MSP protection pairs in the selected network element.

Contents

| Viewing MSP protection                  | 8-223 |
| Parameters for viewing MSP protection  | 8-224 |
Viewing MSP protection

When to use

The MSP connectivity information can be used to check availability and to determine if existing protection is provisioned correctly according to the transmission plan.

Procedure

1. Select Protection -> Transmission -> MSP.
   **Result:** The Provisioned NE MSP Information window is displayed.

2. Make a selection and click Details.
   **Result:** The Details MSP window is displayed.

3. Click Close to exit.
   **Result:** The window closes.

END OF STEPS
Parameters for viewing MSP protection

Working section
Displays the working sections of the selected MSP group.

Protection section
Displays the protection of the selected MSP group.

Active section
Displays which section is carrying traffic.

Switch state
Displays the current switch state of the protection pair.

Selected pair
Displays the selected sections and indicates the alarm status at the working/protection port. This can be Error Free, Failed, or Degraded.

Communication mode
Displays whether the protection is unidirectional or bidirectional. In the case of failure with unidirectional mode the receive side switches. In the bidirectional mode both sides are switched. When the unidirectional mode is displayed the Far End selection is greyed out.

WTR (wait to restore/wait to rename)
If MSP mode is ETSI, WTR is the wait to restore time after the failure on the protected unit has cleared. If msp mode is 1+1 optimized, then WTR is the Wait to rename: after the failure on the protected unit has cleared, the traffic remains on the protection, but the current primary becomes secondary and the other way around.

Near end
Displays the service reference at the Near/Far end. This can be Working, Protection, or None. Also the APS transmitted code is displayed.
Edit MSP protection

Overview

Purpose

To set or change protection on a point-to-point connection.

Contents

<table>
<thead>
<tr>
<th>Editing MSP protection</th>
<th>8-226</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters for editing MSP protection</td>
<td>8-228</td>
</tr>
</tbody>
</table>
Editing MSP protection

When to use

MSP protection should be established when the transmission plan calls for a protection of a particular point to point connection.

Related information

Related procedures are:
- Slot provisioning.
- Port provisioning.

Before you begin

Related prerequisites and precautions are:
- A protected switch is always traffic affecting.
- If the physical timing reference of the units to be MSP protected are assigned to a single logical timing references then these units are no longer available for MSP protection.
- If a port loopback is set on a port, then this port is not available for MSP protection
- MSP pair must be present physically set up on the Near End and Far End Network Elements. In other words, a MSP unit available and fiber pairs connected on both Network Elements.

Procedure

1. Select Protection -> Transmission -> MSP.
   Result: The Provisioned NE MSP Information window is displayed.

2. Make a selection and click Details.
   Result: The Details MSP window is displayed.

3. View the information. To change the information click Edit (for non-revertive MSP greyed out).
   Result: The Edit MSP window is displayed.

4. Make a selection for the WtR Time with usage of the above parameter information and click OK.
Result: The switch window closes and the information window is re-displayed.

5 Click **Close** to exit.

**Result:** The window closes.

END OF STEPS
Parameters for editing MSP protection

Working section
Displays the group of sections defined as working.

Protection section
Displays the group of sections defined as protection.

Active section
Displays which section is carrying traffic.

Switch state
Displays the current switch state of the protection pair.

Selected pair
Displays the selected sections and indicates the alarm status at the working/protection port. This can be Error Free, Failed, or Degraded.

Communication mode
Displays whether the protection is unidirectional or bidirectional. In the case of failure with unidirectional mode the receive side switches. In the bidirectional mode both sides are switched. When the unidirectional mode is displayed the Far End selection is greyed out.

Switch mode
Switch Mode displays whether the protection is Revertive or Non-Revertive. In the case of failure with Revertive mode the traffic switches to the protected TP and switches back when the failure is solved. In the Non-Revertive mode the traffic switches to the protected TP and remains even when the failure is solved.

Switch state
Displays the switch state for MSP.

<table>
<thead>
<tr>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>No change is made to the current state of the protection switch</td>
<td>No Request</td>
</tr>
<tr>
<td>Switch request which conditionally switches service to the working TP. In case a failure is detected an automatic switch will take place to the protection TP.</td>
<td>Manual Switch to working</td>
</tr>
</tbody>
</table>
Switch request which conditionally switches service to the protecting TP. In case a failure is detected an automatic switch will take place to the working TP.

<table>
<thead>
<tr>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch request which conditionally switches service to the protecting TP.</td>
<td>Manual Switch To Protection</td>
</tr>
<tr>
<td>Switch request which enforces switching service to the working line. It prevents automatic switching to the protection line even in case a failure is detected.</td>
<td>Forced Switch To Working</td>
</tr>
<tr>
<td>Switch request which enforces switching service to the protecting TP.</td>
<td>Forced Switch to protection</td>
</tr>
<tr>
<td>Switch request which prevents usage of the protection route for any protection switching activity. This is canceled by the clear command.</td>
<td>Lockout</td>
</tr>
<tr>
<td>The working or protection MS is active and the group state is Signal Failed.</td>
<td>Signal Failed</td>
</tr>
<tr>
<td>The working or Protection MS is active and the group state is Signal Degraded.</td>
<td>Signal Degraded</td>
</tr>
</tbody>
</table>

**WTR (wait to restore)**

WTR is the wait to restore time after the failure on the protected unit has cleared.

**WTR (Wait to restore/Wait to rename)**

Defines either the Wait to Restore Time or the Wait to Rename Time.

If MSP mode is ETSI, then WTR is the wait to restore time after the failure on the protected unit has cleared. If MSP mode is 1+1 optimized, then WTR is the Wait to rename: after the failure on the protected unit has cleared, the traffic remains on the protection, but the current primary becomes secondary and the other way around. Values are 0..60

**Near end**

Displays the service reference at the Near/Far end. This can be Working, Protection, or None. Also the APS transmitted code is displayed.
Add MSP protection

Overview

Purpose
To set protection on a point-to-point connection.

Contents

<table>
<thead>
<tr>
<th>Adding MSP protection</th>
<th>8-231</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters for adding MSP protection</td>
<td>8-233</td>
</tr>
</tbody>
</table>
Adding MSP protection

When to use

To set protection on a point-to-point connection. MSP protection should be established when the transmission plan calls for a protection of a particular point to point connection.

Related information

Refer to

• “Multiplexer Section Protection” (p. 8-21)

Related procedures are:

• Slot provisioning.
• Port provisioning.

Before you begin

Before adding MSP protection determine the following:

• If the physical timing reference of the units to be MSP protected are assigned to a single logical timing references then these units are no longer available for MSP protection.
• If a port loopback is set on a port, then this port is not available for MSP protection
• Ports have to be in the same AU3-AU4 mode
• For 1643 AM or 1643 AMS MSP is already paired. LP1.1 is the working LP2.1 is the protection.
• Do not enable the DCC channel on the protection.

Procedure

1 Select Protection -> Transmission -> MSP.

Result: The Provisioned NE MSP Information window is displayed.

2 Make a selection and click Add.

Result: The Add MSP window is displayed.

3 View the information. To change the information fill in the values with the information above and click OK.
Result: The previous window is displayed.

4 Click Close to exit.

Result: The window closes.

END OF STEPS
Parameters for adding MSP protection

Working section
Displays the group of sections defined as working.

Protection section
Displays the group of sections defined as protection.

Active section
Displays which section is carrying traffic.

Switch state
Displays the current switch state of the protection pair.

MSP pair selection
Working section port shows the available ports on the cards supporting MSP that can be protected. Protection section port will be filled in with the associated protection port once the working section has been selected.

Communication mode
Communication Mode displays whether the protection is unidirectional or bidirectional. In the case of failure with unidirectional mode the receive side switches. In the bidirectional mode both sides are switched. When the unidirectional mode is displayed the Far End selection are greyed out.

Switch mode
Switch Mode displays whether the protection is Revertive or Non-Revertive. In the case of failure with Revertive mode the traffic switches to the protected line and switches back when the failure is solved. In the Non-Revertive mode the traffic switches to the protected line and remains even when the failure is solved.

WTR (Wait to restore/Wait to rename)
If MSP mode is ETSI, then WTR is the wait to restore time after the failure on the protected unit has cleared. If MSP mode is 1+1 optimized, then WTR is the Wait to rename: after the failure on the protected unit has cleared, the traffic remains on the protection, but the current primary becomes secondary and the other way around. Values are 0..60
9 Traffic maintenance

Overview

Purpose

In this chapter the tasks are described which can be executed to test or monitor an existing path or to perform maintenance on an existing path. The first section of this chapter describes the concepts of the maintenance settings for transmission. In this chapter it is assumed that a path is already created. Chapter 8, “Traffic provisioning” describes how to create these transmission paths.

Objective

To set up the network element for testing, monitoring, and maintenance of the transmission paths.

Outcome

The outcome of the maintenance settings can be:

- Traffic that is transported through the network element can be tested and/or monitored
- If protection is used, a switch can be performed when a path has to be rerouted due to maintenance activities
- Alarm messages come up if the traffic contains errors

Contents

<table>
<thead>
<tr>
<th>Concepts</th>
<th>9-3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port types</td>
<td>9-4</td>
</tr>
<tr>
<td>Termination points (TPs)</td>
<td>9-7</td>
</tr>
<tr>
<td><strong>Provision termination points</strong></td>
<td>9-9</td>
</tr>
<tr>
<td>Provisioning termination points</td>
<td>9-10</td>
</tr>
<tr>
<td>Parameters for provisioning termination points</td>
<td>9-12</td>
</tr>
<tr>
<td>Provision a path trace</td>
<td>9-14</td>
</tr>
<tr>
<td>------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Provisioning a path trace</td>
<td>9-15</td>
</tr>
<tr>
<td>Parameters for provisioning a path trace</td>
<td>9-17</td>
</tr>
<tr>
<td><strong>Provision degraded signal thresholds</strong></td>
<td>9-19</td>
</tr>
<tr>
<td>Selecting the threshold for a signal</td>
<td>9-20</td>
</tr>
<tr>
<td>Changing the threshold values</td>
<td>9-22</td>
</tr>
<tr>
<td>Parameters for provisioning degraded signal thresholds</td>
<td>9-23</td>
</tr>
<tr>
<td><strong>Switch SNC protection</strong></td>
<td>9-24</td>
</tr>
<tr>
<td>Switching SNC protection</td>
<td>9-25</td>
</tr>
<tr>
<td>Parameters for switching SNC protection</td>
<td>9-27</td>
</tr>
<tr>
<td><strong>Switch MSP protection</strong></td>
<td>9-28</td>
</tr>
<tr>
<td>Switching MSP protection</td>
<td>9-29</td>
</tr>
<tr>
<td>Parameters for switching MSP protection</td>
<td>9-30</td>
</tr>
</tbody>
</table>
Concepts

Overview

Purpose

This section explains the concepts of the maintenance settings that can be done for Transmission. The information in this section can be used as background information for provisioning these settings. The following concepts are described in this section:

- port types
- termination points.

Contents

| Port types                    | 9-4 |
| Termination points (TPs)     | 9-7 |
Port types

Introduction

A Port is an interface point for signals. A distinction can be made between physical and logical ports. At the logical port the overhead bytes are terminated: in the transmit direction overhead bytes are added, in the receive direction overhead bytes are extracted. Therefore logical ports are also called Termination Points.

The following figure shows the physical and logical ports:

![Physical and Logical Ports Diagram]

Physical ports

The 1643 AM or 1643 AMS network element contains two STM-1/4 line ports and 1 or 2 tributary port units. The first tributary unit has sixteen 2 Mbit/s ports, The second tributary unit is an optional extension unit.

The following table shows the different types of extension units with its port types and number of ports:

<table>
<thead>
<tr>
<th>Extension Unit</th>
<th>number of ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.5 Mbit/s</td>
<td>16 x 1.5 Mbit/s (DS1)</td>
</tr>
<tr>
<td>2 Mbit/s</td>
<td>16 x 2 Mbit/s (E1)</td>
</tr>
<tr>
<td>34 Mbit/s</td>
<td>2 x 34 Mbit/s (E3)</td>
</tr>
<tr>
<td>45 Mbit/s</td>
<td>2 x 45 Mbit/s (DS3)</td>
</tr>
<tr>
<td>X.21</td>
<td>4 x 2 Mbit/s</td>
</tr>
<tr>
<td>TransLAN® Plus</td>
<td>4 x 10/100 BaseT Ethernet</td>
</tr>
<tr>
<td>STM-1 electrical</td>
<td>2 x 155 Mbit/s</td>
</tr>
</tbody>
</table>
### Extension Unit

<table>
<thead>
<tr>
<th>Extension Unit</th>
<th>number of ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>STM-1 1310 nm SH</td>
<td>2 x 155 Mbit/s</td>
</tr>
<tr>
<td>SHDSL</td>
<td>12 x 2 Mbit/s</td>
</tr>
<tr>
<td>Ethernet L2 switch</td>
<td>3 x 10/100 Base-T, 1 x 10/100/1000 Base-T, and 1 x 1000 Base-X Ethernet</td>
</tr>
<tr>
<td>Ethernet private line</td>
<td>8 x 10/100 Base-T Ethernet</td>
</tr>
</tbody>
</table>

**Note:** Refer to *Chapter 5* for 1643 AM and 1643 AMS supported option cards.

### Port names

The name of the physical ports consist of two parts separated by a dot. The first part is related to the slot name, the second part is the port number within that slot.

Example: LP2.1, TP1.3

The name of the logical ports consists of the physical port name followed by the AU-4 number and for low order signals, the VC number (VC-12 or VC-3). The VC number consists of:

- the number of the TUG-3 inside the VC-4
- the number of the TUG-2 inside the TUG-3
- the TU-12 number inside the TUG-2.

### Test loops

An incoming test loop can be set on the 1.5 Mbit/s, 2 Mbit/s, 34 Mbit/s, 45 Mbit/s, and X.21 ports. The input signal is directly routed back to its corresponding output without altering the signal format. This loop can be used to test the connectors. Only one inloop can be set at the same time.

An outgoing test loop can be set on the 1.5 Mbit/s, 2 Mbit/s, 34 Mbit/s, 45 Mbit/s, and X.21 ports. The output signal is directly routed back to its corresponding input without altering the signal format. This loop can be used to test how the signal passes through the system.
If a testloop is enabled, the Abnormal state is activated. After disabling the testloop the cross connections that existed before setting the testloop are restored.

Setting a testloop is achieved by making a unidirectional cross-connection. The termination points of the source and the sink are the same. Setting testloops in only possible on VC-3 and VC-12 level.

The following figure shows test loops for physical ports of Tributary Port Units.
Termination points (TPs)

Introduction

In the termination points the path overhead of the STM-1, VC-4, VC-3 or VC-12 signal is terminated (added or removed). In the AU-4, TU-3 and TU-12 termination points the path overhead is not terminated, but can be monitored.

The following information can be retrieved from the path overhead:
- a Trail Trace Identifier (TTI), used for path trace
- a Signal Label, indicating what type of signal is carried
- error checking information, a signal degraded threshold can be set

Alarms

When a termination point is set to Monitored alarms related to this termination point are reported. A termination point is set to Not Monitored (alarms are not reported) when it is not used.

Path trace

To check whether a path is correctly provisioned a path trace can be set. A label (for example a word) is sent along the path from one termination point to the other. This label is called Trace Identifier (TI). If the TI is a specific string, this string is called Access Point Identifier (API). If the expected API equals the accepted API, the transmission path is well provisioned.

In the path overhead of a VC-4/VC-3 signal, byte J1 in the regenerator section is used to the TI. For a VC-12 signal, byte J2 is used. A 16 byte frame is formed of which one byte is used for error detection. Therefore the string that can be inserted in these bytes has a maximum length of 15 characters (or 30 hexadecimal digits).
TIM detection

If the Trace Identifier Mismatch (TIM) detection is enabled, traffic will be lost when a mistake in the trace string is detected. Upon mismatch, an Alarm Indication Signal (AIS) is inserted in the downstream signal and a Remote Defect Indicator (RDI) is inserted in the upstream signal.

Signal label

The signal label contains information about the signal that is part of the VC. The signal label indicates whether the VC is unequipped, whether it is a structured signal, which type of mapping is used or whether it is an AIS (Alarm Indication Signal).

Signal degrade thresholds

The signal degrade threshold can be set for the Multiplex Section (MS), VC-12, VC-3, and VC-4 levels. The signal degrade threshold determines when a signal is considered degraded. Two parameters can be set:

- number of errored blocks per second
- number of adjacent bad seconds.

The signal is considered degraded, when during the defined number of bad seconds the signal contains more than the defined errored blocks per second. This causes an alarm STM-n Moderate Block Error Rate (n is 0, 1 or 16) or VC-n Moderate Block Error Rate (n is 12, 3 or 4).

On VC-12, VC-3 and VC-4 level the signal degrade threshold is also used as a switching criterion for SNC/N protection switching. If the signal is determined degraded an SNC/N protection switch is performed. SNC/N Protection is described in the chapter "Path Provisioning and Protection".
Provision termination points

Overview

Purpose

The termination points enable the user to set or view parameters derived from data stored in the overhead bytes of the signals.

Contents

<table>
<thead>
<tr>
<th>Provisioning termination points</th>
<th>9-10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters for provisioning termination points</td>
<td>9-12</td>
</tr>
</tbody>
</table>
Provisioning termination points

When to use

The termination points enable the user to set or view parameters derived from data stored in the overhead bytes of the signals. Termination points should be set after provisioning the transmission path according to the transmission plan.

Related information

If the Trace Identifier Mismatch detection (TIM) is enabled, traffic will be lost when a mistake in the trace string is made. Upon mismatch Alarm Indication Signal (AIS) is inserted in the downstream signal and Remote Defect Indicator (RDI) is inserted in the upstream signal (RDI is only inserted if the directionality is set to bidirectional).

The RS and MS termination points of the STM-1 or STM-4 signals are used to set a Signal Degraded Value or for Timing Settings. This is described in section “Provisioning Degraded Signal Threshold”.

Before you begin

The following procedures are related:

- Path Trace Provisioning
- Provision Degraded Signal Thresholds.

Procedure

The purpose of this procedure is to provision termination points. The following termination point types can be provisioned: AU-4, TU-3, TU-12, VC-4, VC-4-4C, VC-3, VC-11, VC-12, or RS.

1. Select Provisioning -> Transport -> Termination Point.
   
   Result: The Termination Point Filter window appears.

2. Select the type of the termination point to be provisioned and fill in its location. Click OK.
   
   Result: The Termination Point List window appears with a list of termination points.

3. Select the termination point from the list and click Details.
Result: The Provisioned Termination Point Information window appears with information about the selected termination point.

4 Click Edit.

Result: The Edit Provisioned Termination Point Information window appears.

5 Fill in the changes and click OK.

Result: The changes are displayed in the Provisioned Termination Point Information window.

END OF STEPS
Parameters for provisioning termination points

Introduction

The following Termination Points can be provisioned for the 1643 AM or 1643 AMS: VC-12, VC-3, VC-4, TU-12, TU-3.

The following list shows which parameters can be set for which termination points

- TP mode: VC-12, VC-3, VC-4
- J0/J1/J2 Trail Trace Identifier (path trace): VC-12, VC-3, VC-4, TU-12, TU-3.
- Signal label: VC-12, VC-3, VC-4
- Degraded Signal Threshold: VC-12, VC-3, VC-4, TU-12, TU-3

Selected TP

The name of the selected termination point.

The termination point is selected by the Slot and Port where the termination point belongs to. The AU4# is 1 when the line ports carry STM-1 signals and 4 when the line ports carry a STM-4 signal.

The name of the termination points consists of the physical port name (slot name and port number) followed by the AU-4 number and for low order signals, the VC number (VC-12 or VC-3). The VC number (also called klm number) consists of:

- k: the number of the TUG-3 inside the VC-4
- l: the number of the TUG-2 inside the TUG-3
- m: the TU-12 number inside the TUG-2.

The following figure shows examples of the TP naming.

TP type

The termination point type indicates where the signal is terminated.

Example: VC-12, TU-3
TP mode

Indicates whether the signal on the termination point will be monitored.
When monitored, alarms are generated related to the selected termination point. When not monitored, no alarms are generated related to the selected termination point.

For TU-12 and TU-3 the TP mode cannot be set by the operator. For TU-12 and TU-3 alarming is 'enabled' once such TP is in use (i.e. Cross-connect is made to such TU).

J0/J1/J2 trail trace identifier

This area is used to provision a path trace. Provisioning a path trace is described in the section "Path Trace Provisioning".

Signal label

The signal label is part of the path overhead of a VC-n signal and indicates what type of signal is carried by the container.

Example: Unequipped, asynchronous, TUG structure, ATM
- Signal Label Accepted (HEX., Description) is the signal label of the received signal
- Signal Label Transmit (HEX., Description) is the signal label of the transmitted signal
Provision a path trace

Overview

Purpose

The purpose of provisioning a path trace is to make sure the traffic is not delivered to the wrong destination.

Contents

| Provisioning a path trace | 9-15 |
| Parameters for provisioning a path trace | 9-17 |
Provisioning a path trace

When to use

A path trace can be set at any time. Path trace provisioning can be done only once, after provisioning a path, to check whether the path is correctly provisioned. Path trace can also be used continuously to check if the traffic is delivered to the correct destination. When provisioning a path trace on a path with traffic on it, take notice of the precautions.

Related information

Before provisioning a path trace determine the following:

- In which termination point is the path trace inserted and in which termination points is it monitored?
- Which label is used as path trace?

Other related information:

- If the Trace Identifier Mismatch (TIM) detection is enabled, traffic will be lost when a mistake in the trace string is made. Upon mismatch, an Alarm Indication Signal (AIS) is inserted in the downstream signal and Remote Defect Indicator (RDI) is inserted in the upstream signal (RDI is only inserted when directionality is set to bidirectional).
- If the identifier is shorter than 15 characters, the rest is filled with zeroes. Therefore the hexadecimal version of a blank identifier will be shown as all zeroes, not blank. Spaces at the end of an identifier will be also hexadecimal zeroes. When other network element types participate in the path this may not be the same. Always check the hexadecimal value.

Before you begin

Related procedures are "Provisioning Cross Connections" and "Provisioning Termination Points".

Procedure

The purpose of this procedure is to provision a path trace.

1. Determine where the termination points of the path are located. If a specific string (API) is used determine the content of the label.

2. Select Provisioning -> Transport -> Termination Point.
3. Select the type of the termination point for which the path trace must be provisioned and fill in its location. Click **OK**.

**Result:** The *Termination Point Filter* window appears.

4. Select the termination point from the list and click **Details**.

**Result:** The *Termination Point List* window appears with a list of termination points.

5. Click **Edit**.

**Result:** The *Edit Provisioned Termination Point Information* window appears.

6. **NOTICE**

*If the Trace Identifier Mismatch (TIM) detection is enabled, traffic will be lost when a mistake in the trace string is made. Upon mismatch, an Alarm Indication Signal (AIS) is inserted in the downstream signal and Remote Defect Indicator (RDI) is inserted in the upstream signal (RDI is not inserted if the directionality is unidirectional)*

Fill in the label used to be transmitted as path trace and/or the label that is expected to be received. If no label is used select Non Specific Byte. Check if the accepted path trace is the same as the expected path trace and enable or disable the TIM detection if necessary. Click **OK**.

**Result:** The path trace is provisioned and displayed in the *Provisioned Termination Point Information* window. If the expected TTI equals the accepted TTI, the transmission path is well provisioned.

**END OF STEPS**
Parameters for provisioning a path trace

To make sure the traffic is not delivered to the wrong destination, a path trace can be set. A label (TTI), for example a word, is inserted in the path overhead. To check if the path is correctly provisioned the received path trace is compared with the expected value. A path trace can be set on the VC-12, VC-3, and VC-4 signals. On TU-12 and TU-3 termination point, only the expected value can be set.

Example of a path trace

J0/J1/J2 trail trace identifier

The Trail Trace Identifier (TTI) is inserted in the path overhead. For STM-N signals the J0 byte in the RSOH is used, for VC-4/VC-3 signals byte J1 is used and for VC-12 signals byte J2 is used. For the TTI a 16 byte frame is composed which includes one CRC-7 byte for error detection. Therefore the TTI can be 15 bytes long (15 characters or 30 hexadecimal digits). The J0/J1/J2 Trail Trace Identifier area is divided into three subsections:

- **Transmitted TTI**: The TTI inserted in the path overhead is sent to the other side of the path.
- **Expected TTI**: The TTI expected from the other side of the path.
- **Accepted TTI**: The TTI actually received.

TI mode

The TI mode can have the following values:

- **Specific String**: The TI is a string with maximum length of 15 bytes. This string is identified in the Access Point Identifier (API). In Alphanumeric or ASCII format any alphanumeric character can be used, in HEX format only 00 .. 7F can be used.
- **Non Specific Byte**: The Trace Identifier matches if it is any constant byte value within the range 00 .. FF. If the byte value is not constant, Trace Identifier Mismatch is assumed. No check between Accepted API and Expected API is performed.
API

The Access Point Identifier (API) is the label that is inserted in the path overhead. This is not valid if the TI Mode is set to Non Specific Byte.

API display mode

As long as the characters forming the API are alphanumeric characters, it is possible to toggle between HEX and Alphanumeric mode. The accepted API displays non-alphanumeric characters as question marks in the Alphanumeric mode. If Alphanumeric box cannot be checked, please delete the content in the API field first.

TIM detection

TIM is Trace Identifier Mismatch comparison between the expected and accepted TTI. If this is enabled and TP is monitored, when the TTIs do not match, a Path Trace Identifier Mismatch alarm is raised.

Important! If the Trace Identifier Mismatch (TIM) detection is enabled, traffic will be lost when a mistake in the trace string is made. Upon mismatch, an Alarm Indication Signal (AIS) is inserted in the downstream signal and Remote Defect Indicator (RDI) is inserted in the upstream signal.
Overview

Purpose

The purpose of provisioning degraded signal thresholds is to define how many errors a signal may have before it is considered degraded. A degraded signal causes a *Moderate Block Error Rate* alarm. A degraded signal can cause an SNC/N protection switch if the path for that signal is SNC/N protected, or an MSP switch if MSP protection is used.

Signal levels

The signal levels on which the degraded signal thresholds can be set are *STM-16, STM-1, VC-4, VC-3 VC-11, VC-12, E3 or DS3.*

Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selecting the threshold for a signal</td>
<td>9-20</td>
</tr>
<tr>
<td>Changing the threshold values</td>
<td>9-22</td>
</tr>
<tr>
<td>Parameters for provisioning degraded signal thresholds</td>
<td>9-23</td>
</tr>
</tbody>
</table>
Selecting the threshold for a signal

When to use

Changing the degraded signal thresholds is only done according to a change in the transmission plan.

Related information

Related information and precautions are:

- the threshold values (number of errored blocks and number of seconds) must be known.
- changing the values of the Signal Degrade Thresholds can degrade the transmission path. Depending on these values alarms are generated and SNC/N or MSP protection switches are made.

Before you begin

Related Procedures are:

- Port Provisioning
- Provisioning Termination Points

Procedure

This procedure describes how the threshold for a specific signal can be changed. A choice can be made between two threshold values. Changing the values of these two thresholds is described in the "Procedure to Change the Threshold Values".

The following table shows the windows in which the degraded signal values for the different signals are displayed. The Actions column shows how to get to these windows.

<table>
<thead>
<tr>
<th>Signal Level</th>
<th>Actions</th>
</tr>
</thead>
</table>
| STM-1        | Perform the following steps  
|              | • Provisioning -> Transport -> Ports  
|              | • Select filter criteria and click OK  
|              | • select the STM-1 or the STM-4 port and click Details  
|              | **Result:** The *STM-1 or STM-4 Port Information* window appears |
Signal Level | Actions
--- | ---
VC-12 or VC-4 | Perform the following steps
• Provisioning -> Transport -> Termination Point
• Select filter criteria and click OK
• Select a VC-12 or VC-4 termination point and click Details
**Result:** The Provisioned Termination Point Information window appears

2 Click **Edit**.

**Result:** The corresponding edit window appears

3 In the Degraded Signal Threshold box make a choice between Threshold 1 and Threshold 2 and click **OK**.

**Result:** The new Threshold is set and its values are displayed in the corresponding information windows.

4 Click **Close**.

**END OF STEPS**
Changing the threshold values

When to use

To change the degraded signal thresholds according to a change in the transmission plan.

Procedure

For each signal level a choice can be made between two threshold values. This procedure describes how to change the values of these two thresholds. Switching between these two thresholds for a specific signal is described in the procedure "Select the Threshold for a Signal.

1. Select Provisioning -> Transport -> DEG Threshold.
   Result: The Provisioned NE Degraded Signal Thresholds window appears with a list of the Threshold values for all signal levels

2. Select one of the signal levels and click **Edit**.
   Result: The Edit Provisioned NE Degraded Signal Thresholds window appears.

3. Change the values for Threshold 1 and/or Threshold 2 and click **OK**.
   Result: Threshold 1 and/or Threshold 2 have new values. The new values appear in the Provisioned NE Degraded Signal Thresholds window.

4. Click **Close**.

END OF STEPS
Parameters for provisioning degraded signal thresholds

Introduction

A Degraded signal is a signal with more Errored Blocks (EB) per second than the defined EB Count value during a period of consecutive seconds defined in Duration (sec). A degraded signal causes a Moderate Block Error Rate alarm. A degraded signal (on VC-12 level) can cause an SNC/N or an MSP protection switch.

Degraded signal thresholds

Two Thresholds can be defined for each signal level to declare a signal degraded. The thresholds are called Threshold 1 and Threshold 2. A choice between these two thresholds can be made in the Edit STM-N Port Information window for the STM-N signal and in the Edit Provisioned Termination Point window for the VC-4, and VC-12 signal.

Signal level

The signal levels on which the degraded signal thresholds can be set are STM-4, STM-1, VC-4 or VC-12.

EB count

In the termination points the signal is terminated and a Bit Interleaved Parity (BIP) check is performed on the received data. The result of this BIP check is compared to the values in the B or V5 bytes in the overhead of the signal. When there is a difference an errored block is detected. The EB Count value determines how many Errored Blocks (EB) are allowed per second, before the second is declared a bad second.

The following table shows the range for the values for each signal type.

<table>
<thead>
<tr>
<th>Signal Type</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>STM-4</td>
<td>1...728000</td>
</tr>
<tr>
<td>STM-1</td>
<td>1..192000</td>
</tr>
<tr>
<td>VC4</td>
<td>1..8000</td>
</tr>
<tr>
<td>VC12</td>
<td>1..2000</td>
</tr>
</tbody>
</table>

Duration (sec.)

The number of consecutive bad seconds to declare a signal degraded.
Switch SNC protection

Overview

Purpose

To switch protection for individual paths on VC-4, VC-3, or VC-12 level.

Contents

| Switching SNC protection | 9-25 |
| Parameters for switching SNC protection | 9-27 |
Switching SNC protection

When to use

The purpose of these steps is to switch lines:

This switch should be requested when a number of specific paths has to be rerouted due to maintenance activities.

Related information

Related precautions and prerequisites are:

- A protection switch is always traffic affecting.
- An SNC path should have been provisioned.
- procedures to set cross connections and their protection.

Before you begin

Set cross connections and their protection.

Procedures

1. Select Protection -> Transmission -> SNC.
   
   Result: The SNC Protected TP Filter window is displayed.

2. Make a selection and click OK.
   
   Result: The Provisioned NE SNC Protection Information window is displayed.

3. Make a selection from the list and click Switch.

   Result: The Switch Provisioned NE SNC Protection Information window is displayed.

4. Make a selection for the Switch Request with usage of the above parameter information and click OK.

   Result: The switch window closes and the information window is re-displayed.

5. Click Close to exit.
Result: The window closes.
Parameters for switching SNC protection

Switch mode

Switch Mode displays the Non-Revertive mode. In the Non-Revertive mode the traffic switches to the protected line and remains even when the failure is solved.

Hold of time

The delay between the moment that the signal fail or degrade condition is set, and the start of the execution of the switch-over. The default value is 0.0 seconds. Values are 0.0 ... 9.9.

Switch Request

The Switch Request descriptions and values are:

<table>
<thead>
<tr>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>No change is made to the current state of the protection switch</td>
<td>No Request</td>
</tr>
<tr>
<td>Executing Clear on a line will undo only the previous switch request that are initiated on that specific line.</td>
<td>Clear</td>
</tr>
<tr>
<td>Will switch the traffic to the working regardless of the state of that leg. This will override a hardware protection switch. This is canceled with the clear command.</td>
<td>Forced To Working</td>
</tr>
<tr>
<td>Will switch the traffic to the protection regardless of the state of that leg. This will override a hardware protection switch. This is canceled with the clear command.</td>
<td>Forced To Protection</td>
</tr>
<tr>
<td>Will switch traffic to the working only when that working is error free and is not satisfying an equal or higher priority request. A hardware protection switch will override.</td>
<td>Manual To Working</td>
</tr>
<tr>
<td>Will switch traffic to the protection only when that protection is error free and is not satisfying an equal or higher priority request. A hardware protection switch will override.</td>
<td>Manual To Protection</td>
</tr>
<tr>
<td>Prevents usage of the protection route for any protection switching activity. This is canceled with the clear command.</td>
<td>Lockout</td>
</tr>
</tbody>
</table>
Switch MSP protection

Overview

Purpose

To perform a switch on a transmission signal in a point-to-point connection. In executing this request, the signal will be switched.

Contents

<table>
<thead>
<tr>
<th>Switching MSP protection</th>
<th>9-29</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters for switching MSP protection</td>
<td>9-30</td>
</tr>
</tbody>
</table>
Switching MSP protection

When to use

The purpose of these steps is to switch MSP protection:

An MSP protection switch should be made if maintenance operations force traffic over a specific point-to-point connection to be rerouted.

Related information

A protected switch is always traffic affecting.

Before you begin

Related procedures are:

- Slot provisioning.
- Port provisioning.
- Add MSP Protection

Procedures

1. Select Protection -> Transmission -> MSP.
   
   **Result:** The Provisioned NE MSP Information window is displayed.

2. Make a selection and click **Switch**.
   
   **Result:** The Switch MSP window is displayed.

3. View the information. To change the switch request click the pull down menu, select a request and click **OK**.
   
   **Result:** The previous window is displayed and the switch is executed.

4. Click **Close** to exit.
   
   **Result:** The window closes.

*END OF STEPS*
Parameters for switching MSP protection

Selected pair

Displays the selected sections and indicates the alarm status at the working/protection port. This can be Error Free, Failed, or Degraded.

Working section

Displays the group of sections defined as working.

Protection section

Displays the group of sections defined as protection.

Active section

Displays which section is carrying traffic.

Switch state

Displays the current switch state of the protection pair.

Switch mode

Switch Mode displays whether the protection is Revertive or Non-Revertive. In the case of failure with Revertive mode the traffic switches to the protected line and switches back when the failure is solved. In the Non-Revertive mode the traffic switches to the protected line and remains even when the failure is solved.

Hold of time

The delay between the moment that the signal fail or degrade condition is set, and the start of the execution of the switch-over. The default value is 0.0 seconds. Values are 0.0 ... 9.9.

Switch request

Displays the switch request for MSP.

<table>
<thead>
<tr>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Request</td>
<td>No request to switch has been issued.</td>
</tr>
<tr>
<td>Values</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Manual Switch to working</td>
<td>Switch request which conditionally switches service to the working TP. In case a failure is detected an automatic switch will take place to the protection TP. This switch request only exists in non-revertive mode.</td>
</tr>
<tr>
<td>Manual Switch To Protection</td>
<td>Switch request which conditionally switches service to the protecting TP. In case a failure is detected an automatic switch will take place to the working TP.</td>
</tr>
<tr>
<td>Forced Switch To Working</td>
<td>Switch request which enforces switching service to the working TP. It prevents automatic switching to the protecting TP even in case a failure is detected. This switch request only exists in non-revertive mode.</td>
</tr>
<tr>
<td>Forced Switch to protection</td>
<td>Switch request which enforces switching service to the protecting TP. It prevents automatic switching to the working TP even in case a failure is detected (only if the switch request has a higher priority than the protection group state).</td>
</tr>
<tr>
<td>LockOut</td>
<td>Prevents usage of the protection route for any protection switching activity. This is canceled with the clear command.</td>
</tr>
</tbody>
</table>
10 Performance monitoring

Overview

Purpose

The purpose of Performance Monitoring (PM) is to offer a set of necessary features that allow to continuously collect, analyse, process, store, and report performance related data by detecting and measuring even subtle changes for SDH, PDH, and LAN signal quality in order to do preventive maintenance. It consists of three main activities: Configuration of the ITM-CIT, measuring and displaying performance data, recovering data stored in bins.

Objectives

The objectives of this chapter are:

• To describe the procedures for configuration of the termination points on the ITM-CIT;
• To describe the procedures for viewing performance measurements;
• To describe the procedures to archive and retrieve logged performance data.

Outcome

A sensitive system that is able to detect, measure, and report subtle transmission performance changes occurring on the network within a predefined time span in order to allow preventive maintenance actions.

Contents

<table>
<thead>
<tr>
<th>Concepts</th>
<th>10-3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>10-4</td>
</tr>
<tr>
<td>The performance monitoring process</td>
<td>10-7</td>
</tr>
<tr>
<td>Performance measurements</td>
<td>10-8</td>
</tr>
<tr>
<td>Performance monitoring</td>
<td>10-13</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>Available PM data</td>
<td>10-27</td>
</tr>
<tr>
<td>Configuration of the ITM-CIT</td>
<td>10-35</td>
</tr>
<tr>
<td>Data Storage and Recovery</td>
<td>10-37</td>
</tr>
<tr>
<td><strong>Configure PM on the ITM-CIT</strong></td>
<td><strong>10-40</strong></td>
</tr>
<tr>
<td>Enabling counter and setting thresholds</td>
<td>10-41</td>
</tr>
<tr>
<td>Editing PM counter thresholds</td>
<td>10-43</td>
</tr>
<tr>
<td>Parameters for configuring PM on the ITM-CIT</td>
<td>10-45</td>
</tr>
<tr>
<td><strong>Display PM data</strong></td>
<td><strong>10-48</strong></td>
</tr>
<tr>
<td>Displaying PM data</td>
<td>10-49</td>
</tr>
<tr>
<td>Parameters for displaying PM data</td>
<td>10-53</td>
</tr>
<tr>
<td><strong>User Provisionable CBS and PBS per flow</strong></td>
<td><strong>10-57</strong></td>
</tr>
<tr>
<td>User Provisionable CBS and PBS per flow</td>
<td>10-58</td>
</tr>
<tr>
<td><strong>Enhanced Ethernet Performance Monitoring</strong></td>
<td><strong>10-59</strong></td>
</tr>
<tr>
<td>General Purpose Ethernet Port Monitor</td>
<td>10-60</td>
</tr>
<tr>
<td>Ethernet Service Monitor</td>
<td>10-62</td>
</tr>
<tr>
<td>Ethernet High Priority, Low Priority Traffic Monitor and User Provisionable LS/SLS Threshold</td>
<td>10-65</td>
</tr>
<tr>
<td>RTD PM counters, RDT/TCA support, and End-2-End Ethernet PM - RTD</td>
<td>10-68</td>
</tr>
<tr>
<td>Enable round trip delay measurements</td>
<td>10-70</td>
</tr>
<tr>
<td>Perform a one-time round trip delay measurement for test purposes</td>
<td>10-73</td>
</tr>
</tbody>
</table>
Concepts

Overview

Purpose

This chapter describes the underlying performance monitoring concepts of the 1643 AM systems.

Contents

<table>
<thead>
<tr>
<th>Introduction</th>
<th>10-4</th>
</tr>
</thead>
<tbody>
<tr>
<td>The performance monitoring process</td>
<td>10-7</td>
</tr>
<tr>
<td>Performance measurements</td>
<td>10-8</td>
</tr>
<tr>
<td>Ethernet performance monitoring</td>
<td>10-13</td>
</tr>
<tr>
<td>Available PM data</td>
<td>10-27</td>
</tr>
<tr>
<td>Configuration of the ITM-CIT</td>
<td>10-35</td>
</tr>
<tr>
<td>Data Storage and Recovery</td>
<td>10-37</td>
</tr>
</tbody>
</table>
Introduction

Purpose of performance monitoring

The purpose of performance monitoring is:

1. to detect degraded performance of the transport functionality in order to support pro-active maintenance activities, for example replacing equipment before the impact of the performance degradation on service becomes unacceptable (maintenance-oriented performance monitoring).

2. to collect performance data over a long period (typically months) in order to verify the quality of the transport service (quality-of-service-oriented performance monitoring).

Near-end and far-end performance monitoring

In principle, two kinds of performance monitoring can be distinguished:

- Near-end performance monitoring
  Performance parameters are derived from bit errors and defects in the incoming signal.

- Far-end performance monitoring
  Performance parameters are derived from the remote information (REI/RDI) in the incoming signal. The meaning of the remote information will be explained in more detail afterwards in this chapter.

Performance monitoring of a bidirectional path

To monitor the performance of a bidirectional path, near-end and far-end performance monitoring information is correlated. The bidirectional path is considered unavailable if at least one of the directions is unavailable.

The following figure shows an example of a bidirectional path:

At NE A, the near-end information represents the performance of the unidirectional trail from NE Z to NE A, while the far-end information represents the performance of the unidirectional trail from NE A to NE Z.
At NE Z, the near-end information represents the performance of the unidirectional trail from NE A to NE Z, while the far-end information represents the performance of the unidirectional trail from NE Z to NE A.

At an intermediate NE I, the near-end information in the direction from NE A to NE Z represents the performance of the unidirectional trail segment from NE A to NE I, while the far-end information represents the performance of the unidirectional trail from NE Z to NE A. The near-end information in the direction from NE Z to NE A represents the performance of the unidirectional trail segment from NE Z to NE I, while the far-end information represents the performance of the unidirectional trail from NE A to NE Z.

At either end of the trail (NE A or NE Z) the combination of near-end and far-end information represents the performance of the two directions of the trail. At an intermediate NE I, the combination of far-end information in the trail signal from NE A to NE Z and far-end information in the trail signal from NE Z to NE A presents the performance of the two directions of the trail.

**SDH performance monitoring**

SDH performance monitoring is based on the evaluation of block errors, where the block size depends on the transmission layer. At the Regenerator Section (RS) layer, a block is equivalent in size to an SDH frame. Therefore, the number of bits in an RS block is dependent on the signal rate. One or more errored bits in the RS parity byte (B1 byte in the RSOH) constitutes a single RS block error. At the Multiplex Section (MS) layer, the number of bits in a block is always 801. The BIP comparison is performed on a per-bit basis. Therefore, a single bit error in the MS parity bytes (three B2 bytes in the MSOH) constitutes a single MS block error. At the higher order path layer, a block is equivalent in size to an SDH path. Therefore, the number of bits in a VC-n block is dependent on the signal rate. One or more errored bits in the parity byte of the higher order path (B3 byte in the VC-n POH) constitutes a single VC-n block error. Concerning the Remote Error Indication (REI), the same approach as used for SONET performance monitoring is also used for SDH performance monitoring.

**STM-64 Overhead Access: M0, M1 source (MS-REI)**

*Source direction:*

In every STM-64 MS termination point the Remote Error Information (REI) is written in the M0 and M1 byte (9,6,1). The REI bytes shall be set to convey the count of interleaved bit blocks that have been detected in error by the BIP-1536 (in the range of [0, 1536]). M0 bit 1 is most significant bit and M1 bit 8 is least significant bit. If interworking with old equipment supporting the single byte REI in M1, the value conveyed is truncated at 255 and inserted in M1. Usage is in conformance with ITU-T Rec. G.707 and ETSI ETS 300417."

**STM-64 Overhead Access: M0, M1 sink (MS-REI)**

*Sink direction:*

...
In every STM-64 MS termination point the received REI is interpreted. If the REI of a received frame is unequal to zero, the corresponding number of errored blocks can be counted for far-end performance monitoring purposes. Usage is in conformance with ITU-T Rec. G.707 (table 9-7 and also table 9-8 for interworking with old equipment that supports the M1 byte only) and ETSI ETS 300417. When this feature is not supported or disabled, the incoming M0 and M1 byte is ignored."
The performance monitoring process

Process description

The performance monitoring process is a three-stage process:

1. **Primary processing**
   - Fundamental parameters are derived from errors detected in the transport signal, classified into bit errors and defects, and accumulated over one-second periods.

2. **Parameter processing**
   - Near-end and far-end performance parameters are calculated based on the evaluation and correlation of the fundamental parameters obtained during the primary processing. Please refer to “Available PM data” (p. 10-27).

3. **Binning and reporting**
   - In the binning and reporting phase, the performance parameters obtained during the parameter processing are stored in accumulation registers (or “bins”) over 15-minutes and 24-hours observation periods.
   - For each performance monitoring point (cf. “Performance measurements” (p. 10-8)), 16 recent (or history) bins for 15-minutes measurements and one recent bin for 24-hours measurements are stored in the NE.
Performance measurements

Introduction

In performance monitoring, the integrity of a signal is continuously verified as it is carried along the fiber. The results of this measurement are analyzed, compared against predefined threshold values for errors, stored on the NE and displayed on the ITM CIT as performance monitoring data. The thresholds must be defined according to your maintenance policy and then configured on the ITM CIT.

Performance measurements can be done on incoming:

- VC-12, VC11, VC4, and VC-3 terminating in the unit;
- MS1 and MS4;
- P12 (ISDN) in egress (SDH to PDH) and ingress (PDH to SDH) ways;
- as well as on LAN or WAN ports.

To measure LAN performance parameters on the 1643 AM or 1643 AMS, a TransLAN® card is required in Tributary slot 2. This card offers four Ethernet LAN ports of different bitrates (2, 4, 6, 8 or 10 Mbits/s).

How to measure PM

*Even Bit Interleaved Parity (BIP)* is the method used to measure performance. The signal integrity is indicated by bit errors in the interface signal.

This method looks at the content of the signal. When a signal is transmitted a BIP check is performed on each STM frame. In this check, the amount of “1” and “0” of the payload is calculated. If the result is an even number, then a “0” is put in the B-Byte of the overhead section of the STM-n next frame. Otherwise if the result is an odd number, then a “1” is put in the B-Byte. At the termination point, a BIP check is performed again on the payload of the received signal and the outcome is compared to the value at transmission.

If there is a discrepancy between the two readings, an error is concluded. Proactive maintenance events are called Threshold Crossing Alerts and are typically raised when too many errored seconds (number of errored frames in one second) are being detected. Parity violations are counted to derive performance data in 15 minutes, and 24 hours measuring intervals, called bins.

Where to measure PM

The quality of the transmission in the network is measured at each termination points, that is where signals are terminated in the network element.
A VC-12 is for example terminated at the PDH 2 Mbit/s physical interface. At the process of termination the appropriate overhead bytes are terminated to provide information about the signal being terminated. Selecting the appropriate TPs to be monitored during the configuration step requires preparation and planning.

**Available TP**

Looking at the table below, the termination points that can be monitored unidirectional and bi-directionally are:

- VC-11, VC-12, VC-3, VC-4

The following termination points support only uni-directional performance monitoring:

- P12 (ISDN), MS–1 and MS-4

**Prerequisite to monitor**

In order to monitor the performance of the network at a given termination point, two prerequisites must be met:

1. The performance parameter(s) counter(s) must be enabled;
2. The port mode must be set to monitored. For more information on the specific procedure to follow, please refer to Chapter 9, “Traffic maintenance”, and specifically to “Provision ports” (p. 5-62). For more information on the concepts related to port modes, please refer to “Concepts” (p. 9-3).

**Bi-directional monitoring**

The 1643 AM or 1643 AMS has the capability, not only to handle unidirectional, but also bidirectional performance monitoring. By setting two termination points at both ends of the path, end-to-end monitoring can be done.

**Maximum number of TPs**

It is possible to simultaneously monitor a number of termination points. The maximum is limited by the number of counters that can be simultaneously enabled. Bidirectional monitoring processes may count as two monitoring points.

The maximum number of monitoring points that can be provisioned on a network element vary according to the type of system controller installed on the 1643 AM or 1643 AMS. Please consult the technical specifications of the network element in the AGP manual.

**Forward and backward monitoring**

On connection termination points (CTPs) the signal is non-intrusively monitored. This kind of monitoring does not terminate the signal but only reads its REI value.
For CTP with a bidirectional path two types of measurements parameters are available:

<table>
<thead>
<tr>
<th>Measurement Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forward</td>
<td>A transmission direction that is referred to when the signal is ingressing the NE at that point. The REI is read from the incoming signal. This will indicate the quality of the end to end (TP to TP) path in the opposite direction.</td>
</tr>
<tr>
<td>Backward</td>
<td>A transmission direction that is referred to when the signal is egressing the NE at that point. The REI is read from the incoming signal on the other side of the NE. This will indicate the quality of the end to end (TP to TP) path in forward direction.</td>
</tr>
</tbody>
</table>

Near end / far end monitoring

In certain applications, it may be desirable to provide performance monitoring data related to both directions of transmission (transmitted/received) from a single end. The received data can be relayed back from the remote end to the local end if there is a bidirectional connection between the nodes. End-to-end bidirectional monitoring processes consist of two termination points (TPs): one at the local side and one at the remote side.

The Far End is the local end to the user. The Near End performance parameter is the data received by the network element at the incoming direction and forwarded to the managing system. The Far End is the remote end to the user.

The table below identifies where the BIP check is performed during monitoring.

<table>
<thead>
<tr>
<th>TP</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Near End</td>
<td>The BIP is calculated on the received signal and compared with the B or V5 byte (VC-12).</td>
</tr>
<tr>
<td>Far End</td>
<td>The BIP is calculated on the sent signal, but at the remote end of the transmission, and compared with the B or V5 byte (VC12).</td>
</tr>
</tbody>
</table>

In Near-End monitoring, the BIP check indicates the quality of the signal transmitted from the remote side to the local side.
In Far-End monitoring, the B values is compared with the BIP calculation if an error is detected on the remote side. An REI is then transmitted upstream. The received REI at the local side indicates the quality of the signal transmitted from the local side to the remote side.

**Example of near end/far end forward/backward monitoring**

The graphic below describes Near End/Far end Forward/Backward monitoring. The termination point (TP) at network element-A is monitored on the receiving end, or Near End where the B-bytes are verified for parity. If there is an error, an REI is sent upstream. The TP at network element-B is monitored on its receiving end, and since it is distal from NE-A, it is referred to Far end.

![Diagram showing near end/far end forward/backward monitoring](image)

Because the path is terminated in NE-A and NE-B these monitoring points are termination points (TPs). In a TP the BIP value is recalculated and compared to the value stored in the received B byte. If an error is detected an REI will be sent to its originating source and the error will be declared as Near End PM data. The REI received will be declared as Far End PM data.

In network element-I the REI value is read and is declared as Backward or Forward PM data of the Connection Termination Points. For example in CTP#1 the Forward PM data consists of the REI transmitted from A to B (and so indicating the quality of the path in the direction from B to A). The Backward PM data in CTP#1 consists of REI transmitted from B to A (and so indicating the quality of the path in the direction from A to B).

**LAN/WAN port monitoring**

Using the *TransLAN®* option card, it is possible to monitor up to 4 X 10/100BaseT Ethernet LAN ports, or 4 WAN ports per card.

The LAN port maps directly from the Ethernet to SDH, to either:
- 1 or 2 concatenated VC3
- 1 to 63 concatenated VC12
When a LAN connection is set up using the TransLAN® option card, PM data about this LAN will be available as long as the counter for an active VC-12 is enabled.
Ethernet performance monitoring

Purpose

The Ethernet performance monitoring counters can be categorized according to the different purposes they are serving.

Types of Ethernet performance monitoring counters

The following types of counters can be distinguished as:

- Counters for basic Ethernet performance monitoring
- Service monitoring:
  - Counters for Ethernet service flow performance monitoring
- Traffic management:
  - High quality traffic counters for Ethernet network load performance monitoring
  - Low quality traffic counters for Ethernet network load performance monitoring
  - Counters for Ethernet congestion monitoring
- Counters for Ethernet service route round trip delay measurements

Basic Ethernet performance monitoring counters

The basic Ethernet Performance Monitoring counters that are supported are as follows:

<table>
<thead>
<tr>
<th>Basic Ethernet PM</th>
<th>Counter Location</th>
<th>Unit</th>
<th>Threshold</th>
<th>X5IP</th>
<th>X4IP</th>
<th>X8PL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet Incom-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ing Number of</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Good Bytes</td>
<td>pCbR /port byte</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Ethernet Outgo-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ing Number of</td>
<td>pCbS /port byte</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Frames</td>
<td>eINF /port packet</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>
### Basic Ethernet PM Concepts

<table>
<thead>
<tr>
<th>Basic Ethernet PM</th>
<th>Counter</th>
<th>Location</th>
<th>Unit</th>
<th>Threshold</th>
<th>X5IP</th>
<th>X4IP</th>
<th>X8PL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet Outgoing Frames</td>
<td>eONF</td>
<td>/port</td>
<td>packet</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Ethernet Incoming Bytes trapped by CPU</td>
<td>eINCP</td>
<td>/port</td>
<td>byte</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Ethernet Outgoing Bytes trapped by CPU</td>
<td>eONCP</td>
<td>/port</td>
<td>byte</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Ethernet Dropped Frames due to Error</td>
<td>ppDe</td>
<td>/port</td>
<td>packet</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Ethernet Incoming Number of Good Unicast Frames</td>
<td>eUPR</td>
<td>/port</td>
<td>packet</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Ethernet Outgoing Number of Unicast Frames</td>
<td>eUPS</td>
<td>/port</td>
<td>packet</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Basic Ethernet PM</td>
<td>Counter</td>
<td>Location</td>
<td>Unit</td>
<td>Threshold</td>
<td>X5IP</td>
<td>X4IP</td>
<td>X8PL</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td>----------</td>
<td>------</td>
<td>-----------</td>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>Ethernet Incom-</td>
<td>eMPR</td>
<td>/port</td>
<td>packet</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>ing Number of</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Good Multicast</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Frames</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ethernet Outgo-</td>
<td>eMPS</td>
<td>/port</td>
<td>packet</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>ing Number of</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multicast Frames</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ethernet Incom-</td>
<td>eBPR</td>
<td>/port</td>
<td>packet</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>ing Number of</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Good Broadcast</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Frames</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ethernet Outgo-</td>
<td>eBPS</td>
<td>/port</td>
<td>packet</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>ing Number of</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Broadcast Frames</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Ethernet service flow performance monitoring counters

Ethernet services are monitored at DiffServEdge ingress ports (UNI and E-NNI ports). Service flows can be identified by a flow descriptor (FD), based on C-tag (C-VID, C-UP), destination MAC address (DA), or IP-TOS byte, and at the E-NNI ports also by a virtual port descriptor (VPD), based on an S-tag (S-VID, S-UP). Please note that, if enumerations or value ranges are used, a VPD describes multiple virtual ports.
The following counters are supported:

<table>
<thead>
<tr>
<th>Ethernet Service Flow</th>
<th>Counter</th>
<th>Location</th>
<th>Unit</th>
<th>Threshold</th>
<th>X5IP</th>
<th>X4IP</th>
<th>X8PL</th>
</tr>
</thead>
<tbody>
<tr>
<td>all incoming bytes for one service flow</td>
<td>aQIB</td>
<td>/port /Service or /virtual port /Service</td>
<td>byte</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>-</td>
</tr>
<tr>
<td>incoming bytes of all green marked frames for one service flow</td>
<td>gQIB</td>
<td>/port /Service or /virtual port /Service</td>
<td>byte</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>-</td>
</tr>
<tr>
<td>incoming bytes of all yellow marked frames for one service flow</td>
<td>yQIB</td>
<td>/port /Service or /virtual port /Service</td>
<td>byte</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>incoming bytes of all red marked frames for one service flow</td>
<td>rQIB</td>
<td>/port /Service or /virtual port /Service</td>
<td>byte</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

**Note:** gQIB is supported in X5IP but not in X4IP.
### Ethernet high quality traffic counters

The Ethernet high quality traffic counters provide link load monitoring per traffic class and color (dropping precedence) for high-priority Ethernet traffic (traffic class 2 or 3, mapped into the egress queues 2 or 3 respectively).

The following counters are supported for Ethernet high quality traffic:

<table>
<thead>
<tr>
<th>High quality traffic ethernet load PM</th>
<th>Counter</th>
<th>Location</th>
<th>Unit</th>
<th>Threshold</th>
<th>X5IP</th>
<th>X4IP</th>
<th>X8PL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>LAN</td>
<td>WAN</td>
<td>LAN</td>
</tr>
<tr>
<td>incoming bytes of green frames with traffic class 2</td>
<td>g2EINB</td>
<td>/NR ingr /TC /color</td>
<td>byte</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>incoming bytes of yellow frames with traffic class 2</td>
<td>y2EINB</td>
<td>/NR ingr /TC /color</td>
<td>byte</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>incoming bytes of green frames with traffic class 3</td>
<td>g3EINB</td>
<td>/NR ingr /TC /color</td>
<td>byte</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>incoming bytes of yellow frames with traffic class 3</td>
<td>y3EINB</td>
<td>/NR ingr /TC /color</td>
<td>byte</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>High quality traffic ethernet load PM</td>
<td>Counter</td>
<td>Location</td>
<td>Unit</td>
<td>Threshold</td>
<td>X5IP</td>
<td>X4IP</td>
<td>X8PL</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------</td>
<td>----------</td>
<td>------</td>
<td>-----------</td>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>LAN</td>
<td>WAN</td>
<td>LAN</td>
</tr>
<tr>
<td>number of incoming green frames with traffic class 2</td>
<td>g2EINF</td>
<td>/NR ingr /TC /color</td>
<td>packet</td>
<td>-</td>
<td>-</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>number of incoming yellow frames with traffic class 2</td>
<td>y2EINF</td>
<td>/NR ingr /TC /color</td>
<td>packet</td>
<td>-</td>
<td>-</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>number of incoming green frames with traffic class 3</td>
<td>g3EINF</td>
<td>/NR ingr /TC /color</td>
<td>packet</td>
<td>-</td>
<td>-</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>number of incoming yellow frames with traffic class 3</td>
<td>y3EINF</td>
<td>/NR ingr /TC /color</td>
<td>packet</td>
<td>-</td>
<td>-</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>High quality traffic ethernet load PM</td>
<td>Counter</td>
<td>Location</td>
<td>Unit</td>
<td>Threshold</td>
<td>X5IP</td>
<td>X4IP</td>
<td>X8PL</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------</td>
<td>----------</td>
<td>------</td>
<td>-----------</td>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>LAN</td>
<td>WAN</td>
<td>LAN</td>
<td>WAN</td>
</tr>
<tr>
<td>incoming layer 1 payload bytes of green frames with traffic class 3 or internal (trapped) frames</td>
<td>c3EIN /NR ingr /TC /color</td>
<td>byte</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>incoming layer 1 payload bytes of green frames with traffic class 2 or traffic class 2 or internal (trapped) frames</td>
<td>c2EIN /NR ingr /TC /color</td>
<td>byte</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>High quality traffic ethernet load PM</td>
<td>Counter</td>
<td>Location</td>
<td>Unit</td>
<td>Threshold</td>
<td>X5IP</td>
<td>X4IP</td>
<td>X8PL</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------</td>
<td>----------</td>
<td>------</td>
<td>-----------</td>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>Loaded Second for incoming traffic with class 3 or internal traffic</td>
<td>i3gEILS</td>
<td>/NR ingr /TC /color</td>
<td>sec</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Loaded Second for incoming traffic with class 3 or class 2 or internal traffic</td>
<td>i32gEILS</td>
<td>/NR ingr /TC /color</td>
<td>sec</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Severely Loaded Second for incoming traffic with class 3 or internal traffic</td>
<td>i3gEISLS</td>
<td>/NR ingr /TC /color</td>
<td>sec</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>
### Ethernet low quality traffic counters

The Ethernet low quality traffic counters provide link load monitoring per traffic class and color (dropping precedence) for low-priority Ethernet traffic (traffic class 0 and 1, mapped into the egress queue 1).

The following counters are supported for Ethernet low quality traffic:

<table>
<thead>
<tr>
<th>Low quality traffic ethernet PM</th>
<th>Counter</th>
<th>Location</th>
<th>Unit</th>
<th>Threshold</th>
<th>X5IP</th>
<th>X4IP</th>
<th>X8PL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>LAN</td>
<td>WAN</td>
<td>LAN</td>
</tr>
<tr>
<td>incoming bytes of green frames with traffic class 0</td>
<td>g0EINB</td>
<td>/NR ingr /TC /color</td>
<td>byte</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Low quality traffic ethernet PM</td>
<td>Counter Location</td>
<td>Unit</td>
<td>Threshold</td>
<td>X5IP</td>
<td>X4IP</td>
<td>X8PL</td>
<td></td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------</td>
<td>------</td>
<td>------------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>incoming bytes of yellow frames with traffic class 0</td>
<td>y0EINB /NR ingr /TC /color</td>
<td>byte</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>incoming bytes of green frames with traffic class 1</td>
<td>g1EINB /NR ingr /TC /color</td>
<td>byte</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>incoming bytes of yellow frames with traffic class 1</td>
<td>y1EINB /NR ingr /TC /color</td>
<td>byte</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>number of incoming green frames with traffic class 0</td>
<td>g0EINF /NR ingr /TC /color</td>
<td>packet</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>number of incoming yellow frames with traffic class 0</td>
<td>y0EINF /NR ingr /TC /color</td>
<td>packet</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>
There is *no thresholding* for Ethernet low quality traffic.

**Ethernet service route round trip delay measurements**

The round trip delay is measured between two virtual switches within an Ethernet network by means of a dedicated configurable test frame that determines the “Ethernet service route”. To enable either a cyclic or a one-time latency measurement to a remote NE in the TransLAN network, whereby the remote NE can be identified by inserting its MAC address in the destination MAC address (DA) field of the test frame. Furthermore, the traffic class, the color (dropping precedence), the VLAN identifier and the length of the test frames can be specified, because these parameters may have influence on the delay. The RTD measurement path follows the currently valid STP-topology. The accuracy of the RTD measurement is 4 ms.

**Functional principle of RTD measurements**

A test frame is sent out from the FROM node. The test frame has the MAC address of the TO node as its destination MAC address (DA) all these influencing characteristics.
**Configuration rules**

Ethernet service route RTD measurements are only supported for virtual switches operating in one of the following modes:

- IEEE 802.1Q VLAN tagging mode with oversubscription (that is, with encoding of the dropping precedence)
- Provider bridge mode

The total number of Ethernet service routes per LAN unit is limited to 1024. If the operational mode of the virtual switch is changed to repeater mode, then the Ethernet service route will be deleted. If an Ethernet service route is deleted, then also the attached PM points (current and historic bins) will be deleted.

**PM counters**

The following counters are supported for Ethernet service route round trip delay measurements:

<table>
<thead>
<tr>
<th>Ethernet service route round trip delay</th>
<th>Counter</th>
<th>Location</th>
<th>Unit</th>
<th>Threshold</th>
<th>X5IP</th>
<th>X4IP</th>
<th>X8PL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>LAN</td>
<td>WAN</td>
<td>LAN</td>
</tr>
<tr>
<td>Minimum round trip delay</td>
<td>mRTD</td>
<td>/ETH_Service_Route</td>
<td>microsecond</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Average round trip delay</td>
<td>aRTD</td>
<td>/ETH_Service_Route</td>
<td>microsecond</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>90.0 percentile of round trip delay</td>
<td>xRTD</td>
<td>/ETH_Service_Route</td>
<td>microsecond</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>99.0 percentile of round trip delay</td>
<td>p900RTD</td>
<td>/ETH_Service_Route</td>
<td>microsecond</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>99.9 percentile of round trip delay</td>
<td>p990RTD</td>
<td>/ETH_Service_Route</td>
<td>microsecond</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Counter</td>
<td>Location</td>
<td>Unit</td>
<td>Threshold</td>
<td>X5IP</td>
<td>X4IP</td>
<td>X8PL</td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>--------------</td>
<td>----------</td>
<td>-----------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>p999RTD</td>
<td>/ETH_Service_Route</td>
<td>microsecond</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>sRTDM</td>
<td>/ETH_Service_Route</td>
<td>number of times</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>uRTDM</td>
<td>/ETH_Service_Route</td>
<td>number of times</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>
Available PM data

Generalities

Performance parameters are measured on a continuous basis at the termination point(s).

The performance parameters are:

- **ES** — Number of Errored Second
- **SES** — Number of Severely Errored Second
- **BBE** — Number of Background Block Errors
- **UAS** — Unavailable Second
- **BiDirUAS** — Bidirectional Unavailable Second
- **BiDirUAPcount** — Bidirectional Unavailable Period Count

Each of these parameters has a threshold. The threshold can be set according to your maintenance philosophy. If no thresholds are manually input, the network element will apply the default threshold values for each parameters. In the event that a measurement parameter exceeds this user-set threshold, the system generates an alarm.

Prerequisite to get an Alarm

Although unacceptable amount of errors were to occur at a termination point during several hours, no alarm would be raised unless you previously have:

- Enabled the *Thresholding* functionality;
- Enabled the performance parameters counters;
- Set the threshold values (TR and RTR) for the counters;
- Set the termination point to *monitored*, as mentioned in Prerequisite to be able to Monitor a TP.

SDH measurement parameters

Each of the measurement parameters has an associated counter. Performance monitoring results are displayed on screen by means of these counters.

The table below describes each performance monitoring measurement parameters:

<table>
<thead>
<tr>
<th>Measurement Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ES</td>
<td>A period of 1 second having one or more blocks in error.</td>
</tr>
</tbody>
</table>
SES

A period of one second having more than x % of its blocks in error. The value of x is called the SES Declaration Threshold. This threshold is default 30 (%). An SES is also counted as an ES.

BBE

An errored block, that does not occur as a part of a Severely Errored Second (SES).

UAS

One second which is contained within an Unavailable Period (UAP). An UAS is not counted as ES or SES.

BiDirUAS

Represents the number of seconds for which the link was unavailable in a period (24hr) for directional monitoring. biDirUAS is counted separately from UAS as it relates to both near and far end data.

BiDirUAPcount

Represents the number of times the link was unavailable in a period (24hrs) for bidirectional monitoring.

Ethernet measurement parameters

Since SDH uses STM-n signals and that LAN uses packets, we cannot use the same parameters to monitor performance in both cases. Therefore, LAN monitoring uses the following parameters:

The parameters and associated link are the following:

<table>
<thead>
<tr>
<th>LAN Measurement Parameters</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>CbR</td>
<td>Kilobytes Received from Ethernet to LAN port or from SDH to WAN port</td>
</tr>
<tr>
<td>CbS</td>
<td>Kilobytes Sent from LAN port to Ethernet or from WAN port to SDH</td>
</tr>
<tr>
<td>pDe</td>
<td>Packets dropped. These packets are received from Ethernet to LAN port and dropped by LAN port or received from SDH to WAN port and dropped by WAN port.</td>
</tr>
</tbody>
</table>
Other related parameters

There are other related performance parameters which, although not directly measured nor displayed on the ITM CIT, are taken into consideration during processing of performance data.

The below table lists other parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Errored Block (EB)</td>
<td>A block having one or more errors. This is determined by the comparing the outcome of the BIP check done before and after transmission. (see note below this table)</td>
</tr>
<tr>
<td>SES declaration threshold</td>
<td>This is the maximum of ES, beyond which it is declared a SES. This is an ITU-standard and is defaulted as the maximum number of admissible EB over one second. For all network elements, EB defaults to 30% of the maximum number of blocks.</td>
</tr>
<tr>
<td>Unavailable Period (UAP)</td>
<td>Interval of at least 10 seconds where the error rate is above the SES threshold. The UAP starts at the first second of a 10 seconds (or more) stretch SES. It stops at the first second of a 10 seconds (or more) duration in which there is no longer any SES occurring.</td>
</tr>
</tbody>
</table>

**Important!** The number of blocks per second depends on the signal itself. A VC-12 has 2000 blocks/s while an STM-N does have 8000 blocks/s. The SES threshold (30%) is calculated from these figures.

**SDH parameters thresholds**

Thresholds can be described as maximum acceptable number of errors, as provisioned by the user and in accordance with maintenance philosophy. The values allocated for those various thresholds are kept on the ITM CIT.

The thresholding functionality is applicable for unidirectional monitoring only. A prerequisite for the system to apply those thresholds and alert maintenance personal that they have been crossed, is to enable the thresholding functionality. Once the thresholding functionality is enabled, the specific values for the thresholds can be input on the ITM CIT. If no specific values are entered, the system reverts to using default values.

The ITM CIT defaults to disabled and can be turned on or off. The thresholding method is an explicit reset method, that is the threshold values must be input in the system.
Threshold types

There are two types of thresholds:
- **Threshold Report (TR):** This value causes a threshold crossing event. When this maximum is reached, the system raises the associated alarm if the prerequisite have been applied (see Prerequisite to get an Alarm). The minimum value for TR is 1 (one).
- **Reset Threshold Report (RTR):** This value causes a resetting of the event. When this threshold is reached, RTR clears the associated alarm. The RTR value is usually lower than the RT value. The minimum value for RTR is 0 (zero).

Both thresholds are independently provisionable per termination point and accumulation period for a given performance monitoring parameter.

Where $X = TR$ and $Y = RTR$

<table>
<thead>
<tr>
<th>If</th>
<th>Then</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nb BBE $\geq$ or equal to $X$</td>
<td>System launches the associated alarm</td>
</tr>
<tr>
<td>$X \geq$ or equal to Nb BBE $\geq$ or equal to $Y$</td>
<td>System stops the associated alarm</td>
</tr>
</tbody>
</table>

Threshold Range and Maximum

Each measurement parameter has a range for the acceptable values for TR. The lower limit for this threshold can never be zero to avoid an alarm storm from the NE to the ITM CIT.

The maximum allowable TR is dependent on:
- the parameter being measured;
- where performance is measured (meaning the TP);
- and the binning period.

The maximum threshold values for each parameter is listed in below:

<table>
<thead>
<tr>
<th>Threshold</th>
<th>Termination</th>
<th>15 Minutes</th>
<th>24 Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>SES</td>
<td>VC-4</td>
<td>810</td>
<td>77760</td>
</tr>
<tr>
<td></td>
<td>VC-12</td>
<td>810</td>
<td>77760</td>
</tr>
<tr>
<td></td>
<td>MS-1</td>
<td>810</td>
<td>77760</td>
</tr>
<tr>
<td></td>
<td>P12</td>
<td>810</td>
<td>77760</td>
</tr>
<tr>
<td>ES</td>
<td>VC-4</td>
<td>900</td>
<td>86400</td>
</tr>
<tr>
<td></td>
<td>VC-12</td>
<td>900</td>
<td>86400</td>
</tr>
<tr>
<td></td>
<td>MS-1</td>
<td>900</td>
<td>900</td>
</tr>
<tr>
<td></td>
<td>P12</td>
<td>900</td>
<td>900</td>
</tr>
</tbody>
</table>
### SHDSL performance monitoring

The performance of SHDSL segments that are terminated on the LTU, SRU and NTU can be monitored. The SHDSL standard (ITU-T Rec. G.991.2) prescribes a set of parameters that needs to be monitored and stored in 15 minute and 24 hour bins for near-end Performance Monitoring. The following table provides an overview of the PM parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CV/BBE</td>
<td>Code Violation/background Block Error</td>
<td>Each CRC6 anomaly is counted a CV/BBE during non-SES and non-UAS seconds</td>
</tr>
<tr>
<td>ES</td>
<td>Errored Seconds</td>
<td>Each second with one or more CRC6 anomaly is counted as an ES, unless that second is UAS</td>
</tr>
<tr>
<td>SES</td>
<td>Severely Errored Second</td>
<td>Each second with 50 or more CRC6 anomalies (&gt; 30%) or one or more LOSW events is counted as an SES, unless that second is UAS</td>
</tr>
<tr>
<td>LOSWS</td>
<td>Loss of SyncWord Second</td>
<td>Each second in which LOSW is declared as LOSWS</td>
</tr>
<tr>
<td>UAS/US</td>
<td>Unavailable Second</td>
<td>Each second that is part of unavailable time (UAT) is counted as UAS. UAT is declared at the begin of 10 consecutive SES and cleared at the begin of ten consecutive non-SES.</td>
</tr>
<tr>
<td>OFS/AIS</td>
<td>OOF or AIS Second</td>
<td>Second containing ab LOSW or AIS event</td>
</tr>
</tbody>
</table>
### Definitions of PM Parameters for SHDSL

For SHDSL, a performance monitoring block coincides with an SHDSL frame. Since the SHDSL frame length is 6 ms, there are 1662/3 blocks per second. The following definitions are applicable for PM parameters that are used for SHDSL segment termination points:

- **UAS:**
  
  Each second that is part of unavailable time is counted as a UAS. Unavailable time starts after ten consecutive SESs. These 10 seconds are part of unavailable time. Unavailable time stops after ten consecutive non-SESs. These 10 seconds are not part of unavailable time.

- **SES:**
  
  Each second in which 50 or more CRC-6 words are in error or in which a LOSW defect is active is counted as a SeverelyErroredSecond, provided the second is not a UAS. An SES detection threshold of 30% is equivalent to 50 errored blocks.

- **ES:**
  
  Each second in which one or more CRC-6 word is errored or in which a LOSW defect is active is counted as an ErroredSecond, provided the second is not a UAS.

- **BBE (CV):**
  
  Each SHDSL frame with an errored CRC-6 word is counted as a Background Block Error (Code Violation), provided the second in which the error occurs is not an SES or a UAS. Hence, the maximum possible number of BBEs per second is 49.

### Ranges and default thresholds

These are the ranges and default thresholds for SHDSL performance monitoring:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>15-minutes bin</th>
<th>24-hours bin</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range</td>
<td>Raise threshold</td>
</tr>
<tr>
<td>BBE</td>
<td>0 - 45000</td>
<td>3000</td>
</tr>
<tr>
<td>ES</td>
<td>0 - 900</td>
<td>120</td>
</tr>
<tr>
<td>SES</td>
<td>0 - 810</td>
<td>15</td>
</tr>
<tr>
<td>UAS</td>
<td>0 - 900</td>
<td>15</td>
</tr>
</tbody>
</table>
The default thresholds are *fix preset* and cannot be changed.

**Plotted performance diagram**

In the figure below an example is given how ES, SES, UAS, and BBE are computed. The number of errored blocks are plotted against time.

In the following figure, three different regions are noticeable. The grey shaded indicate the BBE.

The SES Declaration Threshold is set to 30%, which result in 600 errored blocks, as the maximum tolerable level of BBE for that type of signal. Since a VC–4 signal has 8000 frames per second and a VC-12 has 2000 frames per second, the 30% threshold for a VC-12 signal is lower than for a VC-4 and corresponds to 30% X 2000 or 600 BBE.

In the following figure, three different regions are noticeable.

- **REGION I**: In the first (I) region the SES Declaration Threshold is not reached and therefore only ESs are detected. Since there is no SES in this region, there is no AUS either.
- **REGION II**: In the second (II) region the SES Declaration Threshold is exceeded and several SESs are detected. An SES is also counted as an ES so the total period is also counted as ES. The SES is declared at the beginning of the stretch where the threshold is passed for longer than 10 seconds in a row.
- **REGION III**: In the third (III) region the amount of SES lasts for more than ten consecutive seconds, so UAS is detected. However an UAS is not detected as ES or SES.
Measurement periods

Measurement Parameters data is accumulated over a period of time which is referred to as the measurement period. There are two possible measurement periods:

- 15 minutes
- 24 hours

Directionality

For a given measurement period, the SDH measurement parameters can be tracked in one direction (uni-directional) or both (bi-directional). It is possible to monitor simultaneously:

- uni-directional 15 minutes,
- uni-directional 24 hours
- bi-directional 24 hours.

The table below explains the relationship between termination points, directionality, measurement periods, and the applicable measurement parameters:

<table>
<thead>
<tr>
<th>TP → Parameter ↓</th>
<th>MS1</th>
<th>VC-n</th>
<th>VC-n</th>
<th>LAN WAN</th>
<th>P12 (ISDN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direction and period</td>
<td>UNI 15'/24 hr</td>
<td>UNI 15'/24 hr</td>
<td>BI 24 hr</td>
<td>UNI 15'/24 hr</td>
<td>UNI 15'/24 hr</td>
</tr>
<tr>
<td>ES</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>SES</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>UAS</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>BBE</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>BiDirUAS</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BiDirUAP count</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CbR (Kbytes)</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>CbS(Kbytes)</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>pDe</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

**Important!** VC-n, where n=3, 4, 11, 12.
Configuration of the ITM-CIT

High Level View

The following diagram represents three activities that are available on the ITM-CIT regarding performance monitoring:

- Configuration of the ITM-CIT, binning period, termination points, and thresholds
- Parameters Measurements and Data Display
- Archiving and Data Recovery.
PERFORMANCE MONITORING

ITM-CIT CONFIGURATION

TERMINATION POINTS and PERIOD CONFIGURATION

THRESHOLDS VALUES CONFIGURATION

PARAMETERS MEASUREMENTS

DATA DISPLAY

VIEWING DATA AND PROVISIONNED PARAMETERS

REPORTS (created, displayed, printed)

LOG

DATA ARCHIVING

DATA RECOVERY AND STORAGE (Network element Bins)
Data Storage and Recovery

Measurement periods

Measurement Parameters data is accumulated over a so called measurement period. Three measurement periods are available:

- 15 minutes unidirectional
- 24 hours unidirectional
- 24 hours bidirectional

Bins

Performance monitoring data is stored in

- current PM bins

A bin contains performance data information for each termination point such as:

- Timestamp;
- Elapsed time;
- Suspect indication which is a data flag to indicate that the data stored in the bin is incomplete or invalid.

The table below lists the available bins:

<table>
<thead>
<tr>
<th>Direction</th>
<th>Number of 15 minutes Bins</th>
<th>Number 24 hours Bins</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uni-directional Current</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Uni-directional recent</td>
<td>16</td>
<td>1</td>
</tr>
<tr>
<td>Bi-directional current</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Bi-directional history</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

The uni-directional and bi-directional 24 hours bins store performance data over a span of a current 24 hours period. At the end of the current 24 hours period, the data is time-stamped and sent to the 24 hours recent bin, and the current 24 hours bin is reset to zero.

The uni-directional 15 minutes bins accumulates performance data over a span of 15 minutes periods. At the end of a current 15 minutes period, the data is time-stamped and transferred to the first of the fifteen available 15–minutes recent bins. When all the fifteen minutes history bins are full, the eldest history bin is overwritten by the new information to be transferred.
**Interval (Bin) suppression**

In the event that the current bin data is all zero and that the system indicator is not set, while the actual number of consecutive suppressed intervals is lower than the maximum number of consecutive suppressed intervals, then the current interval can be suppressed. This means that the data would not be transferred to the next available, or recent bin. The default value for the maximum number of consecutive suppressed intervals is zero, but can be provisioned per termination point for each accumulation period.

**UAP log**

The *UAP log* is an additional storage method. This log is a register that holds data of the six most recent periods of UAT. The UAP log timestamps each period of unavailability with a UAT begin and UAT end time. A period of UAT starts at the first second of a first UAS occurrence (see *UAS*, in SDH Measurement Parameters). UAT is implicitly provisioned as soon as a unidirectional termination point is configured. An operator can view the UAP log, maintain log of last month and use the NE data to synchronize the ITM CIT data.

If during an UAT period the NE clock is reset, the current UAT period shall end with a timestamp of the old time and a new UAT period shall be started with a timestamp of the new time.

**UAP counter**

A *UAP counter, called BiDirUAPcount*, tracks the number of unavailable periods. This counter can be viewed and reset by the operator.

**Reset of PM counters**

The ITM CIT offers the possibility to reset the parameters counter for uni and/or bidirectional monitoring in order to assist with maintenance activities. When the management system sends this request to the NE, the bin content is reset for the current 15 minutes bins and the content of the current 24 hours bins associated with a termination point.

Resetting the counters has the following consequences:

- Elapsed time is reset to zero;
- PM counters value (BBE, ES, SES, UAS, UAP) are reset to zero;
- UAPlog counter is NOT affected;
- Suspect indication is set.
**Data Recovery Following Loss of Association**

If the association between ITM-CIT and the NE fails, the ITM-CIT regains information about the lost time by reading the NE bins for the relevant interval. If the association fails for a longer period of time the NE may not be able to store sufficient information for a full recovery.

**Example of Loss of Association**

In the example below the association with the management system has been lost for six hours. Because this NE does have sixteen 15 minutes unidirectional bins only 4 hours of data can be recovered.

**On connection**

While performance monitoring is active the network element will store its most recent data in its bins. On connection the management system will retrieve all data present in the bins.
Configure PM on the ITM-CIT

Overview

Purpose

The purpose of this section is to describe the procedures for configuring the ITM-CIT, in preparation for performance monitoring.

Contents

| Enabling counter and setting thresholds | 10-41 |
| Editing PM counter thresholds          | 10-43 |
| Parameters for configuring PM on the ITM-CIT | 10-45 |
Enabling counter and setting thresholds

When to Use

The following procedures are performed when you want to enable performance monitoring on a termination point, to set the threshold values and the granularity of the monitored period.

Related Information

The items below list other relevant information to this procedure:

- Procedure to set the SDH TP Mode, for the required prior setting of the ports to be monitored. Refer to “Provision ports” (p. 5-62).
- “Concepts” (p. 10-3)

Parameters used in this procedure can be found at “Parameters for configuring PM on the ITM-CIT” (p. 10-45).

Enable counters and set thresholds

Follow this procedure to configure thresholds, thresholding functionality and to enable the counters.

....................................................................................................................................................................................................

1 Select Performance -> PM TP Configuration.

   Result: The Performance Monitoring Point Filter window appears in the PM Configuration mode.

....................................................................................................................................................................................................

2 Select filters for PM Point Type, Slot, Port and the SDH level if applicable (example VC3, VC4, VC12, VC11) and click OK.

   Important! Establishing VC-12 cross connections via a Fast Ethernet card determine the following:
   • Ethernet over SDH only terminates 20 VC12's.
   • Ethernet over SDH uses a fixed mapping so the 21st VC-12 will never be used for transmission.

   When enabling PM on VC-12 cross connections via a Fast Ethernet card, do not use the 21st VC-12.
### Performance monitoring

**Configure PM on the ITM-CIT**

**Enabling counter and setting thresholds**

**Result:** The *Edit Performance Monitoring Point* window appears applying the selected filters.

---

**3** Select the measurement period by clicking either *Unidir 15 Min*, *Unidir 24 hr*, or *Bidir 24 hr* tab.

**Important!** If you selected a LAN point type, the *Bidir 24 hr* tab is not available since bidirectional monitoring is not possible. Also, point types MS, RS, ISDN, and WAN are not available in the bidir 24 hr tab.

---

**4** Enable the counters by marking the *Enable Counters* check box.

**Result:** The checkbox *Enable Counters* is enabled.

---

**5** Enable thresholding by marking the *Enable Thresholding* checkbox.

**Result:** The threshold crossing functionality is enabled. The systems retrieves the last saved TR and RTR values from the NE and reports it in each parameter field. If there is no previously saved TR and RTR values (as for a new termination point), the system will fill in the default threshold values for those parameters (for thresholds range, minimum/maximum, and default values, see “Concepts” (p. 10-3).

The *Enable Thresholding* box is not available for bidirectional 24 hr monitoring.

---

**6** Set the threshold values (*TR* and *RTR*), if defaults are not desired.

For a selected LAN or WAN point type, the only configurable threshold is for parameter *pDe*.

---

**7** Select **OK**.

**Result:** If a *RTR* is greater than its *TR*, a message is displayed regarding the wrong value. The *Edit Performance Monitoring Point Filter* window disappears. The *Active Performance Monitoring Points* window get dynamically updated if they are opened.

The *Performance Monitoring Measurements* window gets only updated by clicking the **Update** button.

---

**End of steps**
Editing PM counter thresholds

When to Use

The following procedures must be performed when you want to enable performance monitoring on a termination point, to set the threshold values and the granularity of the monitored period.

Related Information

The items below list other relevant information to this procedure:

- Procedure to set the SDH TP Mode, for the required prior setting of the ports to be monitored. Refer to “Provision ports” (p. 5-62).
- “Concepts” (p. 10-3)

Parameters used in this procedure can be found at “Parameters for configuring PM on the ITM-CIT” (p. 10-45).

Before you begin

In order to be able to enter values in the various threshold fields, you must:

- Enable the Enable Thresholding checkbox

Edit PM counter thresholds

Follow this procedure in order to modify the values of the counter thresholds

1 Select Performance -> PM TP Configuration.

   **Result:** The PM Point Filter window is displayed. The ITM-CIT is in PM Configuration mode.

2 Select a filter from the proposed lists, for each enabled field.

   **Result:** The Slot, Port and AU4 fields dynamically get enabled according to the PM point type selected.

3 Select OK to apply the selection.

   **Result:** The Performance Monitoring Point Filter window disappears. The Edit Performance Monitoring Point window appears.

4 Select a binning period tab and verify that the Enable Thresholding checkbox is marked.
Result: The editable threshold current counter values are presented for each parameter.

5 Enter the desired values for thresholds.
   It is also possible to return to the default threshold values by clicking Default.
   Please review section on Concepts to know more about threshold defaults.

6 Select OK.
   Result: The Edit Performance Monitoring Point window disappears.

END OF STEPS
Parameters for configuring PM on the ITM-CIT

AU4

Layer of a connection termination point. This list is populated with AU4s if the selected PM Point Type is VC4 (VC-4-4c, VC-4-16c), AU4, TU12, TU2, or TU3. In all other cases this field is greyed out.

BBE

A Background Block Error (BBE) is an errored block not occurring as part of a Severely Errored Second (SES).

Default

Restores the installation TR and RTR default values for each performance parameters of the selected termination point. Greyed out when the Enable Thresholding is unchecked.

Enable counters

Enables/disables the digital counters linked to the active Tab (either 15 Minutes, 24 Hours, or Bidir 24 hr) and selected termination point.

Enable thresholding

Enables/disables thresholding for the monitored parameters of the selected Performance Monitoring point linked to the active Tab. This check box is greyed out if the Enable counters is unchecked.

When Enable Thresholding is changed from disable to enable the value of the TR and RTR is retrieved from the NE. If the value is not available because the termination point is newly created, then the system default value is retrieved.

EB

A block is regarded as Errored Block (EB) if that block does have one or more errors. This is determined by the comparing the outcome of the BIP check done before and after transmission. The number of blocks per second depends on the signal itself. A VC-12 does have 2000 blocks per second while an STM-N does have 8000 blocks per second.

ES

A second is regarded as Errored Second (ES) if this second has one or more blocks in error.

Termination point

Final destination where an incoming signal is terminated in the NE.
WAN, LAN port

A filter that can be applied to identify the WAN or LAN port is monitored for that point type.

PM point type

Displays a list from which you can select a monitorable and available point on the unit card. Changing the point type filter will dynamically re-populate the slot and port combo-boxes, as well as enabling the third field where the layer filter for cross connections or LAN interconnections must be further defined.

Port VC4

Displays a list of VC4 (VC-4-4c, VC-4-16c) ports available on the selected slot. The default is greyed out and empty. Displays the selection of VC4s after slot is selected. If all slots are selected, then all ports VC4 is the only choice possible in this field. The All value is only possible if the originating screen is Active Performance Monitoring Points, and not when it is Edit Performance Monitoring Point.

Selected TP

This field is automatically filled with the value of the PM Point Type selected in the originating Performance Monitoring Point Filter window.

SES

This is an ITU-standard and is defaulted as the maximum number of admissible EB over one second. The SES Declaration Threshold is the cut-off for ES. If the total number of EB over one second exceed this value, it is considered to be an SES. For all network elements, this number of blocks defaults to 30% of the maximum number of blocks (for example, 2400 for a VC-4; 600 for VC-12).

Slot

Displays a list of (virtual) slots in the system that contain possible monitoring points, matching the selected PM Point Type. The default is empty and greyed out. A Point Type must be selected to make selection possible in this field.

TR and RTR

TR stands for Threshold Report and causes a threshold crossing event. The RTR stands for reset threshold report and causes a resetting of the event. The minimum value for RTR is 0 and 1 for TR. As a general rule, RTR must be lower than TR. The range of their possible values varies namely according to the parameters. For more information on those range values, please refer to the section Concepts.
The ITM-CIT will consider these thresholds provided that the *Enable counter* and *Enable Thresholding* are marked. When *Thresholding* is enabled, the TR and RTR values are retrieved from the network element. If the termination point is new (as for a new termination point), the system assigns the default values.

**Unidir 15 min**

In this tab the thresholds for the unidirectional 15 minutes performance monitoring measurements can be set.

**Unidir 24 hr**

In this tab the thresholds for the unidirectional 24 hours performance monitoring measurements can be set.

**Bidir 24 hr**

In this tab the thresholds for the bidirectional 24 hours performance monitoring measurements can be set.

**UAS**

An *Unavailable Second (UAS)* is part of an *Unavailable Period (UAP)*. The UAP starts at the beginning of a 10 consecutive seconds stretch of SES. It stops at the first second of a 10 seconds of more duration in which there is no longer any SES occurring. An UAS is not counted as ES or SES.

**VC3 or VC12 associated to WAN port**

A third filter that can be applied to identify the VC3 or VC12 number associated to a WAN port. The letter “A” stands for the VC4 number, and the letters “BCD” corresponds to the KLM number of the VC3 or VC12.

**VC4, VC3, VC12, P12 (ISDN)**

A third available filter that must be defined to identify the VC4 number is monitored for that point type, at the cross-connect or tributary slot level.
Display PM data

Overview

Purpose

The purpose of this section is to describe the procedures to display the settings of provisioned TP, as well as PM current measurements.

Contents

| Displaying PM data | 10-49 |
| Parameters for displaying PM data | 10-53 |
Displaying PM data

When to use

The following procedures are performed to:

- Display details of any termination point settings
- Display PM and LAN performance data.

Related information

The items below list other relevant information to this procedure:

- Procedure to set the SDH TP Mode, for the required prior setting of the ports to be monitored. Refer to “Provision ports” (p. 5-62).
- “Concepts” (p. 10-3)
- Parameters used in this procedure can be found at “Parameters for displaying PM data” (p. 10-53).

Before you begin

No special prerequisites or precautions are needed when performing these procedures.

The items below gives information on tasks to perform before beginning the procedure:

- A prerequisite for this procedure is to set the port mode to monitored for the TP. See Related Information below.
- The proper LAN card must be installed in TS2 in order to be able to make performance LAN measurements.

Viewing TP settings & PM measurements

Follow this procedure in order to view the active measurement point settings of the NE.

1 Select Performance -> PM Current Measurements.

Result: The Performance Monitoring Point Filter window is displayed. The ITM-CIT is in measurement mode.

2 Select a PM Point Type Slot and its Port, and any additional SDH level “Filter” (p. 10-53) (if applicable). And select OK to apply the selection.

Result: The Active Performance Monitoring Points window appears.

3 Select a Performance Monitoring point from the list of provisioned termination points and Click Measurements...
Result: The Performance Monitoring Measurements window appears.

4 Select a binning period tab and click Updates.
Result: The current values of the monitored parameters get updated in the Performance Monitoring Measurements window.
By selecting the different tabs, all the different performance monitoring measurements can be displayed.

5 Select a termination point from the list and click Edit...
Result: The Edit Performance Monitoring Point window appears and the termination point settings can be viewed and edited.

6 Select a binning period tab and click Default and then, OK.
Result: The values of the measurement parameters fields return to their defined default values.
If all counters need to be reset, select Reset.

7 Select Close to return to the Active Performance Monitoring Points window.
Result: The Performance Monitoring Measurements window disappears and the Active Performance Monitoring Points window reappears.

8 Go back to step 3 to display another point from the list.

9 Display termination points that are not listed in the Active Performance Monitoring Points window by clicking on Filter... and redefine applicable filters. Return to step 3 to view other termination point measurements.

10 Click Close.
Result: The Active Performance Monitoring Points window closes.

END OF STEPS
Viewing LAN measurements

Follow this procedure to view the LAN current PM counter for a selected termination point.

1 Select Performance -> LAN.
   
   Result: The LAN Measurements window is displayed. The ITM-CIT is in LAN measurement mode.

2 Click Update.
   
   Result: Refreshes the window with the latest information.

3 Click Close.
   
   Result: The LAN Measurements window closes.

Viewing unavailable period log

Follow this procedure to view the details of the UAP log.

1 Select Performance -> PM Current Measurements.
   
   Result: The Performance Monitoring Point Filter window is displayed. The ITM-CIT is in measurement mode.

2 Select a PM Point Type and its Slot, Port and any additional SDH level filters (if applicable). And select OK to apply the selection.
   
   Result: The Active Performance Monitoring Points window appears.

3 Select a Performance Monitoring point from the list of provisioned termination points and Click Measurements...
   
   Result: The Performance Monitoring Measurements window appears.

4 Select the UAP tab.
Result: The unavailable period measurements are displayed.

5 Click on Close.

END OF STEPS
Parameters for displaying PM data

AU4

Layer of a connection termination point. This list is populated with AU4s if the selected PM Point Type is VC4 (VC-4-4c, VC-4-16c), AU4, TU12, TU2, or TU3. In all other cases this field is greyed out.

Bits per second

Measurement parameter for the LAN Measurement mode. It is the measurement at the Bridge from/to Ethernet, E1#* from/to Ethernet.

CbR

LAN measurement parameter. Stands for Total_number_of_octets_received. It represents all the octets in each packets that have been successfully received and that are passed to the switch.

CbS

LAN measurement parameter. Stands for Total_number_of_octets_sent. It represents all the octets in packets that come from the switch and transmitted by the port.

Current value

Displays the value of the current counter for the related point and counter.

Dropped packets

Measurement parameter for the LAN Measurement mode. It is the measurement at the Bridge from/to Ethernet.

Errored packets

Measurement parameter for the LAN Measurement mode. It is the measurement at the Bridge from/to Ethernet, E1#* from/to Ethernet.

Elapsed time

Displays the elapsed time since the start of the current bin accumulation till the last update of this screen.

Filter

Opens the **PM Point Filter** window and populates the list.
Measurements

Only active if one selection is made in the list. Opens Performance Monitoring Measurements. More than one instances of measurement can be open at the same time by selecting Points on the list and pressing Measurements.

Monitored parameter

Lists the measurement parameters and their values, which are being monitored.

pDe

LAN measurement parameter for Total number of packets dropped. It represents the incoming packet which is not to be handed over to switch because of format error of any kind.

PM point type

Displays a list from which you can select a monitorable and available point on the unit card. Changing the point type filter will dynamically re-populate the slot and port combo-boxes, as well as enabling the third field where the layer filter for cross connections or LAN interconnections must be further defined.

Port VC4

Displays a list of VC4 (VC-4-4c, VC-4-16c) ports available on the selected slot. The default is greyed out and empty. Displays the selection of VC4s after slot is selected. If all slots are selected, then all ports VC4 is the only choice possible in this field. The All value is only possible if the originating screen is Active Performance Monitoring Points, and not when it is Edit Performance Monitoring Point.

Start time

Displays a list of from which you can select a monitorable and available point on the unit card. Changing the point type filter will dynamically re-populate the slot and port combo-boxes, as well as enabling the third field where the layer filter for cross connections or LAN interconnections must be further defined.

Slot

Displays a list of (virtual) slots in the system that contain possible monitoring points, matching the selected PM Point Type. The default is empty and greyed out. A Point Type must be selected to make selection possible in this field.
Stop time
Displays the elapsed time since the start of the current bin accumulation till the last update of this screen.

Suspect flag
A marker for the data of the 15 minutes and 24 hours bins which is tagged on during specific situations such as:
- the current bins are reset by the ITM-CIT
- the performance monitoring is started and stopped
- the SES threshold is modified
- the time clock changes more than 5 seconds
- the stored data is incomplete or invalid because for example the unit is active but not operational

Termination point
Final destination where an incoming signal is terminated.

TU3 (k00)
A filter that can be applied to identify the TU3 number amongst the possible 3 within the VC4. The letter “K” stands for KLM number and the last two digits are for the TU3 number. TU3 is identified by KLM number 100, 200 or 300.

TU12 (KLM)
A filter that can be applied to identify the TU12 number amongst the possible 63 within the VC4 monitored at a given port. The TU12 is identified by giving its KLM number. An example is 364 where the first digit corresponds to the TUG-3 number (1..3), the second digit to the TUG-2 number (1..7) and the last digit to the TU-12 number (1..3).

Thresholding (15* or 24*)
Displays the activation state of the thresholding for the corresponding point and the Unidirectional 15 minutes counter. If disabled, the value of the state is displayed as “-”.

UAP
Near End unavailable binning period log. The UAP starts at the beginning of 10 consecutive seconds stretch of SES. It stops at the first second of a 10 seconds of more duration in which there is no longer any SES occurring.
Unidirectional 15 minutes
Displays if the displayed PM point Id has an active uni-directional 15 minutes measurement point.

Unidirectional 24 hours
Displays if the displayed PM Point Id has an active unidirectional 24 hours measurement point.

VC3 or VC12 associated to WAN port
A third filter that can be applied to identify the VC3 or VC12 number associated to a WAN port. The letter “A” stands for the VC4 number, and the letters “BCD” corresponds to the KLM number of the VC3 or VC12.

VC4, VC3, VC12, P12 (ISDN)
A third available filter that must be defined to identify the VC4 number is monitored for that point type, at the cross-connect or tributary slot level.

VC12 (ABCD)
A third filter that can be applied to identify the VC12 number corresponding to the monitored LAN interconnection. Each Fast LAN Ethernet connection maps into four VC12. Therefore, the letter “A” corresponds to the VC4 number and the letters “BCD” corresponds to the KLM number of the VC12.
User Provisionable CBS and PBS per flow

Overview

Purpose

The purpose of this section is to describe the procedures for provisioning the CBS and PBS per flow.

Contents

| User Provisionable CBS and PBS per flow | 10-58 |
User Provisionable CBS and PBS per flow

When to use

The following procedure is performed in order to provision the CBS/PBS per flow depending on the traffic class.

**Note:** The User Provisionable CBS and PBS per flow procedure is also applicable to X5IP.

Related information

The items below list other relevant information to this procedure:

- *Procedure to set the SDH TP Mode*, for the required prior setting of the ports to be monitored. Refer to “Provision ports” (p. 5-62).
- “Concepts” (p. 10-3)
- “Ethernet performance monitoring” (p. 10-13)

Before you begin

The items below gives information on tasks to perform before beginning the procedure:

- Proper LAN card must be installed in TS2 in order to be able to make performance LAN measurements.

Provisionable CBS per flow

Follow this procedure in order to view the CBS and PBS per flow.

1. Select **Provisioning → LAN Management → QoS Profile**.
   **Result:** The *NE LAN QoS Profile List* window appears.

2. Select a profile from the *Profile List* and click **Edit**
   **Result:** The *Edit QoS Profile* window appears.

3. In the *Edit QoS Profile* window select the CBS, PBS modes and Traffic class from the drop down list and CIR, PIR, and CBS, PBS size can be provisioned and then click **Ok**.
   **Result:** CBS and PBS per flow are provisioned.

END OF STEPS
Enhanced Ethernet Performance Monitoring

Overview

Purpose

The purpose of this section is to describe the procedures for enhanced ethernet performance monitoring.

Contents

| General Purpose Ethernet Port Monitor | 10-60 |
| Ethernet Service Monitor             | 10-62 |
| Ethernet High Priority, Low Priority Traffic Monitor and User Provisionable LS/SLS Threshold | 10-65 |
| RTD PM counters, RDT/TCA support, and End-2-End Ethernet PM - RTD | 10-68 |
| Enable round trip delay measurements | 10-70 |
| Perform a one-time round trip delay measurement for test purposes | 10-73 |
General Purpose Ethernet Port Monitor

When to use

The following procedure is performed when the user wants to enable the Ethernet Port monitor on each LAN or WAN port, to set the threshold values and the granularity of the monitored period.

Note: The General Purpose Ethernet Port Monitor procedure is also applicable to X5IP.

Related information

The items below list other relevant information to this procedure:

- Procedure to set the SDH TP Mode, for the required prior setting of the ports to be monitored. Refer to “Provision ports” (p. 5-62).
- “Concepts” (p. 10-3)
- “Ethernet performance monitoring” (p. 10-13)

Before you begin

The items below gives information on tasks to perform before beginning the procedure:

- Proper LAN card must be installed in TS2 in order to be able to make performance LAN measurements.
- A prerequisite for this procedure is to set the virtual switch in spanning tree mode “Provisioning a virtual switch in spanning tree mode” (p. 8-132).
- Cross connection should be enabled and VCG should be set to monitored.
- LAN port should be changed to Network port role in the Virtual Switch Information window.

Ethernet Port monitor

Follow this procedure in order to view the Port monitor counter and its threshold.

1. Select Performance → PM TP Configuration.

   Result: The Select Performance Monitoring Points window appears in the PM Configuration mode.

2. Select LAN for PM Point Type and select the Port and then click Add and Ok.
3 Click **Add**.

**Result:** The **Performance Monitoring Point Filter** window appears.

4 **Select LAN** for **PM Point Type** and select the **Port** and then click **Ok**.

**Result:** The **Edit Performance Monitoring Point** window appears.

5 **Select the measurement period** by clicking either **Unidir 15 Min** or **Unidir 24 hr** tab and then **enable the counters** by marking the **Enable Counters** check box.

**Result:** The checkbox **Enable Counters** is enabled.

6 **Enable thresholding** by marking the **Enable Thresholding** checkbox.

**Result:** The threshold crossing functionality is enabled. The system retrieves the last saved TR and RTR values from the NE and reports it in each parameter field. If there is no previously saved TR and RTR values (as for a new termination point), the system will fill in the default threshold values for those parameters (for thresholds range, minimum/maximum, and default values, see “**Concepts**” (p. 10-3).

7 **Select **Ok**.

**Result:** The **Edit Performance Monitoring Point Filter** window disappears. The **Active Performance Monitoring Points** window gets dynamically updated if they are opened.

8 **Select Performance -> PM Current Measurements**.

**Result:** The **Select Performance Monitoring Points** window is displayed. The ITM-CIT is in measurement mode.

9 **Click **Ok**.

**Result:** The **Current Performance Monitoring Measurement** window is displayed along with the Port monitor counters.
When to use

The following procedure is performed when the user wants to enable the Ethernet Service monitoring counters. The ethernet service flow PM counters are also known as flow TP PM, provides performance monitoring for an ethernet pack based on traffic class and color information.

Note: The Ethernet Service Monitor procedure is also applicable to X5IP.

Related information

The items below list other relevant information to this procedure:

- *Procedure to set the SDH TP Mode*, for the required prior setting of the ports to be monitored. Refer to “Provision ports” (p. 5-62).
- “Ethernet performance monitoring” (p. 10-13)
- “Concepts” (p. 10-3)

Before you begin

The items below gives information on tasks to perform before beginning the procedure:

- Proper LAN card must be installed in TS2 in order to be able to make performance LAN measurements.
- A prerequisite for this procedure is to set “Provisioning a virtual switch in spanning tree mode” (p. 8-132).
- Cross connection should be enabled and VCG should be set to monitored.

Service monitor

Follow this procedure in order to view the Service monitor counters.

1. Select **Provisioning → LAN Management → Virtual Switch**.
   
   Result: The *Virtual Switch List* window appears

2. Select a virtual switch from the list and click **Details**.
   
   Result: The *Virtual Switch Information* window appears.

3. Select a LAN port and click **Port Details**.
4 In the **Customer Port Information** window click **Edit**.
   
   **Result:** The **Select Port Role** window appears.

5 In the **Select Port Role** window select **Customer Port** and click **Next**.
   
   **Result:** The **Edit Port Information** window appears.

6 In the **Edit Port Information** window set the **PVID**, select **Default Profile** for **QOS Mode** and click **Ok**.

7 Click **Add Flow Table**.
   
   **Result:** The **Add Flow Table** window appears.

8 Set the **Descriptor** to none and click **Ok**.
   
   **Result:** The **Flow Table** is added.

9 In the **Customer Port Information** window click **Insert Flow Group**.
   
   **Result:** The **Insert Flow Group** window appears.

10 Set the **Descriptor** to cvid=1&&cup=0 , set the **Profile ID** and click **Ok**.

11 In the **Edit Port Information** window select **Flow Configuration** for **QOS Mode**, click **Ok** and **Close**.

12 Select **Performance → PM TP Configuration**.
   
   **Result:** The **Select Performance Monitoring Points** window appears in the PM Configuration mode.

13 Select **Flow TP** for **PM Point Type**, select the **Port**, select the **Flow Table ID** and **Flow Group ID** from the drop down list and then click **Add** and **Ok**.
Result: The Service Monitor is enabled in the Active Performance Monitoring Point List window.

14 Click Add.

Result: The Performance Monitoring Point Filter window appears.

15 Select Flow TP for PM Point Type and select the Port, select the Flow Table ID and Flow Group ID from the drop down list and then click Ok.

Result: The Edit Performance Monitoring Point window appears.

16 Select the measurement period by clicking either Unidir 15 Min or Unidir 24 hr tab and then enable the counters by marking the Enable Counters check box.

Result: The checkbox Enable Counters is enabled.

17 Select Ok.

Result: The Edit Performance Monitoring Point Filter window disappears. The Active Performance Monitoring Points window gets dynamically updated if they are opened.

18 Select Performance -> PM Current Measurements.

Result: The Select Performance Monitoring Points window is displayed. The ITM-CIT is in measurement mode.

19 Click Ok.

Result: The Current Performance Monitoring Measurement window is displayed along with the Service monitor counters.

End of steps
**When to use**

The following procedure is performed when you want to enable the Ethernet High priority and Low Priority Traffic monitor counters, to set the threshold values for the Ethernet High Priority Traffic monitor and the granularity of the monitored period. The high quality and low quality ethernet PM counters provides performance monitoring for an ethernet pack based on traffic class and color information.

**Note:** The Ethernet High Priority, Low Priority Traffic Monitor and User Provisionable LS/SLS Threshold procedure is also applicable to X5IP.

**Related information**

The items below list other relevant information to this procedure:

- *Procedure to set the SDH TP Mode*, for the required prior setting of the ports to be monitored. Refer to “Provision ports” (p. 5-62).
- “Concepts” (p. 10-3)
- “Ethernet performance monitoring” (p. 10-13)

**Before you begin**

The items below gives information on tasks to perform before beginning the procedure:

- Proper LAN card must be installed in TS2 in order to be able to make performance LAN measurements.
- A prerequisite for this procedure is to set “Provisioning a virtual switch in spanning tree mode” (p. 8-132).
- Cross connection should be enabled and VCG should be set to monitored.
- LAN and WAN ports should be changed to Network port role in the Virtual Switch Information window.

**High Priority and Low Priority Traffic Monitor**

Follow this procedure in order to view the High and Low priority Traffic monitoring counters and the User Provisionable LS/SLS Threshold.

1. Select **Performance → PM TP Configuration**.
**Result:** The Select Performance Monitoring Points window appears in the PM Configuration mode.

2 Select **Ethernet HQ Traffic** or **Ethernet LQ Traffic** for **PM Point Type** and select the **Port** and then click **Add** and **Ok**.

**Result:** The Ethernet High Priority Traffic Monitor or the Ethernet Low Priority Traffic Monitor is enabled in the Active Performance Monitoring Point List window.

3 Click **Add**.

**Result:** The Performance Monitoring Point Filter window appears.

4 Select **Ethernet HQ Traffic** or **Ethernet LQ Traffic** for **PM Point Type** and select the **Port** and then click **Ok**.

**Result:** The Edit Performance Monitoring Point window appears.

5 Select the measurement period by clicking either **Unidir 15 Min** or **Unidir 24 hr** tab and then enable the counters by marking the **Enable Counters** check box.

Select the User Provisionable LS/SLS by clicking the **PM Attribute** tab and then the Nominal Data Rate and the LS/SLS estimator should be provisioned.

**Result:** The checkbox **Enable Counters** is enabled.

The **PM attribute** tab is not available for the Ethernet Low Priority Traffic monitor.

6 Enable thresholding by marking the **Enable Thresholding** checkbox.

**Result:** The threshold crossing functionality is enabled. The systems retrieves the last saved TR and RTR values from the NE and reports it in each parameter field. If there is no previously saved TR and RTR values (as for a new termination point), the system will fill in the default threshold values for those parameters (for thresholds range, minimum/maximum, and default values, see “Concepts” (p. 10-3).

The **Enable Thresholding** box is not available for Ethernet Low Priority Traffic monitor.

7 Select **OK**.
Result: The Edit Performance Monitoring Point Filter window disappears. The Active Performance Monitoring Points window gets dynamically updated if they are opened.

8 Select Performance -> PM Current Measurements.

Result: The Select Performance Monitoring Points window is displayed. The ITM-CIT is in measurement mode.

9 Click Ok.

Result: The Current Performance Monitoring Measurement window is displayed along with the High or Low Priority Traffic monitor counters.

END OF STEPS
RTD PM counters, RDT/TCA support, and End-2-End Ethernet PM - RTD

When to use

The following procedure is performed when you want to enable the RTD monitor counters, to set the threshold values and the granularity of the monitored period.

**Note:** The RTD PM counters, RDT/TCA support, and End-2-End Ethernet PM - RTD procedure is also applicable to X5IP.

Related information

The items below list other relevant information to this procedure:

- “Ethernet performance monitoring” (p. 10-13)
- *Procedure to set the SDH TP Mode*, for the required prior setting of the ports to be monitored. Refer to “Provision ports” (p. 5-62).
- “Concepts” (p. 10-3)

Before you begin

The items below gives information on tasks to perform before beginning the procedure:

- Proper LAN card must be installed in TS2 in order to be able to make performance LAN measurements.
- A prerequisite for this procedure is to set the virtual switch in spanning tree mode “Provisioning a virtual switch in spanning tree mode” (p. 8-132).
- “Enable round trip delay measurements” (p. 10-70)

RTD counters

Follow this procedure in order to view the active measurement point settings of the NE.

1. Select Performance → PM TP Configuration.
   **Result:** The Select Performance Monitoring Points window appears in the PM Configuration mode.

2. Select Ethernet Service Route for PM Point Type and enter the Service Route ID and then click Add and Ok
   **Result:** The Ethernet Service Route is enabled

3. Click Add.
4 Select **Ethernet Service Route** for **PM Point Type** and enter the **Service Route ID** and then click **Ok**.

**Result:** The **Edit Performance Monitoring Point** window appears.

5 Select the measurement period by clicking either **Unidir 15 Min** or **Unidir 24 hr** tab and then enable the counters by marking the **Enable Counters** check box.

**Result:** The checkbox **Enable Counters** is enabled.

6 Enable thresholding by marking the **Enable Thresholding** checkbox.

**Result:** The threshold crossing functionality is enabled. The system retrieves the last saved TR and RTR values from the NE and reports it in each parameter field. If there is no previously saved TR and RTR values (as for a new termination point), the system will fill in the default threshold values for those parameters (for thresholds range, minimum/maximum, and default values, see “Concepts” (p. 10-3).

7 Select **OK**.

**Result:** The **Edit Performance Monitoring Point Filter** window disappears. The **Active Performance Monitoring Points** window gets dynamically updated if they are opened.

8 Select **Performance -> PM Current Measurements**.

**Result:** The **Select Performance Monitoring Points** window is displayed. The ITM-CIT is in measurement mode.

9 Click **Ok**.

**Result:** The **Current Performance Monitoring Measurement** window is displayed along with the RTD counters (Frame Delay monitor counters).

**END OF STEPS**
Enable round trip delay measurements

When to use

Use this procedure to:

- create an Ethernet service route for round trip delay (RTD) measurements,
- provision the related parameters of the test frame that is required for RTD measurements,
- start a cyclic RTD measurement.

Note: The Enable round trip delay measurements procedure is also applicable to X5IP.

Related information

The items below list other relevant information to this procedure:

- “Ethernet service route round trip delay measurements” (p. 10-24)

Before you begin

The items below gives information on tasks to perform before beginning the procedure:

- “Provisioning a virtual switch in spanning tree mode” (p. 8-132)

Procedure

1. Select Provisioning → LAN Management → Virtual Switch.
   
   Result: The Virtual Switch List window appears.

2. Select the desired LAN unit from the Physical Switch drop-down list box.
   
   Result: In the Virtual Switch List group box, the virtual switches are displayed that are currently provisioned for that unit.

3. Ethernet service route RTD measurements are only supported for virtual switches operating in one of the following modes:

   - STP virtual switch mode compliant with IEEE 802.1Q VLAN tagging mode with oversubscription (that is, with encoding of the dropping precedence)
   - STP virtual switch mode compliant with IEEE 802.1ad (“Provider bridge mode”)

   Select the desired virtual switch from the Virtual Switch List.

4. Click RTD Measurement.
5 In order to create an Ethernet service route for RTD measurements, click Add.

**Result:** The *Add RTD Ethernet Service Route* window appears.

*Edit an existing Ethernet service route:* To modify the configuration parameters of an existing Ethernet service route for RTD measurements, select the desired Ethernet service route in the *Round Trip Delay Measurements* window and click Edit. The *Edit RTD Ethernet Service Route* window appears.

6 Click Edit to modify the parameters of an existing Ethernet service route for RTD measurements by selecting the desired Ethernet service route in the *Round Trip Delay Measurements* window.

**Result:** The *Edit RTD Ethernet Service Route* window appears.

7 To define the Ethernet service route, provision the parameters of the RTD test frame:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Label</em></td>
<td>A user-provisionable name identifying the Ethernet service route. The label may consist of up to 20 ASCII characters.</td>
</tr>
<tr>
<td><em>Destination Address</em></td>
<td>The MAC address of the remote NE. The value must be a unicast MAC address.</td>
</tr>
<tr>
<td><em>Test Frame VLAN ID</em></td>
<td>The VLAN identifier to be encoded in the S-tag (outermost tag) of the test frame for the RTD measurement.</td>
</tr>
<tr>
<td></td>
<td>The permissible value range is [1 ... 4093].</td>
</tr>
<tr>
<td><em>Test Frame Traffic Class</em></td>
<td>The traffic class to be assigned to the test frame. Possible traffic classes are 0, 1, 2, or 3</td>
</tr>
<tr>
<td><em>Test Frame Color</em></td>
<td>The color (dropping precedence, encoded in the p0 bit) to be assigned to the test frame. Possible values are green (low dropping precedence) or yellow (high dropping precedence).</td>
</tr>
<tr>
<td><em>Test Frame Length</em></td>
<td>The length of the test frame. The length may vary between 64 and 9220 bytes for the X5IP card and the length may vary between 64 and 1650 for the X4IP-V2 card.</td>
</tr>
</tbody>
</table>
8 Click Ok.

**Result:** A cyclic RTD measurement starts with a repetition time of 45 s.
Perform a one-time round trip delay measurement for test purposes

When to use

This procedure is used to perform a one-time round trip delay measurement to a remote NE.

Note: The Perform a one-time round trip delay measurement for test purposes procedure is also applicable to X5IP.

Related information

The items below list other relevant information to this procedure:

- “Ethernet service route round trip delay measurements” (p. 10-24)

Before you begin

The items below gives information on tasks to perform before beginning the procedure:

- “Provisioning a virtual switch in spanning tree mode” (p. 8-132)
- “Enable round trip delay measurements” (p. 10-70)

Procedure

1. Select the Ethernet Service Route in the Round Trip Delay Measurement window and click Test.
   
   Result: The RTD Test window appears.

2. Click Trigger.
   
   Result: A message will appear on the screen with the lines: 15 seconds is needed to finish this test. Are you sure you wish to trigger a one shot RTD measurement?

3. Click Yes.
   
   Result: The RTD Value and Success Indication will be displayed in the RTD Test window.

4. Click Close.

END OF STEPS
Perform a one-time round trip delay measurement for test purposes.
11 MIB Upload/Download

Overview

Purpose

This chapter describes the procedures to be carried out for a NE which will support MIB upload and download by the MIB Upload/Download protocol.

It is possible to upload/download all the MIB data stored in the NE flash memory. The MIB upload is only possible when the MIB is in mibFilled or mibWaiting for Upload state. It is possible to download the MIB to the NE no matter what the current MIB state is. Before the MIB download, the user shall be informed to do a MIB upload and a user confirmation is needed to start a MIB download.

After the MIB is downloaded, user confirmation is needed to restart the NE with the new downloaded MIB. When doing MIB download, the PC shall validate the SW item code of the NE software and the MIB image. Only the SW item code with the same Info Model structure is allowed to be downloaded.

Contents

| MIB Upload to the ITM-CIT (Backup & Restore of MIB image via Q-LAN & PC) | 11-2 |
| MIB Download on a network element (Backup & Restore of MIB image via Q-LAN & PC) | 11-4 |
| To Edit the Node name in the MIB image | 11-6 |
MIB Upload to the ITM-CIT (Backup & Restore of MIB image via Q-LAN & PC)

When to use

Use this procedure to backup the network element database (current program and data) to the ITM Craft Interface Terminal (ITM CIT):

- after initial software installations/upgrades/changes
- after major provisioning data changes
- periodically according to local policy
- before software upgrades/changes
- before major provisioning data changes

Before you begin

Before you begin this task:

- Obtain the work instructions for this task.
- Verify that an ITM-CIT is connected and logged into the 1643 AM system.

Required equipment

The following equipment is required to perform this task.

- ITM Craft Interface Terminal (ITM CIT)
- 1643 AM

MIB Upload

Complete the following steps to backup the network element configuration database to the ITM-CIT.

1. In the MIB upload download tool select an adapter from the Ethernet Adapter List and click Ok.
   
   **Result:** The MIB Upload Download Tool window appears.

2. Click Select and select the Ethernet Adapter.
   
   **Note:** The MIB upload is only possible when the MIB is in mibFilled or mibWaitingForUpload state and it’s important to do a MIB upload before a MIB download.

3. Click Update and select the NE’s MAC Address.
4 Click Upload.

**Result:** The *Save As* window appears and enter the file name and click *Save*.

5 The *Login Name and Password* screen appears, enter the *Login Name* and *Password* and click *Ok*.

**Result:** The MIB Upload/Download Progress window appears and also the Description Edit window appears, where a description can be provided.

6 Click Exit.

**Result:** The *MIB Upload/Download Tool* window closes.

**END OF STEPS**
MIB Download on a network element (Backup & Restore of MIB image via Q-LAN & PC)

Purpose

Use this procedure to restore a previously saved configuration database to a network element.

Before you begin

Before you begin this task:

- Obtain the work instructions for this task and note the database to be restored and the location of the most recent backup files.
- Verify that an ITM-CIT is connected and logged in to the 1643 AM network element (NE) where the database is to be restored.

Required equipment

The following equipment is required to perform this task:

- ITM Craft Interface Terminal (ITM CIT)
- 1643 AM

MIB Download

Complete the following steps to backup the network element configuration database to the ITM-CIT.

1. In the MIB upload download tool select an adapter from the Ethernet Adapter List and click Ok.

   **Result:** The MIB Upload Download Tool window appears.

2. Click Select and select the Ethernet Adapter.

   **Result:** It is possible to download the MIB to the NE no matter what the current MIB state is.

3. Click Browse and select the binary file to be downloaded.

4. Select the NE Name in the NE List, and click Download.

   **Result:** A pop up window will appear with the message:

   Warning
Before Download, you should better upload the current MIB
data first!!!

5 Click Ok.

6 The LoginName and Password screen appears, enter the Login Name and Password and click Ok.

7 The MIB Upload/Download Progress window appears and then a pop up window will appear with the message:
   
   Result: Restart the NE, Confirmed?

8 Click Yes.
   
   Result: In the Select an Action window either select 0: Does not change the MIB state or 1: Change the MIB state to “non-confirmed” by selecting the appropriate radio button.

9 Click Exit.
   
   Result: The MIB Upload/Download Tool window closes.

END OF STEPS
To Edit the Node name in the MIB image

Purpose

Use this procedure to edit the name of the node in the MIB image.

Before you begin

Before you begin this task:

- Obtain the work instructions for this task and note the database to be restored and the location of the most recent backup files.
- Verify that an ITM CIT is connected and logged in to the 1643 AM network element (NE) where the database is to be restored.

Required equipment

The following equipment is required to perform this task:

- ITM Craft Interface Terminal (ITM CIT)
- 1643 AM

Procedure

Complete the following steps to backup the network element configuration database to the ITM-CIT.

1. In the MIB upload download tool select an adapter from the Ethernet Adapter List and click Ok.
   
   Result: The MIB Upload Download Tool window appears.

2. Click Select and select the Ethernet Adapter.

3. Click Browse to select the binary file name.

4. Click Info.

   Result: The MIB Data File Information window appears with the relevant information of the MIB image.

5. Click Edit to enter the new node name.
6 Click Close.

END OF STEPS
To Edit the Node name in the MIB image
12 Software upgrade

Overview

Purpose

This chapter describes how to upgrade the software of the 1643 AM and 1643 AMS.

Upgrading a system to newer releases

A software upgrade is to be performed when upgrading a system to a newer release.

Important! Upgrading to a newer release must be performed as follows:

- Upgrade to a new release,
- Wait until the network is stable,
- If the upgrade is not Ok, downgrade to old release, activate the old SW again.
- If the upgrade was Ok you can continue and for instance enable new features.

If you enable new features in the new release, and, in the worst case, have to
downgrade to a release that does not support the new features will result in NE cannot
restart.

If you had upgraded the SW from Release 1 to Release 2 and due to network
problems later you have to downgrade the system from R2 to R1 you will encounter
different problems.

- Downgrade to Release 1.1.3
  - the core unit will hang first
  - a cold start of the unit will clear the hang up. This will cause a traffic
    interruption of some minutes.
- Downgrade to R1.1.2

The core unit will hang for ever. To restart the core unit it has to - operator has to
visit the NE on side - power on rest or plug-out/plug in of the core units.
# Software upgrade

## Contents

<table>
<thead>
<tr>
<th>Concepts</th>
<th>12-3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software upgrade</td>
<td>12-4</td>
</tr>
</tbody>
</table>

**View software stored in an NE** | 12-6 |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>View software stored in the NE</td>
<td>12-7</td>
</tr>
<tr>
<td>Parameters for viewing the software stored in the NE</td>
<td>12-8</td>
</tr>
</tbody>
</table>

**Upgrade NE software** | 12-9 |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Loading NE software from CD-ROM to ITM CIT</td>
<td>12-10</td>
</tr>
<tr>
<td>Upgrading the software of an NE</td>
<td>12-12</td>
</tr>
<tr>
<td>Parameters for upgrading the software of an NE</td>
<td>12-15</td>
</tr>
</tbody>
</table>

**Switch the stores in an NE** | 12-17 |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch the software stores</td>
<td>12-18</td>
</tr>
<tr>
<td>Parameters for switching the software Stores</td>
<td>12-20</td>
</tr>
</tbody>
</table>
Concepts

Overview

Purpose

This section describes the background information necessary to perform the procedures for upgrading the software.

Contents

| Software upgrade | 12-4 |
Software upgrade

Introduction

The controller software of the network element is stored on the controller unit of the network element. To upgrade this software the new software must be downloaded on the network element. This can be done from the management system.

System controller software

The System Controller contains the software to control and support the network element. The Manufacturers Executable Code (MEC) file contains the complete software package for one network element. The software in the system controller is also used to provide a basic configuration to the units connected to the system controller. These other units obtain the appropriate part of the software package from the System Controller during the system start-up or when a unit is inserted.

Two memory stores

On the System Controller of the 1643 AM are two memory stores that can contain each a different MEC. The store with the software that is executed is called the active store and the other store is called the backup store. In case of a software upgrade, the management system downloads a complete software package to the backup store of the System Controller.

Switch stores

With a switch command from the management system, the software in the backup store can be made active. The switch command switches between the two stores, thus the active store becomes the backup store and vice versa.

Diagram

This diagram shows the software stores in the network element.
Commit the software

After confirmation of a switch command between the active and backup store, the management system loses its association with the network element. If the management system can renew the association with the network element the active store is committed. If the active store is not committed within two hours after the switch, the network element will switch back to the old software load.
View software stored in an NE

Overview

Purpose

Use the inventory information to:

• check which software is stored in a particular network element
• check if a specific software load is active
• retrieve certain codes of the software in the network element
• make an inventory of all network elements that contain a specific software load.

Contents

| View software stored in the NE                        | 12-7 |
| Parameters for viewing the software stored in the NE  | 12-8 |
View software stored in the NE

When to use

Use the following procedure to view the software stored in the NE.

Related information

Theoretical information about software upgrade can be found in “Concepts” (p. 12-3).

Before you begin

Before viewing the software inventories it is assumed that the:

- names and types of the network elements are known
- correct Item Code of the software you want to view is known (only for a Software Inventory).

There are two ways to view an inventory of the software stored in the NE. Use the following table to select the required window.

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Select</th>
<th>Window</th>
</tr>
</thead>
<tbody>
<tr>
<td>View software loaded in a network element</td>
<td>Provisioning -&gt; Equipment -&gt; NE Software Inventory</td>
<td>EMS - Provisioned NE Software Inventory</td>
</tr>
<tr>
<td>View list of NEs with particular software load</td>
<td>Provisioning -&gt; Equipment -&gt; Software Inventory</td>
<td>EMS - Software Inventory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(first a selection window appears where the NE type and the software version can be selected)</td>
</tr>
</tbody>
</table>

Procedure

Use the following procedure to find information about the software installed in a network element.

1. Select Provisioning → Equipment → NE Software Configuration.
   
   Result: The requested NE Software Configuration window appears.

2. Click the Close button to close the window.

End of steps
Parameters for viewing the software stored in the NE

Introduction

It is possible to view the following information about the network element controller software:
- the software version now stored in the active and backup store.
- the store state shows whether the software in the store is valid.

Active store

The software version of the executing code of the software loaded in the network elements active store is described by four codes. In the Software Inventory window only the Item Code is displayed.

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item Code</td>
<td>A code used to uniquely identify any system component.</td>
</tr>
<tr>
<td>Interchangeability Marker</td>
<td>An identification mark to indicate interchangeability among components.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>A number that indicates the sequence number and the year, date, and location of manufacture.</td>
</tr>
<tr>
<td>Com Code</td>
<td>A code which identifies the component.</td>
</tr>
</tbody>
</table>

Backup store

The same codes as those listed for the Active Store are used to describe the software stored in the backup store.

Active store state

The active store contains valid software if the store state is: Store Active.

Backup store state

The backup store contains valid software if the store state is: Store Inactive.
Upgrade NE software

Overview

Purpose

Use this procedure to download new software from the management system into the backup store on the system controller of the network element.

Contents

<table>
<thead>
<tr>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loading NE software from CD-ROM to ITM CIT</td>
<td>12-10</td>
</tr>
<tr>
<td>Upgrading the software of an NE</td>
<td>12-12</td>
</tr>
<tr>
<td>Parameters for upgrading the software of an NE</td>
<td>12-15</td>
</tr>
</tbody>
</table>
Loading NE software from CD-ROM to ITM CIT

When to use

Use this procedure to load the NE software from CD-ROM to your PC.

Before you begin

Before installing the software, the software release number must be known.

The installation program cannot install system files or update shared files if they are in use by other programs. For this reason the user must stop as many Windows applications as possible before starting with the installation procedures.

Installation procedure

Complete the following steps to install the NE software on your PC:

1. Insert the 1643 AM NE software CD-ROM into the appropriate drive of your PC.
   
   **Result:** Autorun will start the install process.

2. **IF** autorun does not start  
   
   **THEN** manually start the program by clicking Start → Run, click on Browse, select the CD-ROM drive, select the required directory and select the executable file which must have the extension .exe, click Open and click ok.
   
   **Result:** The Welcome to the InstallShield Wizard window for 1643 AM appears.

   **IF** autorun starts  
   
   **THEN** no action is required.
   
   **Result:** The Welcome to the InstallShield Wizard window for 1643 AM appears.

3. Click on Next to continue the installation.
   
   **Result:** The Software Licence Agreement window appears.

4. Click Yes to install 1643 AM NE software.
Important! When the (current) NE SW is going to be installed the ITM CIT version that fit's to the NE version is 'hard coded' in the installation routine. This means, in case there's no according directory available (for example, \Lucent Technologies\ITM CIT\<<version identifier>>\Isd\), the installer will create exactly this directory and puts the extracted “Isd” directory below this directory.

Result: The Setup Complete window appears.

5 Click Finish to finish the setup.

END OF STEPS
Upgrading the software of an NE

When to use

Use this procedure to download new software from the management system into the backup store on the system controller of the network element.

Follow this procedure when a new software version must be available on the network element.

To upgrade the software in a network element 2 procedures must be performed:

- Download new software into an NE
- Switch the Software Stores of the NE.

These procedures can also be performed separately.

Important! The software upgrade procedure described in this section only describes the maintenance SW upgrade within a particular release and not the upgrade concept from one release to another.

Related information

Parameters used in this procedure can be found at “Parameters for upgrading the software of an NE” (p. 12-15).

Before you begin

Before starting to download new software make sure:

- that the required controller software is available on the management system or on CD-ROM. If it is located on CD-ROM, you need to install it to your PC first (refer to “Loading NE software from CD-ROM to ITM CIT” (p. 12-10)).
- that there is sufficient time to complete the procedure. The procedure lasts about two hours.
- not to download software into the backup store while the active store is not committed. As long as the active store is not committed the network element may perform an automatic switch.
- not to forget to commit the software after performing a switch. If this is not done the network element will switch back to the previous active software after 2 hours.

Download new software into an NE

Perform the following step to download new software into a network element

1. Select Provisioning -> Equipment -> NE Software Configuration.
**Software upgrade**

**Upgrade NE software**

---

**Result:** The NE Software Configuration window appears with information about the software currently stored in the active and backup store of the network element.

---

2. Click **Edit**.

**Result:** The Edit NE Software Configuration window appears.

---

3. Click **Download**.

**Result:** A window appears allowing for the selection of the appropriate file to be downloaded.

---

4. Browse to the folder where the new software is stored. The new software can be downloaded either from floppies or from the hard drive in the PC. Select the file containing the new software and click **Open**.

**Result:** The Software Download Progress Display window appears and the progress of the software download is displayed.

To abort the software download click **Abort**.

---

**Switch the software stores of the NE**

Perform the following steps to switch the software stores of a network element.

---

1. Determine whether the MIB (Management Information Base) is compatible with the new software. If the MIB is not compatible, the MIB cannot be retained and must be provisioned again with new settings after the software switch or a converted MIB is provided by ITM-SC.

---

2. Select Provisoning -> Equipment -> NE Software Configuration.

**Result:** The NE Software Configuration window appears with information about the software currently stored in the active and backup store of the network element.

---

3. Click **Edit**.
**Result:** The *Edit NE Software Configuration* window appears. Check if the correct software version is stored in the backup store. After the switch this will be the active software running the network element.

4 Fill in the Retain MIB check box if the information in the MIB should be saved. This is only possible if the MIB is compatible with the new software. Not retaining the MIB means that the NE must be provisioned again with the new settings or a converted MIB must be downloaded from by ITM-SC.

Click **Switch**.

**Result:** A confirmation window appears.

5 Click **Yes**.

**Result:** The active and backup store are switched. The ITM-CIT loses its connection to the network element. The network element resets. This takes about 10 minutes.

6 Login to the network element again and select Provisioning -> Equipment -> NE Software Configuration again.

**Result:** The network element is now using the software that was previously in the backup store. The *NE Software configuration* window shows that the current content of the active and backup store. The *Active Store State* is *Active Not Committed*. If the new software in the active store is not committed within 2 hours, the network element will switch the stores back to its previous settings.

7 Click **Commit** in the *Edit NE Software Configuration* window.

**Result:** The software in the active store is committed. The *Active Store State* becomes *Active*. The network element will not switch back to its previous settings.

**End of Steps**
Parameters for upgrading the software of an NE

Introduction

The following parameters are used for Software Upgrade.

Active store

The software version of the executing code of the software loaded in the network elements active store is described by four codes.

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item Code</td>
<td>A code used to uniquely identify any system component.</td>
</tr>
<tr>
<td>Com Code</td>
<td>A code which identifies the component.</td>
</tr>
<tr>
<td>Interchangeability Marker</td>
<td>An identification mark to indicate interchangeability among components</td>
</tr>
<tr>
<td>Serial Number</td>
<td>A number that indicates the sequence number and the year, date, and location of manufacture.</td>
</tr>
</tbody>
</table>

Backup store

Shows the software load that is now stored in the backup store. The same codes are used as in the active store.

Active store state

The following table shows the possible values.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active.</td>
<td>Memory contains a valid code that is being executed.</td>
</tr>
<tr>
<td>Active Not Committed</td>
<td>If no association is made between the management system and the network element after a software switch. The software that was active before the switch is now in the backup store. If the association is not made within 2 hours after the switch, the system will switch the stores back so that the previous active software is made active again. Therefore it is not wise to download software while the active store is in this state.</td>
</tr>
</tbody>
</table>
Backup store state

The state of the backup store can have the following values:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error</td>
<td>Memory has corrupted data.</td>
</tr>
<tr>
<td>Clearing</td>
<td>After the download command has been given the inactive store is cleared first. When the backup store is in this state the software download cannot be aborted. To abort the software download wait until the backup store state is <strong>Store Downloading</strong>.</td>
</tr>
<tr>
<td>Empty</td>
<td>The clearing of the store has been successful and new software will now be downloaded.</td>
</tr>
<tr>
<td>Downloading</td>
<td>Code is being downloaded to the memory.</td>
</tr>
<tr>
<td>Inactive</td>
<td>Memory contains valid code that is not being executed.</td>
</tr>
</tbody>
</table>

Overall state

The Overall State of the system controller shows whether the System Controller unit is available to perform a software update. This state can have two values:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Busy</td>
<td>The controller card is busy. Software download cannot be done until the controller becomes available.</td>
</tr>
<tr>
<td>Available</td>
<td>The controller card is available for updates.</td>
</tr>
</tbody>
</table>
Switch the stores in an NE

Overview

Purpose

Use this procedure to switch between the active and backup stores and thus switch the network element from one software version to another.

Contents

<table>
<thead>
<tr>
<th>Switch the software stores</th>
<th>12-18</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters for switching the software Stores</td>
<td>12-20</td>
</tr>
</tbody>
</table>
Switch the software stores

When to use

When new software is loaded into the backup store and the backup store must become active to execute the new software.

Related information

The following procedures and information are related:

- Download New Software to a Network Element
- View Software Stored in the Network Element
- “Concepts” (p. 12-3).

Before you begin

When carrying out the switch operation pay attention to the following:

- if active and backup stores are switched over, the network element will reset using the software that was previously in the backup store. If this software is invalid, it may not be possible to continue to manage the network element.
- the switch operation may cause an interruption of traffic. This depends on the software that is in the backup store.
- after the confirmation of the switch command the management system loses its association with the network element for approximately 1 minute. If geographic redundancy (GR) is enabled a GR switch may occur
- if active and backup stores are switched over, the network element will reset using the software that was previously in the backup store. If this software is invalid, it may not be possible to continue to manage the network element
- the switch operation may cause an interruption of traffic. This depends on the software that is in the backup store
- after the confirmation of the switch command the management system loses its association with the network element for approximately 1 minute. If geographic redundancy (GR) is enabled a GR switch may occur.

Procedure

Follow these steps to switch to the software in the backup store of the network element:

1. Select Provisioning → Equipment → NE Software Configuration.
**Result:** The NE Software Configuration window displays the contents and states of the software stores of the network element.

2 Select **Edit** to switch to the new software in the selected network elements.

**Result:** The Edit NE Software Configuration window appears. Use this window to switch the active and backup stores.

3 Choose one of two switching modes as described earlier.

4 A confirmation window appears. Click No to return to the Edit NE Software Configuration window or Yes to confirm the software switch.

**Result:** After approximately two minutes the ITM CIT loses its association with the network element. One minute later the association is re-established and the network element works with the new software. If the association is not re-established the stores will switch back after two hours.

5 Click **Close** to exit the window.

**END OF STEPS**
Parameters for switching the software Stores

Introduction

Before switching the stores of the network element it is possible to view the following information about the network element:

- the state of the system controller,
- which software version is now stored in both the stores,
- the state of both stores.

Controller overall state

The Controller Overall State shows whether the System Controller unit is available to perform a software update. This state can have two values:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller Busy</td>
<td>The controller card is busy. Software download cannot be done until the controller becomes available.</td>
</tr>
<tr>
<td>Controller Available</td>
<td>The controller card is available for updates.</td>
</tr>
</tbody>
</table>

Active store

Shows the software load that is now active, stored in the active store.

Backup store

Shows the software load that is now stored in the backup store. This software version will become active after the switch.

Active store state

The state of the active store of the network element can have two values:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Store Active</td>
<td>Memory contains a valid code that is being executed.</td>
</tr>
<tr>
<td>Store Active Not Committed</td>
<td>If no association is made between the management system and the network element after a software switch. The software that was active before the switch is now in the backup store. If the association is not made within 2 hours after the switch, the system will switch the stores back so that the previous active software is made active again. Therefore it is not wise to download software while the active store is in this state.</td>
</tr>
</tbody>
</table>
Backup store state

The backup store contains valid software if the store state is *Store Inactive*.

Switching modes

The possible switching modes are described in the table below:

<table>
<thead>
<tr>
<th>Select</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch (No MIB Clear)</td>
<td>During the switch the MIB in the network element remains unchanged.</td>
</tr>
<tr>
<td>Switch (MIB Clear)</td>
<td>During this switch the network elements MIB is cleared. At the end of</td>
</tr>
<tr>
<td></td>
<td>the procedure the networks elements MIB is cleared and a new MIB must</td>
</tr>
<tr>
<td></td>
<td>be downloaded from the management system to the network element.</td>
</tr>
</tbody>
</table>
13 Engineering orderwire concepts

Overview

Purpose

The purpose of this section is to describe the Engineering orderwire concepts of the 1643 AM.

Contents

| Engineering orderwire | 13-2 |
Engineering orderwire

General description

For 1643 AM, only EOW for STM-1(1), STM-1(2) is available and there are only two user ports, V.11(1) and V.11(2). V.11(1) is connected to STM-1(1) and V.11(2) is connected to STM-1(2).

An external orderwire system can be connected which uses this orderwire channel for transparent data transmission via the 1643 AM transmission network.

The RJ45 connectors to be used for connecting this external orderwire systems are located at the backside of the 1643 AM and have the designation \textbf{E1 TP1} and \textbf{E1 TP2}.

E1 and E2 bytes

For this functionality the bytes E1 and E2 are used as orderwire channels. The RSOH byte E1 is accessible in all network element types, the MSOH byte E2 is only accessible in the multiplexers. The E1 and E2 bytes of both STM-1 interfaces are permanently assigned to User Byte ports.

PCM signals

The data received or transmitted via the G.703 interface represents pulse code modulated signals of voice frequency according to ITU-T Rec. G.711. As encoding rule the A-law is used.

Please note that feedback paths must not occur within an orderwire network. An external orderwire system can therefore only be connected in networks which have no feedback paths. This functionality is only available in meshed networks or networks with a ring structure, if these network structures are interrupted between two NEs for the orderwire traffic.

Number of orderwire branches per NE

There are two orderwire branches per network element, one for the STM-1(1) interface and one for the STM-1(2) interface. Each one gives access to the E1 byte and to the E2 byte.

Call occupies the entire channel

A call always occupies the entire channel, i.e. only one call can be made at any given time via this orderwire channel.
Channel control

The channel control and call signaling are taken over by the connected external orderwire system, and the 1643 AM transmission network serves only as a transmission medium. ITM CIT does not provide any setting options.
Glossary

Numerics

12 digit Numerical Code (12NC)
Used to as the unique identifier of an item or product. The first ten digits identify an item. The eleventh digit specifies the particular variant of the item. The twelfth digit indicates the revision issue. Items for which the first eleven digits are the same are functionally equal and may be exchanged.

5ESS
Number 5 Electronic Switching System

5TAD
Five Tributary Add-Drop subrack

9TAD
Nine Tributary Add-Drop subrack

A

AAU
Alarm Adapter Unit. Radio Relay circuit pack that is used for the collection of external alarms and remote control of external equipment.

AC
Alternating Current

ACU
Alarm Collection Unit. Radio Relay circuit pack that collects of equipment alarms, analogue measurements from internal monitoring points and calculation data.

ADM
Add-Drop Multiplexer

Administrative Unit (AU)
Carrier for TUs

Administrative-Unit Pointer (AU PTR)
Indicates the phase alignment of the VC-n with respect to the STM-N frame. The pointer position is fixed with respect to the STM-N frame.
**Administrator**

See ITM-SC System Administrator.

**Agent**

Performs operations on managed objects and issues events on behalf of these managed objects. All SDH managed objects will support at least one agent. Control of distant agents is possible via local "Managers".

**Alarm**

The notification (audible or visual) of a significant event. See also Event.

**Alarm Indication Signal (AIS)**

Code transmitted downstream in a digital Network that shows that an upstream failure has been detected and also alarmed if the upstream alarm has not been suppressed. Also called to as All OneS.

**Alarm Severity**

An attribute that defines the priority of the alarm message. The way in which alarms are processed depends on the severity.

**Aligning**

Using a pointer to indicate the head of a virtual container, for example, to create an Administrative Unit (AU) or a Tributary Unit (TU).

**ALS**

Automatic Laser Shutdown

**Alternate Mark Inversion (AMI)**

A line code that employs a ternary signal to convert binary digits. In this line code successive binary ones are represented by signal elements that are normally of alternately positive and negative polarity but are equal in amplitude, binary zeros are represented by signal elements that have zero amplitude.

**American Standard Code for Information Interchange (ASCII)**

A standard 8-bit code that is used to exchange information among data processing systems and associated equipment.

**Anomaly**

A difference between the actual and the desired operation of a function.

**ANSI**

American National Standards Institute

**APS**

Automatic Protection Switching

**AS**

Alarm Suppression assembly
Assembly
Gathering together of payload data with overhead and pointer information (an indication of the direction of the signal).

Association
A logical connection between manager and agent through which management information can be exchanged.

Asynchronous
See Non-synchronous.

ATC
Auxiliary Transmission Channel

ATM
Asynchronous Transfer Mode

ATPC
Automatic Transmit-Power Control

AU
Administrative Unit

AU4AD
Administrative Unit 4 Assembler/Disassembler

AUG
Administrative Unit Group

AUTO
Automatic

Automatic Transmit Power Control (ATPC)
Reduces the power output from the transmitter during normal propagation conditions and increases the power output to maximum during fading periods to try to maintain the nominal level of receiver input.

Autonomous Message
A message transmitted from the controlled network element to the ITM-SC that was not a response to a command that originated in the ITM-SC.

B

B3ZS
Bipolar 3-Zero Substitution

B8ZS
Bipolar 8-Zero Substitution
Glossary

BBTR
Backplane Bus TRansceiver

BC
Board Controller

BCC
Board Controller Complex

BIN
BINary

BIP
Bit-Interleaved Parity

BISDN
Broadband Integrated Services Digital Network

Bit Error Ratio (BER)
The ratio of bits received in error to bits sent.

Bit Interleaved Parity (BIP)
A method of error monitoring that uses a specified number of bits (BIP-8)

BLD OUT LG
Build-Out Lightguide

Board Controller Local Area Network (BC-LAN)
The internal local area network that provides communications between the Line Controller circuit pack and board controllers on the circuit packs that are associated with a high-speed line.

Branching
Interconnection of independent line systems.

Broadband Communication
Voice, data, and/or video communication at greater than two Mbit/s rates.

Broadband Service Transport
STM-1 concatenation transport over the SLM for ATM applications.

BUSTR
BUS Transmitter and Receiver

CAS
Channel Associated Signaling
CAT
CATastrophic

CC
Cross-Connection, Cross-Connect

CCIR
See ITU-R.

CCITT
See ITU-T.

CCS
Common Channel Signaling

CEPT
Conférence Européenne des Administrations des Postes et des Télécommunications

Channel
A sub-unit of transmission capacity within a defined higher level of transmission capacity, for example, a CEPT-4 (140 Mbit/s) within a 565 Mbit fiber system.

CIR
Committed Information Rate

Circuit
A combination of two transmission channels that permits bidirectional transmission of signals between two points to support a single communication.

CIT
Craft Interface Terminal

Clear Channel (Cl. Ch.)
A provisionable mode for the 34 and 140 Mbit/s tributary outputs that causes parity violations not to be monitored or corrected before the 34 and 140 Mbit/s outputs are encoded.

Client
Computer in a computer network that generally offers a user interface to a server. See also Server.

CMI
Coded Mark Inversion

CO
Central Office

Co-resident
A hardware configuration where the ITM-SC and ITM-NM applications can be independently active at the same time on the same hardware and software platform without interfering with each
Glossary

other's functioning.

**Common Object Request Broker Architecture (CORBA)**
CORBA allows applications to communicate with one another no matter where they are located or who has designed them.

**Concatenation**
A procedure whereby a multiplicity of Virtual Containers are associated with each other with the result that their combined capacity can be used as a single container across which bit-sequence integrity is maintained.

**Configuration Management (CM)**
Subsystem of the ITM-SC that, among other things, configures the network and processes messages from the network.

**CONN PCB**
Connector Printed Circuit Board

**Container (C)**
Carries plesiochronous signal, the "payload".

**CP**
Circuit Pack

**Craft Interface Terminal (CIT)**
Local manager for SDH network elements.

**CRC**
Cyclic Redundancy Check

**Cross-Connect Map**
Connection map for an SDH network element; contains information about how signals are connected between high speed time slots and low speed tributaries. See also Squelch Map.

**Cross-Polarization Interference Cancellation**
This feature permits both orthogonal polarizations of one Radio Frequency carrier to be used simultaneously, which provides greater spectral efficiency.

**CTP**
Connection Termination Point

**CV**
Code Violation

**DACS**
Digital Access & Cross-connect System
DACScan-T

See Integrated Transport Management Network Manager.

Data Communication Channel (DCC)

The embedded overhead communication channel in the SDH line. The DCC is used for end-to-end communication and maintenance. It carries alarm, control, and status information between network elements in an SDH network.

Data Communication Equipment (DCE)

Provides the signal conversion and coding between the data terminating equipment and the line. The DCE may be separate equipment or a part of the data terminating equipment.

Data Terminating Equipment (DTE)

Originates data for transmission and accepts transmitted data.

Database Administrator

A user who administers the database of the ITM-SC application. See also User Privilege.

DC

Direct Current

DCF

Data Communications Function

DCN

Data Communications Network

DCS

Digital Cross-connect System

DDF

Digital Distribution Frame

Dedicated Protection Ring (DP-Ring)

A protection method used in some network elements.

Default Value Provisioning

The original values are preprogrammed at the factory. These values can be overridden using local or remote provisioning.

Defect

A limited interruption of the ability of an item to perform a required function. The defect may or may not lead to maintenance action this depends on the results of additional analysis.

Demultiplexing

A process applied to a multiplexed signal to recover signals combined within it and restore the distinct individual channels of these signals.
**Digital Link**
A transmission span such as a point-to-point 2 Mbit/s, 34 Mbit/s, 140 Mbit/s, VC12, VC3, or VC4 link between controlled network elements. The channels within a digital link are insignificant.

**Digital Section**
A transmission span such as an STM-N or 565 Mbit/s signal. A digital section may contain multiple digital channels.

**DIL**
Dual In Line

**Directory-Service Network Element (DSNE)**
A designated network element that is responsible for administering a database that maps network element names (node names) to addresses (node Id). There can be one DSNE per (sub)network.

**Disassembly**
Splitting up of a signal into its constituents as payload data and overhead (an indication of the direction of a signal).

**Domain**
The domain of an ITM-SC is the set of all SDH network elements that are controlled by that particular ITM-SC.

**Downstream**
At or towards the destination of the considered transmission stream, i.e. in the direction of transmission.

**DPLL**
Digital Phase-Locked Loop

**DPS**
Data communication Packet Switch

**DR**
Digital Radio

**DRI**
Dual-Ring Interworking

**DS-n**
Digital Signal, Level n

**DTMF**
Dual-Tone Multi-Frequency

**Dual Homing**
An STM-1/STM-4 ring with AM-1 Plus equipment can be dual homed on a ring consisting of Metropolis® ADM (Universal Shelf), Metropolis® ADM (Compact Shelf) or WaveStar® ADM
Dual-Node Interworking
Dual Node Interworking (DNI) is a configuration of two ring networks that share two common nodes. DNI allows a circuit with one termination in one ring and one termination in another ring to survive a loss-of-signal failure of the shared node that is currently carrying service for the circuit.

DUS
Do not Use for Synchronization

DWDM
Dense-Wavelength Division Multiplexing

<table>
<thead>
<tr>
<th>E</th>
<th>EC-n</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Electrical Carrier, Level n</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ECC</th>
<th>Embedded Control Channel</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>EDFE</th>
<th>Ethernet Dropped Frames Errors</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>EH&amp;S</th>
<th>Environmental Health and Safety</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>EINB</th>
<th>Ethernet Incoming Number of Mbytes</th>
</tr>
</thead>
</table>

**Electronic Industries Association (EIA)**
A trade association of the electronic industry that establishes electrical and functional standards.

**Element Management System (EMS)**
See Integrated Transport Management Subnetwork Controller.

<table>
<thead>
<tr>
<th>EMC</th>
<th>ElectroMagnetic Compatibility</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>EMI</th>
<th>ElectroMagnetic Interference</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>EONB</th>
<th>Ethernet Outgoing Number of Mbytes</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>EOW</th>
<th>Engineering Order Wire</th>
</tr>
</thead>
</table>
**Equivalent Bit Error Ratio (EBER)**
The calculated average bit error rate over a data stream.

**Errored Second (ES)**
A performance monitoring parameter.

**ES**
End System

**ESD**
ElectroStatic Discharge

**ESPG**
Elastic Store & Pointer Generator

**ETSI**
European Telecommunication Standardization Institute

**Event**
A significant change. Events in controlled network elements include signal failures, equipment failures, signals exceeding thresholds, and protection switch activity. When an event occurs in a controlled network element, the controlled network element will generate an alarm or status message and send it to the ITM-SC.

**Event Management (EM)**
Subsystem of the ITM-SC that processes and logs event reports of the network.

**Externally Timed**
An operating condition of a clock in which it is locked to an external reference and uses time constants that are altered to quickly bring the local oscillator’s frequency into approximate agreement with the synchronization reference frequency.

**Extra Traffic**
Unprotected traffic that is carried over the protection channels when that capacity is not used for the protection of service traffic.

**Far End Block Error (FEBE)**
An indication returned to the transmitting node that an errored block has been detected at the receiving node. A block is a specified grouping of bits.

**Far End Receive Failure (FERF)**
An indication returned to a transmitting network element that the receiving network element has detected an incoming section failure.

**FAS**
Frame Alignment Signal
**FAW**
Frame Alignment Word

**FC**
Full contact Connector

**FCC**
Federal Communications Commission

**FDDI**
Fiber Distributed Data Interface

**FEP**
Front End Processor

**Free Running**
An operating condition of a network element in which its local oscillator is not locked to any synchronization reference and uses no storage techniques to sustain its accuracy.

**G**
**GARP**
Generic VLAN Registration Protocol

**Gateway Network Element (GNE)**
Passes information between other network elements and management systems via a Data Communications Network.

**Gbit/s**
Gigabits per second

**Geographic Location**
Location of the ITM-SC server. The geographic location is entered as part of the installation procedure of an ITM-SC.

**Geographic Redundancy (GR)**
Allows protection of management for a network element by assigning the network element to two ITM-SCs. The first primary ITM-SC usually manages the Network Element and is now in the protected domain. If the primary ITM-SC or the link between the network element and the primary ITM-SC fails, the secondary ITM-SC will automatically take over management of the network element and is now in the protecting domain. The two ITM-SCs are connected by a peer to peer link, which they use to pass Geographic Redundancy management information to each other. This link must be established before any network element can be protected by Geographic Redundancy.

**GFP**
Generic Framing Procedure
Global Wait to Restore Time
The time to wait before switching back to the timing reference occurs after a timing link failure has cleared. This time applies for all timing sources in a system hence the name global. This can be between 0 and 60 minutes, in increments of one minute.

GNE
Gateway network element - A network element that passes information between other network elements and operations systems via a data communications network.

GUI
Graphical User Interface

GVRP
Generic VLAN Registration Protocol

H

Host Exchange

High Density Bipolar 3 code (HDB3)
Line code for example, 2 Mbit/s transmission systems.

High level Data Link Control (HDLC)
Protocol in the data-link layer of the OSI reference model.

Higher order Path Adaptation (HPA)
Function that adapts a lower order Virtual Container to a higher order Virtual Container by processing the Tributary Unit pointer which indicates the phase of the lower order Virtual Container Path Overhead relative to the higher order Virtual-Container Path Overhead, and assembling/disassembling the complete higher order Virtual Container.

Higher order Path Connection (HPC)
Function that provides for flexible assignment of higher order Virtual Containers within an STM-N signal.

Higher order Path Termination (HPT)
Function that terminates a higher order path by generating and adding the appropriate Virtual-Container Path Overhead to the relevant container at the path source and removing the Virtual-Container Path Overhead and reading it at the path sink.

HMI
Human Machine Interface

HO
High Order
### Holdover

An operating condition of a clock in which its local oscillator is not locked to an external reference but uses storage techniques to maintain its accuracy with respect to the last known frequency comparison with a synchronized reference.

### Host Name

Name of the server on which the ITM-SC is running.

### HP-UX

Unix Operating System for a Hewlett Packard platform.

### HS

High Speed

### Glossary

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>I/O</td>
<td>Input/Output</td>
</tr>
<tr>
<td>ICB</td>
<td>Interconnection Box</td>
</tr>
<tr>
<td>ICP</td>
<td>InterConnection Panel</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Committee</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronic Engineers</td>
</tr>
<tr>
<td>IF</td>
<td>Intermediate Frequency</td>
</tr>
<tr>
<td>IFT</td>
<td>InterFace Terminal</td>
</tr>
</tbody>
</table>

**Integrated Transport Management Craft Interface Terminal (ITM-CIT)**

Local manager for SDH network elements in a subnetwork. Also called as Craft Interface Terminal.

**Intelligent Synchronous Multiplexer (ISM)**

A network multiplexer that is designed to flexibly multiplex plesiochronous and STM-1 tributary port signals into STM-1 or STM-4 line port signals.

**Intermediate System (IS)**

A system that routes/relays management information. An SDH network element may be a combined Intermediate and end system.
IPS
Inter Processor Status

IS
In-Service

IS-IS Routing
The network elements in a management network, route packets (data) between each other using an IS-IS level protocol. The size of a network that is running IS-IS Level 1 is limited, and therefore certain mechanisms are employed to facilitate the management of larger networks. For STATIC ROUTING, it is possible to disable the protocol over the LAN connections and thereby effectively cause the management network to be partitioned into separate IS-IS Level 1 areas. In order for the ITM-SC to communicate with a specific network element in one of these areas, the ITM-SC must identify the Gateway network element through which this specific network element is connected to the LAN. All packets to this specific network element are routed directly to the Gateway network element by the ITM-SC, before being re-routed (if necessary) within the Level 1 area. For DYNAMIC ROUTING an IS-IS Level 2 routing protocol is used that allows a number of Level 1 areas to interwork. The network elements that connect an IS-IS area to another area are set to run the IS-IS Level 2 protocol within the network element and on the connection to other network elements. Packets can now be routed between IS-IS areas and the ITM-SC does not have to identify the Gateway network elements.

ISDN
Integrated Services Digital Network

ISO
International Standards Organisation

ITM-SC Administrator
See ITM-SC System Administrator.

ITM-SC System Administrator
A user of the ITM-SC application with System Administrator privileges. See also User Privilege.

ITU
International Telecommunications Union

ITU-R
International Telecommunications Union - Radio standardization sector. Formerly known as CCIR: Comité Consultatif International Radio; International Radio Consultative Committee.

ITU-T
International Telecommunications Union - Telecommunication standardization sector. Formerly known as CCITT: Comité Consultatif International Télégraphique & Téléphonique; International Telegraph and Telephone Consultative Committee.
**Glossary**

**J**

**Jitter**
Short term variations of amplitude and frequency components of a digital signal from their ideal position in time.

**L**

**LAN**
Local Area Network

**LBA**
Lightwave Booster Amplifier.

**LBO**
Line Build Out - An optical attenuator that guarantees the proper signal level and shape at the receiver input.

**LCAS**
Link Capacity Adjustment Scheme

**LCN**
Local Communications Network

**LDI**
Linear Drop/Insert (Add-Drop)

**LED**
Light Emitting Diode

**LEN**
Local Exchange Node

**LF**
Low Frequency

**LH**
Long Haul

**License key**
An encrypted code that is required to enable the use of specific modules in the ITM-SC. Valid license keys can be obtained from your provider.

**Line**
Transmission line; refers to a transmission medium, together with the associated high speed equipment, that are required transport information between two consecutive network elements, one of which originates the line signal and the other terminates the line signal.
**Line Build Out (LBO)**
An optical attenuator that guarantees the proper signal level and shape at the receiver input.

**Line Overhead Controller (LOC)**
SLM circuit pack that accesses the overhead bytes from the high speed line.

**LNC**
LiNe Controller (SLM)

**LO**
Low Order

**LOF**
Loss Of Frame

**LOM**
Loss Of Multiframe

**Loop Timing**
A timing mode in which the terminal derives its transmit timing from the received line signal.

**LOP**
Loss Of Pointer

**LOS**
Loss Of Signal

**Lower order Path Adaptation (LPA)**
Function that adapts a PDH signal to a synchronous network by mapping the signal into or de-mapping the signal out of a synchronous container.

**Lower order Path Connection (LPC)**
Function that provides for flexible assignment of lower order VCs in a higher order VC.

**Lower order Path Termination (LPT)**
Function that terminates a lower order path by generating and adding the appropriate VC POH to the relevant container at the path source and removing the VC POH and reading it at the path sink.

**LPU**
Line Port Unit

**LPU155**
Line Port Unit 155 Mbit/s

**LRX**
Line Receiver

**LS**
Low Speed
**Glossary**

**LTA**
Line Terminal Application

**LTX**
Line Transmitter

**LTX/EML**
Line Transmitter with Electro-absorption Modulated Laser

<table>
<thead>
<tr>
<th>M</th>
<th>MAF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Application Function</td>
<td></td>
</tr>
</tbody>
</table>

**Management Connection**
Identifies the type of routing used (STATIC or DYNAMIC). If STATIC is selected, Management Connection allows the gateway network element to be identified. See also IS-IS Routing.

**Management Information Base (MIB)**
The database in the network element. Contains the configuration data of the network element. A copy of each MIB is available in the ITM-SC and is called the MIB image. Under normal circumstances the MIB and MIB image of one Network Element are synchronized.

**Manager**
Is capable of issuing network management operations and receiving events

Manager
Capable of issuing network management operations and receiving events. The Manager communicates with the Agent in the controlled network element.

**Manufacturer Executable Code (MEC)**
Network element system software in binary format that is downloaded to one of the stores can be executed by the system controller of the network element.

**Mapping**
Gathering together of payload data with overhead, i.e. packing the PDH signal into a Virtual Container.

<table>
<thead>
<tr>
<th>MDI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Miscellaneous Discrete Input</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MDO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Miscellaneous Discrete Output</td>
</tr>
</tbody>
</table>

**Mediation Device (MD)**
Allows for exchange of management information between Operations System and network elements.
MEF
Maintenance Entity Function (in NE)

MEM
System MEMory unit

Message Communications Function (MCF)
Function that provides facilities for the transport and routing of Telecommunications Management Network messages to and from the Network Manager.

Metropolis® ADM MultiService Mux
A network multiplexer that is designed to flexibly multiplex plesiochronous and/or STM-1 tributary port signals into STM-4 or STM-16 line port signals.

MF
Mediation Function

MFS
Multi Frame Synchronization signal

MIB
The Management Information Base is the database in the node. The MIB contains the configuration data of the node. A copy of each MIB is available in the EMS and is called the MIB image. Under normal circumstances, the MIB and MIB image of one node are synchronized.

MIB image
See Management Information Base.

Midspan Meet
The capability to interface between two lightwave network elements of different vendors. This applies to high speed optical interfaces.

MLAN
MultiLAN

MMI
Man-Machine Interface Also called Human Machine Interface (HMI)

MO
Managed Object

Motif
X-Windows System supplied by Open Software Foundation.

MS
Multiplexer Section
**Glossary**

**MSOH**
Multiplex Section Overhead. Part of the SOH (Section Overhead). Is accessible only at line terminals and multiplexers.

**MSP**
Multiplex Section Protection. Provides capability of switching a signal from a working to a protection section.

**MTBF**
Mean Time Between Failures

**MTBMA**
Mean Time Between Maintenance Activities

**MTIE**
Maximum Time Interval Error

**MTPI**
Multiplexer Timing Physical Interface

**MTTR**
Mean Time To Repair

**Multiplexer Section OverHead (MSOH)**
Part of the Section Overhead. Is accessible only at line terminals and multiplexers.

**Multiplexer Section Protection (MSP)**
Provides capability of switching a signal from a working to a protection section.

**Multiplexer Section Shared Protection Ring (MS-SPRING)**
A protection method used in multiplex line systems.

**Multiplexer Section Termination (MST)**
Function that generates the Multiplexer Section Overhead in the transmit direction and terminates the Multiplexer Section Overhead in the receive direction.

**Multiplexer Timing Source (MTS)**
Function that provides the timing reference to the relevant component parts of the multiplex equipment and represents the SDH network element clock.

**Multiplexing**
A procedure by which multiple lower order path layer signals are adapted into a higher order path, or by which the multiple higher order path layer signals are adapted into a multiplex section.

**NE**
Network element. The NE is comprised of telecommunication equipment (or groups/parts of telecommunication equipment) and support equipment that performs network element functions.
A Network Element has one or more standard Q-type interfaces.

**NEF**
Network element function

**NEM**
Network element manager

**Network Element (NE)**
A network element is comprised of telecommunication equipment (or groups/parts of telecommunication equipment) and support equipment that performs network element functions. A Network Element has one or more standard Q-type interfaces. A network element can be directly managed by a management system. See also Node.

**Network Element Equivalent (NEE)**
The functionality, database size, and processing power that are required from the ITM-SC are different for each type of network element that is supported. Therefore each type represents a certain amount of Network Element Equivalent.

**Network Mediation Unit (NMU)**
Collects fault and alarm events from transmission equipment. The ITM-SC can forward alarms to the NMU. The NMU can forward alarms to an Operations System.

**Network Service Access Point (NSAP)**
An end system address of the System Controller according to ISO 8348 AD2. The format is ISO_DCC_LUCENT, which has the following structure:

**NMC**
Network Maintenance Center

**NMS**
Network Management System

**NNE**
Non-SDH network element

**NNI**
Network Node Interface

**Node**
A node or network element is defined as all equipment that is controlled by one system controller.

**Node**
Defined as all equipment that is controlled by one system controller. A node cannot always be directly managed by a management system. See also network element.
**NOMC**

Network Operation Maintenance Channel

**Non-revertive switching**

In non-revertive switching, there is an active and standby high-speed line, circuit pack, etc. When a protection switch occurs, the standby line, circuit pack, etc., is selected causing the old standby line, circuit pack, etc., to be used for the new active line, circuit pack, etc. The original active line, circuit pack, etc., becomes the standby line, circuit pack, etc. This status remains in effect when the fault clears. Therefore, this protection scheme is “non-revertive” in that there is no switch back to the original status in effect before the fault occurred.

**Non-synchronous**

The essential characteristic of timescales or signals such that their significant instants do not necessarily occur at the same average rate.

**Not Protected Domain**

The Not Protected Domain for the ITM-SC contains all the network elements that are managed by that ITM-SC and are not currently protected by another ITM-SC. If the ITM-SC fails, the network elements in this domain are not managed by any ITM-SC. See also Geographic Redundancy.

**NPI**

Null Pointer Indication

**NRZ**

Non-Return to Zero

**NSA**

Non-Service Affecting

**NUT**

Non pre-emptible Unprotected Traffic

**NVM**

Non-Volatile Memory

**OA**

Optical Amplifier
OAA case tools
A software package/tool to aid the process of requirements, analysis, design, and implementation of object orientated systems.

OAM&P
Operations, Administration, Maintenance, and Provisioning

OC-n
Optical Carrier, Level n

ODF
Optical Distribution Frame

ODU
Optical Demultiplexer Unit

OFS
Out of Frame Second

OI
Optical Interface

OMU
Optical Multiplexer Unit

OOF
Out Of Frame

OOS
Out Of Service

Operations System (OS)
The Operations System is the system that provides operations, administration, and maintenance functions.

Operator
A user of the ITM-SC application with Operator privileges. See also User Privilege.

Optical Line System (OLS)
A high-capacity lightwave system that is designed to multiplex eight optical signals with different wavelengths into one combined signal through an optical fiber. There is a difference of 1.5 micrometer in wavelength between two multiplexed signals.

OS
Operations System - A central computer-based system that is used to provide operations, administration, and maintenance functions.
OSB
Optical Splice Box

OSF
Open Software Foundation Operations System Function

OSF/Motif
The WaveStar® ITM-SC application has an X-windows graphical representation and the components used in the “Graphical User Interface” are OSF/Motif compliant, these components that are comprised of items such as: scrollbars, menus, radio buttons, etc.

OSI
Open Systems Interconnection

OW
(Engineering) Order Wire

P

PABX
Private Automatic Branch eXchange

Paddle Board - Peripheral Control and Timing link (PB-PCT)
A small circuit board used in a 5ESS exchange for protection switching and optical to electrical conversion of the PCT-link.

Path
A logical connection between one termination point at which a standard format for a signal at the given rate is assembled and from which the signal is transmitted, and another termination point at which the received standard frame format for the signal is disassembled.

Path AIS
Path Alarm Indication Signal - A path-level code that is sent downstream in a digital network as an indication that an upstream failure has been detected and alarmed.

Path Overhead (POH)
The Virtual-Container Path Overhead provides integrity of communication between the point of assembly of a Virtual Container and its point of disassembly.

Path Terminating Equipment
Network elements in which the path overhead is terminated.

PC
Personal Computer

PCB
Printed Circuit Board
**PCM**
Pulse Code Modulation

**PCT-link**
Peripheral Control and Timing-link

**PDH**
Plesiochronous Digital Hierarchy

**Peer ITM-SC**
ITM-SC at the other end of the peer-to-peer link.

**Peer to Peer link**
Connection between two ITM-SCs with Geographic Redundancy. The link is used to co-ordinate the management of a network element. See also Geographic Redundancy.

**Performance Monitoring (PM)**
Measures the quality of service and identifies degrading or marginally operating systems (before an alarm is generated).

**Peripheral Control and Timing Facility Interface (PCTFI)**
A proprietary physical link interface that supports the transport of 21 * 2 Mbit/s signals.

**PI**
Physical Interface, Plesiochronous Interface

**PIR**
Peak Information Rate

**PJE**
Pointer Justification Event

**Platform**
Family of equipment and software configurations that are designed to support a particular Application.

**Plesiochronous Network**
A network that contains multiple subnetworks, each of which is internally synchronous and operates at the same nominal frequency, but the timing of any of the subnetworks may be slightly different at any particular instant.

**PLL**
Phase Lock Loop

**PM**
Performance Monitoring - Measures the quality of service and identifies degrading or marginally operating systems (before an alarm is generated).
Glossary

PMA
Performance Monitoring Application

Pointer
An indicator whose value defines the frame offset of a virtual container with respect to the frame reference of the transport entity on which the Virtual Container is supported.

POTS
Plain Old Telephone Service

PP
Pointer Processing

PPC
Pointer Processor and Cross-connect

Primary ITM-SC
ITM-SC that is usually managing a network element. If the primary ITM-SC fails, management of the network element is passed over to the secondary ITM-SC. A network element should be provisioned normally on the primary ITM-SC and then be configured for use on the secondary ITM-SC. See also Geographic Redundancy.

Primary Reference Clock (PRC)
The main timing clock reference in SDH equipment.

Protected Domain
The protected domain for an ITM-SC contains all the network elements for which this manager is the primary ITM-SC and which are protected by another secondary ITM-SC. See also Geographic Redundancy.

Protecting Domain
The protecting domain for an ITM-SC contains all the network elements for which this manager is the secondary ITM-SC. See also Geographic Redundancy.

Protection
Extra capacity (channels, circuit packs) in transmission equipment that is not intended to be used for service, but rather to serve as backup against equipment failures.

Provisioning
Assigning a value to a system parameter.

PSA
Partially Service Affecting

PSDN
Public Switched Data Network
Glossary

**PSF**
Power Supply Filter

**PSF-SIP**
Power Supply Filter; originally designed for an Italian customer.

**PSN**
Packet-Switched Network

**PSTN**
Public Switched Telephone Network

**PT**
Protected Terminal Power-supply filter and Timing circuit pack

**PVID**
Port VLAN ID

**Q-LAN**
Thin Ethernet LAN (10BaseT) that connects the manager to gateway network elements so that management information can be exchanged between network elements and management systems.

**QAF**
Q-Adapter Function (in NE)

**QOS**
Quality Of Service

**Quality Level (QL)**
The quality of the timing signal(s) that are provided to clock a network element. The level is provided by the Synchronization Status Marker which can accompany the timing signal. If the System and Output Timing Quality Level mode is “Enabled”, and if the signal selected for the Station-Clock Output has a quality level below the Acceptance Quality Level, the network element “squelches” the Station-Clock Output Signal, which means that no signal is forwarded at all. Possible levels are: - PRC (Primary Reference Clock) - SSU_T (Synchronization Supply Unit - Transit) - SSU_L (Synchronization Supply Unit - Local) - SEC (SDH Equipment Clock) - DUS (Do not Use for Synchronization).

**RA**
Regenerator Application

**Radio Protection Switching system (RPS)**
The main function of the RPS is to handle the automatic and manual switching from a main channel to a common protection channel in an N+1 system.
Radio Relay (RR)
A point-to-point Digital Radio system to transport STM-1 signals via microwaves.

RCU
Rigid Connect Unit

RCVR Data Distribution Unit (RCVR)
Radio Relay circuit pack that distributes the protection channel and the low-priority traffic in the receiver side.

RDDU
RCVR Data Distribution Unit

RDI
Remote Defect Indicator. Previously known as Far End Receive Failure (FERF).

RDI
Ring Drop/Insert (Add-Drop)

RDSV
Running Digital Sum Violations

Receive-direction
The direction towards the cross-connect.

REGEN
Regenerator

Regenerator Loop
Loop in a network element between the Station Clock Output(s) and one or both Station Clock Inputs, which can be used to dejitterize the selected timing reference in network applications.

Regenerator Overhead Controller (ROC)
SLM circuit pack that provides user access to the SDH overhead channels at repeater sites.

Regenerator Section Termination (RST)
Function that generates the Regenerator Section Overhead (RSOH) in the transmit direction and terminates the RSOH in the receive direction.

REI
Remote Error Indication. Previously known as Far End Block Error (FEBE).

Relay Unit (RU)
Radio Relay circuit pack whose main function is to perform protection switching when the Alignment Switch in the demodulator unit is unable to perform protection switching.
**Restore Timer**

Counts down the time (in minutes) during which the switch waits to let the worker line recover before switching back to it. This option can be set to prevent the protection switch continually switching if a line has a continual transient fault. This field is greyed out if the mode is non-revertive.

**Revertive Switching**

In revertive switching, there is a working and protection high speed line, circuit pack, etc. When a protection switch occurs, the protection line, circuit pack, etc. is selected. When the fault clears, service reverts back to the original working line.

**RF**

Radio Frequency

**RFI**

Remote-Failure Indicator

**RGU**

ReGenerator Unit

**Route**

A series of contiguous digital sections.

**RPS**

Ring Protection Switching

**RSM**

Remote Switching Module

**RSOH**

Regenerator-Section OverHead; part of the SOH.

**RZ**

Return to Zero

**S**

**SA**

Service Affecting Synchronous Adapter

**SAI**

Station Alarm Interface

**SC**

Square coupled Connector

**SD**

Signal Degrade
SDH
Synchronous Digital Hierarchy. Definition of the degree of control of the various clocks in a digital network over other clocks.

SDH-TE
SDH - Terminal Equipment

SEC
SDH Equipment Clock

Secondary ITM-SC
Backup ITM-SC for a network element should the primary ITM-SC fail. A network element should be provisioned normally on the primary ITM-SC and then be configured for use on the secondary ITM-SC. See also Geographic Redundancy.

Section
A transport entity in the transmission media layer that provides integrity of information transfer across a section layer network connection by means of a termination function at the section layer.

Section Adaptation (SA)
Function that processes the AU-pointer to indicate the phase of the VC-3/4 POH relative to the STM-N SOH and assembles/disassembles the complete STM-N frame.

Section Overhead (SOH)
Capacity added to either an AU-4 or to an assembly of AU-3s to create an STM-1. Always contains STM-1 framing and can contain maintenance and operational functions. SOH can be subdivided into MSOH (multiplex section overhead) and RSOH (regenerator section overhead).

SEF
Support Entity Function (in NE)

Self-healing
A network’s ability to automatically recover from the failure of one or more of its components.

Server
Computer in a computer network that performs dedicated main tasks that require generally sufficient performance. See also Client.

Service
The operational mode of a physical entity that indicates that the entity is providing service. This designation will change with each switch action.

Severely Errored Frame Seconds (SEFS)
A performance monitoring parameter.

Severely Errored Second (SES)
A second that has a binary error ratio. SES is used as a performance monitoring parameter.
Glossary

**Severity**

See Alarm Severity

**SH**

Short Haul

**SI**

Synchronous Interface

**SIB**

Subrack Interface Box

**SLC**

Subscriber Loop Carrier

**SLM**

Signal Label Mismatch

**Smart Communication Channel (SCC)**

An HDLC messaging channel between the SDH-TE and the 5ESS host node. Similar to the DCC messaging channels that are located in the STM-N section overhead.

**SML**

Service Management Level

**SMN**

SDH Management Network

**SMS**

SDH Management Subnetwork

**SNC/I**

SubNetwork Connection (protection) / Inherent monitoring

**SNC/NI**

SubNetwork Connection / Non Intrusive monitoring

**SNR**

Signal to Noise Ratio

**Soft Windows**

PC emulator package for HP platforms.

**SOH**

Section Overhead. Capacity added to either an AU-4 or to an assembly of AU-3s to create an STM-1. Always contains STM-1 framing and can contain maintenance and operational functions. SOH can be subdivided in MSOH (Multiplex Section OverHead) and RSOH (Regenerator Section OverHead).
SONET
Synchronous Optical Network

Space Diversity (SD)
Reception of the Radio signal via mirror effects on Earth.

SPB2M
Subrack Protection for 2 Mbit/s Board

Specification and Design Language (SDL)
This is a standard formal language for specifying (essentially) finite state machines.

SPI
SDH Physical Interface Synchronous-Plesiochronous Interface

Squelch Map
Traffic map for SLM Add-Drop Multiplexer network elements that contains information for each cross-connection in the ring and indicates the source and destination network elements for the low-speed circuit to which the cross-connection belongs. This information is used to prevent traffic misconnection in rings that have isolated network elements or segments. See also Cross-Connect Map.

SSM
Synchronization Status Marker

Standby
The operational mode of a physical entity that indicates that the entity is not providing service, but standby. This designation changes with each switch action.

Station Clock Input (SCI)
An external clock may be connected to a Station Clock Input.

Station Clock Output (SCO)
A clock signal that can be used for other systems.

STM
Synchronous Transport Module Building block of SDH.

STP
Spanning Tree Protocol
Stretched Ring (STRING)
An open ring in which each node is an Add-Drop Multiplexer. The end nodes operate with one equipped high-speed line.

STS
Synchronous Transport Signal; used in SONET.

STVRP
Spanning Tree with VPN Registration Protocol

Subnetwork
A group of interconnected/interrelated network elements. The most common connotation is an SDH network in which the network elements have Data Communications Channels (DCC) connectivity.

Supervisor
A user of the ITM-SC application with Supervisor privileges. See also User Privilege.

Supervisory Unit (SU)
Radio Relay circuit pack that gives comprehensive supervision and control facilities to the user by collecting information from the Alarm Collection Units and Alarm Adapter Units.

SVCE
Service

Switch Receive Unit (SWR)
SLM circuit pack that provides the cross-connect in the receive direction between high speed line time slots and low speed tributaries.

Switch Transmit Unit (SWT)
SLM circuit pack that provides the cross-connect in the transmit direction between high speed line time slots and low speed tributaries.

Switching Module (SM)
An access module from the 5ESS switch.

Synchronization Supply Unit (SSU)
A circuit pack that recovers and reshapes the clock signal in order to filter out jitter. Local (SSU_L) and Transit (SSU_T) types are available.

Synchronous
The essential characteristic of time-scales or signals such that their corresponding significant instants occur at precisely the same average rate.

Synchronous Digital Hierarchy (SDH)
A hierarchical set of digital transport structures that is standardized for the transport of suitably adapted payloads over transmission networks.
Synchronous Equipment Management Function (SEMF)
Function that converts performance data and implementation-specific hardware alarms into object-oriented messages for transmission over the DCC and/or the Q-interface. The SEMF also converts object-oriented messages that are related to other management functions so that they can pass across the S reference points.

Synchronous Line Multiplexer (SLM)
A line multiplexer that is designed to multiplex VC-4 and STM-1 tributary port signals into STM-16 line port signals.

Synchronous Network
The synchronization of synchronous transmission systems with synchronous payloads to a master Network clock that can be traced to a single reference clock.

Synchronous Transport Module (STM)
The information structure that is used to support (section layer) connections in SDH.

System Administrator
A user of the computer system on which the ITM-SC application can be installed. See also User Privilege.

System Controller (CTL)
ISM circuit pack that controls the configuration of an Intelligent Synchronous Multiplexer system.

System Controller (SC)
A circuit pack that controls and provisions all units. It also contains the data communication packet switch functionality that is necessary for routing of management information between network elements and their management system.

System Controller (SCT)
SLM Line Terminal and Regenerator network element circuit pack that provides the highest level of system control for the Synchronous Line Multiplexer system. The SCT circuit pack provides overall administrative control of the system. The SCT memory is included in the same one circuit pack.

System Controller (STC)
SLM Add-Drop Multiplexer network element circuit pack that provides the highest level of system control for the Synchronous Line Multiplexer system. The STC circuit pack provides overall administrative control of the system. The STC memory is provided by the MEM circuit pack.

System Controller (SYSCTL)
OLS circuit pack that provides the highest level of system control for the Optical Line System. The SYSCTL circuit pack provides overall administrative control of the system. The SYSCTL memory is provided by the SYSMEM circuit pack.
System Memory Unit (MEM)
SLM Add-Drop Multiplexer network element circuit pack that provides the highest level of system control for the Synchronous Line Multiplexer system. The MEM circuit pack provides memory support for the System Controller (STC) circuit pack.

System Memory Unit (SYSMEM)
OLS circuit pack that provides the highest level of system control for the Optical Line System. The SYSMEM circuit pack provides memory support for the SYSCTL circuit pack.

TCA
Threshold Crossing Alarm

TCP/IP
Transmission Control Protocol/Internet Protocol

TDEV
Timing DEViation

TDM
Timing Division Multiplexing

Template
A collection of parameters that define a specific network element configuration. A template gives the user the opportunity to configure parameters in a network element with a single operation. The template is re-usable and allow the user to configure the parameters in many Network Elements in the same way. A set of default templates is provided, and the user can create new templates and edit or delete user-created ones. Note that a template is always associated with one specific network element type and cannot be used for other network element types.

TERM
Terminal Multiplexer

TGU
Timing Generator Unit

TI
Timing Interface

TLM
TeLeMetry Unit

TLP
Terminal with Line Protection

TMN
Telecommunications Management Network
### Glossary

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>TPU</td>
<td>Tributary Port Unit</td>
</tr>
<tr>
<td>TPU-PCT</td>
<td>Tributary Port Unit - Peripheral Control and Timing link</td>
</tr>
<tr>
<td>TPU155</td>
<td>Tributary port Unit 155 Mbit/s</td>
</tr>
<tr>
<td>TPU2</td>
<td>Tributary port Unit 2 Mbit/s</td>
</tr>
<tr>
<td>TPU34/45</td>
<td>Tributary port Unit 34/45 Mbit/s</td>
</tr>
</tbody>
</table>

**Transmit-direction**

The direction outwards from the cross-connect.

**Trellis Code Modulation**

A combined coding and modulation scheme for improving the reliability of a digital transmission system without increasing the transmitted power or the required bandwidth.

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRF</td>
<td>TRansFer unit</td>
</tr>
</tbody>
</table>

**Tributary**

A signal of a specific rate (2 Mbit/s, 34 Mbit/s, 140 Mbit/s, VC12, VC3, VC4, STM-1, or STM-4) that may be added to or dropped from a line signal.

**Tributary Overhead Controller (TOC)**

SLM circuit pack that allows access to the overhead bytes of the incoming tributary signal.

**Tributary Overhead Controller (TOHCTL)**

OLS circuit pack that allows access to the overhead bytes of the Supervisory channel.

**Tributary Unit (TU)**

An information structure that provides adaptation between the lower order path layer and the higher path layer. Consists of a VC-n plus a tributary unit pointer TU PTR.

**Tributary Unit Pointer (TU PTR)**

Indicates the phase alignment of the VC with respect to the TU in which it resides. The pointer position is fixed with respect to the TU frame.

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSA</td>
<td>Time Slot Assignment</td>
</tr>
<tr>
<td>TSI</td>
<td>Time Slot Interchange</td>
</tr>
</tbody>
</table>
Glossary

<table>
<thead>
<tr>
<th>TTP</th>
<th>Trail Termination Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>TUG</td>
<td>Tributary Unit Group</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>U</th>
<th>UAS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>UnAvailable Seconds</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>UIM/X</th>
<th>A package that is used for developing the WaveStar® ITM-SC GUI for X-windows.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ULDT</td>
<td>Ultra Long Distance Transmission</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unavailable Seconds</th>
<th>A performance monitoring parameter.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Uninterruptable Power Supply (UPS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allows connected computer equipment to gracefully shutdown and therefore prevents damage in the case of a power failure. Also absorbs dips in the power supply.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Universal Co-ordinated Time (UTC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>An indication of the time of an event that is independent of the time-zone in which the event occurred. The local time can be calculated from the Universal Co-ordinated Time.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Upgrade</th>
</tr>
</thead>
<tbody>
<tr>
<td>An upgrade is the addition of new capabilities (feature). An upgrade requires new software and may require new hardware.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>UPL</th>
</tr>
</thead>
<tbody>
<tr>
<td>User PaneL</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Upstream</th>
</tr>
</thead>
<tbody>
<tr>
<td>At or towards the source of the considered transmission stream, i.e. in the direction that is opposite to the direction of transmission.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>A permission of a user that allows to perform actions on the computer system on which the ITM-SC application runs. There are the following different types of users:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>V</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A number, text string, or other menu selection that is associated with a parameter.</td>
</tr>
</tbody>
</table>
VF
Voice Frequency

Virtual Container (VC)
Container with a path overhead.

VLAN
Virtual LAN

VPN
Virtual Private Network

W
Wait to Restore Time (WRT)
The time to wait before switching back after a failure has cleared in a revertive protection scheme. This time can be between 0 and 15 minutes, in increments of one minute.

WAN
Wide Area Network

Wander
Long term variations of amplitude frequency components (below 10 Hz) of a digital signal from their ideal position in time. Wander can result in buffer problems at a receiver.

WaveStar® Integrated Transport Management Subnetwork Controller (ITM-SC)
Manager for SDH network elements in a subnetwork. Also called an Element Management System.

WaveStar® Network Management System (NMS)
Manager for SDH network elements in a network. Formerly known as DACScan-T.

WDM
Wavelength Division Multiplexing

What You See Is What You Get (WYSIWYG)
Information as displayed on the screen will appear in the same way on printed output.

Wideband Communications
Voice, data, and/or video communication at digital rates from 64 kbit/s to 2 Mbit/s.

Windows
Graphical User Interface on PC systems.

Working
Label attached to a physical entity. In the case of revertive switching the working line or unit is the entity that carry service under normal operation. In the case of non-revertive switching this label has no particular meaning.
**Glossary**

- **WS**
  - WorkStation
- **WSF**
  - Work Station Facility

**X**

- **X-Terminal**
  - Workstation that can support an X-Windows interface
- **X-Windows**
  - Graphical User Interface on Unix Systems.
- **XMTR**
  - Transmitter
- **XMTR Switch Unit**
  - Radio Relay circuit pack that performs connections for protection switching and transmission of low priority traffic on the protection channel.
- **XPIC**
  - Cross Polarization Interference Cancellation
- **XSU**
  - XMTR Switch Unit
Index

Numerics
15 minutes, 10-34
15 minutes unidirectional, 10-37
2 Mbit/s signal mapping, 5-66
24 hours, 10-34
24 hours bidirectional, 10-37
24 hours unidirectional, 10-37

Abort, 6-23, 6-72
Acceptance QL, 7-42, 7-44, 7-50
Access control parameters
  view, 3-3
Access node, 8-61, 8-62
Access point identifier
  See: API
Access start time, 3-16
Acknowledged, 6-9
Acknowledged Information Transfer Service (AITS), 4-16
Active section, 8-224, 8-228, 8-233, 9-30
Active store, 12-15
Active system timing source, 7-35, 7-44
Add, 6-72
AIS, 9-8
ALAF, 8-147

Alarm, 6-5, 6-7
Alarm Details, 6-12
Alarm details
  view, 6-20
Alarm indication signal
  See: AIS
Alarm latching, 6-10
  default, 6-11
Alarm list, 6-72
Alarm Lists, 6-12
Alarm Management, 6-1
Alarm Severity Assignment Profile (ASAP)
  ASAP name, 6-62
  ASAP types, 6-48
dcn, 6-49
DEFAULT ASAP, 6-48
equipment, 6-50
ethPath, 6-52
ethPS, 6-53
Maximum number of ASAPs, 6-63
mdi, 6-51
pdhPath, 6-54
pdhPS, 6-53
sdhHOPath, 6-57, 6-57
sdhMS, 6-56
sdhMSP, 6-57
sdhPRS, 6-55
sdhVCG, 6-59
sdsl, 6-60
timing, 6-55
Alarm Signalling Mode, 5-61
Alarm summary
  view, 6-16
Alarm Summary field, 6-23
Alarm supervision, 6-64
Alarm type, 6-72, 6-81
Alarm Type field, 6-23
Alarms, 8-9
  supervise, 6-65
  view, 6-16
Alarms field, 6-23
Alarms Summary, 6-12
Anomaly, 6-5
API, 9-18
  API display mode, 9-18
AU4, 10-45, 10-53
Automatic Update, 6-24
Autonomous Events, 6-7
Available data, 10-27
Index

Delay-sensitive traffic, 8-100
Delete, 6-72
Description, 6-81
Description field, 6-24
Designated port, 8-50
Details, 6-81
Details Button, 6-24
Differential delay, 8-43
Digital Subscriber Line
DSL, 8-30
Directionality, 8-183, 8-191
DNU, 7-9
force, 7-51
Document conventions, xxvii
documentation
numbers, xxix
set; manuals, xxix
Dropped packets, 10-28
Also see: pDe
Dropper / Marker, 8-97
Dropping precedence, 8-95
Dynamic bandwidth adjustment (GbE), 8-44
Dynamic VLAN ID list, 8-76

EB, 10-29
EB count, 9-23
Edit, 6-72
Electrostatic discharge, 1-21
Electrostatic protection, 1-21
EMS connection state, 5-29, 5-52
End-to-end, 10-10
Engineering Order Wire, 13-1
EoS encapsulation, 8-81
Errored Block (EB), 10-45
Errored Second (ES), 10-45
Errored Seconds, 10-8
ES, 10-27
ESD
See: Electrostatic discharge
ESP
See: Electrostatic protection
ESP bonding point, 1-21
Ethernet address, 5-8
Ethernet frame, 8-75
Ethernet frame size, 8-27
Ethernet interface, 8-30
Ethernet over SDH
EoS, 8-30, 8-81
Ethernet over SDH (EoS), 8-27
Ethernet performance monitoring, 10-13
Ethernet Performance Monitoring
Enhanced, 10-59
Ethernet switch, 8-26
Ethertype, 8-74, 8-77, 8-77, 8-78
8-91
Event
archive, 6-14
display, 6-12
Event characteristics, 6-8
Event Status, 6-8
Events categories, 6-7
Events origin
Events flow, 6-5
Failure, 6-5
Failure description, 6-73
Fallback mode, 7-51
Far End, 10-10
Far end, 10-11
Far End Monitoring, 10-10
Fault, 6-5
FDA/CDRH laser classification, 1-13, 1-18
FDA/CDRH Regulations, 1-17
Filter, 6-81
filter, 10-53
Filter Button, 6-24
Filtering, 6-81
Filtering field, 6-24
Filters
set up, 6-17, 6-79
Flow classifier, 8-94
Flow control, 8-68
Flow type, 8-147
Force DNU, 7-51
Force logout, 3-16
Forward, 10-11
Forward monitoring, 10-9
Forward Monitoring, 10-10
Free Running, 7-5

GARP VLAN Registration Protocol (GVRP), 8-54, 8-76
Generic framing procedure, 8-81
Generic Framing Procedure
GFP, 8-30
Generic framing procedure
GFP, 8-81
Generic framing procedure (GFP), 8-27
GFP encapsulation
  VC12–Xv, 8-28, 8-82
  VC3–Xv, 8-29, 8-82
  VC4–Xv, 8-29
Global reported, 6-24
Global severity, 6-25
GVRP, 8-54, 8-88, 8-147

Hardware inventory, 5-37
Hazard level, 1-19
Help, 6-73
  Button, 6-25
Historical Data
  parameters, 6-81
Historical data
  view, 6-79
History alarms, 6-77
History log, 6-78
Hold of time, 9-27, 9-30
Hold off time, 8-221
Hold Over, 7-5
Hub node, 8-61, 8-62

IEC laser classification, 1-13, 1-18
IEC Requirements, 1-17
IEEE 802.1ad VLAN tagging mode, 8-77
IEEE 802.1Q VLAN tagging, 8-76
IM, 5-41
Inactivity time, 3-4
  change, 3-9
info, 6-73
Information, 6-10, 6-73
Insertion and removal facilities, 1-21
Instance, 6-25
Interchangeability Marker
  See: IM
  interface
    Ethernet, 8-30
Interval suppression, 10-38
IP parameters
  edit, 4-62
Isolate state, 5-11
ITM-CIT
  buttons, 2-16
  install, 2-4
  Installation procedure, 2-5, 12-10
  logout, 2-25
  menu, 2-9
  Requirements, 2-4

Jumbo frames, 8-27

LAN
  port label, 8-148
  LAN card, 10-8, 10-11, 10-11, 10-49
  LAN group, 8-26, 8-66, 8-75
  LAN interconnect, 8-68
  LAN interconnect mode, 8-70
  LAN monitoring, 10-11
  LAN parameters, 10-28
  LAN port, 8-25, 8-143
    details, 8-145, 8-151
    egress QoS, 8-143, 8-148
    ingress QoS, 8-143, 8-148

label, 8-143
  member, 8-143, 8-148
LAN port Counter, 10-46
LAN ports, 10-8, 10-11
LAN-VPN, 8-70
LAPD mode, 4-16
LAPD protocol, 4-16
LAPS encapsulation, 8-81
Laser classes, 1-13
Laser safety guidelines, 1-13
Laser safety instructions, 1-16
LCAS
  See: Link capacity adjustment scheme
Learning bridges, 8-39
Line Termination Unit
  LTU, 8-30
Lining Up Mode, 6-30
Lining up Mode
  Blocking Alarms, 6-29
Link Access Procedure SDH
  LAPS, 8-81
Link Access Procedure SDH (LAPS), 8-30
Link capacity adjustment scheme
  LCAS, 8-30
Link capacity adjustment scheme (LCAS), 8-43
Load, 6-73
Local Rroute
  edit, 4-64, 4-71
Lock access, 3-7
Lock out, 7-35, 7-44
  request, 7-36, 7-44
Lock state, 3-4
  change, 3-6
Locked, 7-5
Logging, 6-25
Login, 6-74
Login to an NE, 2-19
Logout
  force, 3-15
Loopback state, 5-67

Maintenance Philosophy, 6-11
  Maintenance-oriented performance monitoring, 10-4
  Management information base, 5-5
  See: MIB
  See: MIB
Management State, 5-29
Manual route
  add, 4-63
  edit, 4-64, 4-71
Maximum bridge diameter, 8-47
MDI, 5-12, 5-53
MDO, 5-57
  Miscellaneous discrete outputs
  See: MDO
Measurement location
  termination point, 10-8
Measurement parameters, 10-27
measurement periods, 10-34
Measurement Periods, 10-37
Measurement prerequisites, 10-9
Measurements, 10-54
Measuring method
  BIP, 10-8
MIB, 5-5, 5-11, 5-25
MIB image, 5-5
MISC_1 … MISC_8
  See: Miscellaneous Discrete Input 1 … Miscellaneous Discrete Input 8
Miscellaneous discrete input
  See: MDI
Miscellaneous Discrete Input 1 … Miscellaneous Discrete Input 8, 6-51
Miscellaneous discrete inputs
  See: MDI
Monitored parameters, 10-54
Most Recent Alarm, 6-25
MSP, 8-225
MSP pair selection, 8-233
MSP protection, 8-222, 9-28
  add, 8-231
  edit, 8-226
  switch, 9-29
  view, 8-223
Near End
  bidirectional, 10-10
Near End Monitoring, 10-10
NE-SW
  install, 12-10
Network
  Synchronization, 7-7
  network element
    name, 6-74
    state, 6-74
  network element Alarm Control Options, 6-28
Network role port, 8-66
Network Termination Unit
  NTU, 8-30
Network-role port, 8-70, 8-75, 8-87, 8-87
Network_side mode, 4-16
Node
  Details, 5-26, 5-48
Node creation, 5-11
Not Reported, 6-9, 6-9
NSAP, 6-74
NSAP address, 5-8

On Connection, 10-39
Outgoing QL, 7-51
Output port timing, 7-47, 7-50
Output state, 7-44
Oversubscription mode, 8-96

Parameters for Displaying Alarms, 6-23
Password, 6-74
  change, 3-12
  configure, 3-12
  confirm, 3-13
  enter, 3-13
Password confirmation, 6-72
Path cost, 8-49
Path trace, 9-7
Path Trace, 9-14
Path trace
  provision, 9-15
Path trace principle, 9-17
Path trace provisioning, 9-17
pDe, 10-54
Peak information rate (PIR), 8-95
Performance measurements, 10-8
Performance monitoring, 8-105
Performance Monitoring, 10-1
Physical ports, 9-4
PM Configuration
  parameters, 10-45
PM Data Display, 10-48
PM measurement
  mode, 10-43
PM point type, 10-46, 10-54
PM Point Type, 10-54
Port, 8-218, 10-46, 10-54
Also see: VC4
Also see: VC4
  provision, 5-63
Port mode, 5-66, 10-9, 10-49
Port mode time, 5-66
Port Monitor, 10-60
Port names, 5-66
Port provision, 10-41, 10-43, 10-49
Port role, 8-85
Port timing state, 7-52
Port Type, 9-4
Port types, 5-66, 9-4
Port VLAN identifier (PVID), 8-76
PRC, 7-7, 7-9
Pre-provisioning, 5-5
Primary reference clock
  See: PRC
Priority, 7-11, 7-36, 7-45
Probable cause, 6-25
Prompt, 6-74
Prompt Alarm, 6-10
Propagation delay, 8-43
Protection section, 9-30
Provider bridge mode, 8-91
Provider bridge tagging mode, 8-77
Provisioning
  bridge priority, 8-52
  LAN and WAN ports details, 8-93
  path cost, 8-52
  port priority, 8-52
Provisioning methods, 5-5
PVID, 8-144, 8-148
Quality level, 7-9
  See: QL
Quality of service, 8-40
Quality of Service, 8-90
Quality-of-service-oriented performance monitoring, 10-4
Queue, 8-99
Queue scheduling method, 8-100
Raise/Clear Delay, 6-30
Raised, 6-8, 6-82
Rapid spanning tree protocol (rSTP), 8-53
Rate control, 8-62
Rate control mode, 8-97, 8-144, 8-148
Rate control modes, 8-96
RDI, 9-8
Reference, 7-29
REI, 10-10, 10-11
  See: Remote Error Indication
Remote accessible NE
  edit, 4-52
Remote accessible Network Element
  add, 4-50
Remote defect indicator
  See: RDI
Remote Error Indication (REI), 10-5
Remote login
  via area option, 4-59
  via configured node list, 4-55
  via neighbors option, 4-57
Remote NE
  view, 6-69
Index

Repeater, 8-66
Repeater mode, 8-57
Reported, 6-9
Reporting class, 6-26
Reporting state), 6-26
Reset counters, 10-38
Re-timed mode, 7-51
Re-timing, 7-15
Root port, 8-49
rSTP
See: Rapid spanning tree protocol
RTR, 10-30

Safety of laser products, 1-17
Scheduler, 8-100
SDH equipment clock
See: SEC
SDH equipment timing source
See: SEC
SDH performance monitoring, 10-5
SEC, 7-4, 7-8, 7-9
Selected pair, 8-218, 8-224, 8-228, 9-30
Selected TP, 10-46
Self-timed, 7-15
Self-timed mode, 7-51
Service level agreements, 8-93
Service Monitor, 10-62
SES, 10-28
SES Declaration Threshold, 10-29, 10-46
Severity, 6-75, 6-81
Severity field, 6-26
SFP inventory, 5-42
SHDSL performance monitoring, 10-31
Signal integrity, 10-8, 10-8
Signal label, 9-13
Signal level, 9-23, 9-23
Signal status, 7-37
Signal type, 7-45
Single-pair High-speed DSL
SHDSL, 8-30
Slot, 8-218, 8-218, 10-46, 10-54
Provisioning, 5-21
Slot Select field, 6-26
SNC protection, 8-184, 8-216, 9-24
edit, 8-220
switch, 9-25
view, 8-217
SNC/N, 8-19
Software
view, 12-7
Software Release Description, xxxi
Software stores
switch, 12-18
Software upgrade, 12-12
Source, 6-75, 6-81
Source field, 6-26
Source selection, 7-45
Spanning tree, 8-72
Spanning tree protocol, 8-47, 8-50
Spanning tree with VPN registration protocol (STVRP), 8-54, 8-66, 8-76, 8-119, 8-123
specific alarm, 6-23
Specific reported, 6-26
Specific severity, 6-26
SRD, xxxi
SSM out, 7-51
SSU, 7-7
SSU-L, 7-7, 7-9
SSU-T, 7-7, 7-9
Standards Compliance, 1-17
Static VLAN ID list, 8-76
Station clock, 7-39
Station clock output, 7-43, 7-45
Status, 6-75, 6-82
Status field, 6-27
STCLK output, 7-45
Stop time, 10-55
STP, 8-148
See: Spanning tree protocol
bridge priority, 8-148
per virtual switch per operation mode, 8-51
root bridge address, 8-148
root bridge priority, 8-149
root cost, 8-149, 8-149
status parameters, 8-51
Strict policing mode, 8-96
Strict priority, 8-100
STVRP, 8-54, 8-76, 8-88
See: Spanning tree with VPN registration protocol
Subscribe, 6-75
Subscribe all, 6-75
Supervision
concepts, 6-13
Supervision list
parameters, 6-72

Alcatel-Lucent - Proprietary
Use pursuant to applicable agreements
Index

view, 6-65
Suppress, 6-27
Suppress Dependency on Station Alarms, 6-30
Suppressed Alarms, 6-27
Switch
request, 7-30, 7-37, 7-45
status, 7-30, 7-37, 7-46
Switch mode, 8-228, 8-233, 9-27, 9-30
Switch priority, 8-48
Switch request, 9-27, 9-30
Switch state, 8-224, 8-228, 9-30
Synchronization supply unit
See: SSU
- local
  See: SSU-L
- transit
  See: SSU-T
System QL, 7-38
System timing, 7-32, 7-35

T
Tagging mode, 8-144, 8-149
TAP properties
edit, 4-65
Templates, 5-5
Termination point, 9-7
Termination Point, 10-45
Termination point, 10-55
  See: TP
Termination points, 8-183, 8-191, 10-9
  provision, 9-10
Test loop, 9-5
Threshold
  select, 9-20
Threshold Crossing Alert, 10-8
Threshold values
  change, 9-22
Thresholding, 10-45, 10-55
  thresholds, 10-8
Thresholds
  Alarms, 10-27
  enable, 10-41
TI mode, 9-17
TIM, 9-8
TIM detection, 9-18
Time, 6-75
Time cleared, 6-27, 6-82
Time raised, 6-27, 6-82
Timing, 7-38
  alarm reporting, 7-52
  Loop, 7-14
  Mode, 7-5
  mode, 7-38, 7-51
Reference, 7-4
  reference assignment, 7-20, 7-21
  Source, 7-20
  state, 7-52
Timing mode, 7-33
Timing source, 7-30
TP, 9-12
  enable, 10-41
TP mode, 9-13
TP type, 9-12
TR, 10-30
TR and RTR, 10-46
Trace identifier mismatch
  See: TIM
Traffic class, 8-98, 8-99
Traffic Monitoring, 10-65
Trail termination point
  See: TTP
Trail Trace Identifier, 9-13
Trail trace identifier, 9-17
Transmission plan, 8-6
Transparent DCC, 4-15
Transparent tagging, 8-75
Trial trace identifier, 9-17
Trunking applications, 8-60
Trunking LAN interface, 8-76
TS0 termination, 5-67
TTP, 9-4
TU12(KLM), 10-55
TU3(KO0), 10-55

U
UAP, 10-28, 10-29, 10-47, 10-55
UAP counter, 10-38
UAP log, 10-38
UAS, 10-28, 10-47
Unacknowledged Information Transfer Service (UIST), 4-16
Unidir 15*, 10-47
Unidir 24*, 10-47
Unidirectional 15 minutes, 10-56
Unidirectional 24 hours, 10-56
Unsubscribe, 6-76
Unsubscribe all, 6-76
Use, 10-68
User priority, 8-98

IN-8
Index

User role
  types, 3-4
  User-Network Side MSect Failure, 4-37, 4-47, 6-33, 6-35, 6-37, 6-38, 6-39
  User-Network Side RSect Failure, 4-37, 4-47, 6-33, 6-35, 6-37, 6-38, 6-39
  User_side mode, 4-16

V  VC allocation (GbE), 8-46
  VC-11 TP, 10-9
  VC-12 TP, 10-9
  VC12(ABCD), 10-56
  VC3 or VC12 (ABCD), 10-47, 10-56
  VC-3 TP, 10-9
  VC-4 TP, 10-9
  VCG, 8-144, 8-149
  Virtual concatenation, 8-28, 8-41, 8-41
  Virtual switch, 8-26, 8-144, 8-149
    create, 8-114, 8-116, 8-120, 8-124, 8-133
    in spanning tree mode, 8-132
    label, 8-144, 8-149
    name, 8-144, 8-149
    provision in LAN interconnect mode, 8-116
    provision in MLAN (VPN) mode, 8-119
    provision in MLAN (VPN) mode with QoS, 8-123
    provision in repeater mode, 8-113
    tagging mode, 8-145
  Virtual switch mode, 8-145

VLAN
  ID, 8-150
  label, 8-150
  status, 8-150
  tagged, 8-150
  trunking, 8-72
  version number, 8-149
  VLAN ID list, 8-76
  VLAN tagging, 8-76
  VLAN trunking, 8-39, 8-60
  VPN tagging, 8-66, 8-75

W  WAN
  port details, 8-151
  WAN port, 8-25
    capacity, 8-146, 8-152
    details, 8-145
    egress QoS, 8-145, 8-150
    ingress QoS, 8-150
    members, 8-150
    name, 8-144, 8-150
  WAN port capacity, 8-146, 8-152
  Weighted bandwidth, 8-100
  Working
    port, 7-31
  Working section, 9-30
  WTR, 8-224, 8-229, 8-229, 8-233