Element Manager User's Manual

Nimbra One
Nimbra 300 series
Nimbra 600 series

NimOS GX4.7

The specifications and information in this document are provided “as is” and are subject to change without notice. All statements, information, and recommendations in this document are provided without warranty of any kind, expressed or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such specifications and information or the result to be obtained from using such specifications or information. Net Insight AB shall not be responsible for any claims attributable to errors, omissions, or other inaccuracies in the specifications or information in this document, and in no event shall Net Insight AB be liable for direct, indirect, special, consequential or incidental damages arising out of the use or inability to use this document.

Net Insight AB
Box 42093
SE-126 14 Stockholm
Sweden

Phone: +46 8 685 04 00
Fax: +46 8 685 04 20
E-mail: info@netinsight.net

October, 2010

Stockholm, Sweden

(NID 3600/A3)

Stockholm, Sweden

Contents

1 About This Manual

1.1 Overview

This manual includes information on how to configure, monitor and maintain network elements of a network, comprising the Nimbra series of multi-service switches, when being installed with the Nimbra Element Manager, system software provided by Net Insight. For further information on how to install and maintain the Nimbra switches please see *Nimbra One / Nimbra300 series / Nimbra 600 series Installation and Maintenance Manuals.*

1.2 Intended reader

This manual is intended for network managers and administrators involved in operation and maintenance of network elements that use Nimbra Element Manager as element management software platform.

1.3 Support and assistance

If you have any questions about how to use your equipment or software, and if you do not find the solution to your problem in this manual, please contact your local equipment and support supplier. If any question still remains, please consult Net Insight's Technical Support Center.

1.4 Organization of content

The contents of this manual are organized as follows:

About This Manual includes information on how to use the manual.

Quick Start Guide contains procedures to set up and run the unit after initial installation.

Maintenance covers software maintenance, such as backup routines and software upgrades.

For Nimbra360, gpio1:0:2 to gpio1:0:9 pins are shown as absent.

Status Monitoring refers to the functions for monitoring the status of the unit.

Control Network contains information on how to set up in-band management and configure the IP routes of a unit.

DTM Configuration covers information about the node administration for the units.

Trunks describe the trunk interfaces that are used to connect nodes into a network.

In Sync and Time Transfer, synchronization principles are defined and the Time Transfer option is elaborated.

Performance Monitoring shows how to use the web interface to set up performance monitoring.

Access Modules covers the access interfaces that are used to feed the network with various kinds of traffic.

Ethernet Transport Service (Ethernet) describes how to setup Ethernet transport and the configuration and maintenance of Ethernet interfaces.

Isochronous Transport Service (ITS) describes how services are used and how to create a video tunnel, a PDH tunnel or a Sonet/SDH tunnel through the DTM network.

Channel Persistence describes what happens to already established channels if nodes along their respective routes are taken down.

In Connection and channel lists all lists available from the web interface are described and explained.

In Source Routing, the concept of source routing is described as well as how to configure a source route.

In Loopback, this diagnostic feature is described.

In Scheduler, the concept is described and how planning and control of resources and utilization in the network is done.

Redundancy for Nimbra 600 explains the basic redundancy principles in the Nimbra 600 Series.

In Module installation, installation of additional modules in operational nodes is described.

Up- and Downgrading describes how to upgrade a node from the web interface.

1.5 Conventions in this manual

1.5.1 Information of specific importance

Note: 	Information for proper function of the equipment is contained in this kind of boxes, which includes the tip heading and symbol.

Tip: 	Information for better understanding and utilization of the equipment is contained in this kind of box, which includes the tip heading and symbol.

1.5.2 Instructions

The instructions given in this manual are numbered in the sequence in which they should be performed, as follows

Initial measure

Next measure

…

1.5.3 Terminal output and keyboard input

Examples of text and commands appearing on a terminal screen are marked with a special font as follows:

```
Example of terminal text output
```

`Example of command <optional parameters>` **[Enter]**

1.5.4 Web interface examples

The configurations shown in the displayed web pages in this document are taken from generic systems and for this reason the parameters might differ from the user's particular configuration.

2 Glossary of Terms

Access device	Access device is a network component that provides access for services to the network. Examples of services are PDH transport and DLE.
ADM	Add/Drop Multiplexer
AES/EBU	Audio Engineering Society/European Broadcasting Union
AIS	Alarm Indication Signal
ASI	Asynchronous SCSI Interface
BBE	Background Block Error
BPDU	Bridge Protocol Data Unit
CATV	Cable TV
CENELEC	Comité Européen de Normalisation Electrotechnique
CLI	Command Line Interface, the method used to communicate over a terminal connection.
CCC	Client to Client Connection
CSC	Client to Server Connection
Control module	The Control module of a DTM switch handles the communication with other. It also handles resource management and network management.
Control slot	A DTM frame is divided into data slots for transferring user data and control slot for sending control messages (DCP messages) between DTM nodes. There are static control slots that are set up initially and cannot be altered and dynamic control slots, which can be set up on demand to change the signaling capacity of a node. Dynamic control slots can be point-to-point, multicast or broadcast. Static control slots are broadcast.
CPU	Central Processing Unit
DCAP	DTM Encapsulation. The mechanism to adapt a service for transport over DTM. DCAP-0/1/2 are defined where DCAP-0/2 refers to ITS services encapsulation and DCAP-1 refers to encapsulation of Ethernet packets.
DEG	Degraded
DLE	DTM LAN Emulation (DLE) allows DTM to be used as a bridge between different segments of an Ethernet network.

DLE client	There is one DLE Client for each Fast Ethernet Device (FED) and one for every directly connected DTM node in the DLE segment.
DNF	DPCP-IP Negotiation Failure
DNU	Do Not Use
DTM	Dynamic synchronous Transfer Mode.
DTM channel	DTM channel is a physical end-to-end channel from sending resource or device. Several DTM channels may exist between two resources. A DTM channel has a specific capacity corresponding to a certain amount of allocated slots. One slot corresponds to a reserved capacity of 512 kbps. A DTM channel of several hops consists of several DTM link channels.
DTM frame	A DTM frame is 125 µs. A DTM frame consists of control slots and data slots. The number of slots depends on the bit rate of the DTM link. The number of frames per second should be the same for all DTM links in a DTM network. This should be arranged by the DTM synchronization scheme.
DTM Link	DTM Link is the physical medium connecting DTM Access Nodes and/or DTM Switches. It is typically an optical fiber, but may be any type of media.
DPCP-IP	DPP Control Protocol for DTM over IP
DPP-IP	DTM Physical Protocol for DTM over IP
DRP	DTM Routing Protocol
DSCP	Differentiated Services Code Point
DST	Daylight Savings Time
DSTI	DTM Service Type Instance. Defines a service instance at a node, and can in many ways be likened to the use of port numbers in TCP.
DSYP	DTM Synchronization Protocol
DVB	Digital Video Broadcasting
ES	Errored Second
Ethernet	Ethernet is a simple LAN protocol originally developed by Digital and Xerox for use with servers and workstations. Later standardized as IEEE 802.3. The success of Ethernet for use with personal computers has put force between further developments towards 10Base-T, Fast Ethernet (100Base-T) and towards Gigabit Ethernet. Ethernet is a CDMA-CD protocol with exponential backoff.
ETS	Ethernet Transport Service
ETSI	European Telecommunications Standards Institute
FCS	Frame Check Sequence
FEC	Fast Ethernet Card
FF	Forwarding Function
GEC	Gigabit Ethernet Card
GMT	Greenwich Mean Time
GPIO	General Purpose Input/Output
GUI	Graphical User Interface

HD/SD-SDI	High Definition/Standard Definition – Serial Data Interface
HTTP	Hypertext Transport Protocol
IETF	Internet Engineering Task Force
IF	Interface
I/O	Input/Output
IP	Internet Protocol is the Internet network protocol handling addressing and routing in the Internet. IP is the fundamental protocol in the Internet and usually works in conjunction with TCP. IP is a connection-less protocol that operates at the network layer (layer 3) of the OSI model.
IPOD	IP Over DTM. Specifies how to run IP directly on top of DTM.
ITS	Isochronous Transport Service
ITU	International Telecommunication Union
IPMC	Internet Protocol Multimedia Communications
IPTV	Internet Protocol TV
LCD	Local Configuration Datastore
LCV	Line code violations
LED	Light Emitting Diode
LOF	Loss of Frame
LOP	Loss of Pointer
LOS	Loss of Signal
MIB	Managed Information Base, a set of data definitions for describing managed objects in a conceptual database that is accessed using SNMP.
MM	Multi Mode
MTU	Maximum Transmission Unit
NC	Node Controller
Node	Network device directly connected to the DTM network, e.g. a switch or access device.
NTP	Network Time Protocol
OC	Optical Channel
OID	Object Identifier
OOF	Out of frame
OS	Operating System, the system that manages all other programs or applications.
OSPF	Open Shortest Path First
PDH	Plesiochronous Digital Hierarchy, a way to multiplex several telephony trunks into one bit-stream
PDH transport	A service that allows transparent PDH connections across a DTM network.
PDH tunnel	The logical connection set up over DTM to allow PDH transport.
PLM	Payload Mismatch

PM	Performance Monitoring
PMM	Performance Monitoring manager
PMM	Performance Manager monitoring
POH	Path Overhead
PPS	Pulse per second
QoS	Quality of Service
RAI	Remote Alarm Indication
RDI	Remote Defect Indication
REI	Remote Error Indication
RFC	Request For Comments
RMS	Root Mean Square
RSTP	Rapid Spanning Tree Protocol
Rx	Receiver
SDH	Synchronous Digital Hierarchy
SCC	Server to Client Connection
SES	Severely Errored Second
SFP	Small Form factor Pluggable
SLA	Service Level Agreement
SLIP	Serial Line IP. A framing protocol for transferring IP packets on serial (point-to-point) links.
SM	Single Mode
SMIv2 Short for SNMPv2	SMI, Structure of Management Information extension for SNMPv2. Specifies a set of rules for naming and defining objects.
SNMP	Simple Network Management Protocol
SNMP manager	Workstation or similar acting as the client in a SNMP based management system. Correct term is SNMP entity acting as notification receiver and command generator.
SNMP agent	SNMP entity acting as server in a SNMP based management system. Correct term is SNMP entity acting as notification originator and command responder.
SNMPv3	Version 3 of SNMP. Extension to SNMP that addresses security and administration.
SONET	Synchronous Optical Network
SPE	Synchronous Payload Envelope
SQC or sqc	Squelchable clock
SS	Slip Second (used for performance monitoring)
SSM	Synchronization Status Message
STM	Synchronous Transport Module
STP	Spanning Tree Protocol
STS	Synchronous Transport Signal

TCP	Transmission Control Protocol. An Internet protocol that provides end-to-end, connection-oriented, reliable transport layer (layer 4) functions over IP controlled networks. TCP performs the following functions: flow control, acknowledgement of packets received and end-to-end sequencing of packets.
TM	Timing Marker
TTL	Timt to live
Tx	Transmitter
UAS	UnAvailable Second (used for performance monitoring)
UAT	UnAvailable Time
UDP	User Datagram Protocol
UNEQ	Unequipped
USM	User-based Security Model
UTC	An abbreviation compromise between Temps Universelle Coordiné (TUC, French) and Coordinated Universal Time (CUT, English). For all practical purposes, it is equal to Greenwich Mean Time (GMT).
VC	Virtual Container
VLAN	Virtual Local Area Network
WDM	Wavelength Division Multiplexer
ZS	Zero Suppression Counter (used for performance monitoring)

3 Quick Start Guide

3.1 Overview

There are some initial configurations, which are needed before the nodes could be used in the network. The instructions in this chapter are intended to guide an operator to quickly get a Nimbra node active in a network.

Note: 	Before these procedures are performed, be sure that the unit is properly installed according to the relevant Installation and Maintenance Manual. In particular, the node should be mounted, grounded and powered. In this quick start procedure, only change parameters specifically mentioned.

This chapter details the configuration needed to get a Nimbra switch operational in a network. The short configuration procedure is:

Set the IP address from the serial interface

Set the of DTM address from the web interface

Save/back-up the configuration

Reboot the node

3.2 Configuration of the IP address

There are two different cases for the IP address. From release GX4.7 there is a default IP address: 192.168.125.125. This address appears in the factory default configuration, which appears when all other configurations are removed and the node is rebooted. The other case is the previous case without default IP address. In order to check if there is a set IP address, connect the PC/Terminal with an IP address on the same subnet and try to ping 192.168.125.125. If there is a reply, the node has the default IP address. In case there is no reply, it has to be assumed that the node has no IP address. In this case, the serial port must be used.

In the default IP address case, change the IP settings (IP address, netmask and gateway) from the web interface. Proceed with saving the configuration and rebooting the node. Then set the IP address of the PC/Terminal to fit the LAN and go ahead with DTM address setting. This procedure is described in chapter 9 DTM Configuration.

If no default IP address is set on the node, i.e. if the node has GX4.6 or earlier system release software running, initially an IP address must be set. When the initial IP configuration on Nimbra nodes is made, the serial connection must be used for IP network parameters. Once the IP settings have been made, subsequent configuration can be made from the Ethernet port and the web interface. All settings can also be made from the Command Line Interface (CLI) and the serial port.

In order to see what is stored in registry, log in to the node (root/neti) and issue command: `registry list`

The factoryDefault configuration should now appear, if system release software GX4.7 or later is running.

To see the contents, write `resedit get -r -n ipconf`

```
nimbra login:
nimbra login: root
Password:
nimbra:/flash/root # resedit get -r -n ipconf
.ipconf
.ipconf.if
.ipconf.if.0
.ipconf.if.0.name       "eth0"
.ipconf.if.0.address
.ipconf.if.0.address.0
.ipconf.if.0.address.0.inet     "192.168.125.125"
.ipconf.if.0.address.0.netmask  "255.255.255.0"
.ipconf.if.0.media
.ipconf.if.0.media.current      "autoselect"
.ipconf.if.0.media.active       "100baseTX full-duplex"
.ipconf.if.0.mac        "00:10:5b:11:48:f3"
.ipconf.if.0.mtu        1500
.ipconf.routes
nimbra:/flash/root # registry list
 0 FactoryDefault
nimbra:/flash/root #
```

Figure 1. FactoryDefault configuration for GX4.7 and later releases.

3.2.1 Initial settings for VT100 terminal emulator

A serial adapter is provided (RJ45-RS232 adapter, NPA0006-0001) to adapt the serial port of the Nimbra node to the PC DSUB-9 connector of the PC. Attach the adapter to the serial port of the PC and connect the other end of the adapter with a straight Ethernet cable to the serial port of the Nimbra node. Use a VT100 terminal emulator like Tera Term or Hyper terminal and log in.

The communication settings are:

Port speed:	38.4 kbps
Data bits:	8
Parity bit:	No
Stop bit:	One
Flow control:	No

3.2.2 IP settings for Nimbra One/Nimbra 300 series

Open a VT100 terminal emulator, with settings given above, on the PC and hit the **Enter** key. Log on to the node (The default user name/password combination is `root/neti)`. List current IP registry by issuing the command

`resedit get -r -n ipconf.if.0`

The system should reply with something like

```
.ipconf.if.0
.ipconf.if.0.name       "eth0"
.ipconf.if.0.address
.ipconf.if.0.media
.ipconf.if.0.media.current      "autoselect"
.ipconf.if.0.media.active       "autoselect"
.ipconf.if.0.mac        "00:10:5b:00:00:1b"
.ipconf.if.0.mtu        1500
```

3.2.2.1 Set the IP address and subnet mask

Create an address structure and set the IP address and subnet mask with the following commands:

```
resedit create -n ipconf.if.0.address
resedit set -n ipconf.if.0.address.0.inet -v x.x.x.x
resedit set -n ipconf.if.0.address.0.netmask -v y.y.y.y
```

`x.x.x.x` is the IP address

`y.y.y.y` is the subnet mask.

3.2.3 IP settings for Nimbra 600 series

Connect a straight Ethernet cable to the serial port of the active node controller module on the 600 series Nimbra node. Connect the other end of the cable to an RJ45-RS232 adapter, NPA0006-0001, connected to a regular DSUB-9 serial port (like COM1) on your working computer.

Using the previously stated settings, connect to the node with a VT100 terminal emulator and hit the Enter key. Log on to the node with the default user name/password combination (`root/neti`). List current IP registry with

```
resedit get -r -n ipconf
```

A typical reply from the node may be:

```
.ipconf
.ipconf.if
.ipconf.if.0
.ipconf.if.0.name       "eth-aux"
.ipconf.if.0.address
.ipconf.if.0.address.0
.ipconf.if.0.address.0.inet     "192.168.101.74"
.ipconf.if.0.address.0.netmask  "255.255.255.0"
.ipconf.if.0.media
.ipconf.if.0.media.current      "autoselect"
.ipconf.if.0.media.active       "100baseTX half-duplex"
.ipconf.if.0.mac        "00:10:5b:20:63:02"
.ipconf.if.0.mtu        1500
.ipconf.if.1
.ipconf.if.1.name       "eth-front"
.ipconf.if.1.address
.ipconf.if.1.media
.ipconf.if.1.media.current      "autoselect"
.ipconf.if.1.media.active       ""
.ipconf.if.1.mac        "00:30:d6:03:94:3e"
.ipconf.if.1.mtu        1500
```

3.2.3.1 Set IP address and subnet mask

Create an address structure and subsequently set the IP address and subnet mask with the following commands:

```
resedit create -n ipconf.if.1.address
resedit set -n ipconf.if.1.address.0.inet -v x.x.x.x
resedit set -n ipconf.if.1.address.0.netmask -v y.y.y.y
```

`x.x.x.x` is the IP address

`y.y.y.y` is the subnet mask.

3.2.4 Set the DTM address

In order to proceed with the web interface, disconnect the serial connection and reconnect the node at the Ethernet port. The PC must have IP connectivity to the node.

Open the web interface (login with root/neti as user/password combination) and navigate to the web page **DTM** → **Addresses**, and click on the **Add address** link.

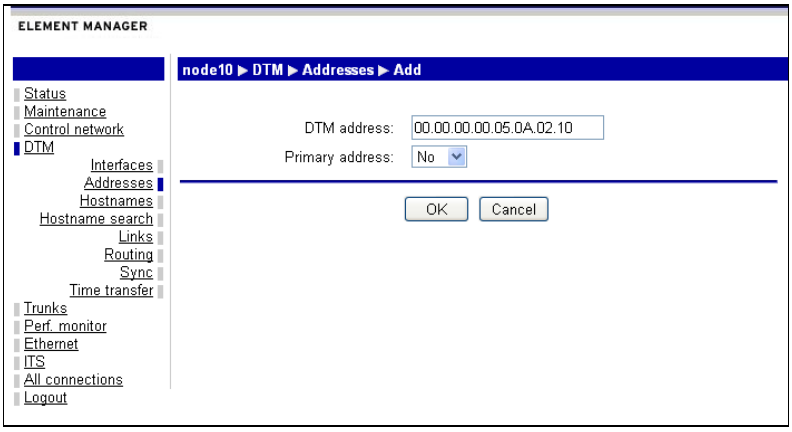


Figure 2. Add DTM address

Set the DTM address of the unit. Make sure that **Primary address** is set to '**Yes**'. Click **OK**.

The **DTM Addresses** page below appears. The DTM loopback address (00.00.00.00.00.00.00.01) is always shown in the list.

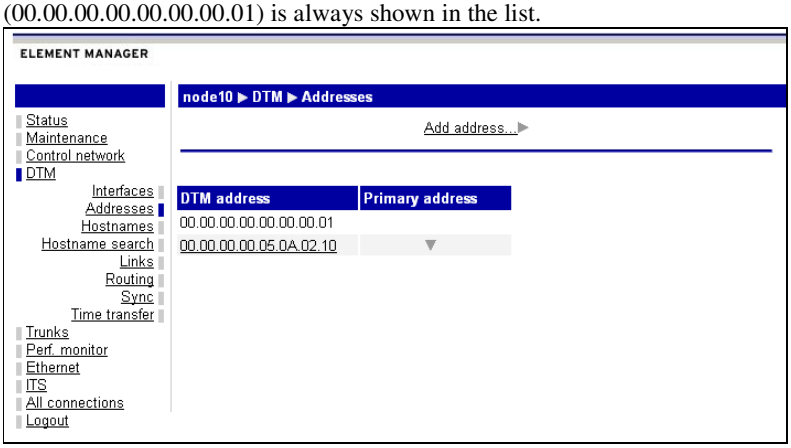


Figure 3. DTM address listing

Note: 	A change in the primary DTM address does not take effect until after the node has been restarted. Remember to save the configuration before rebooting.

3.2.5 Parameter configuration example

There is a CLI configurable parameter, which is neither configurable from the graphical user interface nor from SNMP.

The parameter is called maxAlarmRate and has two possible values, normal (default) or high. Normal means that the hold-off (filtering) time for ITS alarms is 2 s and the wait-to-restore time is 5 s. Corresponding times with maxAlarmRate equal to 'high' is 100 ms and 1 s.

In CLI, the parameter is set to normal with command

```
resedit -n its.maxAlarmRate -v normal
```

The parameter is set to high with

```
resedit -n its.maxAlarmRate -v high
```

The parameter value is displayed with

```
resedit get -r -n its.maxAlarmRate
```

3.2.6 Save the configuration

Navigate to web page **Maintenance** → **Configurations** and click on the **Save configuration** button. The **Save** page appears.

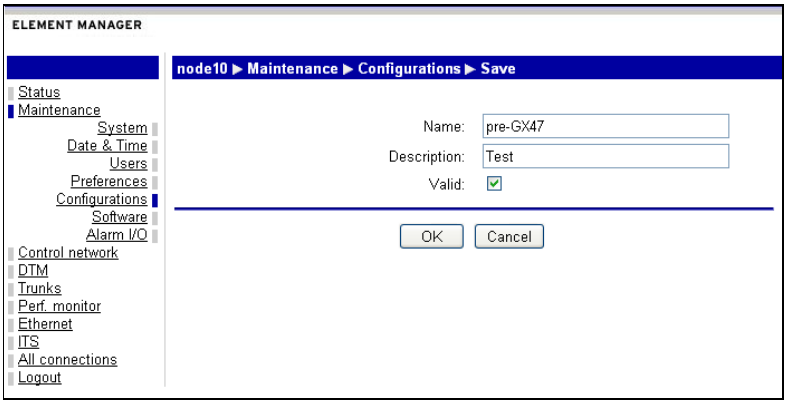


Figure 4. Backup of the configuration; the save page.

Enter a suitable name without spaces and a description of the configuration (optional). Make sure that the '**Valid'** box is checked. Click on the '**OK**' button.

3.2.7 Restart the system

The **Maintenance** → **System** web page is found by following the Maintenance → System link. To restart the system, click on the Restart system link on the page.

In the new window that appears, click on the 'Restart Node' button. 'Restart Node' means that all processes on all modules in the node are restarted, including the node controller.

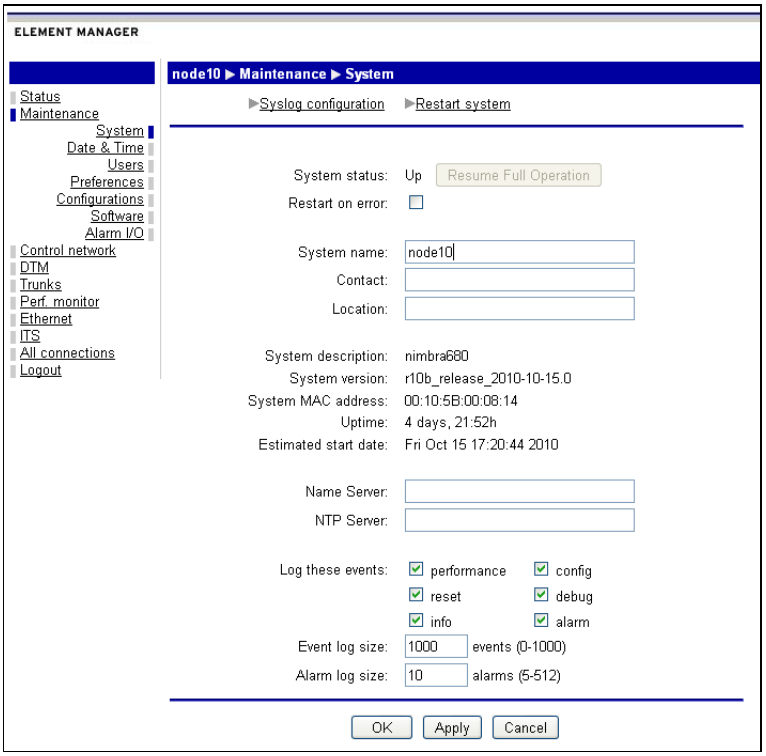


Figure 5. The first configuration page

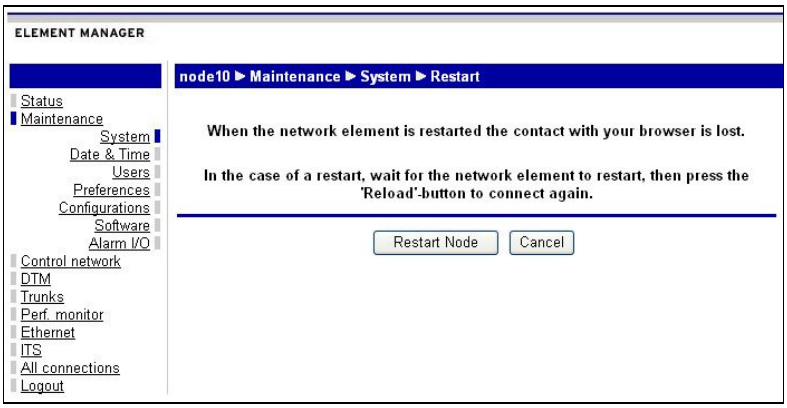


Figure 6. The restart page with 'Restart Node'.

In case the configuration has been changed since last restart, the system asks if the configuration should be saved before rebooting.

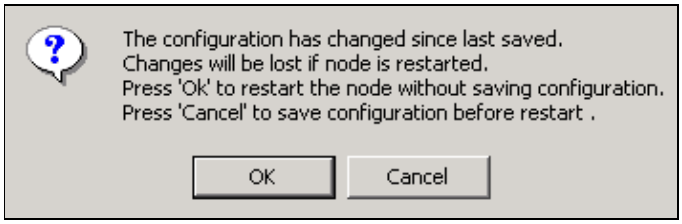


Figure 7. Prompt for restart attempts with changed configuration since last restart. ‘Cancel’ takes the user to the save configuration page directly and ‘OK’ forces a reboot.

When the system is restarted, contact with the browser is lost. After a short time, less than a minute, click on the “reload” button in the web browser to reconnect to the node.

4 Key concepts

4.1 General

In this chapter, a brief description is made of key concepts for DTM networks. They include services, channel, connection and TTP. DTM slot numbering, common for all interface modules, is also described.

4.1.1 DTM slot numbering

Slot and interface numbering is different on different hardware platforms. On Nimbra One, the slots are numbered from 1 (dedicated for node controller) to 8. The different interfaces on the modules are numbered in a way clearly seen on the module front. The interfaces are numbered from 1 and the last number varies depending on the particular interface.

For example, an OC-3/STM-1 Trunk Module in slot six with four ports have the ports numbered sonet/sdh-6:1, sonet/sdh-6:2, sonet/sdh-6:3 and sonet/sdh-6:4.

Slot numbering for Nimbra 300 series nodes are different. In Nimbra 340, the node controller (virtual) slot position is 0. The two available, regular slots are labeled 1 and 2. The interfaces on the modules inserted in these slots are labeled from 1 and upwards. The fixed ASI interfaces are 3:1 and 3:2. Finally, the fixed Gigabit Ethernet Access Module Interface is labeled 4:1. In Nimbra 340-HD and 360, slots 0, 1 and 2 are used in the same manner. In Nimbra 340-HD, the fixed HD-SDI interfaces are labeled 3:1 and 3:2, while in Nimbra 360 the fixed trunk interfaces are labeled 3:1, 3:2, 3:3 and 3:4. In both cases, the Gigabit Ethernet Access Module is labeled 4:1.

4.1.2 Connection, TTP and Channel

Connection, Trail Termination Point (TTP) and Channel are all related concepts. A connection is defined by its two end-points, its TTPs. The channel is defined, in addition to its TTPs, by the route(s) from source to destination TTPs.

5 The User Interface

5.1 Overview

The implemented software provides necessary functionality for node management, such as configuration and monitoring of the units.

Among the functions are:

Network configuration changes

Unit handling

Software diagnostics and upgrade

The graphical user interface (web based) is the normal user interface for all node and network management. Some initial tasks, like setting the first IP address must be done from a text-based terminal connection (CLI). These CLI based initial commands are detailed in the various Installation manuals. In this document, only web browser procedures are described.

5.2 Connecting to the units

Communication with the units is done either locally through a terminal connected directly to the unit, or when the unit is in operation, remotely over the in-band management network (DLE).

5.2.1 Required software

Terminal software: To utilize the terminal connection via the Serial Control Port, a standard terminal emulation software (VT100) is required, e.g. Windows Terminal.

FTP client: FTP is used to transfer the required configuration files to and from the unit.

Web interface: For the web interfaces a standard web-browser able to handle Java-script and cookies should be used. Internet Explorer 5.5, Mozilla 1.4 Netscape 7, Firefox 1.0 or later versions are recommended web browsers.

5.3 Command Line Interface

A Command Line Interface (CLI) is a set of system commands used for management of the Nimbra nodes via Terminal or Telnet software. E.g. the

CLI can be used when connecting to the unit via the Serial Control Port using Terminal software, or when connecting via Telnet (TCP/IP) over the Ethernet Control Port or over the in- management network. Normally the web interface should be used. The CLI is intended mainly for initial configuration operations.

5.4 Web interface

The web interface is the easiest and most straightforward way to communicate with the units. It is designed to be easy to use and to give a good overview of the configuration status of the unit. Monitoring and configuration is typically done from the web interface.

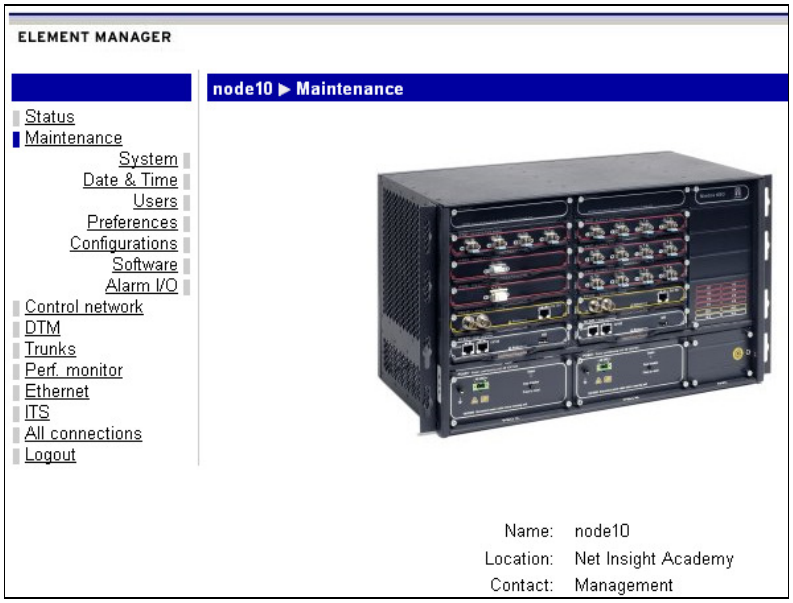


Figure 8. The web based user interface

5.5 Frequently used terms

The following terms and parameters are frequently used throughout this document:

Admin

The administrative status of the object (e.g. route, interface, server, module or function). The operator can either set the administrative status to '**Up**' if the object is to be activated, or to '**Down**' if it is to be deactivated.

Oper

The operational status of the object (e.g. route, interface, server, module or function). '**Up**' indicates that the object is active, while '**Down**' indicates that it is inactive. If the operational status shows **Down** while the administrative status is **Up**, this is an indication of that an error has occurred. **Degraded** indicates that the object is operational, but with deficiency. **Dormant** means that the object is up but temporarily suspended; in waiting for an event to take it up. **Starting** is a transitional state indicating that the object is in a start-up phase. **Absent** indicates that the object is no longer physically present in the node.

5.6 Default username/password

The default username/password combination is

user: **root**
pass: **neti**

5.7 Logging in using the Telnet connection

5.7.1 Terminal connection, General for Nimbra nodes

If the unit has just been installed, a local serial connection must be used to set an IP address on the node according to the appropriate Installation and Maintenance Manual.

Start a Telnet client and connect to the node. When the connection is established, log in to the node (root/neti). Set the IP address according to the particular instruction.

The unit is now ready to receive commands over the web interface.

5.8 Logging in using a web browser

Establish the connection, either locally or remotely, and start the browser.

Enter the name or the IP-address of the unit in the address field. A **Login** page, shown below, appears in the browser window.

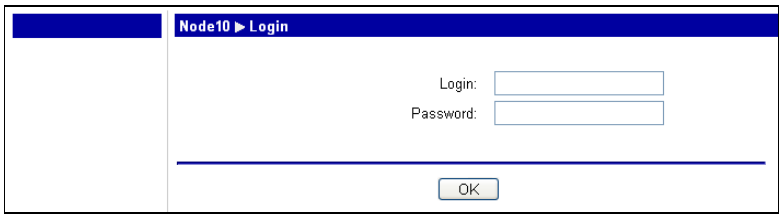


Figure 9. The login page

Enter user name and password. The default user name/password combination is root/neti.

Click **OK**. The start page shown below should appear:

Figure 10. The start page of the Element Manager.

In the lower half of the page some unit information is given. This information can be entered when the unit is installed and can be user modified.

6 Maintenance

6.1 Overview

This chapter describes general maintenance of the unit, like how to back-up and modify configurations, how to set time and date and how to configure the alarm interfaces on the GPIO Auxiliary Module.

The first maintenance web page is shown below.

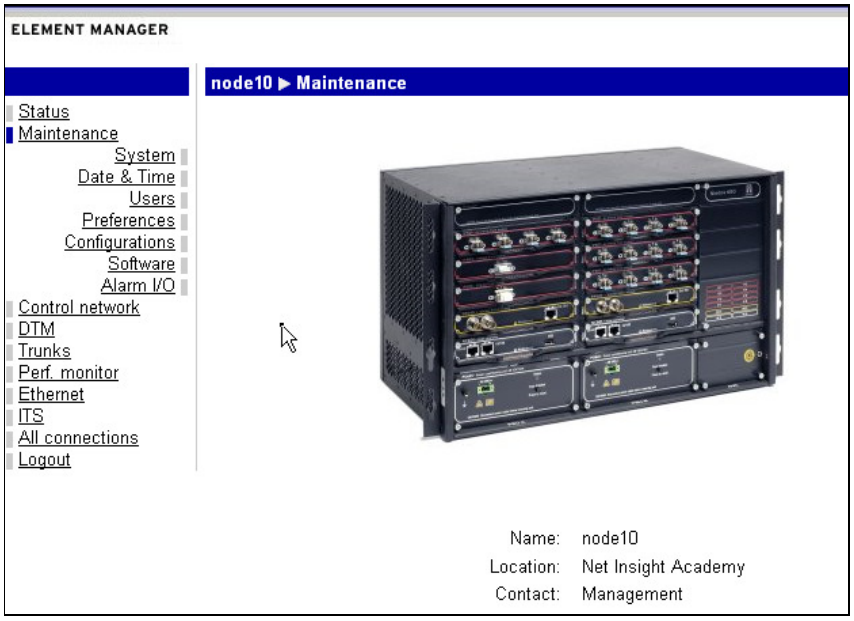


Figure 11. The maintenance web page

The available links on the page are:

System**:** A subset of the administration and log configuration

Date & time**:** Settings of the system clock

Users**:** List of logged in users

Preferences**:** Alarm and event logging preferences

Configurations**:** Handling of unit configurations and backup

Software**:** Handling of Operating System (OS) software

Alarm I/O**:** Configuration of alarms

6.2 Setting of system parameters

The **System** page contains system parameters and a control for software restart of the unit.

The configurable parameters are:

6.2.1.1 *Restart on error*

Default value: 'off'

Type: Boolean variable (tick box)

Range: 'on', 'off'

Description: If persistent channels are set up, these channels are normally kept during a node reboot and the node goes into state 'NoControl'. Checking the tick box disables this feature and causes all channels to be instantly torn down upon a node reboot.

6.2.1.2 *System name*

Default value: empty string

Type: string variable

Range: Text string, up to 63 characters long, without spaces, restricted to letters A-Z, a-z, numbers 0-9 and the characters '-' (dash) and '.' (dot).

Description: The name of the unit, to be used instead of the IP address, for easier recognition in the web page.

6.2.1.3 *Contact*

Default value: empty string

Type: string variable

Range: Text string, up to 100 characters long

Description: The name or the e-mail address of the contact person.

6.2.1.4 *Location*

Default value: empty string

Type: string variable

Range: Text string, up to 100 characters long

Description: The name of the location of the unit.

6.2.1.5 *Name Server*

Default value: none, i.e. no server is configured

Type: IP address

Range: 0.0.0.0 – 255.255.255.255

Description: The IP address of the DNS (Domain Name Server) server. Up to three name servers (with their IP addresses comma separated) can be defined. The system looks them up in entry order (i.e. first IP address is used first; if it doesn't respond the second IP address is tried etc)

6.2.1.6 *NTP Server*

Default value: none, i.e. no server is configured

Type: IP address

Range: 0.0.0.0 – 255.255.255.255

Description: The IP address of the NTP (Network Timing Protocol) server.

6.2.1.7 *Log these events – Performance*

Default value: ticked, i.e. 'on'

Type: Boolean variable (tick box)

Range: 'on', 'off'

Description: The parameter determines if performance events are logged.

6.2.1.8 *Log these events – Config*

Default value: ticked, i.e. 'on'

Type: Boolean variable (tick box)

Range: 'on', 'off'

Description: The parameter determines if configuration events are logged.

6.2.1.9 *Log these events – Reset*

Default value: ticked, i.e. 'on'

Type: Boolean variable (tick box)

Range: 'on', 'off'

Description: The parameter determines if reset events are logged.

6.2.1.10 *Log these events – Debug*

Default value: ticked, i.e. 'on'

Type: Boolean variable (tick box)

Range: 'on', 'off'

Description: The parameter determines if debug events are logged.

6.2.1.11 *Log these events – Info*

Default value: ticked, i.e. 'on'

Type: Boolean variable (tick box)

Range: 'on', 'off'

Description: The parameter determines if information events are logged.

6.2.1.12 *Log these events – Alarm*

Default value: ticked, i.e. 'on'

Type: Boolean variable (tick box)

Range: 'on', 'off'

Description: The parameter determines if alarm events are logged.

6.2.1.13 *Event log size*

Default value: 20

Type: Integer

Range: Read from the node and displayed in the web interface

Description: The parameter defines the size of the event log, expressed as number of events.

6.2.1.14 *Alarm log size*

Default value: 10

Type: Integer

Range: Read from the node and displayed in the web interface

Description: The parameter defines the size of the alarm log, expressed as number of alarms.

The button 'Resume full operation' is grayed out in normal operation.

The Maintenance → System page is shown below.

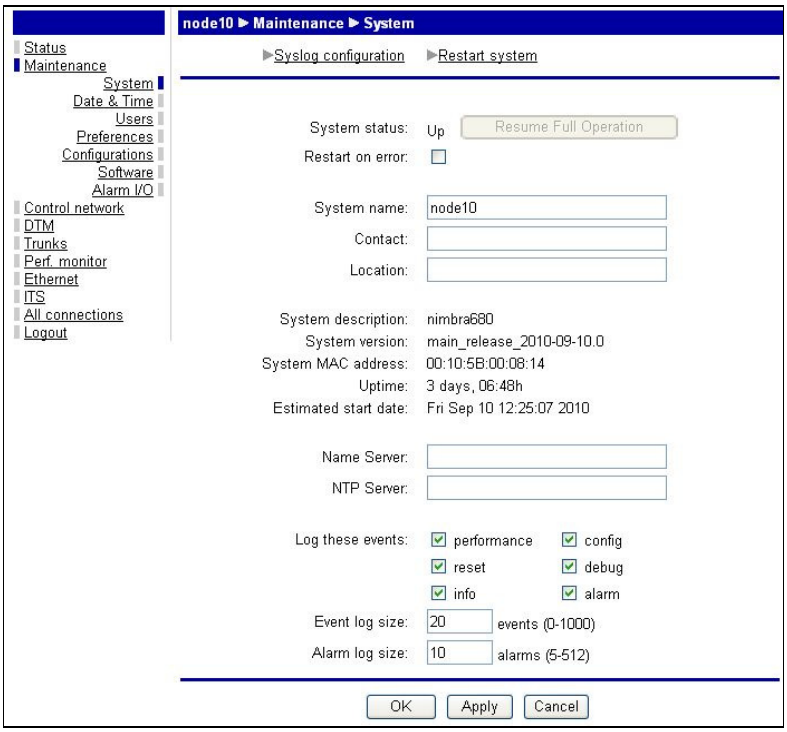


Figure 12. The Maintenance, System page

Set the parameters according to preferences. To make parameters active without leaving the page, click **Apply**. Any changes are made effective immediately. To return to the **Maintenance** page, click **OK**. To make the changes permanent, the new configuration file must be saved.

The syslog file is configured from the Syslog configuration link. The configuration is discussed more in detail in the Syslog section of the For Nimbra360, gpio1:0:2 to gpio1:0:9 pins are shown as absent.

Status Monitoring chapter of this manual.

6.3 Restart the system

Note: 	Save the configuration before restarting. Otherwise the parameter changes will be lost! Refer to Configuration handling.

Navigate to web page Maintenance → System. Click on the link Restart system on the top of the page. In the new window that appears, click on 'Restart node'.

'Restart node' means that all processes on all modules in the node are restarted, including the node controller.

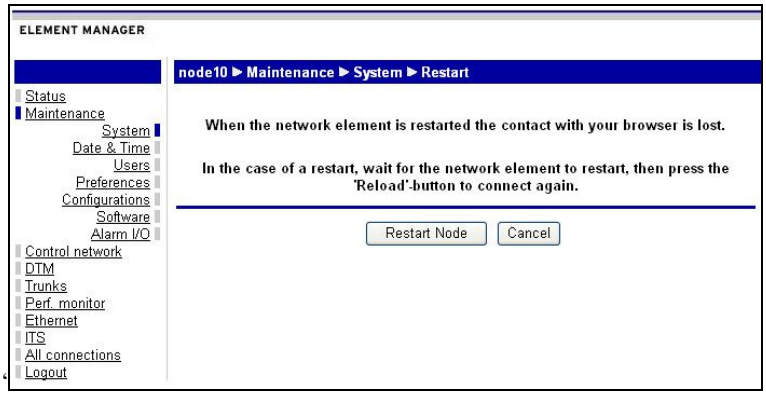


Figure 13. The restart page

When the system is restarted, the contact with the browser is lost. After a short time (less than a minute) the contact should automatically be reestablished.

6.4 Date and time setting

This section is intended to set and reset the internal clock of the unit.

Follow the links to the Maintenance → Date & Time page, shown below.

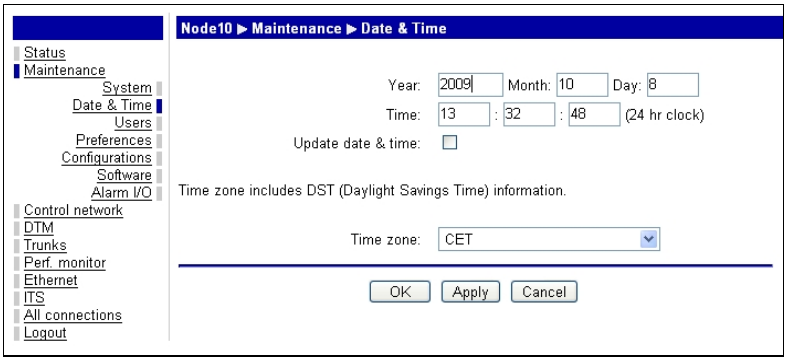


Figure 14. Date & time page

Enter the revised date and time info in the entry fields.
For the time, use the *hh:mm:ss* format. To avoid involuntary change of the parameters, the 'Update date & time' tick box must be selected for any changes to take effect when the 'OK' or 'Apply' button is clicked.

Terms and parameters found on the web page:

UTC: Coordinated Universal Time (abbreviated as UTC) is the standard time common to every place in the world.

DST: Daylight Savings Time

Time zone: Name of the standard time zone used, which is selectable from a drop down menu.

Standard offset to UTC: Hours to add/subtract to the local time (no DST included) to reach UTC, e.g. GMT+2, GMT-4.

If **DST** (Daylight Saving Time) is to be enabled, select as Time Zone a proper city like Europe/Stockholm or America/Chicago. In these time zones, relevant DST information is included.

Note:	If the internal clock is set to a time or date in the future, all users are automatically logged out from the system.

6.5 Users

The user menu lists currently active users. Users can be added and their privilege level can be modified.

6.5.1 Add or modify users and access levels

Follow the Maintenance → Users link shown below.

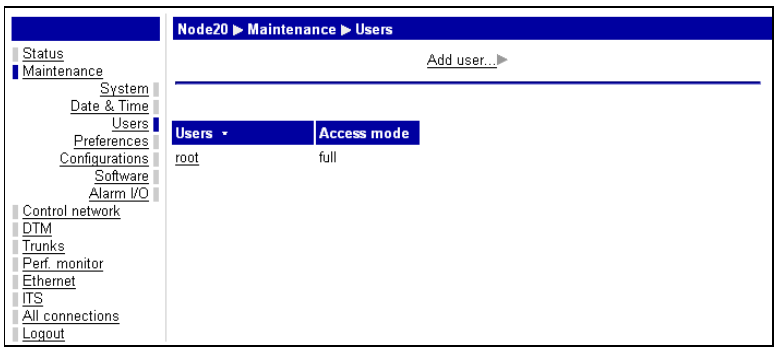


Figure 15. The Users page

Click on the Add user… link. The Add Users page (see below) appears.

Enter User name, Access Mode (Full access or Read only access) and Password (twice). Click on the 'OK' button. The test session should be up and running.

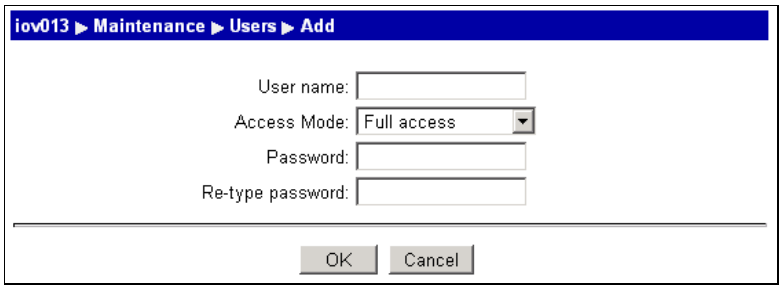


Figure 16. The Add Users page

Parameters for the Add → Users → Add users … link:

6.5.1.1 *User name*

Default value: none

Type: String variable

Range: 1-50 characters long

Description: The user name for the defined user.

6.5.1.2 *Access mode*

Default value: Full access

Type: Access rights

Range: 'Full access', 'Read only access' and/or others displayed in the web interface.

Description: The access rights or privilege level of the created user.

6.5.1.3 *Password*

Default value: none

Type: Encrypted string

Range: 1-50 characters long password.

Description: Password for the created user.

6.5.1.4 *Retype password*

Default value: none

Type: Encrypted string

Range: 1-50 characters long password.

Description: Password for the created user. This password must match the previous line for the setting to take effect.

To modify the settings for an already created used, go to the page and make the changes. After confirming the changes with 'OK' or 'Apply' the settings are in effect but the configuration must be saved for the settings to remain after a reboot.

6.6 Preferences

The node contains one set of preferences for event and alarm presentation for each authorized user, controlled from the Maintenance → Preferences link. Here, the contents and size of the event and alarm log can be set, according the procedure below.

The configurable parameters are:

Parameter	Description	Type
Visible events	Type of events that the user can see. There are six different types: performance, reset, info, config, debug and alarm.	Boolean
Visible alarms	Type of alarms that the user can see. There are five different alarm categories the user can select: acknowledged alarms (i.e. alarms actively acknowledged by the user) plus alarms of severity levels warning, minor, major and critical.	Boolean
Event log size	Number of events kept in the log and presented for the operator. Note: The log cannot contain more events than is set in the Systems page.	Integer
Auto refresh	The refresh interval for the alarm list information.	30 s (default) is recommended

Figure 17. Configurable parameters, user preferences

Click on the **Maintenance → Preferences**. The **Preferences** page, shown below, appears.

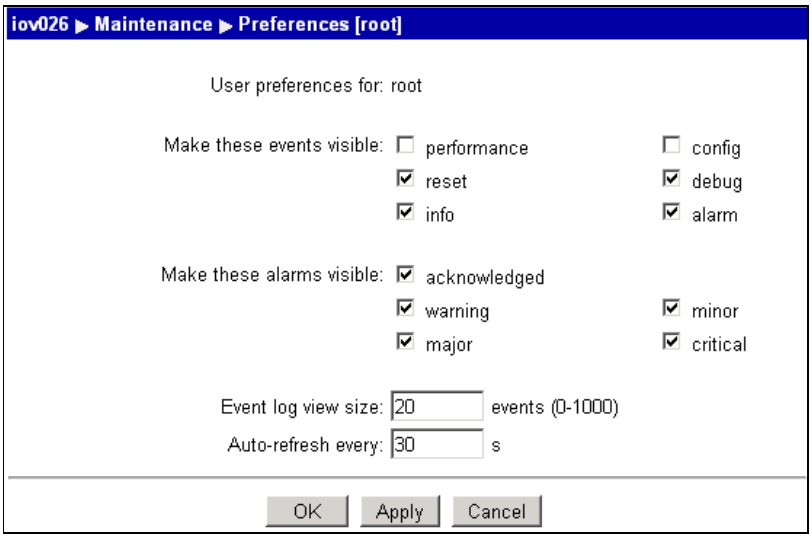


Figure 18. Maintenance, Preferences page

Enter the desired information for the currently logged in user and click on the 'OK' or 'Apply' button and return to the Maintenance main page. Back up the configuration changes, so they don't disappear after a reboot.

The default settings are that all events and alarms are visible, the event log size is 20 events and the auto-refresh interval is 30 seconds. The range of the event log view file size is read from the module.

6.6.1 Configuration handling

In order not to risk losing the configuration when changes have been verified and approved, the configuration should be backed up.

Click on the Maintenance menu link and then click on Configurations. The Maintenance → Configurations page appears.

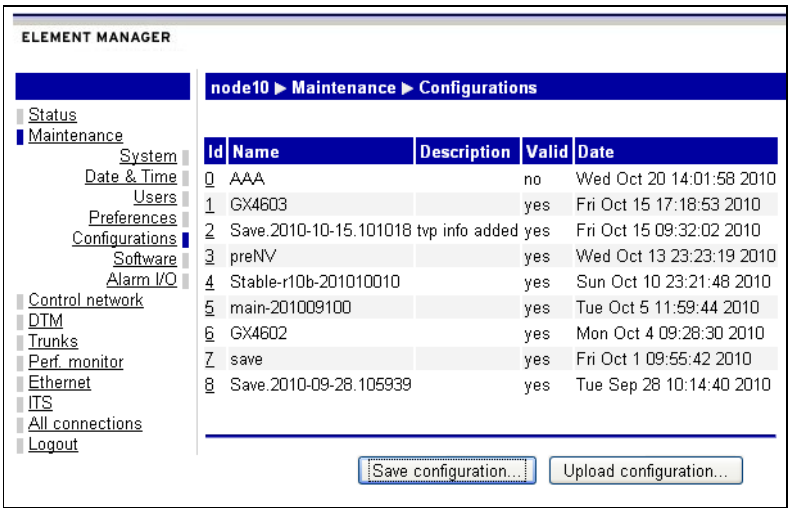


Figure 19. Configurations page

The table shows active and previous configurations stored in flash memory. The active configuration is at the top of the table.

The table shows the following information:

Parameter	Description
Id	The index number of the configuration
Name	A user-defined name of the configuration
Description	An optional user-defined description of the configuration
Valid	Indicates if the configuration is allowed(valid) on reboot or not
Date	Date and time when the configuration was saved

Figure 20. Maintenance → configuration parameters

Tip:

If Valid is set to “Yes” for more than one configuration, the first configuration with Valid set to “Yes” is used at reboot.

The previous configurations are retained in the unit until they are deleted. To make a previous configuration in the list active, set the Valid flag to ‘No’ for all configurations prior to the one to be used and restart the node.

The term “active” is used for the valid configuration with the lowest index number.

6.6.2 Saving the current configuration

Navigate to the Maintenance → Configurations page according to the previous section. When the ‘Save configuration’ button is clicked, the ‘Save configurations’ page appears:

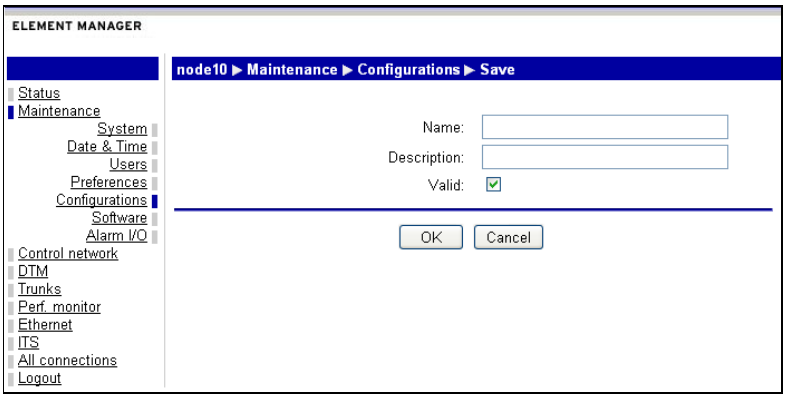


Figure 21. Backup (save) configuration to the node

Enter a name for the configuration in the **Name** entry field, and a suitable description in the **Description** field. The **Valid** checkbox must be ticked.

Click '**OK**'.

A dialogue box pops up, indicating that the operation may take a while. The Maintenance → Configurations page reappears with the new configuration active once the operation is concluded.

6.6.3 Download of configurations to PC

Note:

Changes in a valid configuration occur when the unit is restarted. If the active configuration is made inactive or deleted the entire system is affected on restart, as another configuration becomes active.

Only one configuration can be active at any given time.

Navigate to the Maintenance → Configurations page according to the previous section.

Click on the Id of the configuration to be modified in the Id column. The 'Edit configurations' page appears.

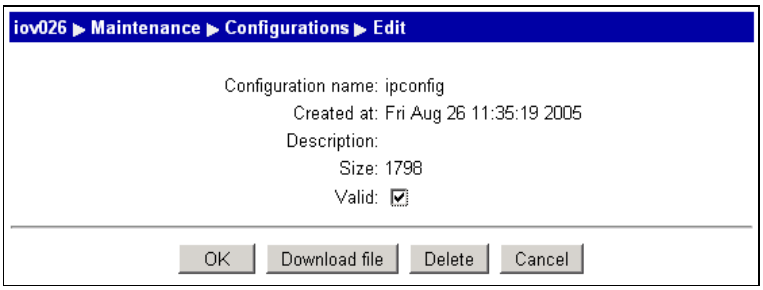


Figure 22. Edit configuration

Information about the configuration, such as name, when it was created, a description and its size, is shown. The only parameter that can be set here is the 'Valid' flag.

A click on 'Download file' downloads the configuration to a workstation/PC.

Click OK. The Maintenance → Configurations page appears, reflecting the modification.

6.6.4 Upload configurations from PC

To upload a prepared configuration file to the unit, use the following procedure:

Navigate to the Maintenance → Configurations page according to the previous section and click on the 'Upload configuration' button. The Upload page appears.

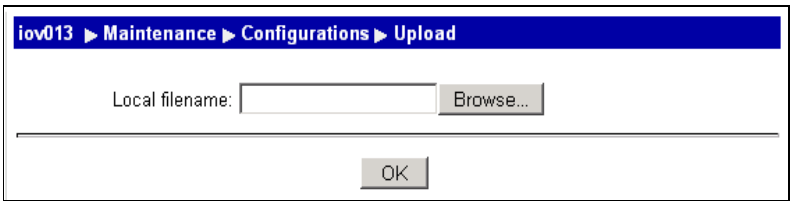


Figure 23. Upload configuration page

Click on the **Browse** button. A standard File Open dialogue box appears. Select the desired file and click the **OK** button.

The Confirm uploaded configuration page, appears.

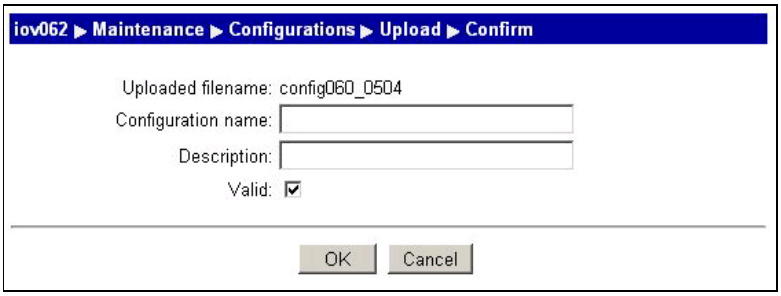


Figure 24. Confirmation page

Enter an appropriate name and a description for the configuration in the Name and Description entry fields. The Valid checkbox should be ticked.

Click the 'OK' button. The Maintenance → Configurations page reappears with the new active configuration at the top of list.

6.6.5 Switching configurations

To make a previous configuration active, the 'Valid' option has to be set to No for all configurations prior to the wanted one in the list. This is done by following these steps: Enter the Maintenance → Configurations page according to the previous section. Click on the name of the configuration to be modified in the Name column. The Edit configuration page appears.

Make the configuration inactive by clearing the 'Valid' checkbox.

If necessary, repeat to make other configurations inactive. After setting all needed configurations to inactive (i.e. 'not Valid'), restart the node. The node becomes active with the configuration file with the lowest Id number that is 'Valid'.

6.6.6 Delete a configuration

Note: 	If the active configuration is deleted, the entire system is affected after the unit is rebooted, as another configuration becomes active. If no reboot takes place, nothing immediate happens.

Enter the Maintenance → Configurations page according to the previous section. Click on the id of the configuration to be modified in the Id column. The Edit configuration page appears.

To delete the configuration, click on the 'Delete' button. Confirm the action in the confirmation window that opens. The configuration is removed directly.

6.7 Software maintenance

New software and firmware is easily installed on the Nimbra switch directly from the web interface. The newly installed soft- and firmware combination is activated upon a manual reboot of the node.

Running and installed software images, also known as GX system releases, are shown on the Maintenance → Software page below. The 'Running image' is currently active and the 'Installed image' becomes active upon reboot. An image consists of a directory structure with a number of files and can be downloaded from a Net Insight ftp or http server.

It is also shown how well the different soft- and firmware modules are aligned to a single GX-release in the variable 'System alignment status'. This variable can have five values: full, weak, vulnerable-strong, vulnerable-weak and unaligned.

The meaning of the different variable values is:

Alignment	Meaning
full	All running, primary and secondary images reported by swap must match entries in the current Packages.list file: the image is found and the board criteria matches the board article number and revision
weak	All running and primary images reported by swap match entries in the current Packages.list file but some secondary images differ. Restart of a board or the entire node is OK if all boards boot from their primary image. If a board with different primary and secondary images fails to boot the primary image but succeeds with the secondary image this board may become unusable. (Double error: board reboot and image failure)
vulnerable-strong	All primary images reported by swap match entries in the current Packages.list file but some running images differ (node controller and at least one interface board); all secondary images are the same as the corresponding primary images. Restart of the node will give full alignment.
vulnerable-weak	All primary images reported by swap match entries in the current Packages.list file but some running images differ (node controller and at least one interface board); at least one secondary image is different from the corresponding primary image. Restart of the node will give weak alignment.
none	All other cases

Figure 25. Possible values for the parameter ‘System alignment status’

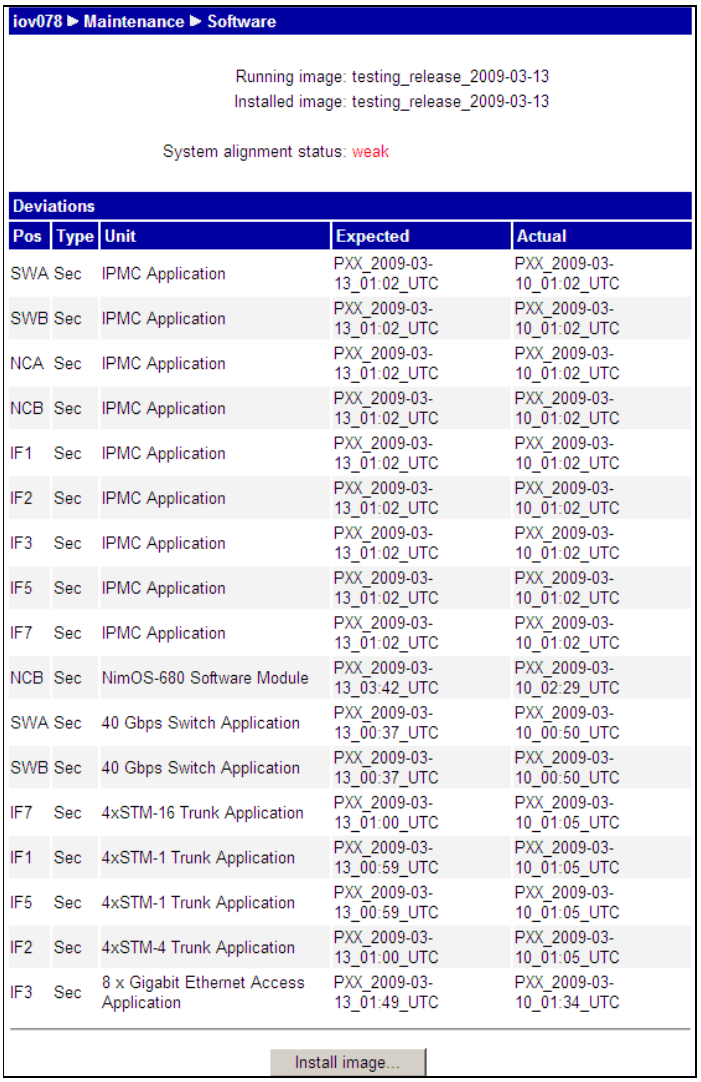


Figure 26. Maintenance, Software page

The following information is shown:

'Running image'**:** Currently running image

'Installed image'**:** Image that boots upon restart of the node

The alignment between different software modules is shown in the variable System alignment status. If its value is not full, all discrepancies are listed.

To install a new image, click on the 'Install image …' button. A new page asking for a URL with the location of the repository of the new image appears (see below). The repository is the "top directory" of the image.

To install the image, simply provide the URL and click on install. Observe that the currently running software image is active until the node has been rebooted.

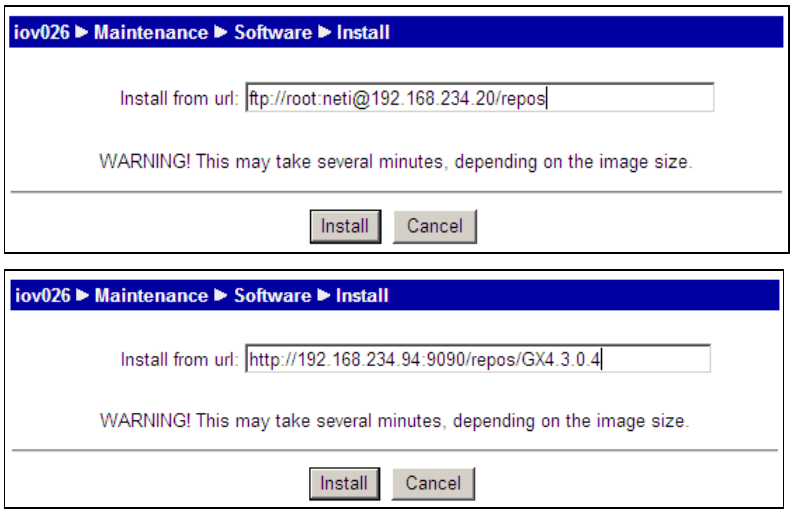


Figure 27. Maintenance, Software, Install page for ftp and http servers.

For a better understanding of what this web page does, please consult the Up- and Downgrading chapter.

6.7.1 Alarm I/O configuration

In the current release, alarm in- and output signals are supported for Nimbra One, Nimbra 340 and all Nimbra 600 series nodes.

Nimbra One and Nimbra 340 have one configurable output, between pin 5 and pin 9 on the (single) DSUB-9 physical contact and six configurable input pins (pins 2-4 and 6-8). Nimbra 600 has 16 different configurable interfaces/pins on two DSUB-9 physical contacts located on the GPIO alarm module front.

The pins are numbered according to the following principle:

1:0:<pin number> for Nimbra One or 340

1:<DSUB number on module (1 or 2)>:<pin number> for Nimbra 600.

Example: gpio1:1:4, gpio1:2:8 and gpio 1:0:5 (Nimbra One/340). For Nimbra 600, pin #7 (of both contacts) is connected to ground and is not configurable.

To configure pins of Nimbra One or 340, proceed as follows (Nimbra 340 is shown as an example):

Enter the Maintenance → Alarm I/O page by clicking on the link. Initially, no alarm pins are configured, which is displayed as direction ‘unused’ in the list. Click on the direction of the pin, i.e. the link unused of the pin to be configured.

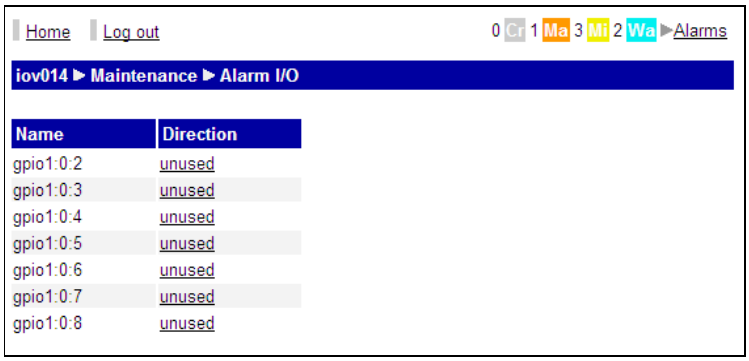


Figure 28. Alarm I/O configuration page for Nimbra 340.

A new submenu appears.

Figure 29. Alarm I/O configuration direction page

To start configuring the pin, select Direction 'Output' for pin 5 or Direction 'Input' for pins 2-4 and 6-8 and click on the OK button. The main Alarm I/O menu reappears.

Select the pin to be configured by clicking on the link to the pin (in the example below, on the link gpio1:0:2).

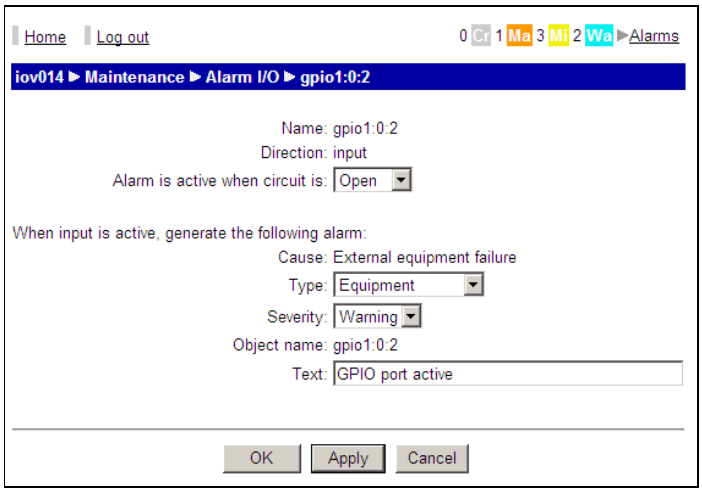


Figure 30. Alarm I/O configuration page of a specific interface/pin

To start configuring the interface/pin, select if the alarm is active when the circuit (pin to common ground, pin 9) is open/high or when it is closed/low. Make the additional parameter settings:

Parameter	Default	Possible values
Type	Equipment	Communications Environmental Equipment Processing error Quality of Service
Severity	Warning	Warning Minor Major Critical
Text	GPIO port active	Text string

Figure 31. Alarm I/O configuration parameters

Proceed by clicking on the 'Apply' or 'OK' button. The configuration is complete.

To configure pins of Nimbra 680, proceed as follows:

Enter the Maintenance → Alarm I/O page by clicking on the link. Initially, no alarm pins are configured, which is displayed as direction 'unused' in the list. Click on the direction of the pin, i.e. the link unused of the pin to be configured.

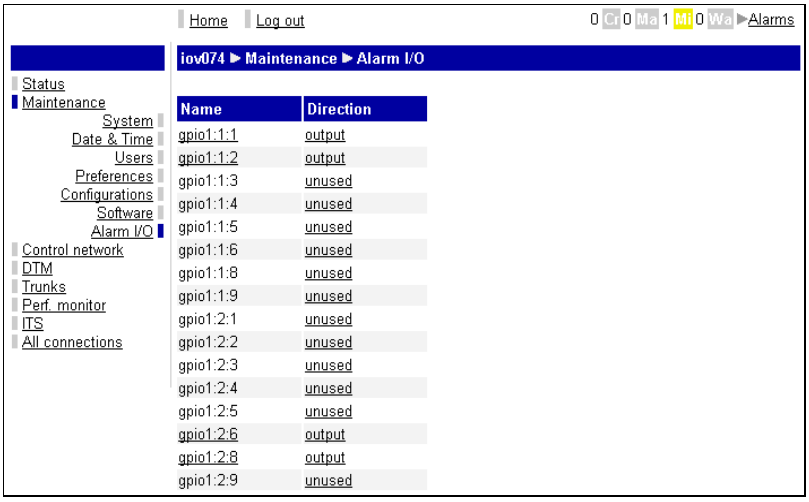


Figure 32. Alarm I/O configuration page for Nimbra 680.

A new submenu appears.

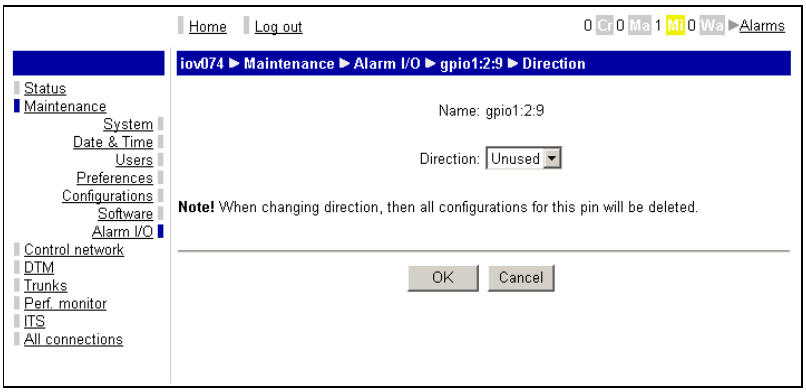


Figure 33. Alarm I/O configuration direction page

To start configuring the pin, select Direction 'Output' or 'Input' as desiredand click on the OK button. The main Alarm I/O menu reappears.

Select a pin to be configured by clicking on the link to it (in the example below, on the link gpio1:2:9 on the main alarm I/O configuration page).

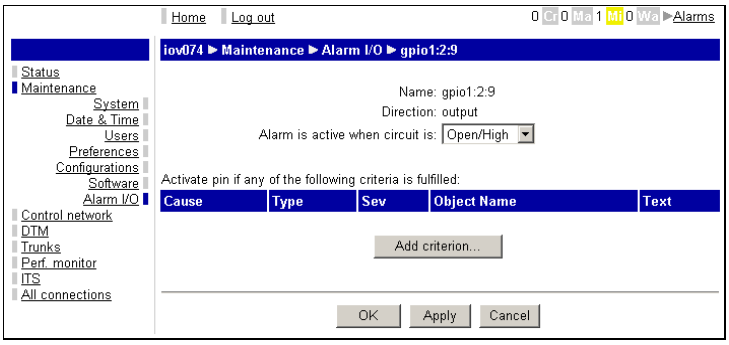


Figure 34. Alarm I/O configuration page of a specific interface/pin

To start configuring the interface/pin, select if the alarm is active when the circuit (pin to common ground, pin 7) is open/high or when it is closed/low. Proceed by clicking on the 'Apply' or 'OK' button.

Now up to eight different criteria can be chosen to activate the alarm. In order to add a criterion, click on the 'Add criterion …' button.

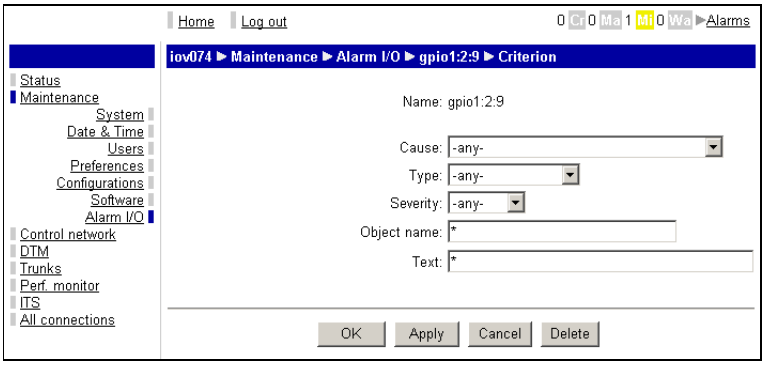


Figure 35. Alarm I/O configuration page for a specific criterion.

Select 'Cause', 'Type' and 'Severity' according to preferences. For these alarm properties, a drag-and-drop menu guides the user to the available alternatives. For alarm properties 'Object name' and 'Text', the '*' character

may facilitate the selection, but no drag-and-drop help is available. The '*' character matches any characters to the right of its position, e.g. LO* matches both LOS and LOF. If in doubt about object name and text, it is strongly suggested that the default string '*' is kept.

Click on the Apply button if one (or more) additional criterion is wanted; otherwise use the OK button. Add all criteria. If satisfied, the criteria cause the pin to become active on an 'or-basis' (i.e. if one or more of the criteria is satisfied, the pin becomes active).

To remove a configuration, just click on the output link on the Maintenance → Alarm I/O page, select 'Unused' and click on 'OK' or 'Apply'.

Note: 	If 'Cause', 'Type', 'Severity', 'Object name' and 'Text' has been selected in a manner not consistent with software defined alarms, the particular criterion cannot be satisfied and thus never generates an alarm. This condition does not in itself generate an alarm. In order to avoid the situation, use the –any-selection whenever in doubt.

For Nimbra360, gpio1:0:2 to gpio1:0:9 pins are shown as absent.

7 Status Monitoring

7.1 Overview of status monitoring

This chapter describes how general supervision of status and configuration is performed over the web interface.

The start web page for status monitoring is shown as below.

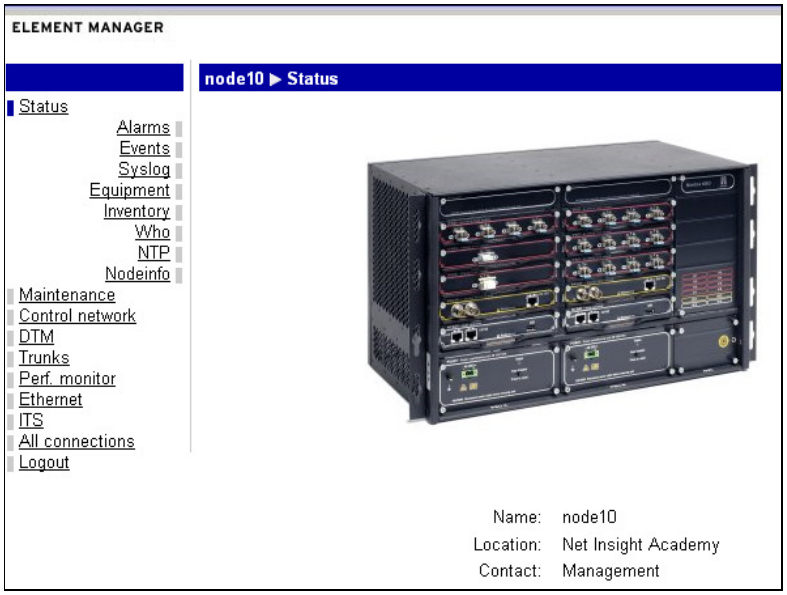


Figure 36. The start web page for Status

The status subpages are:

Alarms**:** present the alarms in the unit.

Events**:** present the events in the node.

Syslog**:** presents a log of the system.

Equipment**:** lists the installed equipment in the unit.

Inventory**:** presents the cards in the node including all the information about it such as: Art no, Rev and serial number.

Who**:** shows the users that are logged in to the unit.

NTP**:** shows NTP servers (clocks) available for the node

Nodeinfo: is a link to create a nodeinfo file, needed for advanced troubleshooting.

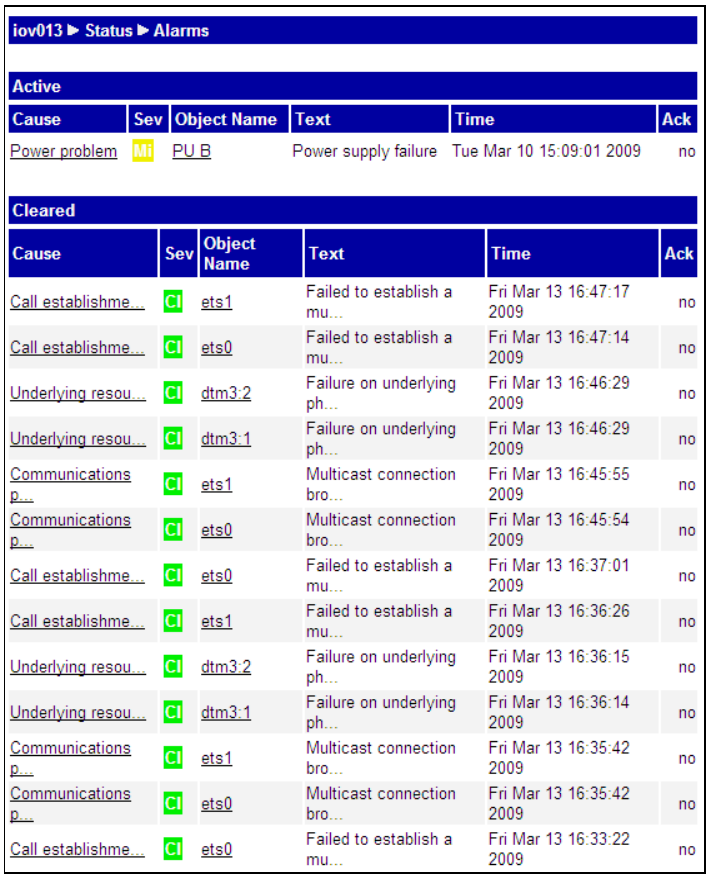
7.2 Alarms and events

An alarm is the reporting of a fault or a condition in the system. The alarm is always active or cleared, meaning that an alarm is indicating an actual status. It should always be possible to examine the fault condition, and from this determine whether an alarm exists or not. An event is something that happens within the system, but is not necessary a fault or condition. All alarms are events, but the reverse in not necessarily true.

Note: 	The alarm list will present the alarms which are defined under Maintenance →Preferences.

7.2.1 The alarms page

When clicking on the Status → Alarms link, the following page appears:



iov013 ▶ Status ▶ Alarms

Active

Cause	Sev	Object Name	Text	Time	Ack
Power problem	MI	PU B	Power supply failure	Tue Mar 10 15:09:01 2009	no

Cleared

Cause	Sev	Object Name	Text	Time	Ack
Call establishme...	CI	ets1	Failed to establish a mu...	Fri Mar 13 16:47:17 2009	no
Call establishme...	CI	ets0	Failed to establish a mu...	Fri Mar 13 16:47:14 2009	no
Underlying resou...	CI	dtm3:2	Failure on underlying ph...	Fri Mar 13 16:46:29 2009	no
Underlying resou...	CI	dtm3:1	Failure on underlying ph...	Fri Mar 13 16:46:29 2009	no
Communications p...	CI	ets1	Multicast connection bro...	Fri Mar 13 16:45:55 2009	no
Communications p...	CI	ets0	Multicast connection bro...	Fri Mar 13 16:45:54 2009	no
Call establishme...	CI	ets0	Failed to establish a mu...	Fri Mar 13 16:37:01 2009	no
Call establishme...	CI	ets1	Failed to establish a mu...	Fri Mar 13 16:36:26 2009	no
Underlying resou...	CI	dtm3:2	Failure on underlying ph...	Fri Mar 13 16:36:15 2009	no
Underlying resou...	CI	dtm3:1	Failure on underlying ph...	Fri Mar 13 16:36:14 2009	no
Communications p...	CI	ets1	Multicast connection bro...	Fri Mar 13 16:35:42 2009	no
Communications p...	CI	ets0	Multicast connection bro...	Fri Mar 13 16:35:42 2009	no
Call establishme...	CI	ets0	Failed to establish a mu...	Fri Mar 13 16:33:22 2009	no

Figure 37. Alarms page

More information about the alarms is available by clicking on the link under the ‘Cause’ heading.

The table shows the **Active** and **Cleared** alarms in lists and it shows the alarms in the lists as follows.

Cause	Describes the cause of alarm
Sev	Shows the severity of the alarm. The following values are possible: Cr Critical (red) The critical severity level indicates that a service affecting condition has occurred and that an immediate corrective action is required. Ma Major (orange) The major severity level indicates that a service affecting condition has developed and an urgent corrective action is required. Mi Minor (yellow) The Minor severity level indicates the existence of a non-service affecting fault condition and that corrective action should be taken in order to prevent a more serious fault. Wa Warning (blue) The warning severity level indicates the detection of a potential or impending service affection fault, before any significant effects have been felt. Info Information Cl Cleared (green) The cleared severity level indicates the clearing of one or more previously reported alarms.
Object name	The alarm causing object.
Text	More detailed text about the alarm.
Time	Time stamp for the alarm.
Ack	Flag that tells if the alarm has been acknowledged or not. Not available for events.

Figure 38. Description of alarm and event properties. For a specification of the different alarms, see document nid2004.pdf (Alarms list).

To find the event list rather than the alarm list, click on links Status and then Events. The Events page appears.

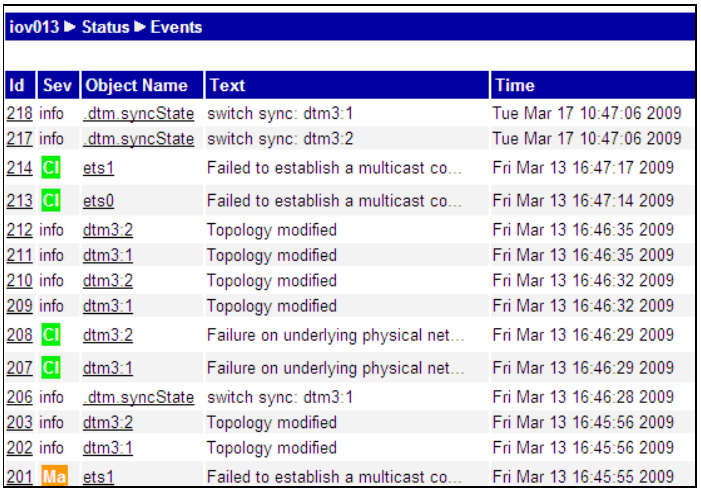


Figure 39. Events page

7.2.2 Acknowledging an alarm

The alarms remain in the ‘Alarm monitor’ ‘field at the top of the web page until the alarm has been acknowledged. To acknowledge an alarm, do the following:

Enter the ‘Alarms’ page according to the previous section. Click on the alarm event to be acknowledged in the **Cause** column. The **Edit** page appears.

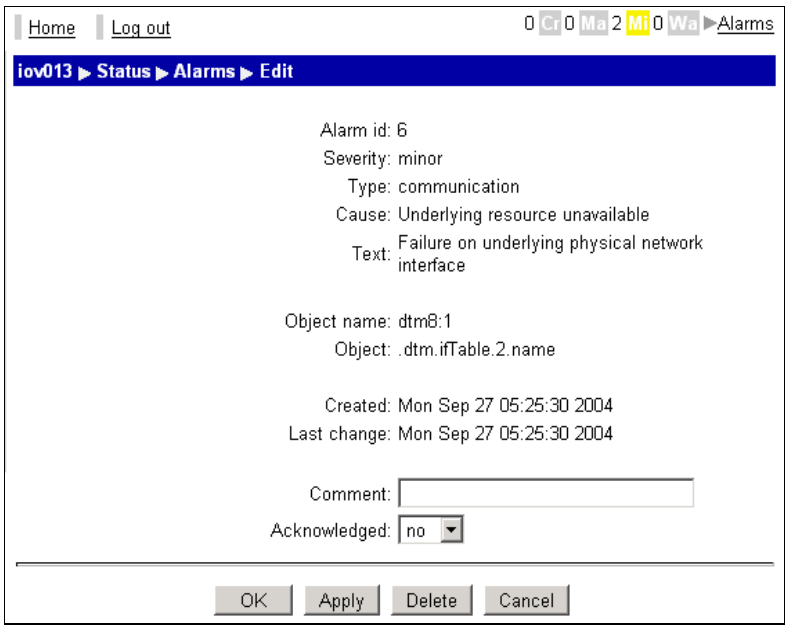


Figure 40. Acknowledge alarm page

This page shows the same information as the alarm list, with the addition of an editable Comment field and an Acknowledged drop-down menu.

Enter any desired comment, set the Acknowledged drop-down menu to ‘Yes’ and click ‘Apply’ or ‘OK’.

The Alarms page now appears with Ack (alarm acknowledgement) set to “yes”.

Note:	In some circumstances the cause of the alarm cannot be removed or the alarm should not be acknowledged until later. In this case, use the Comments field to pass on any comment regarding the alarm event. Note that the action of acknowledging an alarm does not remove the alarm from the alarm list.

7.3 Syslog

The **Syslog** page lists a log of the system. To access the page, click on the Status link and then on the Syslog link. The Syslog page contains two links, Latest and Older, which takes the user to the latest entries in the syslog or to older entries. For Nimbra 600 with dual Node Controllers, latest and older syslogs are available for both Node Controllers (shown).

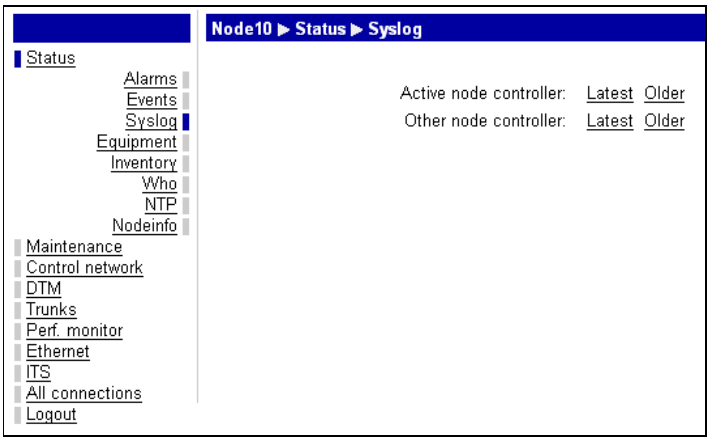


Figure 41. The Syslog page for a Nimbra 600 with dual Node Controllers.

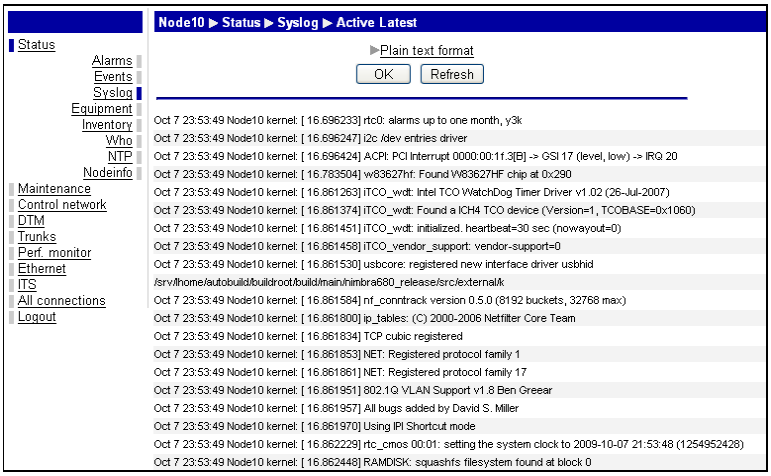


Figure 42. The Syslog page (latest) for the active node controller.

Syslog is configured from the Maintenance→System→Syslog configuration link. The default configuration is

```
*.*;local1.!=info -/var/log/messages
*.alert /dev/console
```

This configuration logs all system messages, except from local1 info level (that pertains to the creation, modification and deletion of DTM OAM objects), to the file `/var/log/messages`. Furthermore, it also displays all critical messages on the console. The syntax of the configuration items adheres to the standard BSD syslog implementation as described in the "`syslog.conf`" man page of most Linux systems.

Note:	It is important that the filename, of the file to which the logged messages are written, is preceded with a "-" sign. Otherwise the performance of the node can degrade significantly.

An alternative useful setting is

```
*.*;local1.!=info @<IP address of central syslog daemon>
```

This setting will send all system messages over UDP port 514 to a central syslog server. This is a convenient way of consolidating node system and events messaging information in a simple way. Note that the syslog protocol does not guarantee that messages are transferred between sender and listener.

Generally some care should be taken when changing syslog settings since flooding of messages that should be written to the internal flash memory can severely affect the performance of the node.

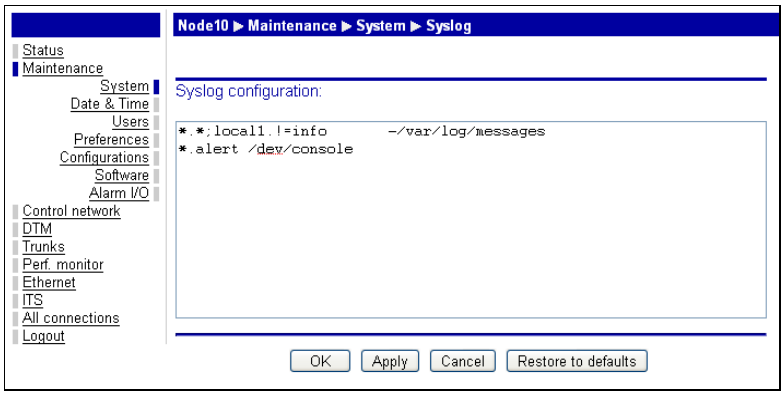


Figure 43. Definition of the syslog file.

7.4 Equipment

The Equipment page lists the installed modules and gives a temperature reading of the unit. To access the page, click on the Status → Equipment link. The following page appears:

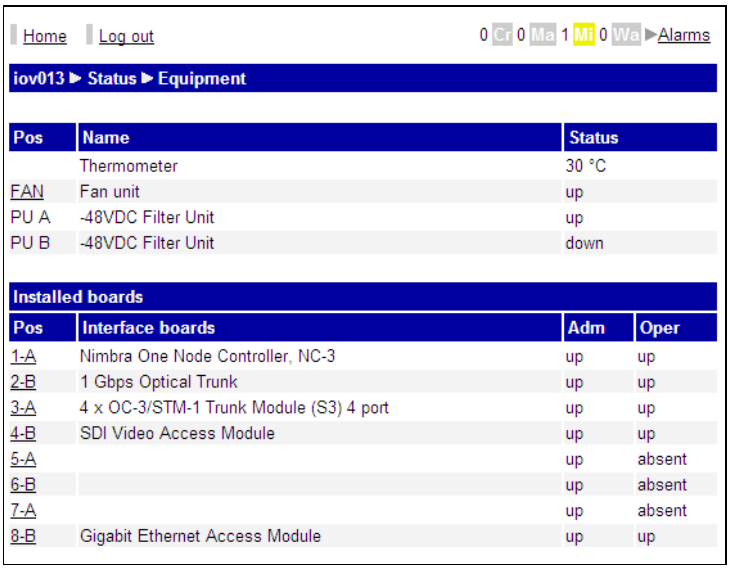


Figure 44. Equipment page

In order to configure the fan unit (in particular the 'Enable air filter replacement alarm'), the link FAN should be used. The following page then appears:

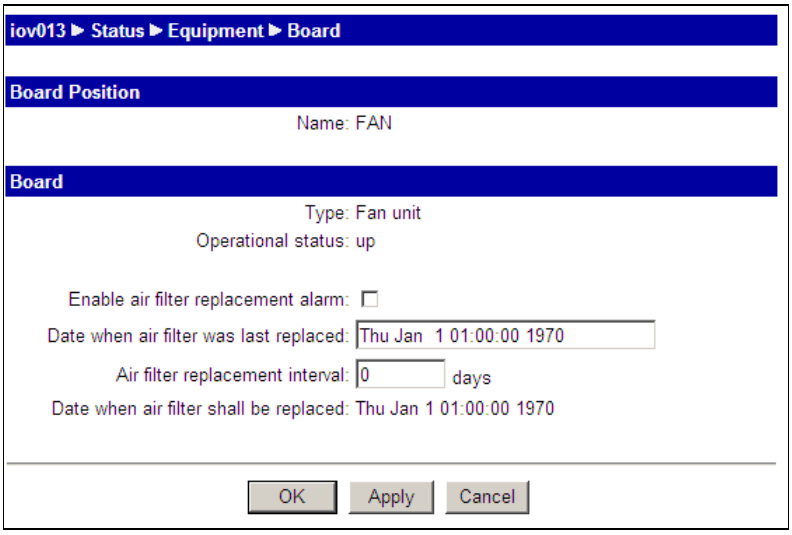


Figure 45. Configuration of the 'Air filter replacement alarm'.

When a filter is replaced or when the function is first enabled, the 'Date when air filter was last replaced' and 'Air filter replacement interval' are filled out and the 'Enable air filter replacement alarm' tick box is selected. Subsequently, the 'Apply' button should be pressed. The variable 'Date when air filter shall be replaced' is calculated and presented on the web page. An alarm is presented when this date is passed, which indicate that a replacement is needed. The severity of the alarm is warning.

For suitable air filter replacement intervals, please see the relevant Installation and Maintenance manual. Default values, ranges and formatting of the parameters are indicated in the table below:

Parameter	Default	Range	Format	Comment
Enable air filter replacement alarm	Disabled	Disabled or Enabled	Tick box	
Date when air filter was last replaced	Thu Jan 1 01:00:00 1970	1970-2038	Thu Jan 1 01:00:00 1970	Weekday (Mon, Tue, Wed, Thu, Fri, Sat, Sun) is ignored
Air filter replacement interval	0	0-24855	Integer	
Date when air filter shall be replaced (variable)	Thu Jan 1 01:00:00 1970	1970-2038	Thu Jan 1 01:00:00 1970	Calculated as 'Date when air filter was last replaced' plus 'Air filter replacement interval'

Figure 46. Air filter replacement parameters and variables.

7.4.1 Setting the administrative status of a module(board)

To set the administrative status of a board, follow the Status → Equipment link. Click on the position (Pos) of one of the modules. The Board page appears.

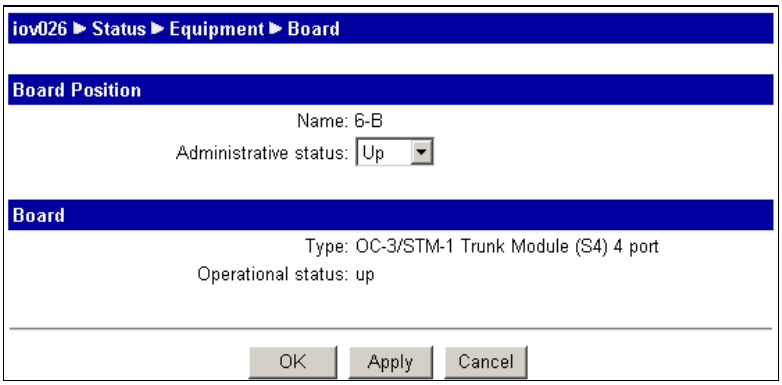


Figure 47. Board page

In the roll-down menu, the Administrative status is set to 'Up' or 'Down'. Click on 'OK' or 'Apply' to change the setting.

The status of the card can be verified in the administrative status and operational status columns of the Status → Equipment page.

Note:

A change in the Administrative Status of the standby Node Controller needs to be saved (i.e. the configuration needs to be saved) in order for the change to remain in place after a system reboot.

7.4.2 Allocating backplane capacity in Nimbra 600

Note: 	The following applies only when using 40 Gbps switch modules in the Nimbra 680 or when using 80 Gbps switch modules in Nimbra 688. When using 80 Gbps switch modules in Nimbra 680 or 160 Gbps switch modules in Nimbra 688, there is always 10 Gbps allocated to each interface position. 40 Gbps switch modules for Nimbra 688 is not supported.

In the Nimbra 680/688 switch, it is possible to configure the capacity allocated to a board position. Capacity is allocated in a row-pair fashion. A row-pair consists of the two adjacent slots in the same row (for example IF3 and IF4). The left position has an odd IF number (for example IF3). The total capacity of a row-pair is always 10 Gbps. The capacity can be allocated to the two slots as follows:

Option	Left slot	Right slot
1 (default)	5 Gbps	5 Gbps
2	10 Gbps	0 Gbps

Figure 48. Backplane capacity allocation in Nimbra 680/688.

Default is that both IF positions in the row-pair have 5 Gbps allocated. If the left column interface module should have the whole capacity of the row-pair, the module has to be configured for that. This is described below.

Trunk and access modules can be classified in three different categories. Some modules always require 10 Gbps switching capacity, some modules never require 10 Gbps switching capacity and some modules require 5 or 10 Gbps switching capacity depending on how they are used.

This allocation scheme implies the following restrictions of how interface boards can be used in the switch.

Left slot	Right slot
4 x OC-3/STM-1 Trunk 4 x OC-12/STM-4 Trunk	4 x OC-3/STM-1 Trunk 4 x OC-12/STM-4 Trunk
4 x OC-48/STM-16 Trunk (using ports one and two)	4 x OC-48/STM-16 Trunk (using ports one and two)
8 x Video Access Module (configured for 5 Gbps)	8 x Video Access Module (configured for 5 Gbps)
8 x Gigabit Ethernet Access (5 Gbps)	8 x Gigabit Ethernet Access (5 Gbps)
OC-192/STM-64 Trunk	None
4 x OC-48/STM-16 Trunk (using all four ports)	None
8 x Video Access Module (10 Gbps)	None
8 x Gigabit Ethernet Access (10 Gbps)	None
6 x IP/Ethernet Trunk Module (5 Gbps)	6 x IP/Ethernet Trunk Module (5 Gbps)
6 x IP/Ethernet Trunk Module (10 Gbps)	None

Figure 49. Left/Right slot usage for currently available boards.

To change the capacity allocation of an IF position, do the following:

Note:	Note that both slots of a row-pair are affected, according to the Figure above, by changing the capacity of one slot. Both boards in the row-pair will be restarted.

Follow the Status → Equipment link and click on the position of one of the modules. Note that it is only possible to change capacity on the left module in a row-pair, i.e. on positions IF1/3/5/7. The corresponding right slot capacity is adjusted though, according to the previous discussion.

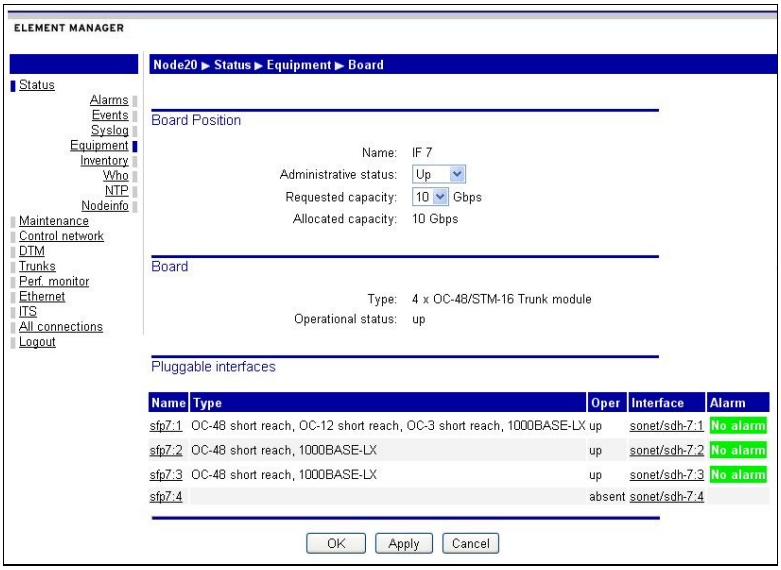


Figure 50. Edit board page, Nimbra 600 series

Select the Requested capacity, 5 or 10 Gbps and click ‘Apply’ or ‘OK’. Furthermore, on this page information from the various mounted SFPs is available (Digital Diagnostics). Click the sfp link, like sfp7:3, and the web page shown below is displayed.

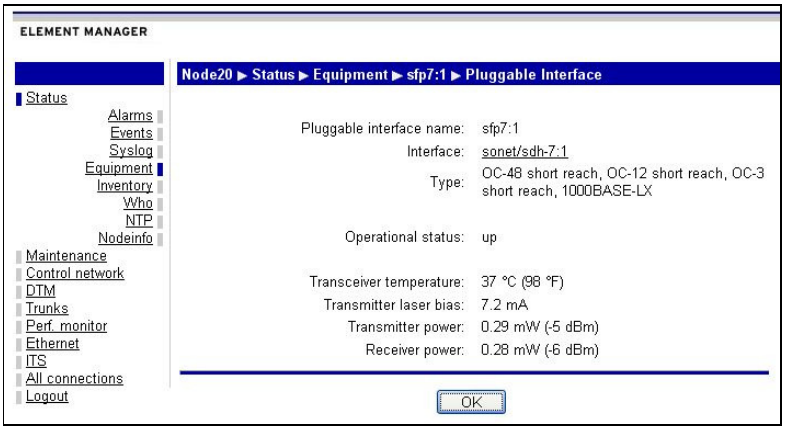


Figure 51. Pluggable interface page, where information from the particular SFP is displayed.

7.5 Inventory

The Inventory function describes the physical entities installed in the system.

A Physical entity or Physical component represents an identifiable resource within a managed system. Typically, physical entities are resources like communications ports, backplanes, sensors, daughter-cards, power supplies and the overall chassis which can be managed. However, software/firmware images are also considered to be physical entities in this (inventory) context, although they cannot be touched.

The Containment tree describes how entities are structured and contained within each other. The use of the position entity allows modeling where a resource is absent, i.e. a board slot position may be empty only to be filled out later. The containment tree is listed in the inventory table.

To access the Inventory page, proceed as follows:

Click on the Status → Inventory; the Inventory page appears.

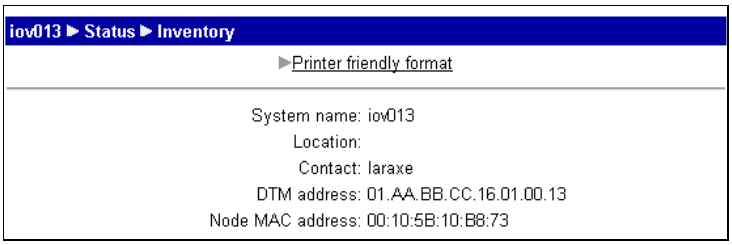


Figure 52. The Inventory page, first part

On the Inventory page you find a link, Printer friendly format. Clicking on the link creates a version of the inventory page suitable for printing.

On the inventory page, the containment tree of the entire node is displayed, i.e. what resources are available in the node and how they are structured.

Type	Properties
Chassis	Nimbra-One
	Art no: NA Rev: 1.10.0.0
	Serial no: NDF00002B9
Position	Firmware
Image	FW - ISM_2 (Nimbra One Base Unit)
	Art no: NA Rev: 1.3.0.0
Position	1
Board	Nimbra One Node Controller
	Art no: NA Rev: NA
	Serial no: NA
Position	Running
Image	N1_baseSW
	Art no: NSS0005-001 Rev: 3.2
Position	Primary
Image	N1_baseSW
	Art no: NSS0005-001 Rev: 3.2
Position	Secondary
Image	GX3_1_4
	Art no: NA Rev: NA
Position	Bootloader
Image	N1_boot
	Art no: NSS0003-0001 Rev: 3.0.4
Position	Firmware
Image	NA
	Art no: NA Rev: NA

Figure 53. The Inventory page, second part

For Boards on which more than two FW-images could be stored, i.e. Control Module (Node Controller), Gigabit/Fast Ethernet or OC-3/STM-1 access modules, the image that is running is indicated as follows:

Primary: Image stored as primary

Secondary: Image stored as secondary

Running: Image that is running (could be either the primary or secondary)

For boards on which only one FW-image could be stored, only the primary image is presented. Here, the primary image must be running.

7.6 Who (is currently logged in)

This link (Status → Who) lists all current users. It can be used for checking if other users are logged in to the unit over web GUI (Graphical User Interface). Click on the link Status → Who; The Status Who page appears.

iov013 ▶ Status ▶ Who

Username	Tty	From	Login	Expire
root	N/A	192.168.101.10	06:46:54	17:30:22
root	N/A	10.100.5.142	09:18:31	17:32:45
root	N/A	10.100.3.191	14:30:44	17:24:05

Figure 54. The Status Who page

The table shows information about other logged in users; user name, Tty (type of terminal used), From (IP address), Login (time) and Expire (time). Inactive users are automatically logged out at Expire time.

7.7 NTP (Network Time Protocol)

Follow the link (Status → NTP) and you'll find the various NTP servers available for the node listed. The table shows information about available clocks in the node.

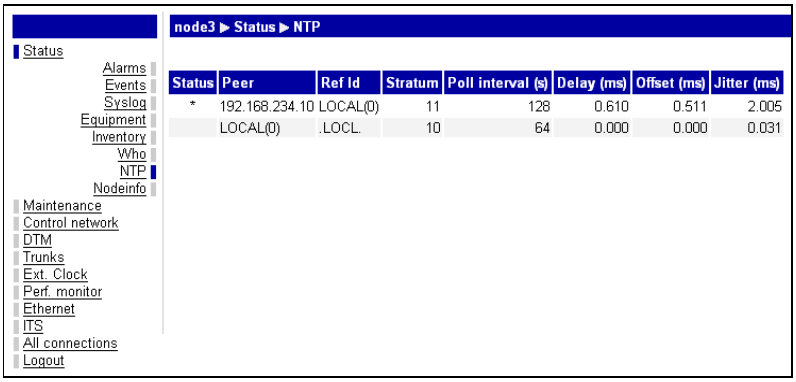


Figure 55. The Status NTP page

Listing	Description
Status	'*' means active NTP, ' ' inactive
Peer	Address of the clock source (NTP)
Ref Id	(IP) Address of the clock source/NTP
Stratum	Stratum level of the clock source/NTP
Poll interval (s)	is the time between two consecutive interactions with the clock source/NTP
Delay (ms)	The time for the NTP signal to go from the node to the NTP server and back
Offset (ms)	is the time offset used by the node to allow for time transfer delay
Jitter (ms)	is the jitter exhibited by the NTP servers

Figure 56. Headers on the Status → NTP page

7.8 Nodeinfo

In order to generate and download a diagnostic file about the node that is needed for advanced troubleshooting, the link System → Nodeinfo should be followed.

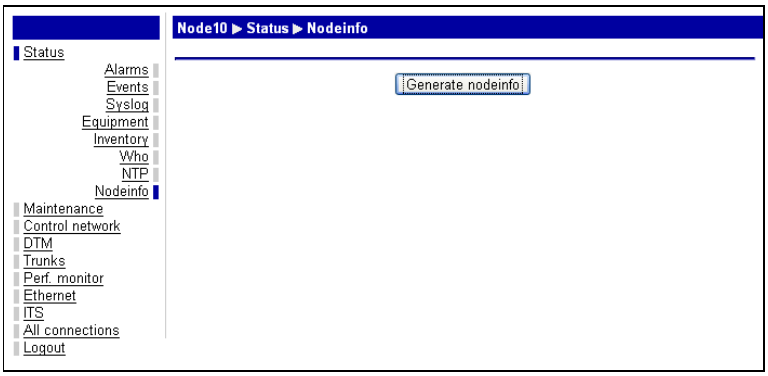


Figure 57. Nodeinfo

The nodeinfo file is generated and saved in the node if the button 'Generate nodeinfo' is clicked and the choice is confirmed in the pop-up window.

When the file is generated, it can be viewed (View nodeinfo log). It can also be downloaded or deleted directly (if the file was generated by mistake).

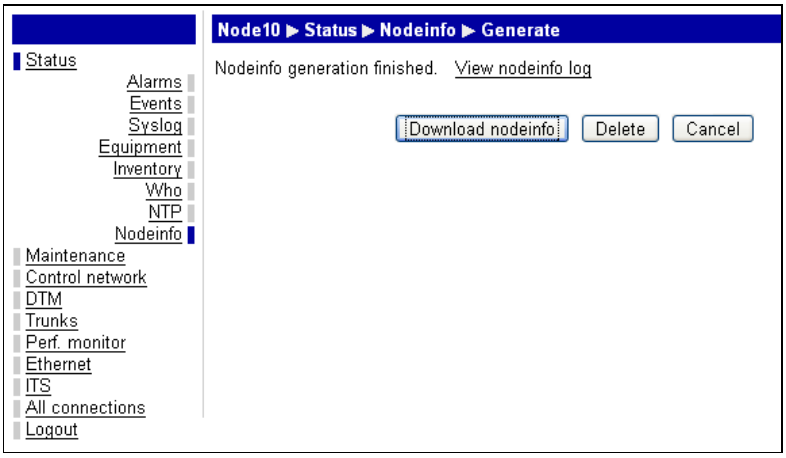


Figure 58. Nodeinfo page when the file has been generated.

8 Control Network

8.1 General about In-band management

The management network is used for managing the nodes in the Nimbra network. It is used when an operator or application accesses the nodes using e.g. telnet, HTTP or SNMP. The network is also used by some other protocols, such as NTP (Network Time Protocol).

Typically, the type of traffic on a management network is from one of a few management stations located on a network outside the Nimbra network. Management stations interact with relevant nodes when provisioning connections, collecting network statistics or checking the status of the nodes. Alarm messages are usually sent from the managed nodes to a limited number of management stations.

When managing the nodes, there is rarely any communication between the nodes. Communication is done with the network management stations, either from a network management system such as Nimbra Vision, or from a web browser or telnet session. This traffic is routed via the gateway. Typically, only a limited number of nodes in the Nimbra network reached are simultaneously from a management station.

8.1.1 Ethernet DLE

DLE (DTM LAN Emulation) emulates a LAN (Local Area Network) as an Ethernet segment on top of Net Insights network. It is implemented using channels throughout the network. Seen from DLE, each node in the segment has direct connectivity to all other nodes, as on an Ethernet segment. The underlying physical topology of the DTM network is not related to the topology of the segment, e.g. two nodes on the same DLE segment may be located far away from each other.

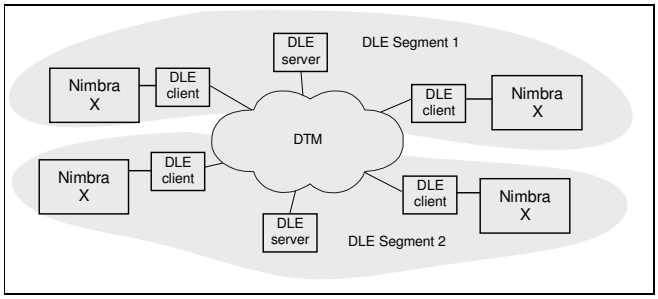


Figure 59. Two separate DLE segments.

Note:	Note that the DLE segment is a logical segment. The physical topology exists only on the DTM level.

8.1.2 IP and routing

Each node that is connected to the DLE segment has a virtual IP interface assigned, allowing it to communicate with other nodes on the segment using IP. A gateway routes the IP packets to and from the segment. This means that each segment has its own IP network address. Routing can be to other networks, i.e. DLE segments, or to an out-band IP network.

Routing will load the Control Module CPU of the gateway node. The number of packets that can be routed will therefore be limited by the capacity of the Control Module.

8.1.3 DLE clients

Each virtual Ethernet interface is implemented by the DLE client, one client per virtual interface. When Ethernet packets are sent from one node to another within the segment, the client will establish a channel to the remote node. The remote node would establish a return channel for any reply. This means that from each node, there will be a channel established to every other node in the segment to which packets have been sent. To reduce the number of channels in a segment, channels can be torn down automatically or manually when they are no longer used.

It is also possible to force all traffic to go through the server and avoid setting up channels between DLE clients completely. This means that all DLE clients share one channel from the server for all traffic.

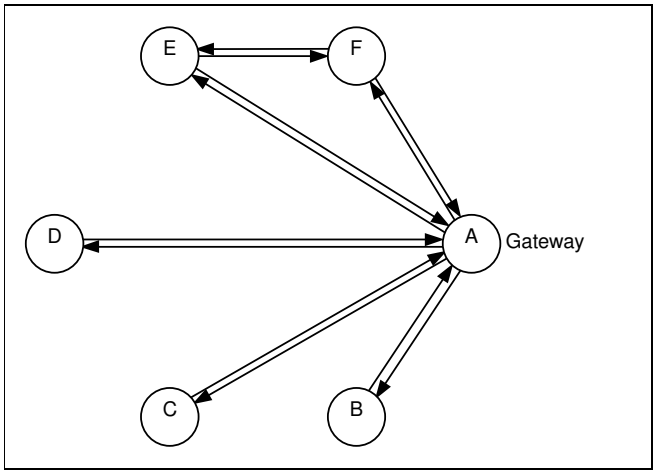


Figure 60. A DLE segment with channels between DLE clients

In this illustration it is assumed that all nodes have communicated via the gateway. So the gateway (A) has channels connected to and from all the nodes. Communication has also occurred between node (E) and (F) resulting in a channel between these two nodes. Channels that are not used has been torn down, hence no channels exists between any other nodes.

It is possible to have multiple clients on a single node, implementing multiple virtual Ethernet interfaces.

Client to Server Channels and Server to Client Channels are used for broadcast packets, and for DLE signaling.

Client to Client Channels are used for peer-to-peer communication.

8.1.4 DLE server

Each DLE segment has a DLE server. The responsibility of the server is to provide information to the clients about the other nodes in the segment, and thus aid the clients in establishing their connections. Because the client and server must be able to at all time communicate, permanent channels are established between client and the server. One channel is established from each client to the server, and one multicast channel is established from the server to all the clients.

The channels between server and clients are also used when distributing broadcast packets. The broadcast packets from a client are sent to the server, which distributes it to all the other clients on the segment using the multicast channel from the server to the clients. I.e. broadcast packets will not result in establishment of new channels between two clients. Packets are also distributed in the same way if the channel from one client to the other client is not established. Typically, this would be during the period when a channel is being established.

8.1.5 Multiple DLE servers

It is possible to use multiple DLE servers for a single segment. The servers co-operate and allow for redundancy.

At any time, a client is connected to only one server. When multiple servers are used, the servers are interconnected through multicast channels, one in each direction. Client packets that would be sent via the server to other clients are also replicated by the server and sent to the peering servers for distribution to their connected clients.

Setting up a segment with multiple servers, and where sets of clients are connected to different servers, implements redundancy between servers.

Multiple servers can be used as alternative servers for the client. For each client, it is possible to configure alternative servers, where the alternative servers must serve the same segment. When a client establishes a channel to a server, it will try the servers in order until successful. If a server would go down, the client establishes a new channel to a server, trying them in order until successful. This implements redundant servers.

8.2 Configuration

Management traffic requires only moderate bandwidth. It is therefore adequate to use 512 kbps (equals one DTM slot) per channel, both between DLE servers (server-server) and DLE clients (client-client). As the DLE client-to-server communication is only used for signaling and broadcasting, 512 kbps is sufficient for these channels as well.

The recommendations in this document are for an in-band management network that is used exclusively for management of the Nimbra nodes. No consideration has been taken for allowing other traffic.

To limit the load on the DLE server, there is a recommended maximum of DLE clients in one segment per server.

To limit the load on the gateway, there is a recommended maximum number of nodes with traffic routed through the gateway.

For availability reasons, when a single DLE server is used, it is recommended that the gateway for a DLE segment is located on the same node as the DLE server.

The timeout to tear down unused channels is infinite, but can be configured.

Critical parameters	Nimbra One	Nimbra 300	Nimbra 600
Maximum recommended number of DLE clients for one DLE server	16	16	64
When working as gateway: maximum recommended number of nodes to route traffic for	255	255	1000
Maximum recommended number of DLE clients on a node	3	3	3

Figure 61. Configuration recommendations of the DLE in-band network used for managing the nodes from external management stations

8.3 Building networks with DLE

When building in-band management networks using DLE, use the recommendations previously listed.

For networks larger than the number of nodes recommended within one DLE segment, it is suggested that a tree of segments is built and intermediate nodes acts as gateways between the segments. Note that the root of the tree will have to route traffic to and from all of nodes to the external network.

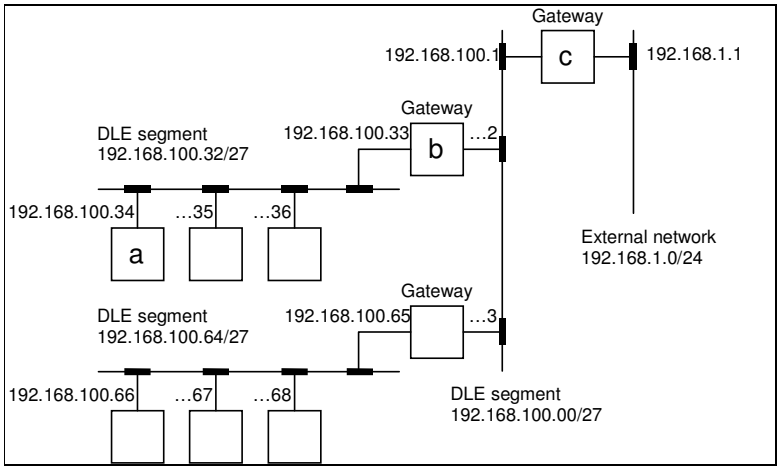


Figure 62. Example of a network with three DLE segments built as a tree, and one external network

The DLE segments have a netmask of 255.255.255.224 meaning that there can be 30 nodes on each network (one address is the network, and one is the broadcast address). The gateways route packets between the DLE segments and the external network.

If the Nimbra network consists of more nodes than what is recommended as the maximum for one gateway, it is recommended to split the network into separate in-band management networks and route the traffic to the external network with a dedicated node as the gateway.

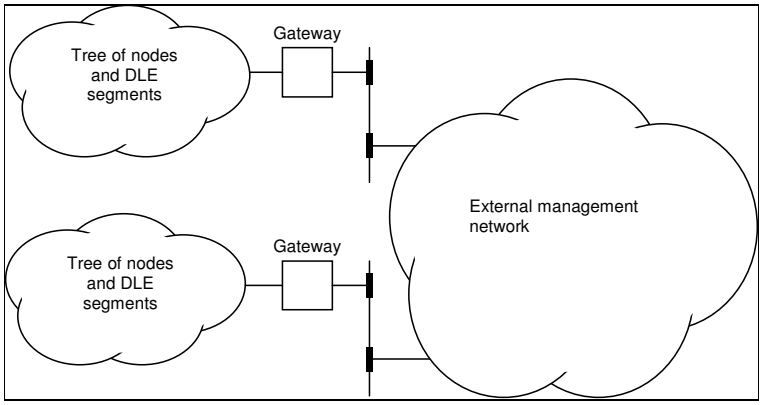


Figure 63. Large networks are divided into smaller networks, each with its gateway to the external management network

8.4 IP routing

Setting up DLE only configures the individual DLE segments. As with all IP networks, routing must be configured in each node to be able to route the traffic in and out of the DLE segment. Setting up IP routing for a DLE segment is not different from setting up IP routing in general.

A routing entry consists of a destination, a netmask and a gateway. When a packet is sent to a node outside the network, the IP address to the node is masked with the netmask of a route. If the masked IP address matches the destination of the route, the packet is forwarded to the gateway specified in the route. The gateway must be located on the local IP sub-network.

On each node in the DLE segment, a default gateway routing entry should be specified, or routes must be specified to all remote destinations. This is used to determine where to forward packets to nodes outside the DLE segment. The default route is specified as destination 0.0.0.0 with netmask 0.0.0.0. This entry will match all IP addresses. The gateway shall be the IP address of the gateway on the DLE segment.

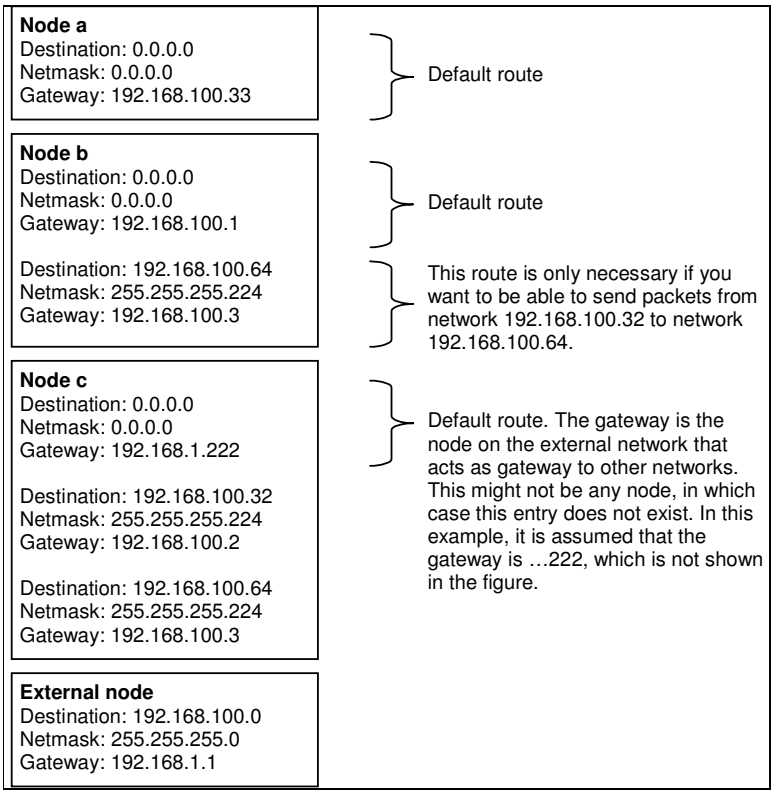


Figure 64. Routing tables for a previously discussed network.

Note: Node c must have two routing entries, in addition to the default route, one to each network (DLE segments).

8.5 Control Network

This section describes how to use the web interface to set up IP and SNMP parameters for in- and out-band management. The starting web page for Control network is shown below.

Figure 65. The Control network web page

The sub-sections (links): In-band servers, In-band clients, IP interfaces, IP routing conf, IP routing table and SNMP.

8.6 In-band servers

DLE servers use one single multicast channel for connecting to all peering DLE servers. Each server is responsible for re-establishing its originating multicast channel in case (parts of) it goes down, after verifying that the peering server still is configured as a peer.

A DLE server must be configured in one of the units of the network, according to the following procedure.

8.6.1 Configuration parameters for In-band servers

8.6.1.1 Administrative status

Default value: 'Down'

Type: Boolean variable (only two states possible)

Range: 'Down', 'Up'

Description: The parameter determines if the server is thought to be active (Up) or inactive (down).

8.6.1.2 *Purpose*

Default value: Empty string

Type: String variable

Range: Length 0-255 characters

Description: The parameter is an arbitrary character string that can be used for identification purposes.

8.6.1.3 *DSTI (DTM Service Type Instance)*

Default value: 32769 for first defined server on the node, 32770 for the second etc

Type: Integer

Range: 0-65535

Description: The parameter is the instance number of the DLE server, i.e. the identifier of this particular service. It is recommended to keep the default value.

8.6.1.4 *Server - Client connection capacity*

Default value: 0.485 Mbps, i.e. one slot per frame

Type: Real number

Range: 0 to the capacity of the trunk between server and client

Description: The capacity between the server and the client.

8.6.1.5 *Server - server connection capacity*

Default value: 0.485 Mbps, i.e. one slot per frame

Type: Real number

Range: 0 to the capacity of the trunk between the servers

Description: The capacity between the server and the back-up server.

8.6.2 Advanced settings

From this link, the parameters of the exponential back-off algorithm of the re-connect time out are set. Also, the connection can be defined as having "Precedence", which means that in case an intermediary node goes down, this particular connection is taken down with priority and a replacement connection is set up with priority (i.e. it has precedence over other connections).

Minimum interval: The starting value of the back-off algorithm, 10 ms. After tear down of a connection, connection re-establishment is attempted immediately; if this attempt fails, another attempt is made after 10 ms.

Maximum interval: The final value of the algorithm, 50000 ms. The re-establish mechanism will wait not longer than 50000 ms to re-establish a channel.

8.6.3 Destination settings

Clicking on this link gives the user a way to define peering DLE servers. These DLE servers operate on the same control level and work together for redundancy and load balance.

8.6.3.1 *Addition of a DLE Server*

Navigate to web page Control Networks → In-band servers and click on the 'Add server' button.

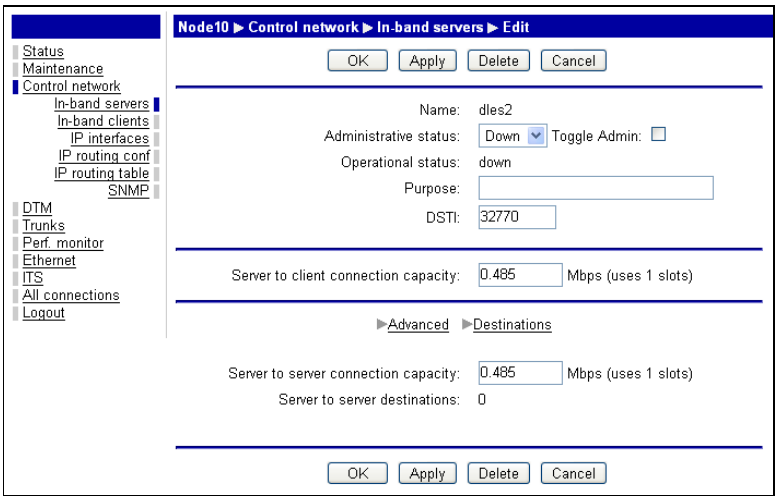


Figure 66. In-band Servers Edit page

To activate the DLE server, set the Administrative status in the drop-down menu to Up and enter the DSTI and the capacity of the server to client. Also enter the capacity between servers (Server to server). To save, click 'Apply' or 'OK'.

8.6.3.2 *Peering DLE Server*

Click on the link Destinations and then Add destinations …, in order to add one or more destination(s) to peering servers.

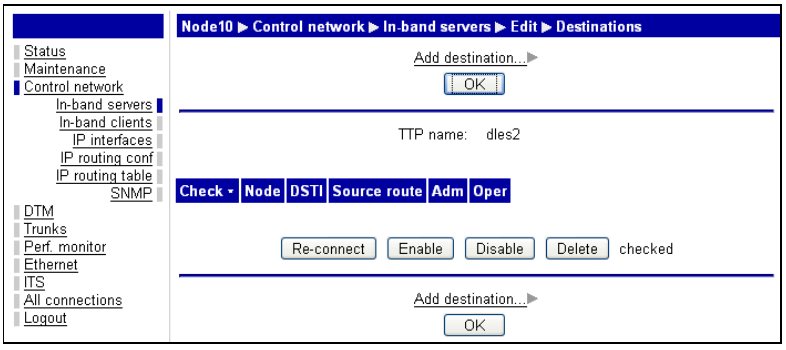


Figure 67. In-band Servers page

Select the appropriate tick boxes and click on the correct button

Re-connect: if the secondary path is used, the switch examines if it is possible to use the primary path. If it is, it reverts to the primary path.

Enable: Enables the checked destination(s)

Disable: Disables the checked destination(s)

Delete: Deletes the checked destination(s)

Observe that these destinations define server-to-server connections and not server-to-client connections.

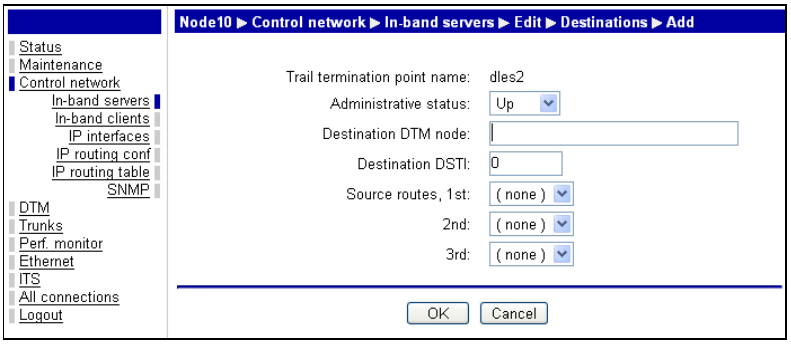


Figure 68. In-band Servers page

Enter Administrative status, Destination DTM node address, Destination DSTI and select if source routes should be used. Click on OK to set the server destination.

8.7 In-band clients

An In-band client must be configured on every node in the segment, including the node(s) with the In-band server. The web page where the configuration is made is found by following the Control → In-band client link.

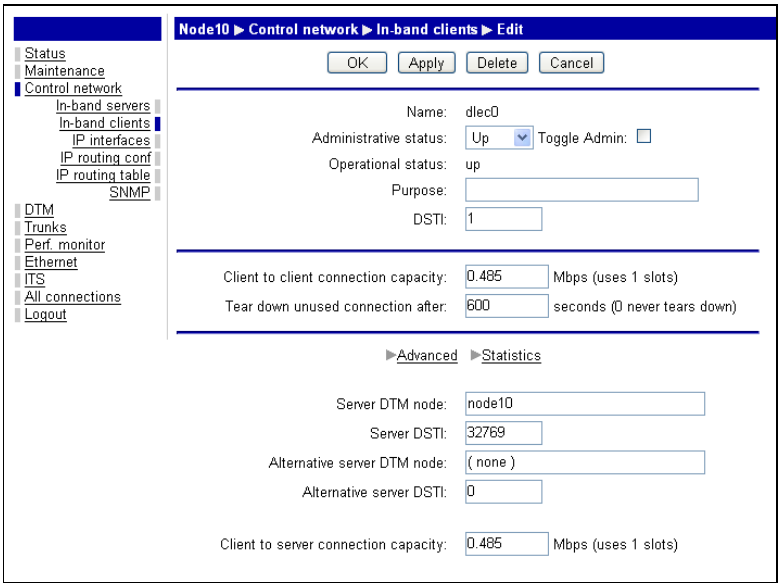


Figure 69. In-band client configuration page

8.7.1 Configuration parameters for In-band clients

8.7.1.1 Administrative status

Default value: 'Down'

Type: Boolean variable (only two states possible)

Range: 'Down', 'Up'

Description: The parameter determines if the client is thought to be active (Up) or inactive (down).

8.7.1.2 Purpose

Default value: Empty string

Type: String variable

Range: Length 0-255 characters

Description: The parameter is an arbitrary character string that can be used for identification purposes.

8.7.1.3 DSTI (DTM Service Type Instance)

Default value: 0 for first defined client on the node, 1 for the second etc

Type: Integer

Range: 0-65535

Description: The parameter is the instance number of the DLE client, i.e. the identifier of this particular service. It is recommended to keep the default value.

8.7.1.4 Client to Client connection capacity

Default value: 0.485 Mbps, i.e. one slot per frame

Type: Real number

Range: 0 to the capacity of the trunk between server and client

Description: The capacity between the client and other clients.

8.7.1.5 Tear down unused connection after

Default value: 600 seconds

Type: Integer

Range: 1 – 9999999

Description: The time after which an unused connection is torn down. Zero is a special value that means that the link is never torn down.

8.7.1.6 *Server DTM node*

Default value: none

Type: DTM address or hostname of DLE server

Range: 00.00.00.00.00.00.00.00 - FF.FF.FF.FF.FF.FF.FF.FF or hostname

Description: The DTM address or hostname of the In-band (DLE) server.

8.7.1.7 *Server DSTI*

Default value: 0

Type: Integer

Range: 0-65535

Description: The parameter is the instance number of the DLE server that the defined client attaches to. Observe that this default is different than the default setting of the server itself (which is 32769).

8.7.1.8 *Alternative Server DTM node*

Default value: none

Type: DTM address or hostname of back-up In-band (DLE) server.

Range: 00.00.00.00.00.00.00.00 - FF.FF.FF.FF.FF.FF.FF.FF or hostname

Description: The DTM address or hostname of the back-up In-band (DLE) server.

8.7.1.9 *Alternative Server DSTI*

Default value: 0

Type: Integer

Range: 0-65535

Description: The parameter is the instance number of the alternative DLE server that the defined client attaches to.

8.7.1.10 *Client - server connection capacity*

Default value: 0.485 Mbps, i.e. one slot per frame

Type: Real number

Range: 0 to the capacity of the link between the client and the server/back-up server.

Description: The capacity between the client and the server.

The Advanced settings are identical to those of the In-band server; see section *Setting up In-band servers* for additional information.

To set the parameters, select the web page by following the link Control Networks → In band Clients, chose the values and click on 'Apply' or 'OK'.

8.8 Bandwidth requirements of DLE

The bandwidth required by the In-band control function can be divided into three different parts: server-to-client connections, client-to-server connection and client –to-client connection. In the illustration, the server and gateway are both located on node A. Nodes B and C have each a client connected to the server.

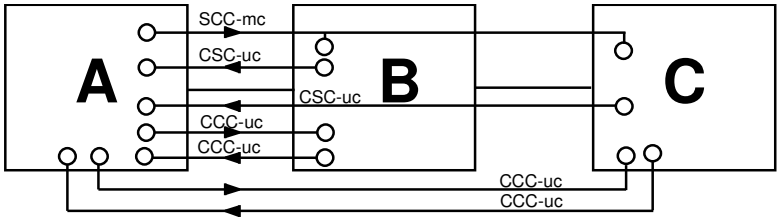


Figure 70. Bandwidth requirement example. Node A has a DLE server and is the gateway to the outside world. Nodes B and C each run a DLE client.

SCC - Server to Client Connection is a multicast channel. This channel is up all the time. If all clients are on a long chain, this channel takes one slot on every link.

CSC - Client to Server Connection is the return channel from the client to the server. This channel is a unicast channel and the server terminates one channel from each client connected to the server. This return channel is always up.

CCC - Client to Client Connection is a unicast channel which is established between two DLECs. This is the channel where normally all traffic between the clients travels. The channel is by default torn down after 600 seconds without transmitted data and is automatically reestablished when there is new traffic. The channel normally exists between the gateway and all DLECs. If Nimbra Vision is used, this channel stays up all the time since NV polls every node every 120 seconds. It is possible to force data traffic to use SCC and CSC (all data traffic is routed via the DLES server) by setting the CCC bandwidth to zero slots on all DLECs. However, if CCC is configured to use zero slots, there is a risk that DLES is overloaded with too much data and the result might be that the DLE server crashes.

In our example, the bandwidth requirement is:

From A to B 1 SCC + 2 CCC = 3 DLE slots

From B to A 2 CSC + 2 CCC = 4 DLE slots

Note that the CCCs between nodes B and C are omitted in the illustration.

8.9 IP interfaces

IP interface menu configures the physical and logical Ethernet address of the interface as well as the IP address for all logical In-band clients. This section describes how to change the address of the physical and logical Ethernet interface and also how to change the netmask of the subnet.

Follow the Control Networks → IP interfaces web page.

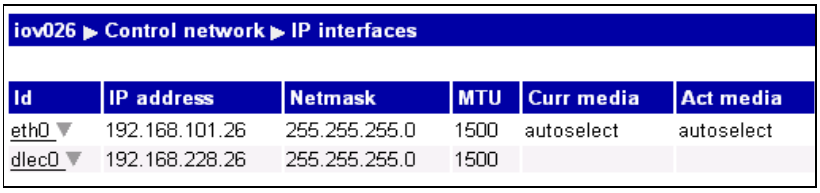


Figure 71. IP interfaces page

eth0: The physical address of the Ethernet interface.

dlec0: The logical address of the In-band client.

Click on the Id of the interface that should be changed.

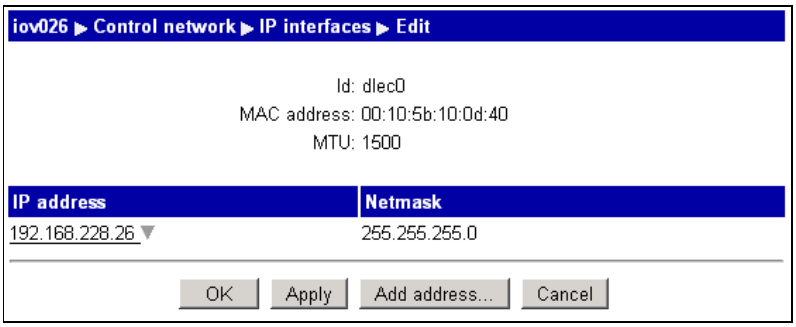


Figure 72. IP address page

Click on the IP address and make the changes to the address and the netmask. Alternatively, click on the 'Add address...' button in order to add a valid IP-address.

Note: 	Certain settings of IP address will make further contact with the node impossible. This should be considered before the 'OK' or 'Apply' button is clicked.

8.10 IP routing configuration

8.10.1 Routes

In order to enable routing outside an In-band segment, routes have to be configured from the segment to the wider network. Some default routes are always configured in a node, e.g. to the subnet of a configured Ethernet interface and to the loopback interface.

Note: 	An IP route must be configured on every node in the DLE segment. It will tell the node where to send IP traffic to a node outside the DLE segment.

Click on the Control Networks → IP routing table links to get an overview of the defined IP routes.

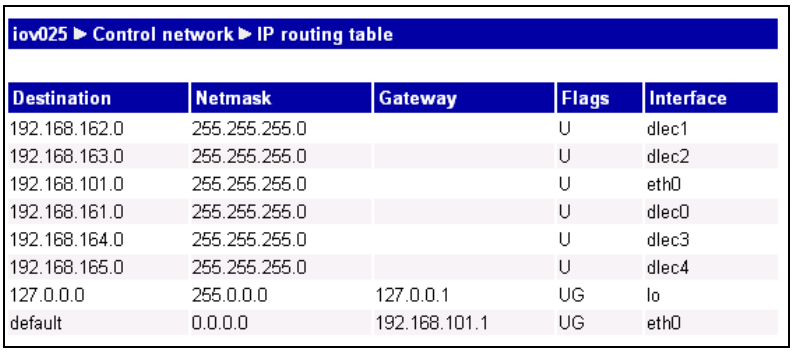


Figure 73. IP routing table page. Default means all addresses not otherwise mentioned.

U means that the routing entry is up, in other words active. G means that in order to reach the destination you should use the gateway that is "pointed out" by the routing entry.

The first six entries describe that you can reach 192.168.101.0, 192.168.161.0, 192.168.162.0, 192.168.163.0, 192.168.164.0 and 192.168.165.0 directly without gateway. The seventh entry, 127.0.0.0 is for the local host, which always will be there. The last entry describes how to reach all other IP-addresses (i.e. through the gateway 192.168.101.1).

8.10.2 Setting up IP routes

The configurable parameters for a route are:

Parameter	Description	Type
Destination	The destination IP network that the route will use. 0.0.0.0 is displayed as default	Mandatory
Netmask	The network mask to apply for the destination network. E.g. netmask 255.255.255.0 (or netmask 0.0.0.0 for the default route)	Mandatory
Gateway	The IP address of the node that is connected to the outside network.	Mandatory

Figure 74. Configurable routing parameters

Click on the Control Networks → IP Routing Conf link. The IP routing conf page appears. This page contains the configured IP routes on the node.

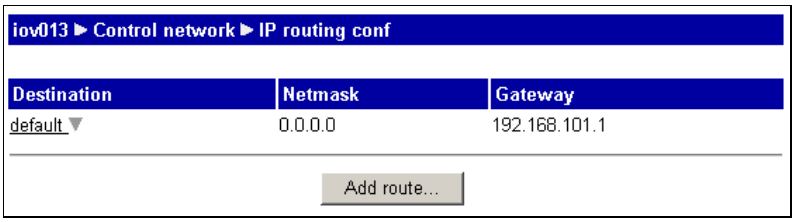


Figure 75. IP routing configuration page; default means 0.0.0.0, i.e. all addresses.

Click on the Add route link, the Add page appears.

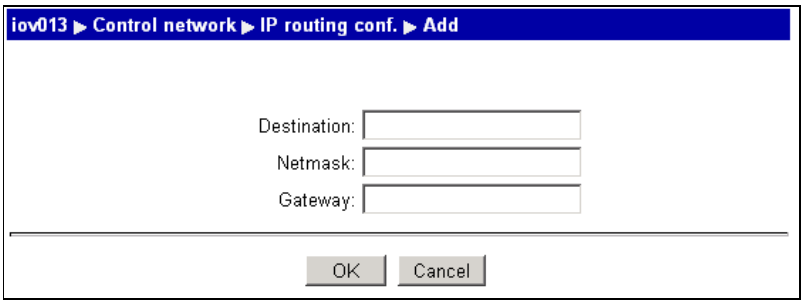


Figure 76. Add IP route

Enter the parameters and click on 'OK'. The Routing configuration page reappears with one new entry.

8.10.3 IP route reconfiguration

To reconfigure an IP route, follow these steps:

Navigate to web page Control Networks → IP Routing conf and click on the route to be verified or reconfigured. The Edit page appears.

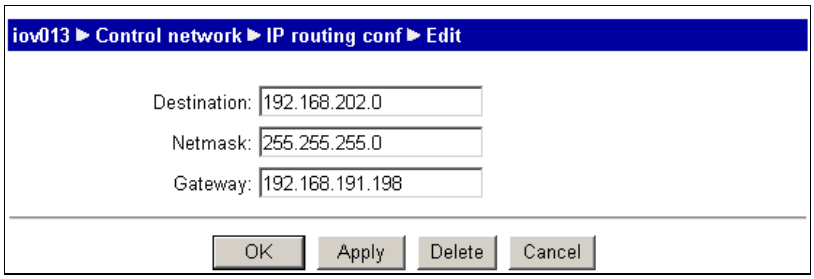


Figure 77. Edit IP route

Make the settings and click 'OK' or 'Apply'. To delete the route, click on 'Delete'. The Routing configuration page reappears modified.

If required, back up the configuration changes to the node controller.

Note that asymmetric routing may cause problems with SNMP/telnet/ftp.

8.11 SNMP configuration

This chapter describes the SNMP (Simple Network Management Protocol) configuration for the network element. It describes setting up of community names, SNMPv3 user, and notification receivers.

Click on the Control Network → SNMP link. The SNMP configuration page appears.

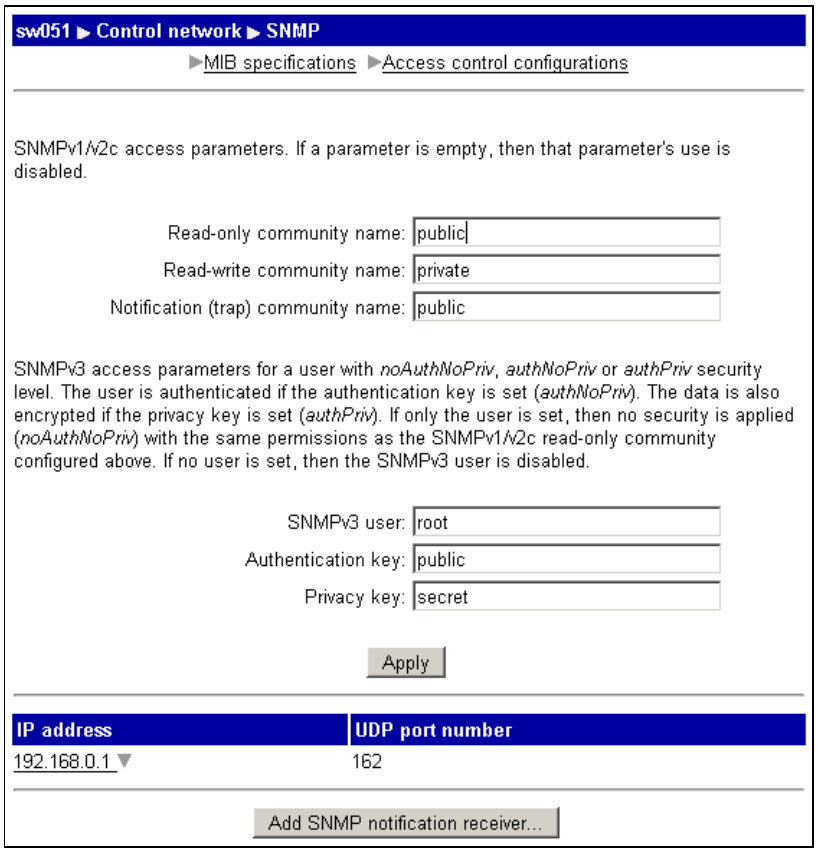


Figure 78. SNMP configuration page

The page shows information about the SNMP community names and user configuration. The SNMP agent is a full SNMPv1/v2c/v3 agent that supports SNMPv3 security levels *noAuthNoPriv*, *authNoPriv* and *authPriv*. It also shows the configured notification receivers.

Read-only community name is the community name for SNMPv1/v2c read (i.e. get) operations. If set, then get operations using this community is accepted, while write (i.e. set) operations are not accepted using this community.

Read-write community name is the community name for SNMPv1/v2c read (i.e. get) and write (i.e. set) operations. If set, then SNMPv1/v2c read and write operations using this community are accepted.

Notification (trap) community name is the community used when sending notification. If set, notifications are sent as SNMPv2 traps with this community.

SNMPv3 user is a user name used in SNMPv3 communication with the node. If set, SNMPv3 operations using this USM user are accepted using a security level that depends on the Authentication key and the Privacy key, as described below.

Authentication key is the passphrase used for SNMPv3 authentication of the SNMPv3 user. If empty, then the authentication check is disabled, e.g. security level is *noAuthNoPriv*. If set, but the Privacy key (see below) is not set, then only authentication check is done, e.g. security level is *authNoPriv*, If set, and the Privacy key is set, then authentication check is done, and the data is encrypted, e.g. security level is *authPriv*.

If authentication check is disabled, then the user has read-only permission, just as if using SNMPv1/v2c with the Read-only community name. If authentication check is enabled, then the user has read/write permission, just as if using SNMPv1/v2c with the Read-write community name.

Privacy key is the passphrase used for SNMPv3 encryption. If set, SNMPv3 operations are also encrypted, e.g. security level is *authPriv*. To use encryption, then the Authentication key must also be set.

The page also shows information about the SNMP notification receiver configuration as follows. A notification receiver is the management station that will process notifications (SNMP traps) sent from the network elements. You may send notifications for multiple management stations.

IP address shows the IP addresses of the configured SNMP notification receivers. UDP port number shows the UDP (user data protocol) port number for the notification receivers. 162 is the standard port and configured as default port.

The link Access control configurations opens a page that allows for advanced configuration of the SNMP agent, including setting up a detailed access control.

The link MIB specifications opens window from where it is possible to download the Net Insight enterprise MIB specifications supported by the network element.

8.11.1 Addition of an SNMP notification receiver

Follow the link Control Network → SNMP and click on the button 'Add SNMP notification receiver …'. The Add SNMP notification receiver page appears.

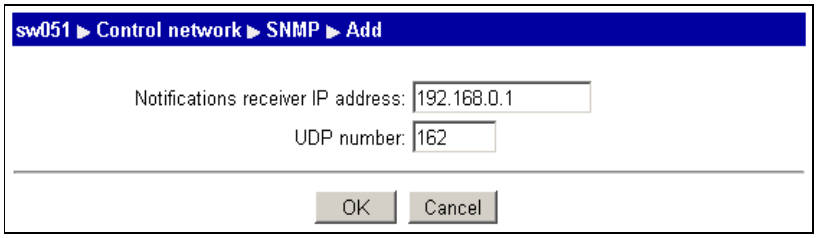


Figure 79. Add SNMP notification page

Add the IP address and UDP port number for the trap receiver.

Click 'OK' to add the new notification receiver. The configuration page will be loaded again, updated with the new notification receiver.

8.11.2 Editing or deleting a SNMP notification receiver

Follow the link Control Network → SNMP and click on the IP address of the notification receiver that should be edited or deleted.

In the page that appears, the IP address and UDP port number can be changed. Edit the IP address and UDP port number and click on the 'OK' or 'Apply' button to execute the change.

To delete the notification receiver, click the 'Delete' button. The configuration page is loaded with the notification receiver removed.

8.11.3 Access control and advanced setup

Advanced configuration of the SNMP agent is done from the Access control configurations link. It is suggested that this option is only used by experienced and knowledgeable users of SNMP agent configuration.

Generally, this page is used for setting up the Local Configuration Datastore (LCD) of the SNMP agent. The LCD describes the configuration of the SNMP agent. All of the SNMP agent configuration can be done using this page. But because the most common configuration of the agent is the setting of community names, the SNMPv3 user, and the notification receivers, the setting up of that data is preferably done using the SNMP page instead. However, the configuration done on the SNMP page is internally processed as if entered directly into the LCD.

Please refer to section *SNMP page internal data* below for a description on how the form on the SNMP page is internally represented and related to the LCD.

The default configuration of the LCD adds configurations to the SNMP agent, which are used by the community names, SNMPv3 user, and the notification receivers configured on the SNMP page. Modifications and additions to the configuration can be done here.

The following is the default configuration:

Access entries for the *notifiers*, *readers*, *writers*, *authUsers* and *privUsers* principals are configured from the SNMP configuration page. These define the permissions for the different principals. You can modify these entries to change the permissions of these community names and SNMPv3 users.

A family tree, *All,* which includes all the OIDs, is used when setting up the access entries.

Entries that define how notifications (traps) are sent are included.

The configuration is done using entries in a text box.

To edit the SNMP agent configuration, select the link Access control configurations from the SNMP configuration page. The Access control configurations page appears.

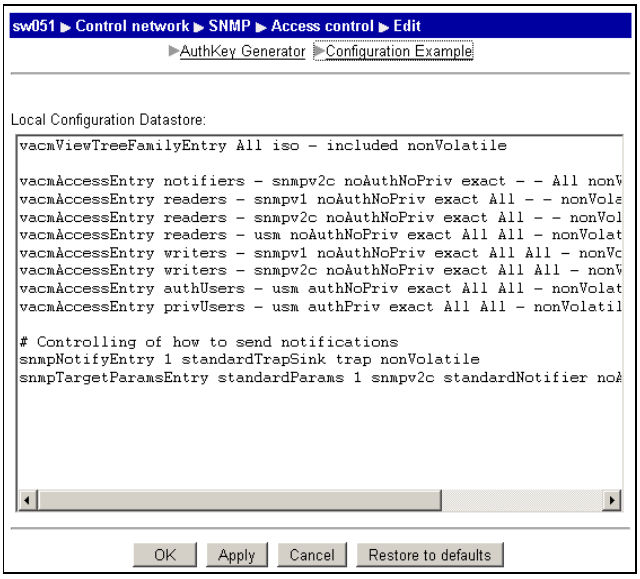


Figure 80. Access control configurations page

Modify the configuration in the Local Configuration Datastore text box. The button 'Restore to defaults' loads the default configuration into the text box. To apply the new configuration, click the 'Apply' (or 'OK') button.

When the configuration is applied, it will pass a syntax control. If the configuration contains syntax errors, the page will be reloaded with errors shown.

The link AuthKey Generator opens a window where an authentication key or privacy key can be encoded for use in the LCD.

8.11.4 SNMP page internal data

Setting up data on the SNMP page is equivalent to setting up data on the 'Access control configurations' page. This section describes how the equivalent setup on this page corresponds to the form on the SNMP page.

Note that the entries here assume at least the default configuration in the LCD, as the definitions in the LCD are referred to from the internal entries.

Setting of a Read-only community name with the value public on the SNMP page is equivalent to:

```
snmpCommunityEntry 1 public standardReader localSnmpID \
   - - nonvolatile
vacmSecurityToGroupEntry snmpv1 standardReader readers
nonvolatile
vacmSecurityToGroupEntry snmpv2c standardReader readers
nonVolatile
```

Setting of Read-write community name with the value private on the SNMP page is equivalent to:

```
snmpCommunityEntry 2 private standardWriter localSnmpID \
   - - nonvolatile
vacmSecurityToGroupEntry snmpv1 standardWriter writers
nonvolatile
vacmSecurityToGroupEntry snmpv2c standardWriter writers
nonVolatile
```

Setting of Notification community name with the value public on the SNMP page is equivalent to:

```
snmpCommunityEntry 3 public standardNotifier localSnmpID \
   - - nonvolatile
vacmSecurityToGroupEntry snmpv2c standardNotifier \
   notifiers nonVolatile
```

Setting of SNMPv3 user name, authentication key and privacy key on the SNMP page is equivalent to one of the following entries, depending on the entered data. When entering user name root only:

```
usmUserEntry localSnmpID root usmNoAuthProtocol \
   usmNoPrivProtocol nonVolatile - - -
vacmSecurityToGroupEntry usm root readers nonVolatile
```

or when entering authentication key public:

```
usmUserEntry localSnmpID root usmHMACMD5AuthProtocol \
   usmNoPrivProtocol nonVolatile – public –
vacmSecurityToGroupEntry usm root authUsers nonVolatile
```

or when also entering privacy key secret:

```
usmUserEntry localSnmpID root usmHMACMD5AuthProtocol \
usmDESPrivProtocol nonVolatile – public secret
vacmSecurityToGroupEntry usm root privUsers nonVolatile
```

Setting of Notification receiver with IP address 192.168.0.1 and port 162 adds the following per added notification receiver. The *index* will always be an integer value unique per entry.

```
snmpTargetAddrEntry index snmpUDPDomain 192.168.0.1:162 1500
3 \
   standardTrapSink standardParams nonVolatile
255.255.255.255:0 2048
```

8.11.5 Format of SNMP configuration

The Local Configuration Datastore (LCD) is represented by a text format, where each line represents an entry. Actually, an entry in the LCD is representing an entry in an SNMP table. The different field for an entry represents columnar objects in the tables. The format of an entry is in general:

Keyword value…

The keyword represents the type of entry, and the value is a list of fields in the entry separated by spaces. The keyword is actually describing what SNMP table to configure, and the field values are the columnar objects.

Entries may span multiple lines by using a backslash (\) at the end of the entry's lines.

White-space (space) is ignored.

String values that contain blanks must be delimited by quotation marks (").

A line is considered a comment and ignored if it starts with a hash (#).

Some fields shall have an OBJECT IDENTIFIER as the value. An OBJECT IDENTIFIER is the complete OID from the root or the MIB tree, written as numbers separated by dots. E.g. an OBJECT IDENTIFIER for the sysName object defined in the MIB-2 systems group would be `1.3.6.1.2.1.1.5`.

If the OBJECT IDENTIFIER is not part of an enterprise specific object, the OBJECT IDENTIFIER may be substituted by its name. The sysName object would thus be `sysName`. It is possible to start the OBJECT IDENTIFIER with a substituted name, and continue with the remaining fields. The sysName could be written as `system.5` because system represents 1.3.6.1.2.1.1, or as `mib-2.1.5`. Similar, all the enterprise MIB objects can start with `enterprises`, as this represents 1.3.6.1.4.1.

The following entry keywords are supported. For full description on the meaning of the entry, please refer to the description in the corresponding RFC.

Keyword	See also
snmpCommunityEntry	RFC3584
usmUserEntry	RFC3414
vacmViewTreeFamilyEntry	RFC3415
vacmAccessEntry	RFC3415
vacmSecurityToGroupEntry	RFC3415
snmpNotifyEntry	RFC3413
snmpTargetAddrEntry	RFC3413
snmpTargetParamsEntry	RFC3413
snmpNotifyFilterEntry	RFC3413
snmpNotifyFilterProfileEntry	RFC3413

Figure 81. SNMP table entries as keywords

8.11.6 Configuration Procedure

The configuration procedure involves the following steps:

Define an SNMPv3 user or community.

Define a family of view sub-trees, MIB views. The MIB view defines a set of managed information that may be accessed.

Define a group and with associated access rights. The group is assigned the MIB views for read, write and notification access.

Assign SNMPv3 user or SNMPv1/v2c community names to the group.

The associations between the MIB views, the groups and the principals (users/community names) are shown in the figure below.

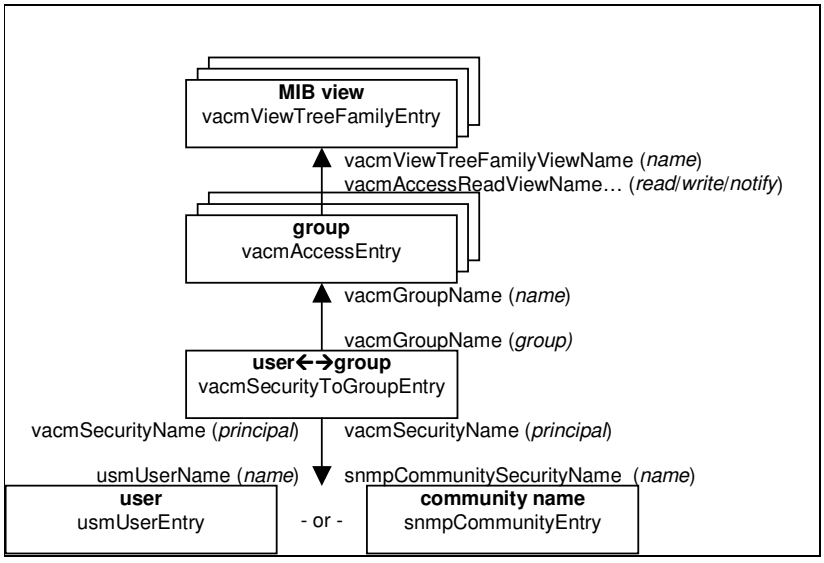


Figure 82. MIB views, groups and users or community names

8.11.7 Defining SNMPv3 Users

At least one SNMPv3 user must be configured for the SNMP agent to send and receive SNMP messages using the SNMPv3 protocol. (SNMPv1 and SNMPv2c do not have users. Instead they have community names, see section *Defining Community*.) The preferred way to define a user is to use the **SNMP** page.

A user is defined in the User-based Security Model, USM.

Note that an USM user is not the same as the element manager users used for the CLI or web access of the Nimbra network element. Hence, the users defined for the element manager are not known by the SNMP agent, and the element manger does not know about the USM users.

A user entry is represented by the tag **usmUserEntry**. The format of the entry is:

```
usmUserEntry engineID name authProtocol privProtocol storage
target authKey
```

engineID is always **localSnmpID**, which represents the SNMP agent's administratively-unique identifier.

name is the user name, as a human readable string of up to 32 characters.

authProtocol is the authentication protocol that must be used when sending and receiving messages for this user. The authentication protocol is used to authenticate the user. The value is **usmNoAuthProtocol** if no authentication protocol shall be used, **usmHMACMD5AuthProtocol** if HMAC-MD5 protocol shall be used, or **usmHMACSHAAuthProtocol** if HMAC-SHA shall be used. (This value is actually an OBJECT IDENTIFIER that represents the authentication protocol.)

privProtocol is the privacy protocol that must be used when sending and receiving messages for this user. The privacy protects the messages from disclosure. The value is **usmNoPrivProtocol** if no privacy protocol shall be used, or **usmNDESPrivProtocol** if CBC-DES shall be used. (This value is actually an OBJECT IDENTIFIER that represents the privacy protocol.)

storage describes how the entry is stored. This is always **nonVolatile**.

target is always a dash (**-**).

authKey is the user's authentication password. If no authentication protocol is used, the value shall be a dash (**-**). (The password is converted to a key at run-time.) The password can be given in clear text , or as an encrypted string. To encrypt the password, use the Auth Key Generator on the Edit Access Control page.

8.11.8 Defining Community

At least one SNMPv2 community must be defined for the SNMP agent to send and receive SNMP messages using the SNMPv1/v2c protocols. The preferred method to define community names is using the **SNMP** page.

```
snmpCommunityEntry index community name engineID conext
target \
   storageType
```

index is a unique index string. It does not mean anything, but must be unique.

community is the community name string that will be used.

name is the name of this entry, and will be used as the *principal* to refer to the entry when setting up the security, see *Defining Groups and Access Rights*.

engineID is always **localSnmpID**, which represents the SNMP agent's administratively-unique identifier.

context is the name of the context to which the group is part of. To gain access by this entry, the specified context must be in use. On the Nimbra network elements, the context is always the default context, which is represented by a dash (**-**).

target is always a dash (**-**).

storage describes how the entry is stored. This is always **nonVolatile**.

8.11.9 Defining MIB Views

A family of view sub-trees is a definition that includes or excludes managed information forms a MIB view. A MIB view is used for defining a set of managed information that may be accessed. The definition of the family view of sub-trees may include wildcards. If no wildcards are used, the family of view sub-trees becomes a single sub-tree.

If there are multiple sub-trees defined, then the one with most sub-identifies in its OID is used. If multiple sub-trees are defined with the same number of sub-identifiers, then the lexographically greatest is used.

A MIB view is represented by one or multiple sub-trees. An entry is represented by the tag **vacmViewTreeFamilyEntry**. The format of the entry is:

```
vacmViewTreeFamilyEntry name subtree mask type storageType
```

name is the human readable name for a family of view sub-trees, i.e. the name for the MIB view. This is a printable string of no more than 32 characters. Multiple entries may define one MIB view, which in this case all must have the same *name*. The name is used when defining groups (see *Defining Groups and Access Rights*).

subtree is an OBJECT IDENTIFIER that identifies a sub-tree of the MIB, i.e. what managed objects to include or exclude from the MIB view. The sub-tree is combined with the *mask*.

mask is a bit mask which, in combination with the *subtree* defines a family of view sub-trees. The bit mask is represented as a sequence of hexadecimal bytes separated by colons. Each byte is within the range 0x00 to 0xff. A zero-length string is represented by a dash (–).

The bit mask is a series of zeros and ones, where the zeros represent wildcards, and the ones represent an exact match. The bit mask is applied on the *subtree*, where the first bit masks the first sub-identifier, and so on. The bits are grouped to bytes, which are represented by the substring **00** through **ff**, and are all separated by colons (**:**). The last byte is padded with ones at the end to fill out to a complete byte.

type indicates whether the entry shall define a family of sub-trees that shall be included or excluded from the MIB view. The value of this field is **`included`** or **`excluded`**.

storageType describes how the entry is stored. This is always **`nonVolatile`**.

8.11.9.1 Example 1

The example defines a view names "All" that allows access to everything (actually, everything under the 1 branch in the MIB tree).

```
vacmViewTreeFamilyEntry All iso - included nonvolatile
```

8.11.9.2 Example 2

The example defines a view named "noIfTable", that allows access to everything except to the ifTable.

```
vacmViewTreeFamilyEntry noIfTable iso - included nonvolatile
vacmViewTreeFamilyEntry noIfTable 1.3.6.1.2.1.2.2 - excluded
\
   nonVolatile
```

8.11.9.3 Example 3

The example shows how to define a family of view subtrees that only allows access to row 9 in the ifTable. The 10th bit is a zero, which makes the 10th sub-identifier in the subtree a wildcard (don't care). This is the columnar object.

Parameter	Byte 1		Byte 2	
full subtree (OID)	1.3.6.1.2.1.2.2.1.0.9			
subtree (OID)	1.3.6.1	2.1.2.2	1.0.9	
mask	1111	1111	101	
padded mask	1111	1111	1011	1111
mask in hexadecimal	0xff		0xbf	
mask as value	ff:bf			

Figure 83. Parameters for a family of view subtrees

```
vacmViewTreeFamilyEntry if9 1.3.6.1.2.1.2.2.1.0.9 ff:bf
included nonVolatile
```

8.11.10 Defining Groups and Access Rights

A group is associating the MIB views with access rights A group is represented by one or multiple entries, for different accesses. An entry is represented by the tag **`vacmGroupName`**.

```
vacmAccessEntry name prefix model level match read write
notify storageType
```

name is the name of the group. The name is a string of up to 32 characters. The is used when associating access rights to users (see *Assigning Users*).

prefix is the name of the context to which the group is part of. To gain access by this entry, the specified context must be in use. On the Nimbra network elements, the context is always the default context, which is represented by a dash (**-**). (The prefix could be the complete name of the context, or the prefix of a context, as defined by *match*; see below.)

model is the security model to which the group belongs. In order to gain access by this entry, the specified security model must be in use. The security model can be `snmpv1`, `snmpv2c` or `usm` for SNMPv3 using the USM.

level is the minimal security level. In order to gain access by this entry, the security level in use must at least be the specified security level. The value is `noAuthNoPriv` if no authentication shall be required, and `authNoPriv` if authentication using HMAC-MD5 is required. If multiple entries are equally indexed, except for this value, then the one with the highest security level is applied.

match specifies how the *prefix* shall be matched. For the Nimbra network elements, it does not make sense to set the value to anything except `exact`. The value can be `exact` of `prefix`.

read is the name of the MIB view (see *Defining MIB Views*) that shall be used to control what management information can be read. In order to gain read access by this entry, the MIB view must allow access of the management information.

write is the name of the MIB view (see *Defining MIB Views*) that shall be used to control what management information can be written. In order to gain write access by this entry, the MIB view must allow access of the management information.

notify is the name of the MIB view (see *Defining MIB Views*) that shall be used to control what management information can be included in a notification. In order to gain read access for notifications by this entry, the MIB view must allow access of the management information.

storageType describes how the entry is stored. This is always `nonVolatile`.

8.11.10.1 ***Example***

```
vacmAccessEntry FullAccessUser - usm authNoPriv exact All All
All onVolatile
```

The example defines a group named "FullAccessUser" that requires the user to have at least the security level "authNoPriv" (authenticated, but not encrypted). The group permits access to the MIB view "All" for read (responding to snmp-get operations), write (accept snmp-set operations) and for notifications.

8.11.11 Assigning Users

A user must be associated with a group, where the group defines the access rights for the user. For SNMPv1 and SNMPv2c, which do not have the user concept, the community name is used instead.

An entry maps a security model and its user or community name to a group. An entry is represented by the tag `vacmSecurityToGroupEntry`.

```
vacmSecurityToGroupEntry model principal group storage
```

model defines the security model for the entry. The model is either `snmpv1`, `snmpv2c` or `usm`.

principal is the user name for the security model USM (see *Defining SNMPv3 Users*), or the security name that represents the community name for SNMPv1/v2c. A default security name is public. The community name for the public security name is modified from the web page Status | SNMP config.

group is the name of the group (see *Defining Groups and Access Rights*) to which the user or community name shall be associated.

storage describes how the entry is stored. This is always `nonVolatile`.

8.11.11.1 Example 1

The example associates the USM user "root" with the group "FullAccessUser".

```
vacmSecurityToGroupEntry usm root FullAccessUser nonVolatile
```

8.11.11.2 Example 2

The example associates the community name "public" for SNMPv2 access to the group "ReadOnlyUser".

```
vacmSecurityToGroupEntry snmpv2c public ReadOnlyUser
nonvolatile
```

9 DTM Configuration

9.1 Overview of DTM configuration

This chapter describes how to use the web interface to configure monitor the DTM-layer. The start web page for DTM is shown below.

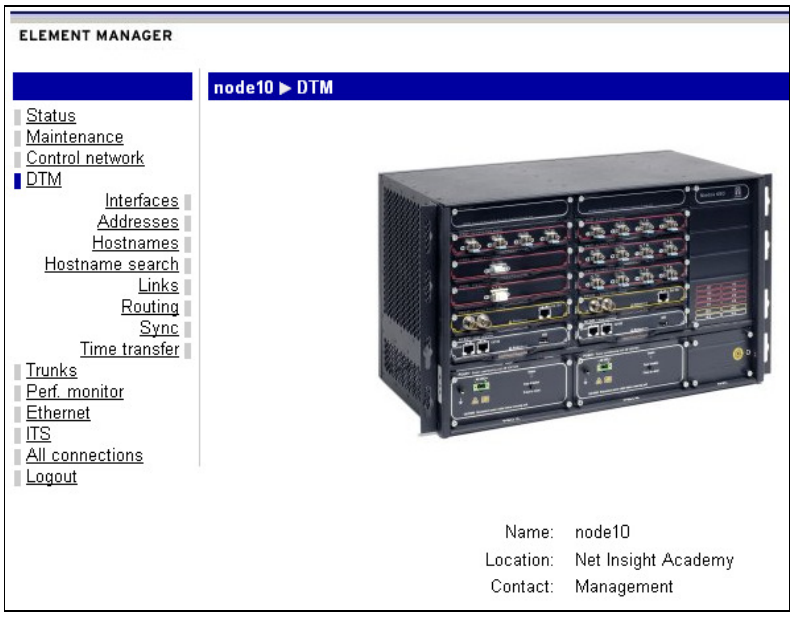


Figure 84. The start web page for DTM

The sub-sections (links) are: Interfaces, Addresses, Hostnames, Hostname search, Links, Routing, Sync and Time transfer.

Note:	Make sure to have all the information that the operation requires, before starting any configuration operation. This will help you to minimize any downtime of the system.

9.2 Interfaces

The starting web page for Interfaces is presented.

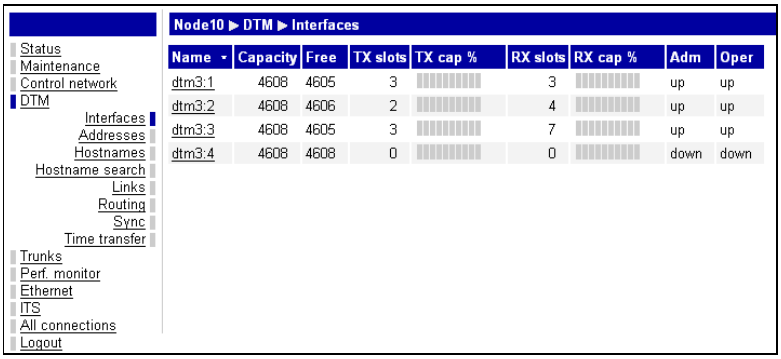


Figure 85. DTM interfaces page

The table lists the DTM interfaces that are present in the unit. For each interface the following is presented: Name (name of the interface), Capacity (in slots), Free (unused capacity, in slots), Tx slots (used slots in the Tx direction) and Tx cap % (used slots in per cent in the Tx direction), Rx slots and Rx cap % (used slots in the Rx direction). In addition, Adm and Oper shows the Administrative and Operational state of the interface. The interface name is written as “dtmX:Y”, where X is position of the card and Y position of the port, on the card.

9.2.1 Editing a DTM interface

To edit a DTM interface, click on the Name of the interface that should be edited.

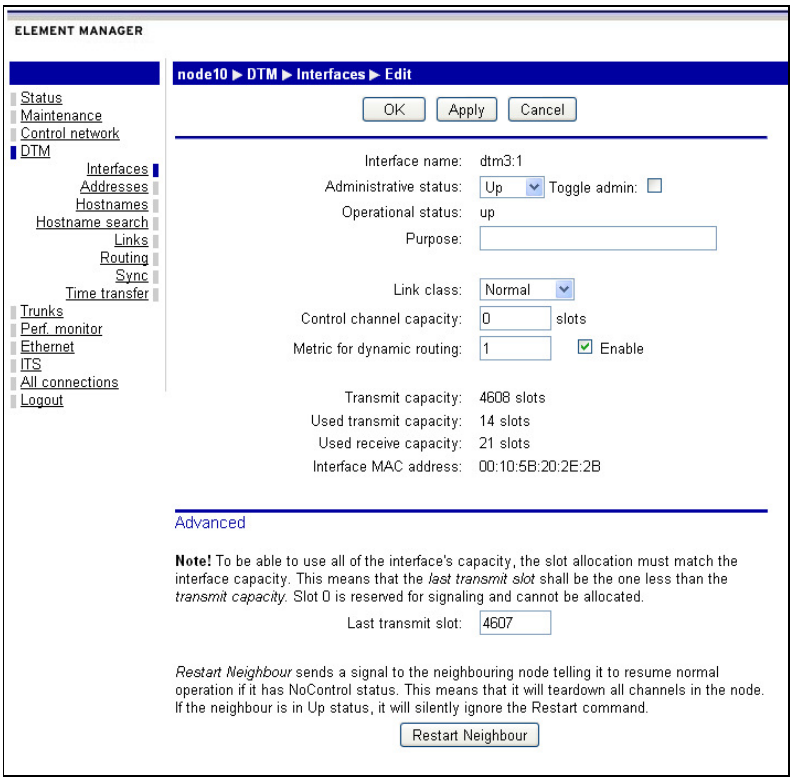


Figure 86. DTM Interface, Edit page, top part

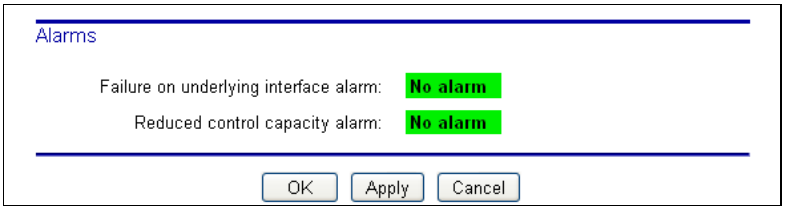


Figure 87. DTM Interface, Edit page, bottom part

The configurable parameters are:

Parameter name	Description	Type
Admin. status	The administrative status of the board.	Mandatory
Toggle Admin	The Toggle Admin option automatically sets the Administrative status to Down momentarily and then to Up again.	Optional
Link class	Normal, Persistent or Nailed. See persistent channels for description.	Mandatory
Control channel capacity	Bandwidth of the control channel, expressed in slots per DTM-frame (1 slot = 512 kbit/s)	Mandatory
Metric for dynamic routing	The cost of using this interface when dynamic routing is used.	Mandatory
Enable	Mark Enable, if dynamic routing should be used.	Mandatory
Last transmit slot	Selects the last slot used for payload. Must be between one plus first transmit slot to one minus transmit capacity.	Mandatory

Figure 88. Configurable parameters for a DTM interface

Read-only parameters are:

Parameter	Description
Interface name	The interface id, written as “dtmX:Y” (where X is position of the card and Y position of the port).
Oper. status	The operational status of the board.
Transmit capacity	The total number of time slots available for transmission on this interface.
Used transmit capacity	The number of used time slots from this node to the peering node.
Used receive capacity	The number of used time slots from the peering node to this node.
Interface MAC address	A globally unique hardware identifier for this interface card.
Failure on underlying interface alarm	An error reported by the underlying trunk interface. (LOF loss of frame.)
Reduced control capacity alarm	The node is not able to signal the remote node. This usually indicates a problem in the TX direction for the link.

Figure 89. Read-only parameters (variables) of a DTM interface

9.3 Addresses

This chapter describes how to configure the DTM addresses of the unit. The DTM address must be configured before any configuration of services can be done.

Each node can have one primary DTM address and several alias addresses. The primary address (marked with a symbol in the “Primary address” column), in the table below, is always used as the source address when the node establishes a channel. In addition to the primary address, a node also accepts channels to all its alias addresses.

The address “00.00.00.00.00.00.00.01” is a loop back address that all nodes listen to. It is equivalent to the address 127.0.0.1 in an IP-node.

Click on the DTM menu item and then click on Addresses. The Addresses page appears.

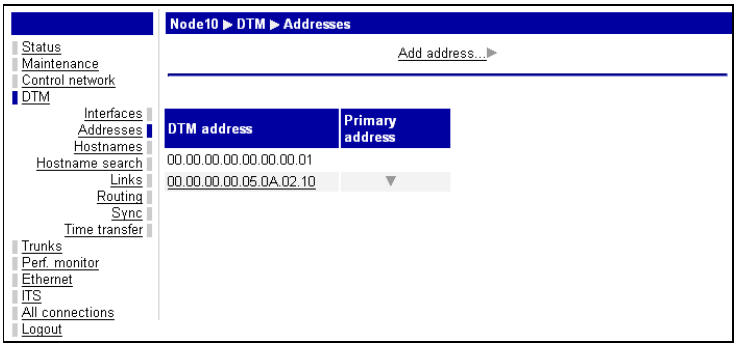


Figure 90. DTM address page

The table shows information of the configured addresses as follows:

DTM address: The configured DTM address for the unit and one loopback (always 00.00.00.00.00.00.00.01) address to the back plane.

Primary address: Shows which address is the primary address for the node. Note that a node can only have one primary address.

9.3.1 Adding a DTM address

Go to the DTM addresses page and click on the Add address link. The ‘Add address’ page appears.

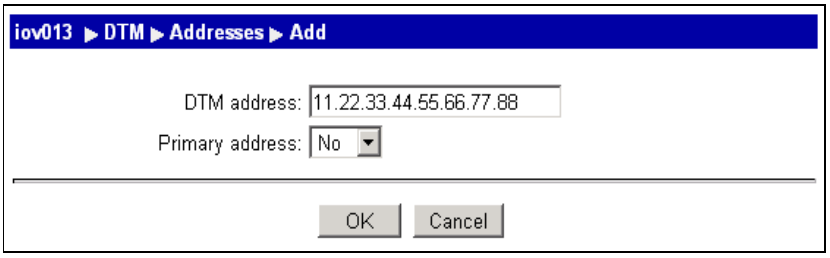


Figure 91. Add DTM address page

Enter the DTM address and whether the address is Primary or not and then click ‘OK’. The DTM addresses page will reappear with the new address listed in the table.

Back up the configuration changes and restart the node.

9.3.2 Editing or deleting a DTM address

Go to the DTM addresses page and click on the address that is to be revised or deleted. The following page appears:

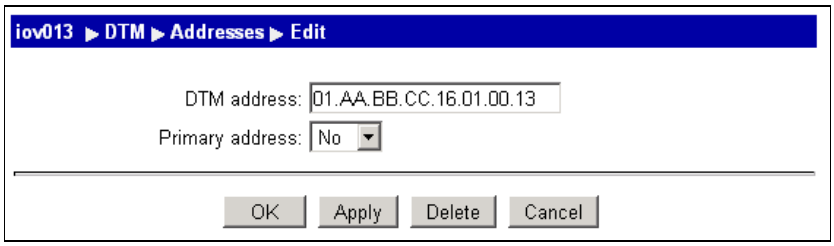


Figure 92. Edit DTM address page

Change the parameters as desired and click ‘Apply’ or ‘OK’.

Note:	If the primary address of the node is changed, the configuration must be saved and the node must be restarted for the changes to take effect. Note also that the address change does not affect existing channels.

9.4 Hostnames

Nodes in a DTM network can be assigned names using the hostnames function. Hostnames are configured locally in each node and used as aliases for a DTM address.

To configure host names, click on the link DTM → Hostnames. The following page appears.

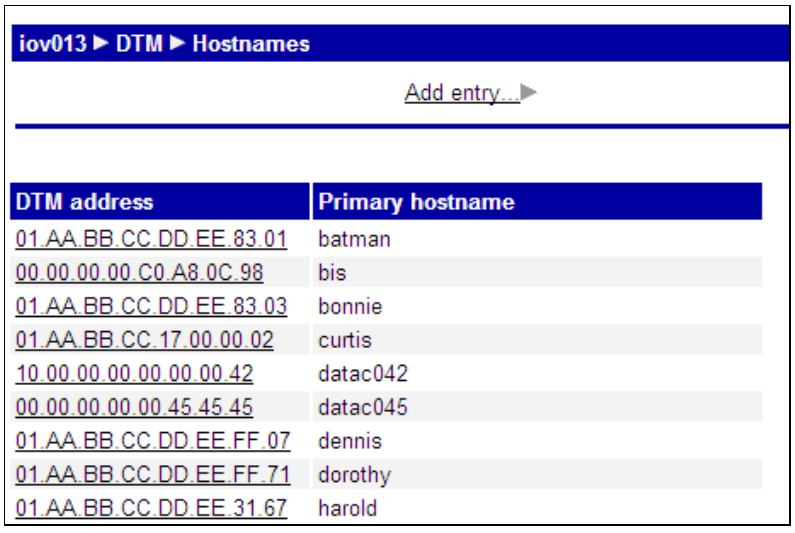


Figure 93. Hostnames page

The Hostnames page shows the DTM nodes with their DTM addresses and primary hostname. Remember to include the list of the hostnames in every node; all the nodes in the network must know all the hostnames!

9.4.1 Adding a host

Go to the hostnames page and click on the **Add entry …** link. The following page appears:

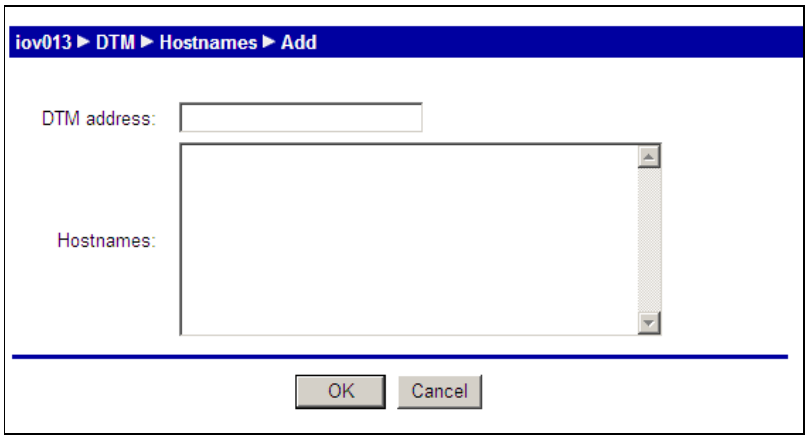


Figure 94. Add DTM hostnames page

Enter the DTM address and the selected hostname associated with the address. Click 'OK'. The DTM hostsnames page reappears with the defined address and hostname.

There are some syntax rules for host names. Host names can consist of letters, numbers and characters dot '.' and dash '-', but must start with a letter. Examples of hostnames are:

```
this.is.a.good.host.name
```

```
this-also-works.fine.
```

It is possible, but not recommended to specify several names per address, by entering each name on a separate line. Only the name on the first line will be shown on the hostname page; use several entries with the same DTM address instead if the need exist.

A list of host name suffixes may be defined in the web interface. The completion function searches for a match, starting with the top suffix defined in the list. To access the suffix definition page, follow the DTM → Hostname search link.

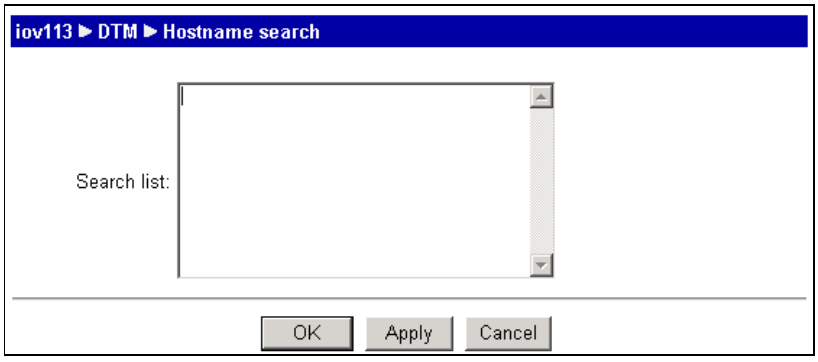


Figure 95. Editing DTM hostname suffixes

9.4.2 Editing or deleting hostnames

Navigate to the DTM hostnames page and click on the address for the host to be edited or deleted. The Edit DTM Hostnames page appears.

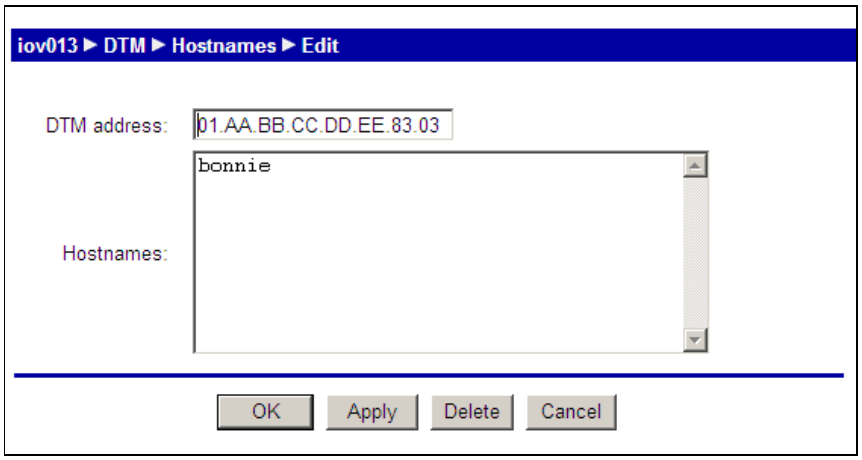


Figure 96. Editing DTM hostnames

Change the parameters and click 'Apply' or 'OK.

To delete a host, click the 'Delete' button. The DTM hostnames page reappears with the host removed from the table.

Note:

Changes to a hostname does not affect channels that have already been established. The hostname table is only consulted when a channel is established.

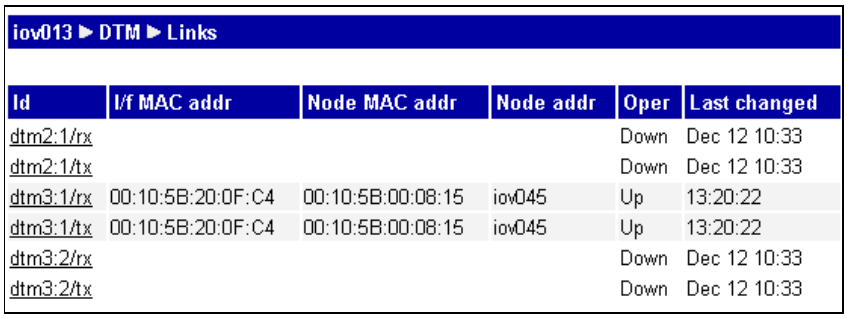
9.5 Links

The Links page shows all DTM links that the node is connected to. The page can be used to check if links to surrounding nodes have been properly established. For each link id there should be two addresses; the node address and the address to the remote node.

The link-table lists all the links that this node is attached to along with all other nodes that are attached to these links. Each line in the table represents an interface and the node that the interface is located in.

Each link starts with an Id, which is equal to the Id of a local interface. It lists the other interface connected to that link before starting a new link with a new id.

Click on the DTM → Links link. The Links page appears.



iov013 ▶ DTM ▶ Links

Id	I/f MAC addr	Node MAC addr	Node addr	Oper	Last changed
dtm2:1/rx				Down	Dec 12 10:33
dtm2:1/tx				Down	Dec 12 10:33
dtm3:1/rx	00:10:5B:20:0F:C4	00:10:5B:00:08:15	iov045	Up	13:20:22
dtm3:1/tx	00:10:5B:20:0F:C4	00:10:5B:00:08:15	iov045	Up	13:20:22
dtm3:2/rx				Down	Dec 12 10:33
dtm3:2/tx				Down	Dec 12 10:33

Figure 97. DTM links page

Id: The local interface that is connected to the link.

I/F MAC addr: Lists the MAC address of the interface. The top one is the local interface and the one below is to the remote node.

Node MAC addr: Lists the MAC addresses of all nodes connected to the link. The top one is the local node MAC and the one below is the interface in the remote node.

Node addr: Shows the node address of all nodes connected to the link. The top one is the local node address and the one below is the remote node.

Oper: Operational Status (OperStatus)

Last change: Time for last DTM link change

9.6 Routing

9.6.1 General

To establish channels in a network, the nodes must know where to find all other nodes in the network. The process of finding a path from node A to B in the network is called routing.

Routing in a DTM network has a lot in common with routing in an IP network. The table below lists the main differences between IP-routing and DTM routing.

Parameter name	IP	DTM
What is routed?	Packets	Channel-setup requests
How do you specify how to reach a destination?	One nexthop per destination	All possible nexthops to the destination.
Address type	IP address	DTM address

Figure 98. Differences between routing in an IP network and a DTM network

This section describes how to configure routing. There are two different ways to configure routing:

Static routing where the routing tables are configured manually.

Dynamic routing where a routing protocol calculates the routing tables automatically.

Note: 	Do not mix dynamic routing with static routing since this can lead to errors that are difficult to troubleshoot.

9.6.2 Static routing

To use static routing, it is necessary to configure each node in the network with information on how to reach all other nodes in the network. For nodes with a single interface and a single neighbor, this is as easy as instructing the node that all other nodes can be reached via that neighbor; but for nodes with multiple interfaces it is necessary to configure which neighbor to use to reach each destination or group of destinations.

Static routing is configured in the Routing Table. The routing table can be seen in the DTM → Routing page. The routing table consists of a number of routing entries. Each routing entry contains the fields shown below.

Field	Description
Destination	The destination and prefix together specify which destinations this routing entry is valid for; refer to section *Addresses* for a description of addressing. The destination must be a numeric DTM address.
Prefix	The number of significant bits in the destination address.
Next hop	One possible next hop node that can be used to reach the destination node(s). The next hop must be the DTM address of a neighboring node.
Type	Shall be set to “Static” for static routing entries. See the chapter on DRP for a description of “Link Prefix” and “Area Prefix”.
Metric	The cost of using this route entry. If there are several routes to the same destination, then routes with the lower metric are tried before routes with higher metric
Adm	Administrative status for the route. Routes with Adm set to down are ignored when making routing decisions.

Figure 99. The routing entries

When a node needs to find a nexthop for a destination it looks in the routing table for all entries that match the destination address. This gives the node a list of a number of different nexthops that it should try to use to reach the destination.

Note:

If there are several routing entries with different prefix lengths that are valid for a destination, then only the entries with the longest prefix will be used. If there are several entries with the same prefix length, then they will all be tried in order of increasing metric.

Note:

If the routing is poorly configured in a node, the operation of the entire network can be affected.

9.6.3 Dynamic routing

Instead of configuring the routing tables manually in each node; a routing protocol can be used to populate the routing table automatically. This is called dynamic routing. In a DTM network, the routing protocol DRP can be used.

Dynamic routing has the following advantages over static routing:

Less manual configuration required for large networks.

Automatically updated routing tables when a new node is added to the network or when the network topology changes.

Automatic routing is not error-prone.

The DRP Protocol is a routing protocol that is very similar to OSPF, but it has been adapted to the unique characteristics of the Net Insight’s technology. It automatically calculates the routing tables in all nodes and updates them as changes are detected in the network.

To use DRP, all that is necessary is to enable DRP on all nodes in the network and then remove all the static routing entries that have been added to the nodes as shown in the section on Static Routing.

9.7 Static routing

9.7.1 Adding, editing or deleting a static route

Follow the link DTM → Routing. The starting web page for Routing configuration is shown.

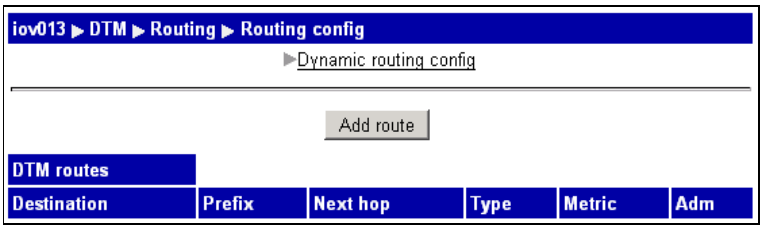


Figure 100. Routing

Click on 'Add route' or the specific link that is edited or deleted; the Route page appears.

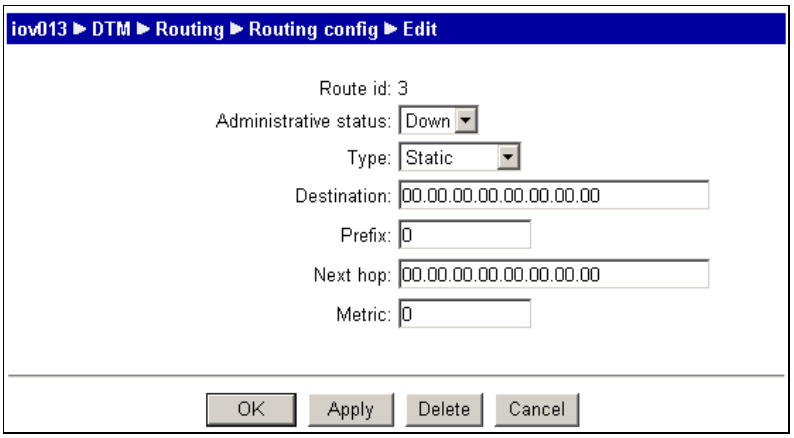


Figure 101. The edit route page

Route id: States the id of this routing entry.

Administrative status: The Administrative status for the defined routing entry; 'Down' means that the route is ignored, 'Up' means that the routing entry shall be used.

Type: The type of routing entry. Set to static for static routes. (Link prefix and Area prefix are for dynamic routing.)

Destination: The address of the remote node or network.

Prefix: The length of netmask for the remote subnet.
E.g. Prefix 64 = FF.FF.FF.FF.FF.FF.FF.FF
E.g. Prefix 56 = FF.FF.FF.FF.FF.FF.FF.00
E.g. Prefix 48 = FF.FF.FF.FF.FF.FF.00.00

Next hop: The DTM address of the neighboring node that can be used to reach the destination.

Metric: The cost associated with using this route. A route with a lower metric will be tried before a route with a higher metric.

Set the Admin status to ‘Up’ in the drop down list. Enter the Destination network or node address. Enter the Prefix.

Enter the Next hop, and set the Type to static.

Enter the Metric parameter.

Click on the ‘OK’ button to set the route and ‘Delete’ to remove the route.

The Routes page will reappear with the changes set.

9.8 Dynamic routing

9.8.1 Setting the dynamic routing parameters

Go to the routing configuration web page and click on the Dynamic routing config link

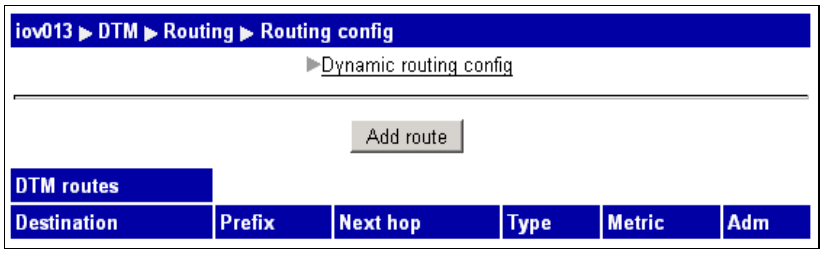


Figure 102. Dynamic routing

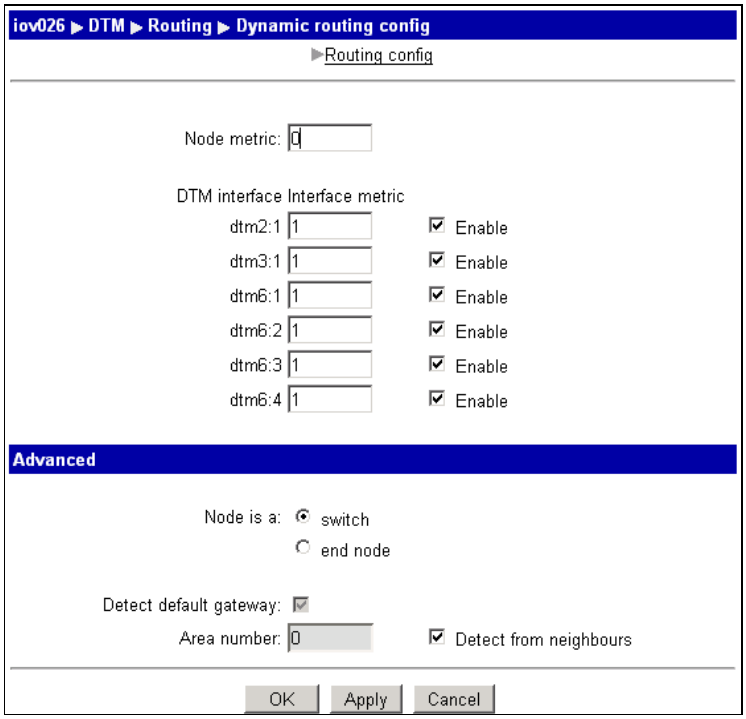


Figure 103. Routing entries

The goal of DRP is to find the lowest-cost path from source node to destination node. The cost of a path is defined as the sum of the cost of all switches and outgoing interfaces that the path uses. A good base configuration for DRP is to set the cost of all outgoing interfaces to 1 and the cost for passing through all nodes to 0. This means that the lowest cost path is always be the path that passes through the least number of links. In some circumstances, the operator might have a different opinion on what the lowest cost path is. It is then possible to classify some links or switches as “more expensive” than other links. This is done via a set of configuration variables called “metrics”.

Changes to the Metric settings in a node will be automatically propagated to all other nodes in the network and they will update their routing tables accordingly. This process can however take some time (on the order of seconds in smaller networks) before all nodes have received the new information. Changes to metrics do not affect channels that are already established.

Node metric: The cost of switching a channel in this node.

Interface metric: The cost of setting up an outgoing channel via this interface.

Enable: Should this node communicate and exchange routing information with a neighbor via this interface? This check box should normally be enabled when using DRP. It can be disabled when DRP should not be used via specific interface, e.g. if that interface connects to another operator and you don’t want to exchange routing information automatically with that operator.

9.8.2 Advanced settings

If a node is attached to the rest of the DTM network with a single point-to-point link, the node doesn’t need a complete routing table. The only routing entry necessary is the default route to the node on the other side of the point-to-point link. In DRP terminology, this type of node is called an end-node; all other nodes are called switches.

Note: 	If a node is configured as an end node, it can only originate and terminate channels; it cannot switch channels.

Detect default gateway: Ticking this box forces the node to automatically find its gateway. This is only relevant for end-nodes.

Detect from neighbors: Ticking this box makes the node request its area number (see below) from its neighbor(s).

Area number: By default, DRP distributes information about all nodes and links to all nodes in the DTM network. This allows all nodes to make "optimal" routing decisions since they have complete knowledge about the current topology. As the network grows larger, the amount of information distributed by DRP grows and eventually becomes too much for a node to handle efficiently. Exactly how large a network must be before the amount of routing information becomes too large depends on both the number of nodes, the connectivity between the nodes (i.e. the number of links) and the types of nodes in the network. It also depends on how often the network topology changes. As a rule of thumb, it is possible to run a network with 250 nodes

without worrying about the amount of routing information. If your network is larger than that, you should consider using Areas.

Areas are also useful to limit the amount of routing-information distributed between two different operators.

9.8.3 Area Definition

An area is defined as a set of interconnected nodes configured with the same area number. All nodes in an area must be able to reach all other nodes in the area without passing through a node that belongs to a different area.

A node can only belong to one area.

Links do not belong to an area. A link can interconnect two nodes that belong to different areas.

Two nodes that belong to the same area will exchange information about all nodes and links within their area. Two nodes that belong to different areas will only exchange Area Prefix routes (see below).

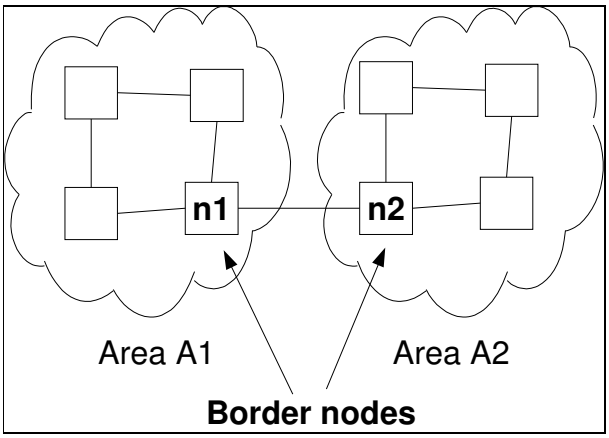


Figure 104. A network divided into two areas.

A node that is a member of one area, but has one or more links to a node in another area, is called a border node.

9.8.4 Area Planning

Dividing a network into areas require careful planning. There are a number of issues to consider before deciding where a network should be split into areas.

First of all, the connectivity between areas should be as simple as possible. A node in one area will not know anything about what another area looks like on the inside. It only knows the shortest path to the area, not which path is shortest towards a particular destination inside another area. Therefore, all border-nodes for an area should preferably have more or less the same cost towards all destinations inside the area.

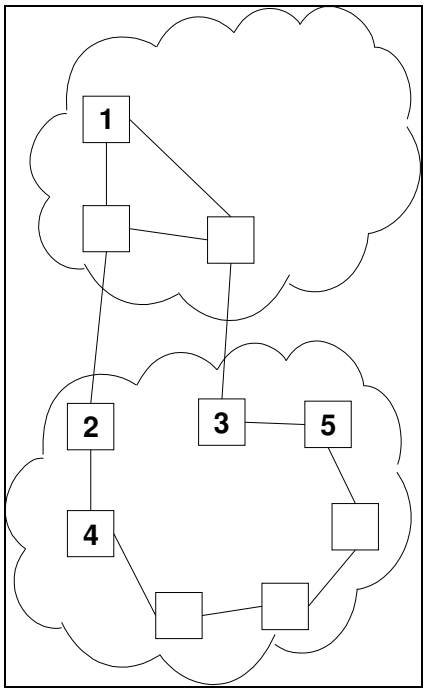


Figure 105. A network that has been divided into two areas in a bad way.

In the illustration, the distance from node 1 to node 5 is shorter if the channel is routed via node 3 than if it is routed via node 2. And the distance from node 1 to node 4 is shorter via node 2. But if a single area prefix route is used, then node 1 will think that the distance to nodes 4 and 5 are the same and it doesn't matter if it routes the traffic via node 2 or 3. This will lead to sub-optimal routing decisions.

This problem can be fixed by using more than one area prefix route to tell nodes in the upper area if there are some groups of nodes that are cheaper to reach via one of the border nodes than via the other. The extreme would be to add one area prefix route per node in the area, but then you would be better off with all nodes in a single area.

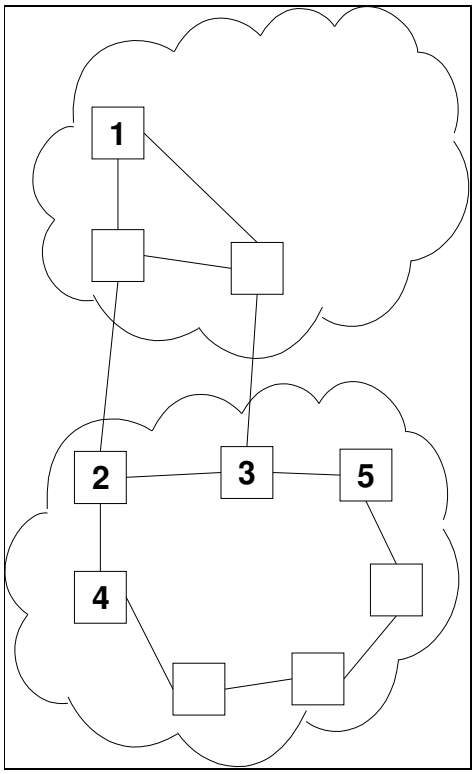


Figure 106. A better way to build the network. Note the new link between nodes 2 and 3.

A better network layout is shown here. Here, a new link has been added between nodes 2 and 3. This means that it matters less if node 1 chooses to run the channel via node 2 or node 3.

All nodes in an area should share a common addressing prefix. This prefix is independent from the area number; it is only needed to announce to nodes in other areas which nodes reside in this area. It is possible to have nodes with different prefixes within an area, as long as one area prefix route is configured in each border node for each address prefix in the area.

9.8.5 Area Prefix Routes

Area Prefix routes are used to distribute information about which nodes are inside an area to nodes in other areas. They are configured in the border nodes and they are only distributed to nodes in other areas, i.e. not to nodes in the same area as the border node that the area prefix route is configured in. Area Prefix routes received from another node are distributed to all nodes in the same area as the receiver, but not to nodes belonging to other areas.

Example: an area prefix route configured in node n1 in Figure 104/Figure 107 is distributed to all nodes in area A2. This route tells nodes in area A2 that they can reach nodes in area A1 by going through node n2.

9.8.6 Directly Connected Areas

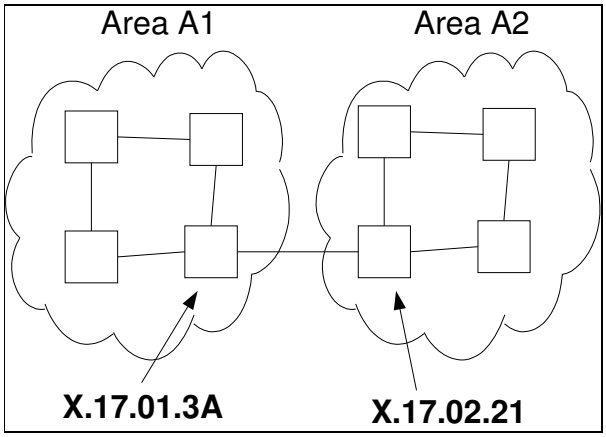


Figure 107. A network with two areas.

In the above example, the network has been divided into two areas called A1 and A2. All nodes in area A1 have addresses in the range X.17.01.00/56 (X is used here as a short-hand for 00.00.00.00.00) and the nodes in area A2 have addresses in the range X.17.02.00/56. If no area prefix routes are used, nodes in area A1 are not able to establish channels to nodes in area A2 and vice versa.

To allow nodes in area A1 to find nodes in area A2, an area prefix route must be added to node X.17.02.21. This area prefix route should advertise the network X.17.02.00/56 to nodes in area A1.

To allow nodes in area A2 to find nodes in area A1, an area prefix route must be added to node X.17.01.3A. This area prefix route should advertise the network X.17.01.00/56 to nodes in area A2.

9.8.7 Indirectly Connected Areas

If two areas are not directly interconnected, area prefix routes must be configured for all areas that can be reached through that area.

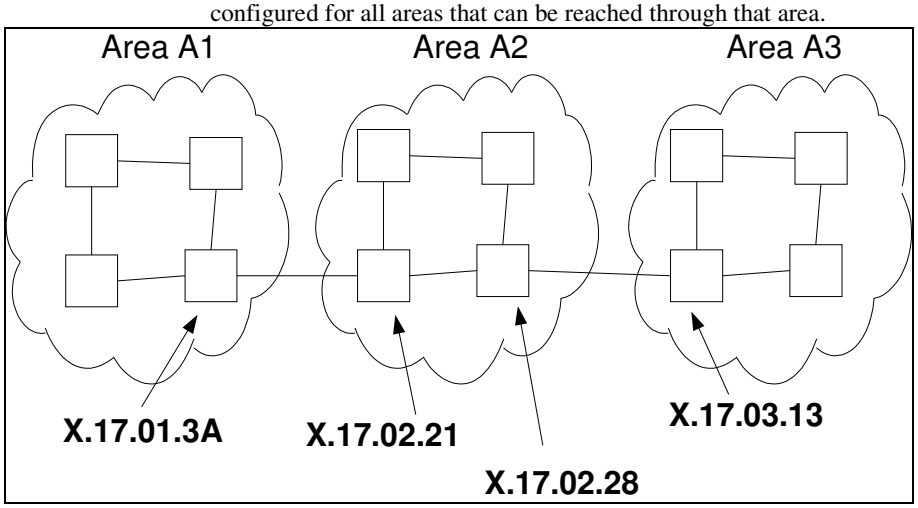


Figure 108. A network with three areas.

In the above example, the following area prefix routes must be configured:

To allow nodes in area A1 to find nodes in area A2, an area prefix route must be added to node X.17.02.21. This area prefix route should advertise the network X.17.02.00/56 to nodes in area A1.

To allow nodes in area A1 to find nodes in area A3, an area prefix route must be added to node X.17.02.21. This area prefix route should advertise the network X.17.03.00/56 to nodes in area A1.

To allow nodes in area A2 to find nodes in area A1, an area prefix route must be added to node X.17.01.3A. This area prefix route should advertise the network X.17.01.00/56 to nodes in area A2.

To allow nodes in area A2 to find nodes in area A3, an area prefix route must be added to node X.17.03.13. This area prefix route should advertise the network X.17.03.00/56 to nodes in area A2.

To allow nodes in area A3 to find nodes in area A1, an area prefix route must be added to node X.17.02.28. This area prefix route should advertise the network X.17.01.00/56 to nodes in area A3.

To allow nodes in area A3 to find nodes in area A2, an area prefix route must be added to node X.17.02.28. This area prefix route should advertise the network X.17.02.00/56 to nodes in area A1.

9.8.8 Metrics for Area Prefix Routes

Each area prefix route has an associated metric that decides how "expensive" it is to use this particular path to the area. This is useful if two areas are interconnected by two different pairs of nodes where one path is preferred over the other. It is also useful if it is possible to reach an area both directly and via another area. Then the area prefix routes can be configured so that the direct path has a lower cost than the path via another area.

9.8.9 Configuration

To implement DRP areas in your network, the following configurations must be made:

Configure the area number that the node shall belong to in each node. This is done from the DTM → Routing → Dynamic routing config link.

Configure area prefix routes in the border nodes. This is done from the DTM → Routing link.

Note that the area prefix is only configured in the area prefix routes; you never actually configure the area prefix for an area. The correlation between an area and an area prefix is only maintained to make it possible to configure a single area prefix route that covers all nodes in an area and no other nodes.

9.8.10 Addition of a dynamic routing entry

To add a dynamic route, follow the DTM → Routing link; the DTM routing config page appears.

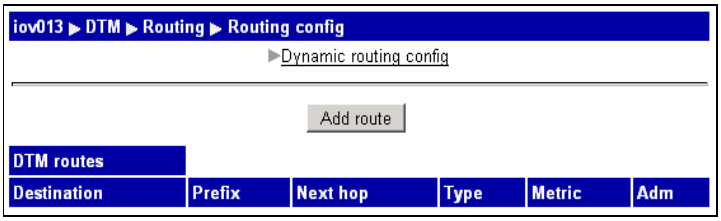


Figure 109. Dynamic routing

Click on the 'Add route' button. Enter the parameter values and click 'OK'.

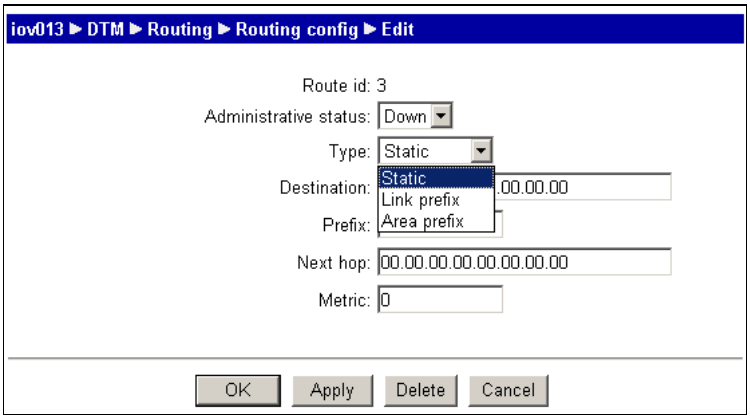


Figure 110. Dynamic routing

For dynamic routes the type could be set to:

9.8.10.1 *Link Prefix*

If there are many end-nodes with addresses with a common prefix attached to a single switch, then it is possible to announce all the end-nodes as a single route instead of announcing them individually. This is done by configuring the end-nodes as end node (in Dynamic routing config) and adding a link-prefix route in the switch.

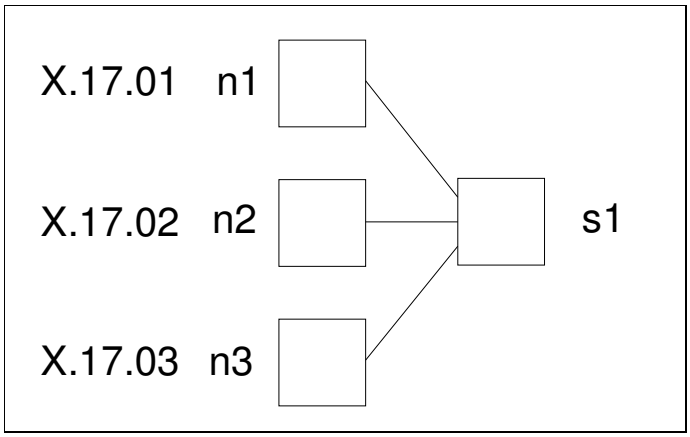


Figure 111. Routing entries

Nodes n1, n2 and n3 are configured as end-nodes and they have DTM addresses that all fall in the range X.17.00/60 (i.e. from X.17.00 to X.17.0F). A link-prefix route can therefore be added to the node s1. This means that instead of announcing n1, n2 and n3 individually, s1 will announce only X.17.00/60. Instead of each node in the DTM network having three separate routes for n1, n2 and n3, they will only have a single route that covers all three of them.

9.8.10.2 *Area Prefix*

A network can be divided into areas to increase the scalability of DRP. Each area is identified with an area number that must be configured in each node belonging to the area. The default value of the area number is zero. A border node is a node that has at least one neighbor that resides in another area. Two border nodes with different area numbers will not become adjacent and exchange topology state information.

9.8.11 Editing a dynamic routing entry

To edit a dynamic routing entry, follow the DTM → Routing link and click on the address of the route to be edited. The page below appears:

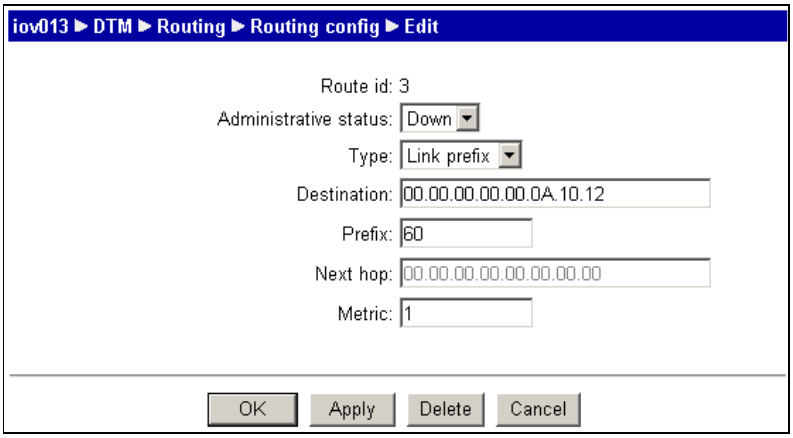


Figure 112. DTM Routing config page

Enter the values that should be changed. Click **Apply** or **OK**.

9.8.12 Deleting a dynamic routing entry

To delete a routing entry, follow the DTM → Routing link. Click on the address of the route to be deleted.

Set the Administrative status to 'Down' from the drop-down menu and click 'Apply' or 'OK'.

Click on the 'Delete' button. The routing entry is deleted.

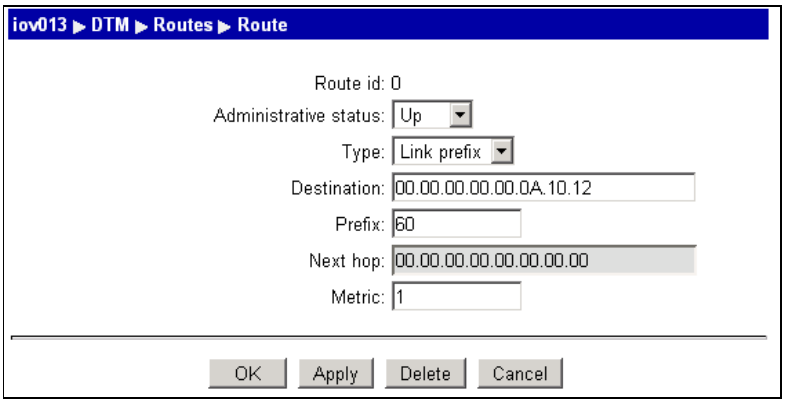


Figure 113. Delete a routing entry

10 Trunks

10.1 Overview of Trunks

Trunks of various types connect the nodes of a Nimbra network. The trunks can be of different types; 8B/10B, SONET/SDH, PDH and IP/Ethernet.

The trunk interface manager supports 8B10B, SONET/ SDH, PDH and IP/Ethernet interfaces. The main functional areas covered by the manager are Trunk interface configuration including alarm reporting and performance monitoring. Performance Monitoring is described in a separate chapter.

Normally, the trunk is configured from one web page, but the IP trunk and the Ethernet it runs over are configured on two separate web pages.

10.1.1 Trunk Modules, Nimbra One

There are several different trunk modules. Some of the cards are turnable and some are available in type A and B versions.

Trunk Modules	Data rate	Category
OC-48/STM-16 X-ADM Module	2 488 Mbps	SDH/SONET
OC-12/STM-4 Trunk Module (DTM 622 Trunk Module)	622 Mbps	SDH/SONET
2 x OC-12/STM-4 Trunk Module	2 x 622 Mbps	SDH/SONET
4 x OC-3/STM-1 Trunk Module	4 x 155 Mbps	SDH/SONET
OC-3/STM-1 Trunk Module (DTM 150 Trunk Module)	155 Mbps	SDH/SONET
4 x DS3/E3 Trunk/Access Module	DS3 45 Mbps E3 34 Mbps	PDH
3 x IP/Ethernet Trunk Module	1 000 Mbps	IP/Ethernet

Figure 114. Available Trunk Modules for Nimbra One.

10.1.2 Trunk Modules, Nimbra 300

There are several versions of trunk modules, according to the table below. From a web management point of view, all Nimbra 300 trunk modules have a Nimbra One mirror image and behave identically as it in the GUI interface. Hence, no separate description is made of Nimbra 300 Series trunk modules.

Trunk Modules	Data rate	Category
OC-48/STM-16 X-ADM Module	2 488 Mbps	SDH/SONET
OC-12/STM-4 Trunk Module	622 Mbps	SDH/SONET
2 x OC-12/STM-4 Trunk Module	622 Mbps	SDH/SONET
4 x OC-3/STM-1 Trunk Module	155 Mbps	SDH/SONET
4 x DS3/E3 Trunk/Access Module	DS3 45 Mbps E3 34 Mbps	PDH
3 x IP/Ethernet Trunk Module	1 000 Mbps	IP/Ethernet

Figure 115. Available trunk modules for Nimbra 340.

10.1.3 Fixed trunk interfaces for Nimbra 360

Nimbra 360 has integrated fixed SDH/SONET trunk interfaces on the base unit. One interface type is installed among the options below. The difference is in the firmware, which can be changed in the field. In addition, the IP/Ethernet trunk can run on two of the fixed ports, provided that the hardware supports it.

Trunk Interfaces, Nimbra 360	Data rate	Category
OC-48/STM-16 X-ADM Interface (2 ports)	2 488 Mbps	SDH/SONET
OC-12/STM-4 Trunk Interface (4 ports)	622 Mbps	SDH/SONET
OC-3/STM-1 Trunk Interface (4 ports)	155 Mbps	SDH/SONET
IP/Ethernet Trunk Interface; requires Nimbra 360, HW version B (2 ports)	1000 Mbps	IP/Ethernet

Figure 116. Fixed trunk interfaces for Nimbra 360.

10.1.4 Trunk Modules, Nimbra 600

There are several versions of trunk modules, according to the table below. These modules look slightly different in the web interface than corresponding ones in the web interface of the Nimbra One/300.

Trunk Modules	Data rate	Category
OC-192/STM-64 Trunk Module	9 952 Mbps	SDH/SONET
4 x OC-48/STM-16 Trunk Module	2 488 Mbps	SDH/SONET
4 x OC-12/STM-4 Trunk Module	622 Mbps	SDH/SONET
4 x OC-3/STM-1 Trunk Module	155 Mbps	SDH/SONET
6 x IP/Ethernet Trunk Module	Configurable,up to 1000 Mbps	IP/Ethernet

Figure 117. Trunk Modules for Nimbra 600.

10.1.5 Trunk interfaces configuration

The starting web page for the Trunks link is shown in below.

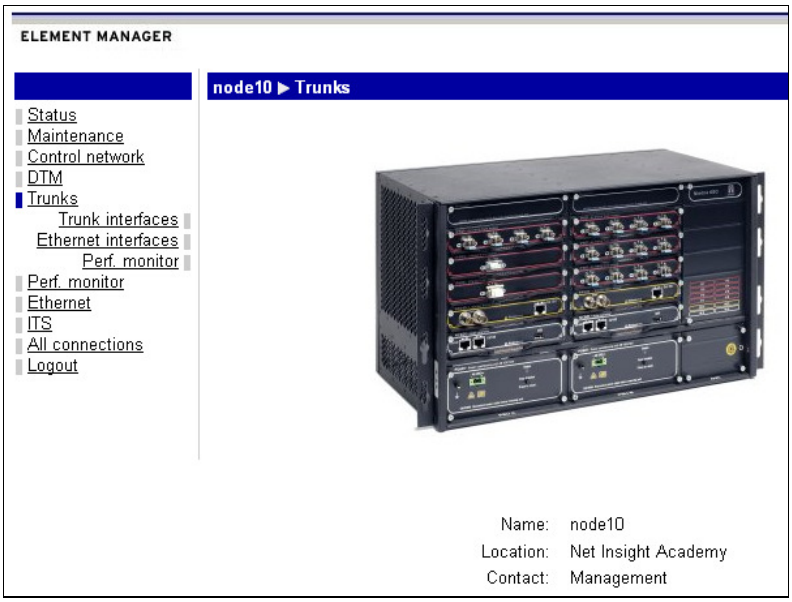


Figure 118. The starting web page for Trunks

The sub-links are: Trunk Interfaces, Ethernet Interfaces and Perf. monitor. Trunk Interfaces is where the various trunk modules are configured and their state is monitored. Ethernet Interfaces is where IP/Ethernet trunk interfaces are configured and Perf. monitor is where performance monitoring for the various interfaces is defined. Performance monitoring (PM) is the process whereby transported data is supervised for quality deterioration. Performance monitoring uses SNMP counters (ITU-T G.826 like) on trunks, interfaces and connections. For further information, see the chapter on Performance Monitoring.

To configure the trunk interfaces, just follow the link to Trunk Interfaces. Select the trunk to be configured by clicking on the Name of the trunk (e.g. sonet/sdh-3:1, pdh-5:1, ipt-5:4).

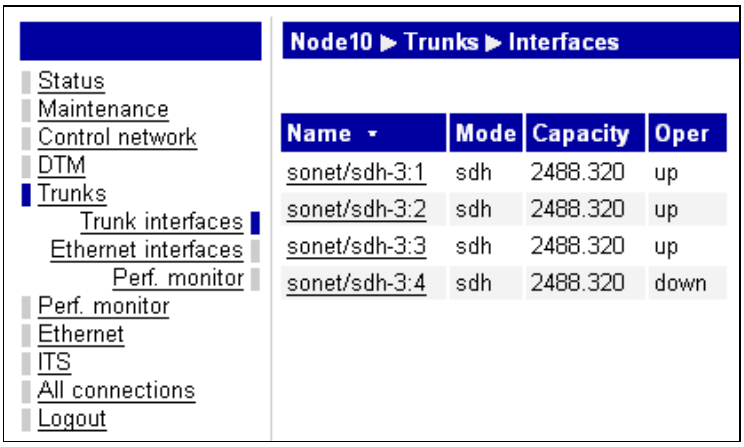


Figure 119. Trunk Module configuration page

The following information is presented; Name is the name of the interface, according to Net Insight naming convention, Mode is the type of interface, Capacity is the total capacity of the trunk interface in Mbps and Oper is the operational status of the trunk interface (up, down, absent, starting or degraded)

10.2 Editing SDH/SONET Trunk Interfaces

The basic structure of the configuration page is kept constant for the various interfaces in Nimbra One and Nimbra 300.

First, interfaces specific variables are presented, followed by configurable parameters. These parameters are followed by additional configurable "advanced" parameters under the advanced heading and sometimes by additional variables. Finally, the alarm status is presented.

The common Read-only parameters (variables) are:

Parameter	Description
Interface name	The interface name. Written as "sonet/sdh-X:Y" where X is slot position of the module and Y port position of the interface on the module.
Operational status	The operational status of the board
Speed	Capacity of the interface
SOH S1 (SSM)	Synchronization Status Message (4 bits) in the section overhead
Description	The number of slots available for transmission on this interface. Used on OC-3/STM-1 Trunk Module only

Figure 120. Read-only parameters for SDH/SONET interfaces

Additional variables for OC-48/STM-16 X-ADM Module are:

Parameter	Description
Transceiver temperature	Temperature of the transceiver
Transceiver laser bias	Laser bias current of the transceiver laser
Transceiver power	Optical power transmitted from the transceiver
Receiver power	Optical power received on the transceiver

Figure 121. Additional variables for the OC-48/STM-16 X-ADM Module

The **configurable** parameters for the common interfaces are:

Parameter	Description
Suppress Alarms	When the service is up and running as intended, alarms are by default suppressed. In order to enable the alarms, the suppress alarms tick boxes must be unmarked. All: When marked, all alarms are suppressed. AIS: Alarm indication signal. RDI: Remote defect indicator.

Figure 122. Configurable parameters for common interfaces

The configurable Advanced parameters for SDH/SONET trunk modules are:

Parameter	Description	Comment
Transmit sync source	Define the sync source for the transmitting (Tx) interface. The parameter can have two values, 'interface' and 'loop'. The default setting is 'interface', which uses the node sync source as source for the outgoing Tx interface. 'loop' means that the incoming Rx signal is reused on the Tx interface. This setting should not be used at both ends of the link!	Not used for OC-48/STM-16 X-ADM Trunk Module or Nimbra 600 OC-48/STM-16 Trunk modules
H1 SS bits	Different between Sonet and SDH. This value is the value of the SS bits in the H1 byte in the Sonet/SDH section overhead. Older Sonet/SDH equipment may require other values than the default values (00 Sonet; 10 SDH)	
POH C2 byte	Path overhead The C2 byte in the path overhead specifies what type of network is used. ITU-T has not yet assigned a C2 value for DTM networks, so for DTM networks use '05' as the ITU-T 'experimental' value.	Used on 4 x OC-3/STM-1 Trunk Module and OC-48/STM-16 X-ADM Module

Signal failure filter period	Delay time for 1+1. The time that the nodes waits for the underlying network (SDH/SONET/WDM) to re-establish connection, in order to avoid a switch-over. Default 50 ms, Range 0-2000 ms	
Degraded defect (DEG) period	Configuration parameters for the "Degraded" alarm, according to ITU G.806 fir the interface. Period, default 5 sec.	Not used for OC-48/STM-16 X-ADM Trunk Module or OC-3/STM-1 (DTM 150) Trunk Module
Degraded defect (DEG) threshold	Configuration parameters for the "Degraded" alarm, according to ITU G.806 for the interface. Number of block errors. Default 1200.	Not used for OC-48/STM-16 X-ADM Trunk Module or OC-3/STM-1 (DTM 150) Trunk Module

Figure 123. Configurable Advanced parameters for SDH/SONET trunks.

Additional read-only parameters (variables) are presented under the Advanced heading:

Parameter name	Description
Error counters	B1 Section overhead B2 Line overhead B3 Path overhead M1 Remote indication of B1 G1 Remote indication of B3
Pointer adjustment event, positive and negative	RXPJE+ RXPJE- TXPJE+ TXPJE-
Overhead bytes	SS=2 C2=5 (default)

Figure 124. Additional advanced read-only parameters

The OC-3/STM-1 Trunk Module only display error counters B2 and B3.

The Alarms parameters are presented at the bottom of the table as:

Alarm	Description
Opto module	Alarms from SFP. The Opto Module alarm is not available for the OC-3/STM-1 Trunk Module.
Unequipped (UNEQ)	This alarm is received from the other end of the link, indicating that the payload is not usable.
Los of signal (LOS)	Loss of signal. No signal detected on SONET/SDH network interface, no light in the fiber.
Los of frame (LOF)	Loss of frame. Unable to align SONET/SDH frame, no light in the fiber.

Los of pointer (LOP)	Loss of pointer. No pointer for where payload is.
Alarm indication signal, line (AIS-L)	Alarm indication signal, line or defect detected by upstream SONET/SDH network interface.
Alarm indication signal, path (AIS-P)	Alarm indication signal, path or defect detected by upstream SONET/SDH network interface.
Remote defect indication, line (RDI-L)	Remote defect indication, line or defect detected by downstream SONET/SDH network interface.
Remote defect indication, path (RDI-P)	Remote defect indication, path, RDI-P or defect detected by downstream SONET/SDH network interface.
Payload mismatch (PLM)	Payload mismatch.
Degraded signal (DEG)	Degraded signal
Loopback	Loopback alarm, NA

Figure 125. Alarms parameters

As an example, configuration of one interface on the OC-12/STM-4 Trunk Module is given.

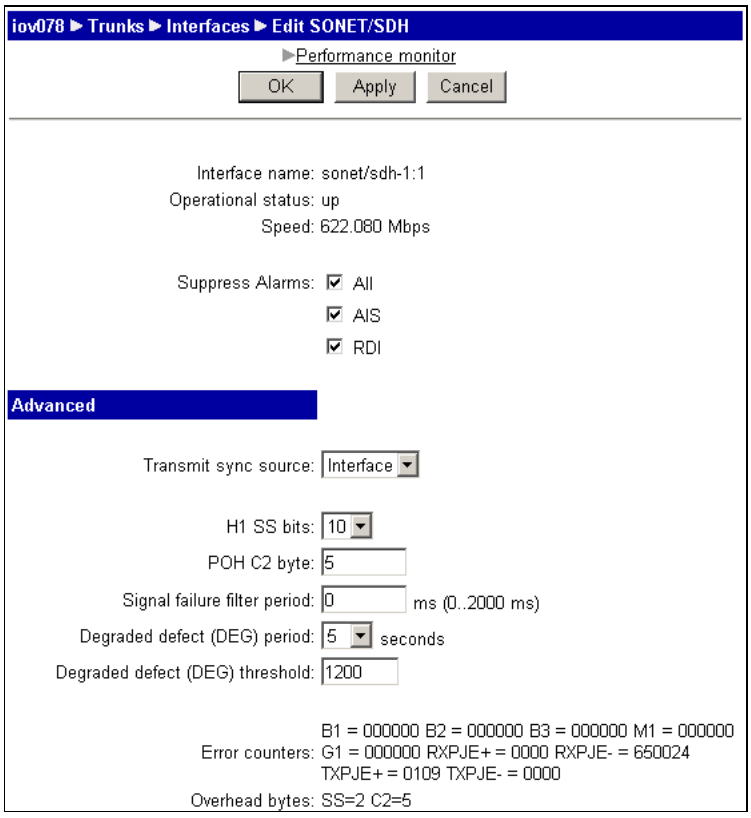


Figure 126. Configuration page of the OC-12/STM-4 module, part one

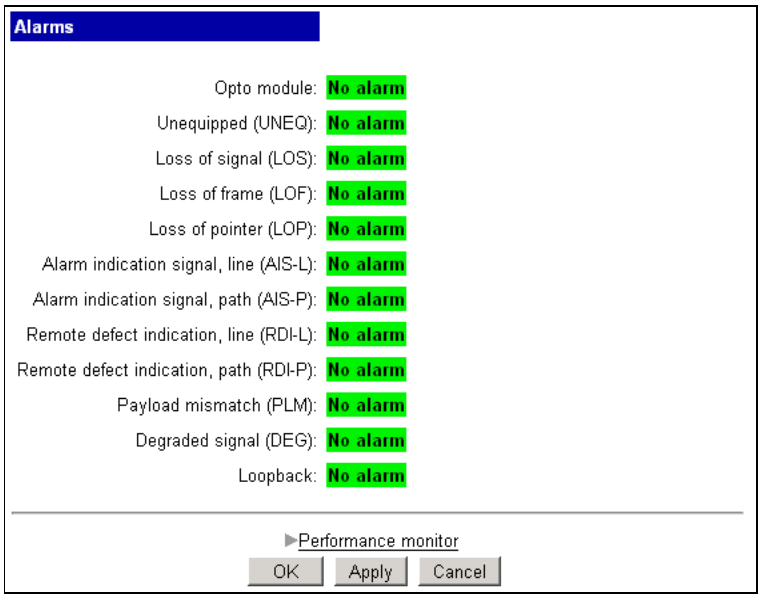


Figure 127. Configuration page of the OC-12/STM-4 module, part two

Set the parameters and click on 'Apply' (keeps the web page open) or 'OK' (moves you to the Trunk Interfaces web page).

10.2.1 Optional FEC version for 4 x OC-3/STM-1 Trunk

FEC155 Firmware Module is a value added firmware module for the 4 x OC-3/STM-1 Trunk Modules. Currently, it requires variant NPS0009-XS31 (Nimbra One) or NPS0009-3S31 (Nimbra 300 Series) of the Trunk Module. It provides comprehensive forward error correction to the trunk module. Typically it should be used when running traffic over unreliable media such as microwave links that are prone to bit and burst errors. All services are protected since FEC works on the link level. The module performs Reed-Solomon encoding/decoding and Row/Column interleaving.

Reed-Solomon encoding/decoding performs a (255,239) encoding/decoding of the data and can detect and correct up to 8 bytes of an STS-3c SPE/VC-4 row.

Note: Only two of the four physical interfaces will be usable when running the board in FEC mode.

The module is easy installable on the NPS0009-XS31/NPS0009-3S31 variant of the 4 x OC-3/STM-1 Trunk Module by a remote firmware upgrade; please see the Up- and Downgrading chapter, chapter 23 of this document.

10.3 Editing the DS3/E3 Trunk interfaces

The presented variables are:

Variable	Description
Interface name	The interface name, written as “pdh-X:Y” where X is number of the slot in the chassis and Y is the number of the port on the module.
DTM interface	The name of the DTM interface, written as dtmX:Y. X and Y are used as for the Interface name.
Oper. status	The operational status of the board. ‘Up’, ‘Down’, ‘Absent’ or ‘Dormant’
Speed	The capacity of the interface
Mode	The operational mode of the node, DS3 or E3. The mode (DS3/E3) has to be the same on the entire module, but mixing DS3 and E3 on different modules within a node is allowed.

Figure 128. Variables of the DS3/E3 Interface

The configurable parameters for the DS3/E3 Trunk Interface are:

Parameter	Description
Suppress Alarms	When the service is up and running as intended, alarms are by default suppressed. In order to enable the alarms, the suppress alarms tick boxes must be unmarked. All: When marked, all alarms are suppressed. AIS: Alarm Indication Signal. RDI/RAI: Remote Defect Indicator/Remote Alarm Indication

Figure 129. Configurable parameters of the DS3/E3 Trunk Interface

The Advanced parameters:

Parameter	Description
Line build out (DS3 only)	For operation with physical cable lengths over 68 m (225 feet), the 'Line build-out' variable must be selected. With the selection, operation up to 137 m (450 feet) is feasible.
SSM/TM code (E3 only)	Synchronization Status Message/Timing Marker code. Can assume values 0-15 or auto. Auto is recommended.
Receive sync (RX_FSYNC) source	Select receive DTM sync source. Either the recovered bit clock (Line) or the recovered DTM Start of Frame signal (FSP). Normally set to Line, but if Time Transfer is used the parameter must be set to FSP. Also, in this case, the interface must be reset, i.e. the administrative status must first be taken down and then reset to up. Obviously, this only applies to the case where the administrative status is up already.
Signal failure filter period	Delay time for 1+1. The time that the nodes waits for the underlying network (SDH/SONET/WDM) to re-establish connection, in order to avoid a switch-over. Default 50 ms, Range 0-2000 ms
Degraded defect (DEG) period	Configuration parameters for the "Degraded Signal" alarm, according to ITU G.806 for the interface. Period, default 5 sec (Number of sequential bad seconds to set/clear DEG), settable from a roll-down menu to an integer between 2 and 10
Degraded defect (DEG) threshold	Configuration parameters for the "Degraded Signal" alarm, according to ITU G.806 for the interface. Number of block errors to declare a bad second. Default 1200.
Overhead information	BIP 00000 (Number of detected BIP-8 errors since last reload of this page); REI 00000 (Number of detected remote error indications since last reload of this page); LCV 11920 (Number of detected line code violations since last reload of this page); CP 00000; P 00000 (Number of detected P-bit errors since last reload of this page)

Figure 130. Advanced parameters of the DS3/E3 Trunk Interface

The **Alarms** parameters are presented at the bottom of the table as:

Parameter	Description
Unequipped (UNEQ/IDLE)	This alarm is received from the other end of the link, indicating that the payload is not usable.
Loss of signal (LOS)	Loss of signal. No signal detected on PDH network interface.
Loss of frame (LOF/OOF)	Out of frame. Unable to align PDH frame.
Alarm indication signal, line (AIS)	Alarm indication signal, line or defect detected by upstream network interface.
Remote defect indication, line (RDI/RAI)	Remote defect indication or defect detected by downstream network interface.
Payload mismatch (PLM)	Payload signal label mismatch.
Degraded signal (DEG)	Degraded signal.

Figure 131. Alarms parameters of the 4 x DS3/E3 Trunk Module

Navigate to the **Trunks|Interface** and then on the trunk interface that should be edited.

Make all your choices and click on Apply or OK. Apply doesn't change the web page, whereas OK takes you back to the **Trunks|Interface** web page.

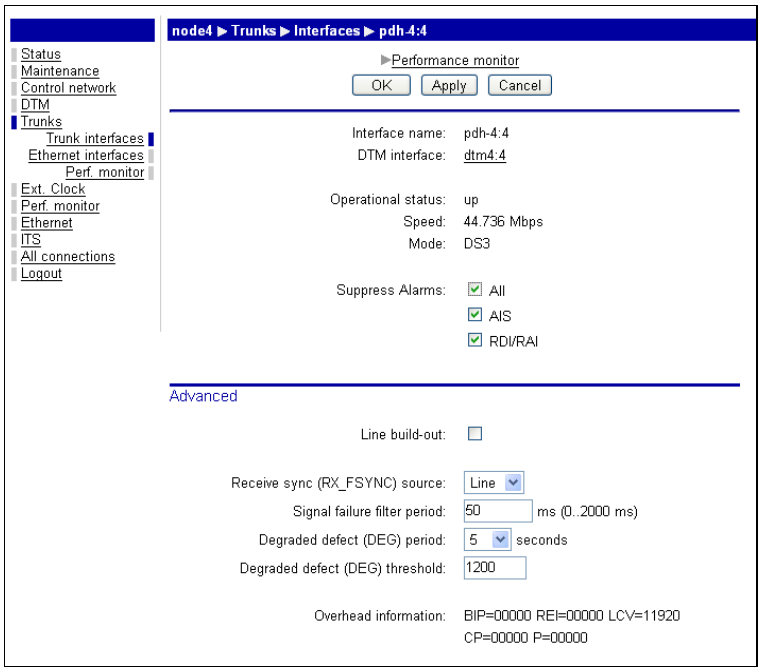


Figure 132. Edit the Trunk parameters on a DS3/E3 Trunk Interface

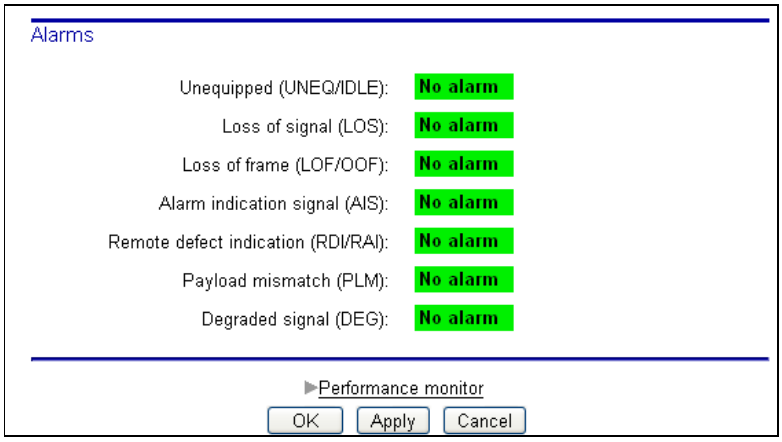


Figure 133. Alarms of a DS3/E3 Trunk Interface.

10.3.1 Configuration of DS3/E3 mode

For a 4 x DS3/E3 Trunk/Access Module used as a trunk module, it is not possible to set the DS3/E3 mode of the module from the web GUI. The DS3/E3 mode can only be set for the entire module at boot time, i.e. it must be decided whether the node shall run the 4 x DS3/E3 trunk modules in DS3 or E3 mode. This is done on a per-module basis. A change of configuration requires a change in the file `modeprobe.conf` and a reboot of the node.

The mode is set by editing the file `/flash/etc/modeprobe.conf`.

The string `options mau-50 e3=2,3,4 ds3=5,6,7,8` makes all 4 x DS3/E3 trunk/access modules used in trunk mode operate with the E3 protocol if placed in slots 2-4 and with the DS3 protocol if placed in slots 5-8.

To operate all modules in E3 mode, write `options mau-50 mode=0`.

To operate all modules in DS3 mode, write `options mau-50 mode=1`.

An empty `modprobe.conf` file sets all modules to DS3 mode (default).

After the file has been edited, the node has to be rebooted.

For system release versions prior to GX4.3.0.0, it is not possible to mix E3 and DS3 trunks. The entire node must be set to either DS3 or E3 mode.

The configuration of E3/DS3 mode for a slot position does not affect the operation of other board types, i.e. it is possible to use any interface module in a DS3/E3 configured slot. The configuration only applies for DS3/E3 trunk/access modules uses as trunk modules.

If the 4 x DS3/E3 Trunk/Access Module is used as an access module, DS3 or E3 is configurable from the web interface per interface. Trunk/access operation is determined by what firmware is installed on the module.

10.4 Editing the IP/Ethernet trunk interface

This part of Element Manager is structured in a way that is intended to facilitate for the user to keep track of all configurable parameters, their ranges, their type, any special values and a short description of each variable.

IP Trunks, the underlying physical Ethernet interface and the DTM interface that runs on top of the IP trunk interface are all configured from links in the left column of the main web menu.

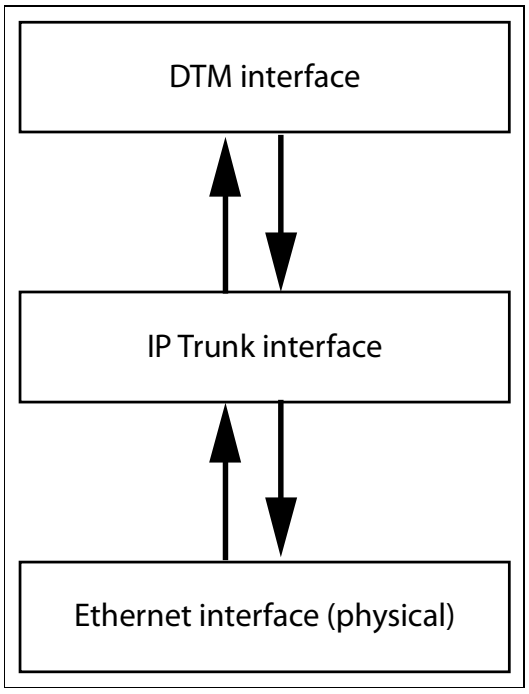


Figure 134. The interface structure of the IP trunk.

Configuration of IP trunks starts from the link Trunks in the left column. Clicking on the link Trunks displays additional links: Trunk interfaces, Ethernet interfaces and Perf. Monitoring. An illustration of the configuration follows the description of parameters, variables and alarms.

The IP trunk interface is able to send and receive up to 81297 Ethernet packets per second. The minimum number of packets sent/received is 1000 per second.

In GX4.7, a mechanism for IP trunk shutdown after persistent loss of connectivity is introduced. When connectivity is restored, the link will be re-established.

10.4.1 Configurable interface parameters

10.4.1.1 Tx slots (Tx bitrate)

Default value: The default Tx slot rate is 0, i.e. the trunk is by default disabled. Tx bitrate is internally computed from the Tx slot rate.

Type: Integer

Range: Displayed immediately to right of the field.

Description: It is possible to express the transmitted capacity either as number of slots per DTM frame or directly as bitrate. Only one of the fields should be filled out; the other field is automatically computed as soon as the fill-out field is left. A Tx slot value of 0 means that the trunk is taken down in the transmit direction.

10.4.1.2 Suppress alarms - all

Default value: "yes", i.e. ticked

Type: text string

Range: possible values "yes" or "no"

Description: The suppress alarm tic box for all alarms can be used to suppress all alarms.

10.4.1.3 Suppress alarms - AIS

Default value: "yes", i.e. ticked

Type: text string

Range: possible values "yes" or "no"

Description: The suppress alarm tic box for the AIS (Alarm indication signal) alarm can be used to suppress the AIS alarm.

10.4.1.4 Suppress alarms - RDI

Default value: "yes", i.e. ticked

Type: text string

Range: possible values "yes" or "no"

Description: The suppress alarm tic box for the RDI (Remote Defect Indication) alarm can be used to suppress the RDI alarms.

10.4.1.5 Local IP address

Default value: 169.254.0.0

Type: IP address, xxx.yyy.zzz.aaa where xxx, yyy, zzz and aaa all are integers in the range 0-255.

Range: 0.0.0.0-255.255.255.255

Description: This is the IP address of the configured trunk interface.

10.4.1.6 Subnet mask

Default value: 255.255.255.0

Type: IP address, xxx.yyy.zzz.aaa where xxx, yyy, zzz and aaa all are integers in the range 0-255.

Range: 0.0.0.0-255.255.255.255

Description: This is the subnet mask of the configured trunk interface.

10.4.1.7 Gateway IP address

Default value: 0.0.0.0

Type: IP address, xxx.yyy.zzz.aaa where xxx, yyy, zzz and aaa all are integers in the range 0-255.

Range: 0.0.0.0-255.255.255.255

Description: The default address used to reach remote locations in other subnets.

10.4.1.8 Remote IP address

Default value: 169.254.0.0

Type: IP address, xxx.yyy.zzz.aaa where xxx, yyy, zzz and aaa all are integers in the range 0-255.

Range: 0.0.0.0-255.255.255.255

Description: This is the IP address of the remote (peer) trunk interface.

10.4.1.9 Transmitted frame type

Default value: "untagged"

Type: text string

Range: One of "untagged", "priotagged" or "vlantagged"

Description: "Untagged" means that neither VLAN-tags nor prio-tags are attached to the packets' header. "vlantagged" means that all packets are labeled in the 'VLAN ID field. "Priotagged" means that VLAN id tags on incoming packets are ignored and outgoing packets are not labeled with a VLAN ID. However, the prio field in the header is set in the Ethernet priority field (default: 0, type: integer, range: 0-7) and determines the priority of the packets.

10.4.1.10 DiffServ Code Point

Default value: 0

Type: integer

Range: 0-63

Description: Differentiated Services Code Point is a number that the customer assigns IP packets over the trunk. It defines a networking architecture that specifies a mechanism for classifying, managing network traffic and providing QoS guarantees.

10.4.1.11 VLAN id

Default value: N/A

Type: integer

Range: 1-4094

Description: VLAN id is a VLAN tag attached to Ethernet frames that are of transmitted frame type 'vlantagged'.

10.4.1.12 Ethernet priority

Default value: 0

Type: integer

Range: 0-7

Description: Ethernet priority is a setting that determines the priority of the Ethernet frames. It is assigned to Ethernet frames that are of transmitted frame type 'vlantagged' or 'priotagged'. Differentiated Services Code Point is a number that the customer assigns IP packets over the trunk. It defines a networking architecture that specifies a mechanism for classifying, managing network traffic and providing QoS guarantees.

10.4.1.13 Maximum transmission unit

Default value: 1500

Type: integer

Range: 64-1500

Description: IP maximum transmission unit.

10.4.1.14 Time to live

Default value: 30

Type: integer

Range: 0-255

Description: Maximum number of hops allowed between originating interface and terminating IP interface.

10.4.1.15 Forward Error Correction Transmit Mode

Default value: "none"

Type: text string

Range: Alternatives that are supported by the hardware, shown in a drop-down menu.

Description: "none" means that the function is disabled. "1D" means that the "1D" form of Forward Error Correction (FEC) is used for transmission (column checksum) from this interface. "2D" means that the 2D form of FEC is used for transmission (column + row checksums) from this interface.

10.4.1.16 Forward Error Correction 'Transmit rows'

Default value: 4

Type: integer

Range: Displayed immediately to right of the field, as supported by hardware.

Description: Number of rows in the transmit FEC matrix. The product of FEC Transmit rows and FEC Transmit Columns must be below 100. The parameter is grayed out if it can't be configured.

10.4.1.17 Forward Error Correction 'Transmit columns'

Default value: 1

Type: integer

Range: Displayed immediately to right of the field, as supported by hardware.

Description: Number of columns in the transmit FEC matrix. The product of FEC Transmit rows and FEC Transmit Columns must be below 100. The parameter is grayed out if it can't be configured.

10.4.1.18 Loopback

Default value: "none"

Type: text string

Range: Alternatives that are supported by the hardware, shown in a drop-down menu. The alternatives can be 'near end', 'far end', 'both' or 'none', all seen from the DTM side. Currently only 'none' is supported.

Description: Sets the DTM loopback mode.

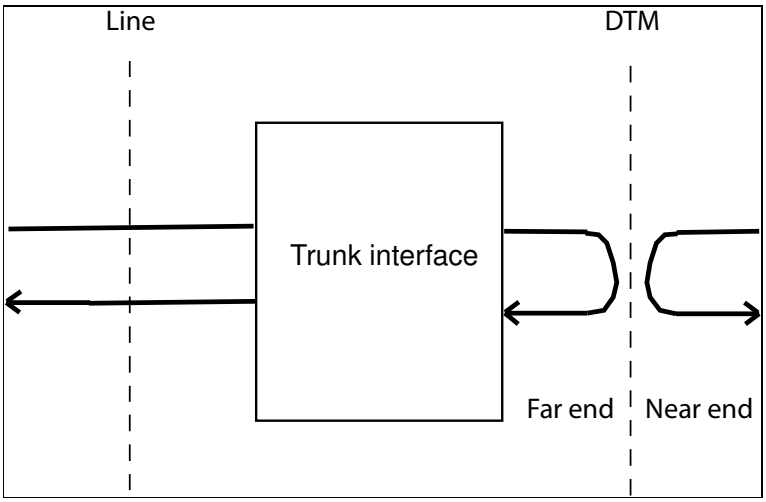


Figure 135. Loopback, as seen from the DTM side.

10.4.1.19 Loopback reset timeout

Default value: 0

Type: integer

Range: 0-65536

Description: Sets the time (in seconds) for loopback activity. After the loopback reset timeout, the DTM interface reverts to normal operation. The value zero has a special meaning, namely that the 'Loopback' function is disabled. This parameter is only possible to set if 'Loopback' is not equal to none.

10.4.1.20 Signal failure filter period

Default value: 0

Type: integer

Range: 0-2000

Description: The signal fail filter delay time (in milliseconds), i.e. a system set delay before a signal fail alarm is generated (after its detection). Not implemented in the current release.

10.4.1.21 Degraded defect (DEG) period

Default value: 2

Type: integer

Range: 2-10

Description: Number of consecutive seconds that exceed the threshold before the DEG alarm is generated. Not implemented in the current release.

10.4.1.22 Degraded defect (DEG) threshold

Default value: 0

Type: integer

Range: 0-8000

Description: Number of acceptable errored blocks per second. A higher error rate starts the time counter towards the DEG alarm.

10.4.1.23 Pacing criterion

Default value: "overhead"

Type: text string

Range: "overhead", "latency"

Description: Defines whether pacing is based on minimum latency ("latency") or minimum overhead ratio ("overhead"). Minimum latency means that at least one packet is transmitted per DTM frame. Minimum overhead ratio means that the packets are sent when the MTU is filled and not before.

10.4.1.24 Jitter tolerance

Default value: 2000

Type: integer

Range: 0-10000000

Description: The tolerated jitter and wander of the IP interface, given in microseconds.

10.4.2 IP trunk interface variables

10.4.2.1 Rx slots (Rx bitrate)

Type: Integer

Description: The variables Rx slots and Rx bitrate are proportional. These variables are configurable from the remote (peer) interface as Tx slots/Tx bit rate. If the Rx slot value is zero, the trunk is taken down from the other end.

10.4.2.2 Forward Error Correction, Receive mode

Type: text string

Description: The FEC receive mode is equal to the FEC transmit mode defined on the remote (peer) interface. The value "none" means that the (FEC) function is disabled. "1D" means that the "1D" form of Forward Error Correction (FEC) is used (column FEC) to this interface. "2D" means that the 2D form of FEC is used (column + row FEC) to this interface.

10.4.2.3 Peer abilities, Max Rx slots

Type: integer

Description: The maximum amount of slots that the remote (peer) IP trunk interface can accommodate. If the parameter Tx slots exceed this value, an alarm is raised and the trunk connection cannot be established.

10.4.2.4 Peer abilities, (Forward Error Correction) Max Receive Mode

Type: text string

Description: The highest FEC Max Receive Mode that is possible on the interface, when the FEC Receive Mode is classed as “none” (lowest), “1D” or “2D” (highest).

10.4.2.5 Peer abilities, (Forward Error Correction) Max Receive rows

Type: integer

Description: The highest FEC Max Receive rows that is possible on the interface.

10.4.2.6 Peer abilities, (Forward Error Correction) Max Receive columns

Type: integer

Description: The highest FEC Max Receive column that is possible on the interface.

10.4.2.7 Peer abilities, (Forward Error Correction) Max Receive elements

Type: integer

Description: The maximum number of Data Elements in the receive side FEC matrix that is supported by the remote (peer) interface.

10.4.2.8 Path delay variation (µs)

Type: real number

Description: The RMS (root mean square) value of the path delay variation i.e. standard deviation value of the IP path delay (µs). The value represents a momentary snapshot.

10.4.3 Configuration of the IP trunk

This procedure describes how to configure an IP trunk in a point-to-point configuration. The transmitting node is node 11.

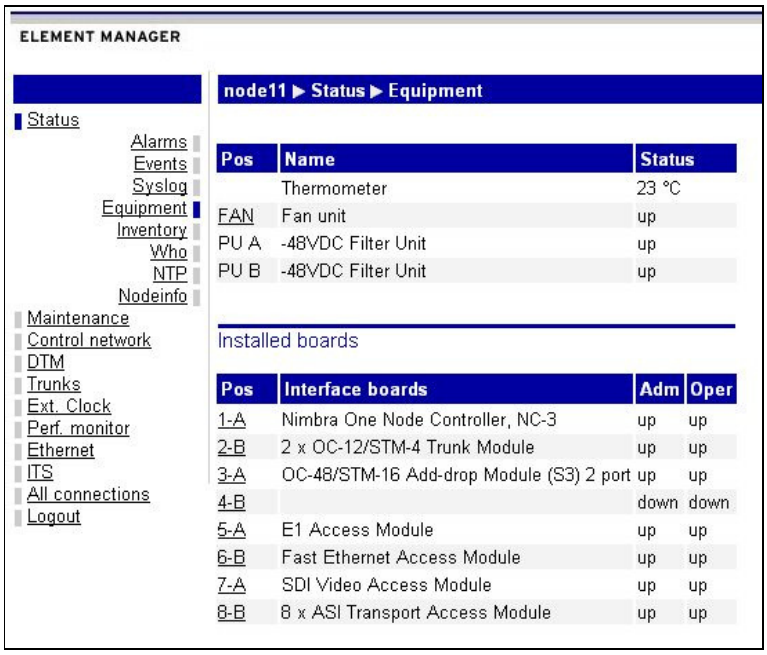


Figure 136. Node prior to installation of IP Trunk in slot #4.

Start with inserting the module into the slot in Nimbra One or Nimbra 300 series node. Set the administrative status to 'up'. The module can now be identified from the Status → Equipment link. The IP trunk is also available as a fixed interface on Nimbra 360.

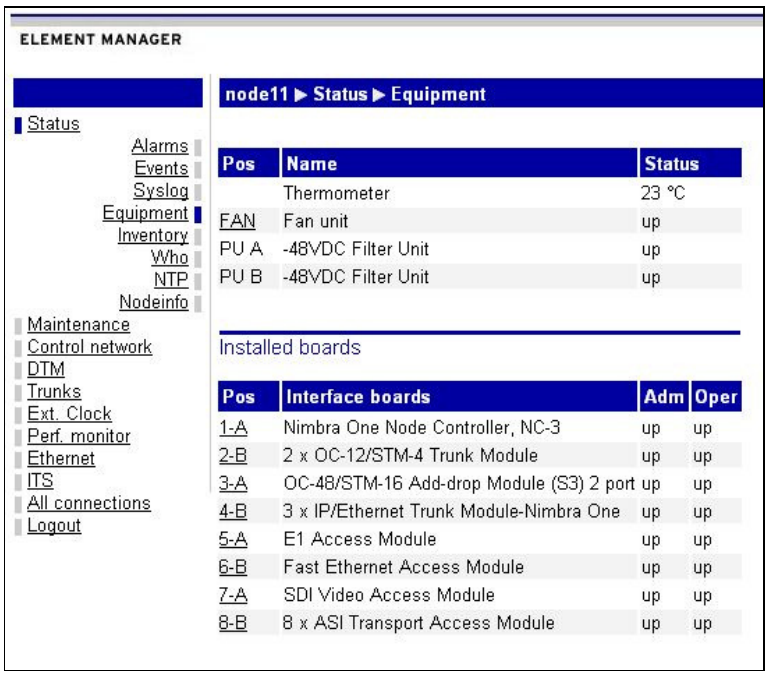


Figure 137. Node with installed IP Trunk module in slot # 4.

Connect the Ethernet cable or fiber. It is imperative that this step is followed, as DTM interfaces do not exist prior to this step is carried out and hence no DTM links can be established.

Now follow the link for Ethernet interfaces and select the appropriate interface, like etht-4:1. Make sure the administrative status is 'up'. Proceed with corresponding IP-trunk configuration, found under Trunk interfaces → ipt-4:1 in this example.

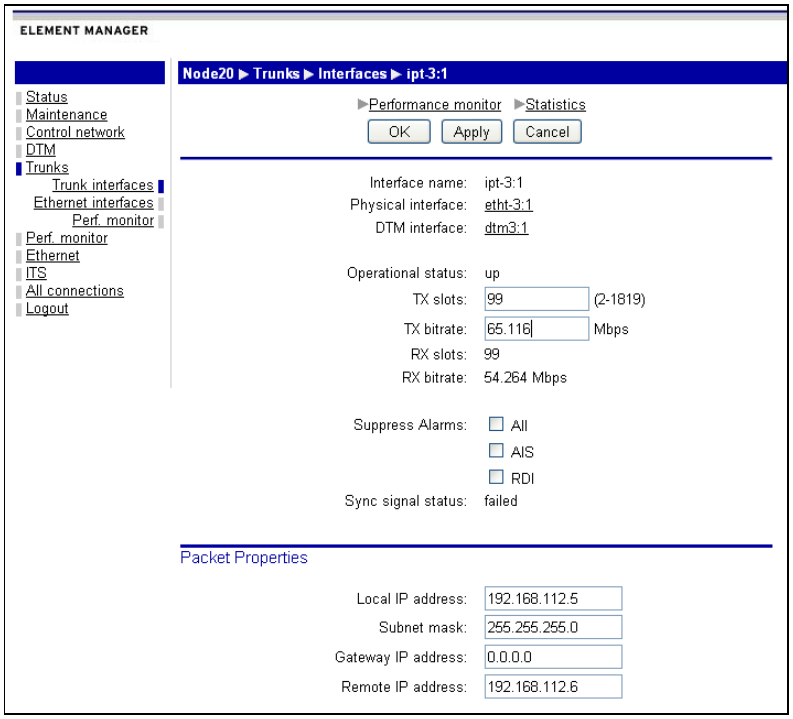


Figure 138. Configuration of IP Trunk, part one.

To configure the capacity of the IP trunk, fill in either TX slots or TX bitrate. Internally, TX slots are used. If TX bitrate is filled out, an integer number of TX slots is automatically filled out in the TX slots field and the TX bitrate is reduced slightly.

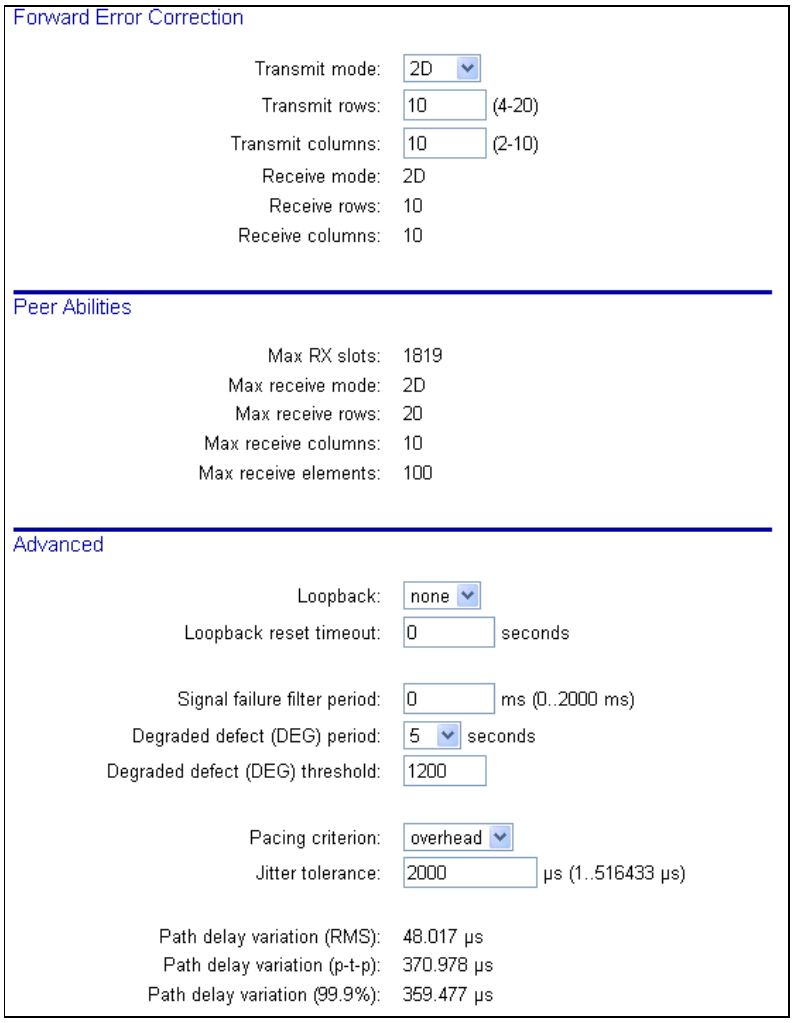


Figure 139. Configuration of IP Trunk, part two.

Make appropriate IP settings for local and remote (destination) node. Set netmask (always) and gateway if appropriate. It is essential that IP configuration is made properly, as no link is established otherwise.

Some additional settings are needed. The type of tagging used; VLAN, FEC, MTU and TTL. It is strongly suggested that all advanced settings are kept with their default values.

Once all Ethernet and IP trunk settings have been made on both sides of the connection, the DTM interfaces must have its administrative status set to ‘up’. Now the IP trunk should be connected.

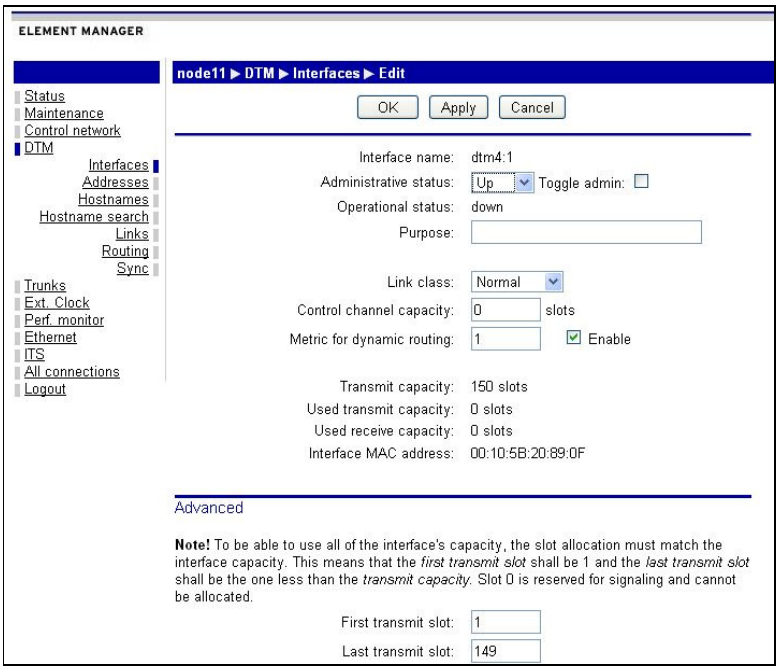


Figure 140. DTM interface configuration of the IP trunk.

10.4.4 Ethernet Interface Parameters

The Ethernet configuration is quite simple, but on the main page there are three different links for Basic settings, Advanced Settings and Statistics.

10.4.5 Basic settings

10.4.5.1 Administrative Status

Default value: 'Down'

Type: 'Down', 'Up'

Description: The module can be set to administratively active ('up') or inactive ('down').

10.4.5.2 Purpose

Default value: The empty string

Type: text string, up to 255 characters long

Description: A text tag that can be entered by the user for various purposes.

10.4.6 Advanced settings

The advanced settings concern the negotiation of operating mode with the remote (peer) interface.

10.4.6.1 Autonegotiate

Default value: 'On'

Type: Boolean variable

Range: 'On, 'Off'

Description: The variable describes if this feature (autonegotiate) is enabled or disabled.

10.4.6.2 Advertised speed

Default value: '1000,100,10'

Type: Text string, describing the available speeds of the Ethernet interface.

Range: 'auto','1000,100,10','1000,100','100,10','1000','100','10'

Description: A list of supported Ethernet interface speeds.

10.4.7 Alarms

The listing of alarms, made in the web browser on the IP interface configuration page, indicates for a selection of alarms if they are active or not. For alarms that are not active, the text "No Alarm" is displayed on a green background. For alarms that are active, the text "Alarm" is displayed on a background color associated with the severity of the alarm. For example, an alarm with severity critical is displayed on a red background and an alarm with severity warning is displayed on a cyan colored background. The listed alarms are:

10.4.7.1 Loss of signal (LOS)

Description: This alarm is received when the signal on the receive interface is missing.

Severity: Critical

10.4.7.2 Loss of frame (LOF)

Description: This alarm is received when the frame on the incoming signal cannot be properly aligned.

Severity: Critical

10.4.7.3 Loss of pointer (LOP)

Description: This alarm is received when the pointer of the incoming signal is missing (Bad alignment of DTM frames).

Severity: Critical

10.4.7.4 Loss of multiframe (LOM)

Description: This alarm is received when the FEC matrix on the incoming signal cannot be aligned.

Severity: Minor

10.4.7.5 Alarm Indication Signal (AIS)

Description: This alarm is received when a defect is detected by upstream equipment.

Severity: Warning

10.4.7.6 Remote Defect Indication (RDI)

Description: This alarm is received when a defect is detected by downstream equipment.

Severity: Warning

10.4.7.7 Degraded signal (DEG)

Description: This alarm is received when the signal on the IP network interface is degraded.

Severity: Critical

10.4.7.8 DPCP-IP negotiation failure (DNF)

Description: This alarm is received when the two trunk interfaces cannot set up a DTM link between each other.

Severity: Critical

10.4.7.9 Loopback

Description: This alarm is received when the interface is set by the user to loopback mode.

Severity: Warning

10.4.7.10 ICMP Alarm

Description: This alarm is generated when the node receives an ICMP error message. The text can be one of: 'Redirect', 'Target unreachable', 'Source quench' or 'Parameter problem' depending on the problem, when the signal on the receive interface is missing or misread.

Severity: Warning

10.4.7.11 *Configuration alarm*

Description: The alarm is raised when a new board is detected that cannot support the current configuration in O&M. Further information can be found in the errorMessage variable for each object configured on the board. The alarm can be cleared by reconfiguring each object that has an errorMessage, deleting the configuration from O&M, or by disabling the board in the Equipment Manager.

The probable cause is 'configuration or customization error' and the text is: "Object is not correctly configured".

Severity: Minor

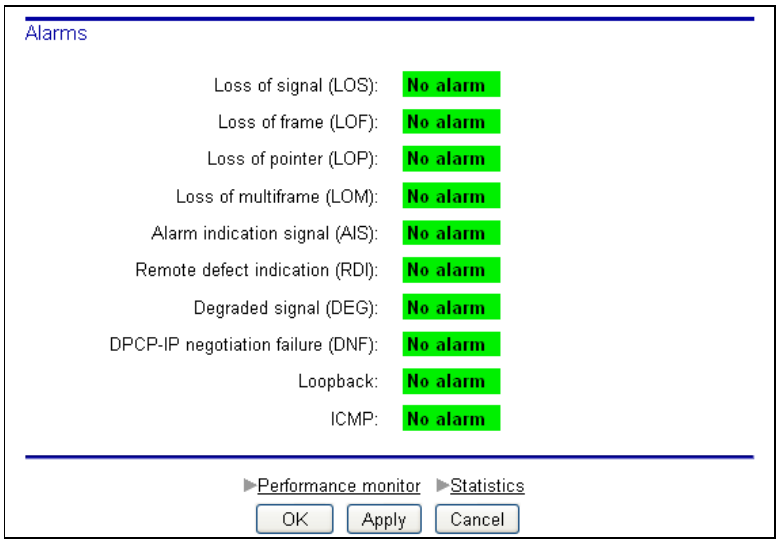


Figure 141. IP Trunk alarms

10.5 Statistics

10.5.1 General

Statistics is available on two separate levels for the IP trunk. One level is the underlying Ethernet/IP layer and one level is the DPP-IP Trunk level. In this description the available counters are described in separate sections.

10.5.2 DPP-IP Trunk level statistics

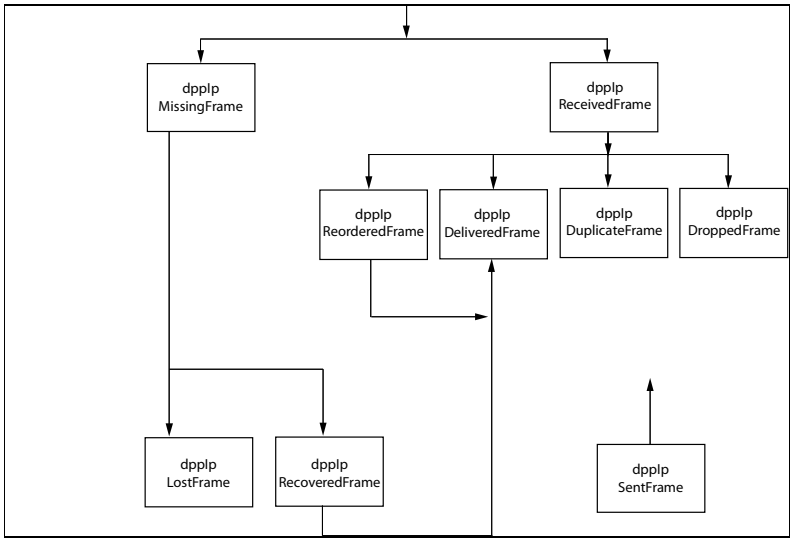


Figure 142. Relationship between the various DPP-IP counters

10.5.2.1 dppipDeliveredFrames

Description: The total number of DPP-IP frames that have been received and delivered to the DTM interface.

10.5.2.2 dppipDroppedFrames

Description: The number of DPP-IP frames that have been received and have not been delivered since the interface was unable to align its data into the DTM trunk stream.

10.5.2.3 dppipDuplicateFrames

Description: The number of DPP-IP frames that were received with a sequence number of an already processed DPP-IP frame.

10.5.2.4 dppipLostFrames

Description: The number of missing DPP-IP data frames that could not be delivered to the DTM interface.

10.5.2.5 dppipMissingFrames

Description: The number of DPP-IP frames that were missing in the frame sequence, i.e. the expected sequence number was not found in the DPP-IP framing buffer.

10.5.2.6 dppipReceivedFrames

Description: The total number of DPP-IP frames that have been received.

10.5.2.7 dppipRecoveredFrames

Description: The number of missing DPP-IP data frames that were recovered by the FEC procedure.

10.5.2.8 dppipReorderedFrames

Description: The number of DPP-IP frames that were received out of order, but could still be aligned to the DPP-IP frame sequence.

10.5.2.9 dppipSentFrames

Description: The number of DPP-IP frames that were sent on the DTM interface.

10.5.3 Ethernet/IP level statistics

These statistical counters are specified in IETF RFC 1213 or IETF RFC 2819.

10.5.3.1 etherStatsBroadcastPkts

Description: The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.

10.5.3.2 etherStatsCollisions

Description: The best estimate of the total number of collisions on this Ethernet segment.

10.5.3.3 etherStatsCRCAlignErrors

Description: The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive. The packet had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

10.5.3.4 etherStatsDropEvents

Description: The total number of events in which packets were dropped by the probe due to lack of resources. Note that this number is not necessarily the number of packets dropped; it is just the number of times this condition has been detected.

10.5.3.5 etherStatsFragments

Description: The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

10.5.3.6 etherStatsJabbers

Description: The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

10.5.3.7 etherStatsMulticastPkts

Description: The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.

10.5.3.8 etherStatsOctets

Description: The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).

10.5.3.9 etherStatsOversizePkts

The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.

10.5.3.10 etherStatsPkts

Description: The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

10.5.3.11 etherStatsPkts1024To1518Octets

Description: The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

10.5.3.12 etherStatsPkts128To255Octets

Description: The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

10.5.3.13 etherStatsPkts1519ToMaxSizeOctets

Description: The total number of packets (including bad packets) received that were between 1519 and the highest allowed frame size.

10.5.3.14 etherStatsPkts256To511Octets

Description: The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

10.5.3.15 etherStatsPkts512To1023Octets

Description: The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).

10.5.3.16 etherStatsPkts64Octets

Description: The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).

10.5.3.17 etherStatsPkts65To127Octets

Description: The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

10.5.3.18 etherStatsUndersizePkts

Description: The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.

10.5.3.19 ifInDiscards

Description: The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free buffer space.

10.5.3.20 ifInErrors

Description: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

10.5.3.21 ifInNUcastPkts

Description: The number of packets, delivered by this sub-layer to a higher (sub-) layer, which were addressed to a multicast or broadcast address at this sub-layer.

10.5.3.22 ifInOctets

Description: The total number of octets received on the interface, including framing characters.

10.5.3.23 ifInUcastPkts

Description: The number of packets, delivered by this sub-layer to a higher sub-layer, which were not addressed to a multicast or broadcast address at this sub-layer.

10.5.3.24 IfInUnknownProtos

Description: The number of packets received via the interface, which were discarded because of an unknown or unsupported protocol.

10.5.3.25 IfOutDiscards

Description: The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free buffer space.

10.5.3.26 IfOutErrors

Description: The number of outbound packets that could not be transmitted because of errors.

10.5.3.27 IfOutNUcastPkts

Description: The total number of packets that higher-level protocols have requested to be transmitted to a non-unicast (i.e., a subnetwork-broadcast or subnetwork-multicast) address, including those that were discarded or not sent.

10.5.3.28 IfOutOctets

Description: The total number of octets transmitted out of the interface, including framing characters.

10.5.3.29 IfOutUcastPkts

Description: The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or

broadcast address at this sub-layer, including those that were discarded or not sent.

10.5.4 Forward error correction

In order to configure the basic parameters of forward error correction, FEC transmit mode must be set. This variable has three possible values: “none”, 1D or 2D. “None” means that the FEC function is disabled. 1D or 2D indicates that one or two parity checks are made, as described below.

The FEC matrix, defined by ‘FEC, transmit rows’ and ‘FEC, transmit columns’ parameters can have one or two sets of parity sums. These parity sums are data packets of the same size as the data packets in the matrix. The packet size is defined by the MTU parameter, which is an integer in the range 64-1500 (default 1500). To create the 1D parity sum packet, bits of the same position in all packets in one column are added and divided modulo-2. In the example below, for the first bit of the 1D parity check sum of the first column, 1+0+1=2, which is congruent with 0 (modulo-2). In other words, the parity check sum in an even number. This is true for the second, third and forth bits as well in this example.

For 2D FEC mode, corresponding check sums are formed for both the row and the column. In this case, the column check sums are used first to correct erroneous packets. After this operation is finished, a second correction is made with the row check sums. With this method, it is sometimes (but not always) possible to correct dual faults in one row or column.

Observe that the size of the packets in the illustration below is kept well below the real minimum packet size (64 octets), to improve clarity.

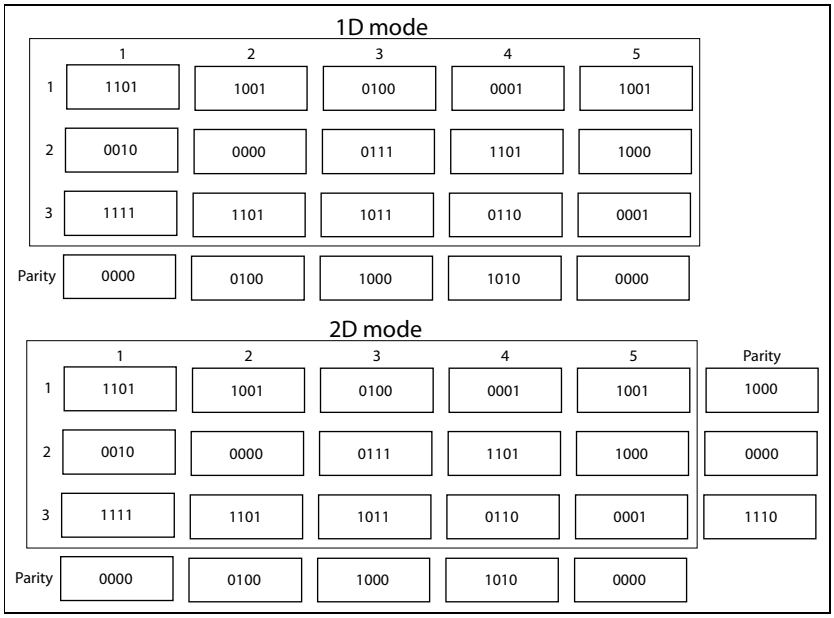


Figure 143. Structure of the FEC matrix for FEC Modes 1D and 2D.

10.5.5 Statistics

In order to view the different statistical counters previously described, follow the proper link. The statistical measures have been divided into DPP-IP

counters available from the Trunks→Trunk Interfaces→Interface name→Statistics link and Ethernet/IP counters available from the Ethernet Interfaces→Interface name →Statistics link (display of all counters).

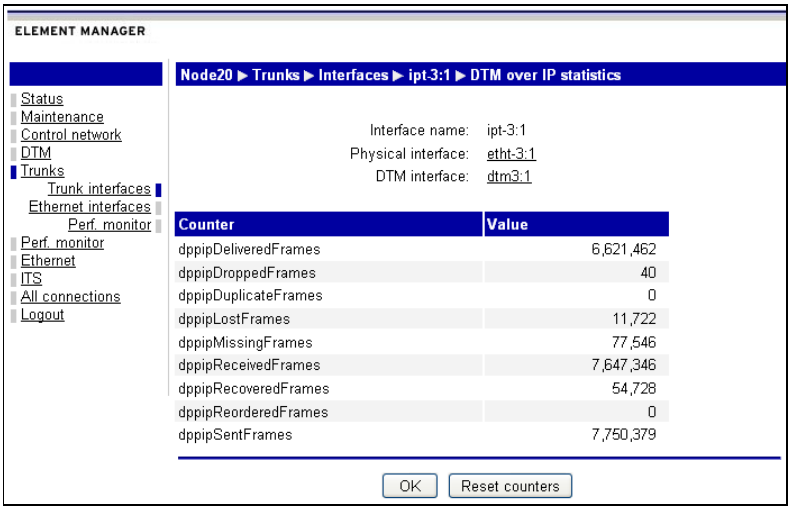


Figure 144. DPP-IP Statistical counters

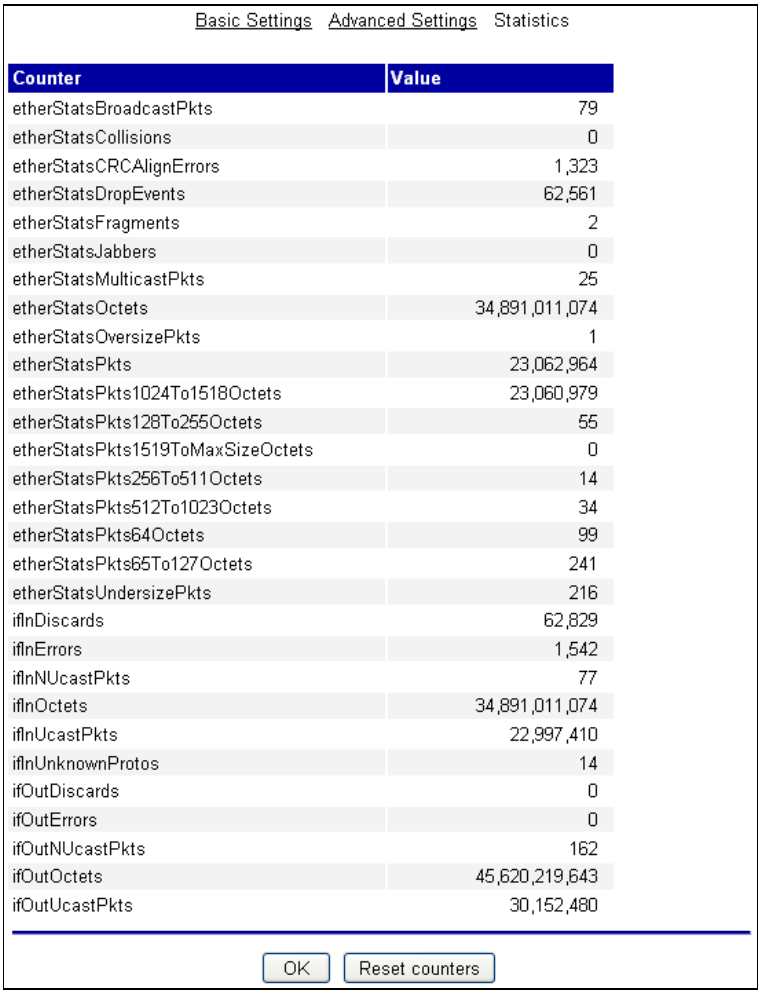


Figure 145. Ethernet statistical counters

11 Sync and Time Transfer

11.1 General

This chapter describes the synchronization principles of ETSI 201 803 networks, also known as DTM networks. While many aspects of network synchronization principles is similar to what is found in SDH/SONET networks, DTM has introduced some important new features in order to achieve an automated and robust network synchronization. This extra functionality reduces the burden of synchronization planning to a minimum and also reduces the risk for bad configuration of the synchronization network.

This chapter provides an understanding of the synchronization principles of Nimbra SDH/SONET/DTM networks and advises the user about configurational settings.

11.1.1 Relationship between SDH/SONET and DTM synchronization

DTM essentially augments SDH/SONET with higher granularity and non-hierarchical multi-service switching. Information carried in DTM frames inside SDH/SONET frames must be synchronized. DTM maintains its own synchronization mechanism that spans over the entire switched DTM network layer, independent of lower layer transport. DTM is usually transported over SDH/SONET, but it can also be transported over PDH (DS3/E3) or over IP/Ethernet (TP Trunk).

The synchronization mechanism is highly automated, in a plug-and-play fashion, and involves a bare minimum of manual configuration. In this document the essential guidelines are provided on how to configure SDH/SONET and the DTM synchronization in Nimbra equipment.

11.1.2 Synchronization considerations

11.1.2.1 SDH/SONET

The SDH/SONET interface does in principle not need to be synchronized since pointer justifications will handle any (normal) frequency differences that can occur. It is always best when every part of the network is synchronized to all other parts, but it is not critical for the operation of the DTM network, under most circumstances, if the SDH/SONET part of the

network is not perfectly synchronized. There are mechanisms in the DTM layer that handles these imperfections.

11.1.2.2 DTM

The primary role of DTM network synchronization is to synchronize information carried in DTM frames for switching. A secondary purpose is to maintain a timing quality level of the transported signal that is required by the most demanding services, such as transport of studio video content. The synchronization mechanism in Nimbra nodes addresses both these issues.

11.1.2.2.1 The synchronization signal

The synchronization signal in a DTM network is an 8 kHz clock that is extracted from the DTM frame start. The frame start is depending on the type of trunk interface, but for ETSI standardized, SDH/SONET interfaces the DTM frame start is equal to the start of the VC-4 -Xc/STS-3Xc, i.e. the J1 byte in the path overhead. On older trunk interfaces (i.e. the 1-port OC-3/STM-1 trunk and the OC-48/STM-16 trunk interface in the Nimbra 291) the DTM frame was "floating" in the VC-4 -Xc/STS-3Xc and had a special frame start pattern, which identified the frame start. The 4 x DS3/E3 trunk uses the A1A2 frame alignment word as frame start in the E3 mode. In DS3 mode, a 125 µs frame is mapped into the DS3 payload and the A1A2 frame alignment word of this frame is used as frame start.

In the IP/Ethernet trunk the frame sync signal is encoded as a time-stamp in the DPP-IP overhead in the IP/UDP packet.

11.1.2.2.2 SDH/SONET and DTM sync in co-operation

In a modern SDH/SONET/DTM network, the two synchronization mechanisms are co-operating. DTM maintains its own "overlay" timing domain, which is governed by the DTM synchronization reference clock. This timing domain controls and synchronizes the transmission of the DTM frames, i.e. the VC-4 -Xc/STS-3Xc of the network. The frequency difference between this domain and the various parts of the SDH/SONET network is handled by pointer justifications in the SDH/SONET layer.

11.1.2.2.3 Sync transport over IP/MPLS/Ethernet networks

The sync system treats IP/MPLS/Ethernet networks in the same way as a SDH/SONET network. An 8 kHz clock is transported over the packet network and recovered to become the node synchronization signal. Of course, the transport properties of a packet based network are different from those of a synchronous or optical network. The IP/Ethernet trunk has different mechanisms, like Forward Error Correction, to overcome packet loss and jitter that are prevalent in the packet network.

11.1.2.2.4 Summary

The DTM synchronization mechanism has a number of advantages compared to traditional synchronization methods. The most important are:

- Mostly automatic, a minimum of configuration is required
- Eliminates synchronization configuration errors and synchronization path loops
- Robust against link, node, and reference clock failures
- Interworks with SDH/SONET synchronization
- Is forgiving to SDH/SONET synchronization mis-configuration

- Works over a heterogeneous infrastructure including dark fiber, wavelength, SDH, SONET, PDH (E3/DS3) or IP/MPLS/Ethernet
- Works automatically over any topology, including a mix of mesh, ring, star, bus or point-to-point topologies
- Works over any mix of transport technologies, such as optical, coax and microwave networks

11.2 Synchronization in detail

The synchronization architecture is based on the following components:

- DSYP, the network-wide synchronization protocol
- Node synchronization, node specific functionality
- Interface synchronization, SDH/SONET specific parts

All nodes in a network are synchronized to a common reference source in a master-slave scheme. The synchronization topology is a minimum spanning tree that is calculated by a node distributed algorithm, which assures shortest path between the reference source and all nodes. Hence synchronization loops are eliminated. During a fault, affected nodes enter hold-over mode until a new spanning tree has been calculated. This takes at most a couple of seconds. In hold-over mode, phase and frequency continuity is maintained, i.e. nodes are acting as “fly-wheels”.

11.2.1 The DSYP Protocol

DSYP, the DTM Synchronization Protocol, is a protocol that exchanges synchronization information between nodes of the network. The protocol data unit that is exchanged contains information about:

- Node ID of synchronization master, i.e. the node that is connected to an external reference clock
- Priority of the sync master
- Number of nodes traversed to reach the sync master
- Other maintenance information

11.2.1.1 Operation in a fault-free network

All nodes exchange DSYP information with its neighbors. Based on the information, a distributed algorithm (Bellman-Ford) calculates a minimum spanning tree that ensures that each node in the network is synchronized to the sync master along the path with minimum number of hops. In case there are several sync masters in the network, the one with the highest prio (lowest prio number) will be selected as sync master. If the active sync master fails, the network will automatically synchronize to the next highest prio sync master. There can be up to 14 sync masters in a network. If two sync masters have the same prio set, the sync master with lowest node ID (MAC address) is used and an alarm is issued. Finally, if there is no assigned sync master in the network, the used master clock is the node clock of the node with the lowest ID (MAC address).

Different node types have different quality of their node clocks. Running the network without an external clock reference may be adequate for certain

applications, but it is strongly recommended to have at least one primary and one secondary (backup) external reference.

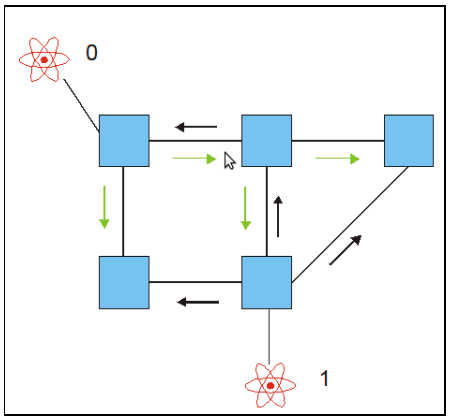


Figure 146. Synchronization of a DTM network. During fault free operation, the network is synchronized to the external reference clock 0. A minimal spanning tree is built from this clock to all other nodes. When it fails, the network is synchronized to the backup master; clock 1.

11.2.1.2 *Operation during network faults*

In case of a link or node failure, downstream nodes will detect Loss of Frame Synchronization (LOFS). This alarm moves the node synchronization function into a hold-over state in which the node continues to run at the network frequency that it had learned while locked to the sync master. Meantime DSYP calculates a new minimum spanning tree and eventually signal to the node sync function that there is a new sync path available. The node sync then selects the new interface as sync interface. Typically, the process takes a couple of seconds; thus the time the node spends in hold-over mode is negligible from a timing/wander perspective.

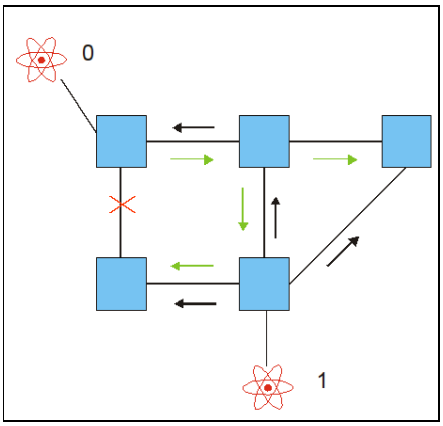


Figure 147. A fault on the leftmost link will automatically result in a new minimal spanning tree from sync master 0. During recalculation of the spanning tree, the involved nodes (in this case the lower left node) will be in hold-over mode.

11.2.2 The node synchronization function

The node synchronization function coordinates all synchronization tasks that are local to the node. Among these are

- Selection of node synchronization source (as ordered by DSYP)
- Smoothing of the synchronization signal
- Distribution of the smoothed signal to all outgoing trunk interfaces
- Providing a hold-over mode in case of lost synchronization source
- Ensuring phase continuity when changing sync source
- Supervision of available sync sources

11.2.2.1 Selection of source

A Nimbra node has three possible types of sync sources, which is selected by the DSYP protocol as described before. The sources are:

1. An external reference clock attached to the “Sync In” port
2. The incoming signal from a trunk interface.
3. The built-in node clock

The order above reflects their relative importance. However, since the DTM network is fully synchronous, there can be only one sync master active in the network at any given time. Hence the most common sync source for a node is an incoming signal from a trunk interface. The built-in node clock is only used if there is no external reference clock in the network. Then one node (the one with the lowest MAC address) becomes the timing reference source from its built-in oscillator.

When the network is physically divided into two or more parts by a node or link failure, the part without contact with the external reference source is synchronized according to the description above. This case essentially means that the network has been split into two or more separate networks. If there is connectivity such that services can connect, then synchronization also can, and will, be re-established.

11.2.2.2 Sync enable/disable on DTM interfaces

In all releases up to GX4.7, synchronization information is carried automatically over the DTM interface and DTM layer. On the receiving side of the link, there is always a synchronization signal to recreate from the link. The synchronization signal selected by the node is then the signal with lowest priority number. If no external clock sources are available, the internal clock of the node with the lowest MAC address is used.

A feature, included from system software release GX4.7, is synchronization enable/disable on DTM-interfaces. By default, this parameter is enabled on all DTM interfaces.

This feature makes it possible for the user to manually disable the incoming DTM synchronization, per interface. The usage of this feature is in cases where the synchronization information of a particular DTM interface is unreliable and should not, under any circumstances, be used at the receiving node. As a consequence, the disabled sync information is not propagated to other nodes in the network from the node with the disabled interface.

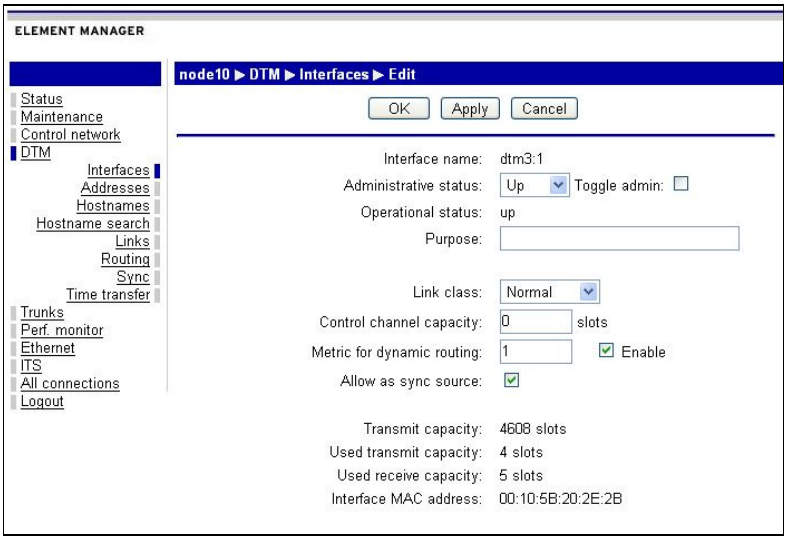


Figure 148. By deselecting 'Allow as sync source', the user selects not to extract synchronization information from the DTM interface.

11.2.2.3 Smoothing of the sync signal

Smoothing of the sync signal is done with a digital phase-locked loop (PLL) that smoothes out jitter from for example pointer justifications on the SDH/SONET layer. The smooth signal is then distributed to all outgoing trunk interfaces such that all outgoing frames are aligned and synchronized with this signal.

11.2.2.4 Hold-over mode

If the node sync function detects that the current sync source is unavailable, the node enters hold-over mode. In hold-over mode, the node sync signal is obtained from the built-in oscillator, which is adjusted to the average of the frequency of the sync signal over a certain time before the fault. The time spent in hold-over mode before a new sync source is found, is in general much shorter than in traditional SDH/SONET networks. Consequently, phase drift and wander associated with it, is negligible.

11.2.2.5 Phase continuity

When DSYP orders a new sync source, the node sync function must ensure that the outgoing phase is undisturbed. This is done by adding, to the new sync source, an amount of phase corresponding to the difference between the new sync sources and the node sync signal. This makes the outgoing sync signal "transparent" to sync changes.

The node sync function also monitors and maintains the available sync sources.

11.2.2.6 IP/Ethernet trunk

The same fundamental concepts are kept for providing sync over an IP/MPLS/Ethernet network, but the methods for recovering the sync signals are adjusted to handle the higher levels of jitter and wander associated with a packet based transport.

11.3 SDH/SONET synchronization

As mentioned in the introduction SDH/SONET synchronization is non-critical, since DTM maintains a "timing overlay synchronization network" independent of timing of lower layers. However, Nimbra equipment has SDH/SONET sync functionality and these will be described here and the differences among interfaces will be described in a separate chapter.

11.3.1 Timing modes

The functionality of the Nimbra trunk interfaces with respect to SDH/SONET is to set a timing mode for the line interface. Each trunk interface support all or a sub-set of the following timing modes:

- Network timing: The line rate is synchronized to the DTM network frequency.
  Applies to: All newer Nimbra One/300 trunks, 4 x DS3/E3, all Nimbra 600 series trunks
- Interface timing: The line rate is synchronized to an on-board local oscillator. Applies to: 4xOC-3/STM-1 Trunk (NPS0009-X/3S32), OC-12/STM-4 Trunk and 4xOC-3/STM-1 Access.
- Loop timing: The line rate is synchronized to the incoming line frequency. Applies to: 4xOC-3/STM-1 Trunk (NPS0009-X/3S32), OC-12/STM-4 Trunk and 4xOC-3/STM-1 Access

In Interface timing mode, the line frequency is asynchronous with the DTM Network timing and pointer justifications are performed in the transmit direction in order synchronize the VC-4 -Xc/STS-3Xc to the line rate.

In Loop timing mode, the line frequency can be asynchronous but it may also be synchronous with the DTM network timing if the SDH/SONET network is synchronized with the same reference clock that synchronizes the DTM network. In this case, we have a fully synchronous network, since we have then no pointer justifications at all. If not, pointer justification in the transmit direction applies as in the Interface mode described above.

Finally in Network timing mode line rate is synchronized to the DTM network frequency and hence no pointer justifications are needed in the transmit direction. In this case we can also have a fully synchronous SDH/SONET/DTM network if the same reference clock is used for both SDH/SONET and DTM.

The IP/Ethernet trunk is timed in a way that is similar to the Network timing mode, although there is no real corresponding concept for line timing of a packet stream.

11.3.2 Transport of SDH/SONET synchronization

Note that when running in either “Interface” or “Loop” timing modes the trunks are not intended for SDH/SONET sync transport; they are rather “DNU” (Do Not Use for synchronization) clocks. This applies especially for the older trunk interfaces, the 1-port OC-3/STM-1 and OC-12/STM-4 trunk, which have Stratum 4 clocks. The 4 x OC-3/STM-1 Trunk/Access Module has a Stratum 3 clock and can, if necessary, be used to source synchronization to a SDH/SONET sub-net. From a SDH/SONET synchronization perspective these boards should be considered as SDH/SONET termination equipment.

Interfaces that support Network timing mode can be used to transport SDH/SONET synchronization, provided that the network is synchronized by a suitable external reference clock. This applies to the OC-48/STM-16 X-ADM and the 4 x DS3/E3 trunk modules.

11.3.2.1 Hold-over and free-running properties

As mentioned before, a Nimbra switch is never in hold-over for longer than at maximum a couple of seconds. This is by the design of the DTM synchronization mechanism. During this time, the clock in hold-over mode obtains the network frequency as learned while we are in a clocked state. The effects of the residual frequency difference between the real network frequency and the sourced frequency in the short hold-over time is about 0.1 ppm and is negligible due to the short time the node is actually in hold-over.

Thus there is no such state as “free-running” for a DTM network, unless the network is not synchronized to an external reference clock of good quality. If the network does not have an external clock source, the network is synchronized to one of the nodes internal clock that is free-running. Since all other node-clocks are locked to this internal clock, all network timing properties are also governed by this clock. Now, the timing properties are governed by the quality of the node clocks. In Nimbra 300 and 600 series switches, they are of SEC/Stratum 3 quality and in Nimbra One they are of Stratum 4 quality. Unfortunately, it is not possible to set a node as sync master in order to use a node with a better clock. The choice is made by DSYP (the node with lowest node-ID (MAC address) acts as sync master). For this and other reasons, it is recommended to use an external clock reference, see 11.5.1.

11.4 IP/Ethernet Trunk

The synchronization performance of the IP/Ethernet trunk is affected by the quality of the IP connection. The more packet jitter, the more jitter/wander on the recovered sync signal. The quality of the IP/Ethernet trunk can be monitored by inspecting the Synchronization Signal Status. This Status has three values[1]

[1] The limits (i.e. when to make a transition from state to another) in the initial GX4.5 release are can be considered temporary and will be adjusted after feedback from use in real networks, since lab networks and network simulators may not provide the same typical packet jitter distributions as in real networks.

Normal – Recovered node sync is of G.813 quality, i.e. of the same quality as given by a SDH/Sonet equipment clock (ADM).

Degraded – Recovered sync is not of G.813 quality, due to packet delay variations outside what can be handled, but is still used. Performance degradation can be expected.

Failed – Recovered sync is not usable, the node selects another synchronization source as decided by the DSYP protocol. Frame slips can be expected.

11.5 Configuration recommendations

11.5.1 External reference clocks - requirements

A strong general recommendation is to use an external reference clock with high accuracy and stability. Some networks works perfectly well without an external reference clock while other networks may function but with lower service quality. Some networks may fail to operate completely without an external clock reference. In the table some suggestions are listed:

Ext. reference clock needed?	Network contains	Why?
Yes, must have	Nimbra One with OC-48/STM-16 X-ADM or 2 x OC-12/STM-4 Trunk or 4 x OC-3/STM-1 Trunk (newer - X/3S32) or 4 x DS3/E3 Trunk Nimbra 680	If there is no external reference clock, the network may synchronize to a Nimbra One with a built-in Stratum 4 oscillator, and since the listed trunk supports only network timing mode this may result in a line rate that exceeds the ±4.6 ppm SDH/SONET standard limits.
Yes, preferred	SDI Video service	This service has a very hard requirement on drift rate that can only be guaranteed with a high stability clock reference.
No	None of the above	OK for smaller networks with less requirements on wander performance, such as for Ethernet transport for example.

Figure 149. External clock recommendations.

The requirements on the external reference clock are:

- High stability (preferably Stratum 1 or sourced from GPS)
- 2.048 MHz output, according to ITU-T G.703.13, sine or square wave[2]
- Alternatively, a 1.544 MHz output with the same electrical properties as the 2.048 MHz clock described above may be used.

D4, SF or ESF formatted T1 timing signals cannot be used as synchronization source.

[2] Note that 2.048/1.544 MHz signals shall be “clock signals”, i.e. sine or square wave. The port does not support E1/DS1 framed signals. The external sync in port automatically detects if a 2.048 or 1.544 MHz clock is attached.

Note:	Please note, D4, SF or ESF formatted T1 timing signals cannot be used as synchronization source.

Nimbra 360 can also use a10 MHz signal as reference input.

Redundant GPS controlled sources are preferable. If the primary reference clock goes down, DSYP will switch over to a secondary reference clock with the same frequency, and thus avoid a possible frame-slip in the transition process.

It is recommended to connect the external reference clock to a centrally positioned node, in order to get as few hops as possible to all or most nodes and make the reference clock easily available for maintenance.

11.5.2 External reference clocks – configuration

The external reference clock is configured on two separate web pages. They are found from the DTM → Sync and Ext clock → Interfaces. Configurations are node type specific and described later in this chapter.

11.5.2.1 Priority and admin status

The reference clock, both for sync usage and time transfer usage, must have administrative state set to 'Up' to be active. To set admin state, click on the DTM link and subsequently on the Sync link. The following page appears.

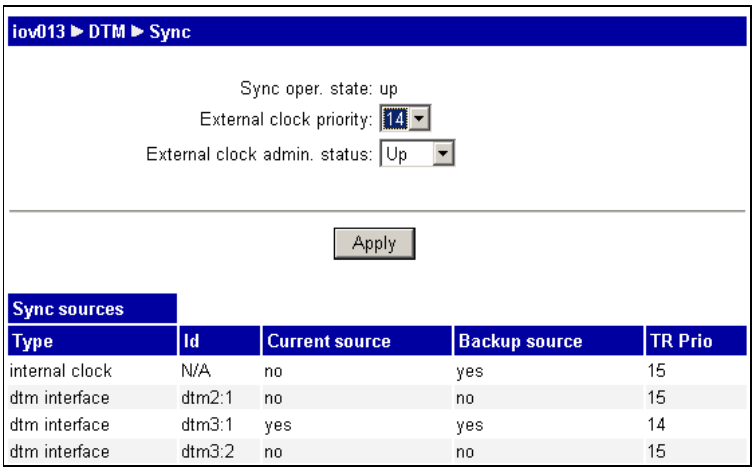


Figure 150. The Sync page

The web page shows the different synchronization sources and their status, as follows:

The Sync operational state variable can be either 'Up' (the unit is synchronized), 'Pending' (the unit is starting up), or 'Down' (error in sync function). The error is shown in the Alarms list.

The External clock priority parameter can be set to an integer between 0 and 14. The lower the priority setting is, the higher the priority is.

The External clock administrative status can be set to 'Up' or 'Down'. If it is set to down, the clock cannot be used by the node; if it is set to 'Up' it is available to the node.

Type: Specifies if the clock is internal, external or if timing is obtained from another node via a DTM link.

Id: Shows interface Id for all interfaces.

Current source: ‘Yes’ if this source is currently used, ‘No’ otherwise.

Backup source: ‘Yes’ if the clock is the current backup source, ‘No’ if it isn’t.

TR Prio: Priority (0 to 15); the lower this number, the higher the clock priority.

When using only internal sync, all clocks have TR prio 15 as they are internal. The node with the lowest Node Mac/If address is the sync master.

External clocks have lower TR Prio (i.e. higher priority), but if two external clocks are assigned the same priority (which shouldn't be the case) and these clocks are highest in priority, the system will detect this, send an alarm, and choose the one with lowest Mac/If address of the node to which they are attached as sync master.

11.5.2.1.1 Fault Indications

The external clock interfaces do not provide any alarms. Instead alarms are handled through DSYP and Time Transfer objects in following way:

Input faults generate a ‘No external sync source available’ alarm from DSYP. More details concerning faults can be viewed as ‘Defects’ from SQC itself.

Output faults (PPS+10MHz) generate a ‘Threshold crossed’ alarm from time transfer. More details concerning faults can be viewed as ‘Defects’ from SQC itself.

On 360, faults are also indicated by LED colors in following ways:

Sync RX+TX: PPS status green, sync status green on success and red on defects.

Sync RX: PPS status black, sync status green on success and red on defects.

Sync TX: PPS status green, sync status black.

PPS+10MHz RX: PPS status green on success and red either on PPS defects

10MHz defects (PPS cannot work without a valid 10MHz signal), sync status green on success and red on 10MHz defects.

PPS+10Mhz TX: PPS + Sync status green on success and red on defects.

11.5.2.1.2 Defects

Details on the faults described in the previous chapter can be found by following the link External Clock → Interfaces and sqc-1 or sqc-2 depending on which clock is under consideration.

Defect	Description
Loss Of Signal (LOS)	No input signal detected.
Loss Of Frame (LOF)	Input signal not properly aligned to reference clock. Most frequently caused by too large frequency deviation between reference clock and input signal (should probably be renamed to something better).
Signal Frequency Mismatch (SFM)	Input frequency does not match requirements of operational mode (e.g. 2048kHz in PPS+10Mhz operational mode).
Excessive Phase Deviation (EPD)	Output realignment limit has been exceeded.
Loss Of Alignment (LOA)	Output reassignment limit has been exceeded.
Ok	No defect detected

Figure 151. Details of Defects of the squelchable clocks described above.

11.5.2.1.3 Sync Source Selection

As previously, if an external clock has administrative status 'Up', it is selected as timing source unless an input signal failure occurs or an external clock with higher priority exists in network.

For PPS+10MHz, both input signals must be valid for the external clock to be selected as timing source. In theory, only a valid 10MHz should be enough; however since there is no dedicated alarm for PPS and since an alternative external clock with both PPS and 10MHz available may exist in network, this solution is a good trade off.

11.5.2.2 Node specific configuration

The node specific configuration is made from the link Ext. clock → Interfaces.

11.5.2.2.1 Nimbra One

In Nimbra One nodes, one external clock interface is available. The external clock source is attached to the front of the node with an SMB connector (75 Ω). This is the only available clock interface for Nimbra One. In the web interface, the clock is configured.

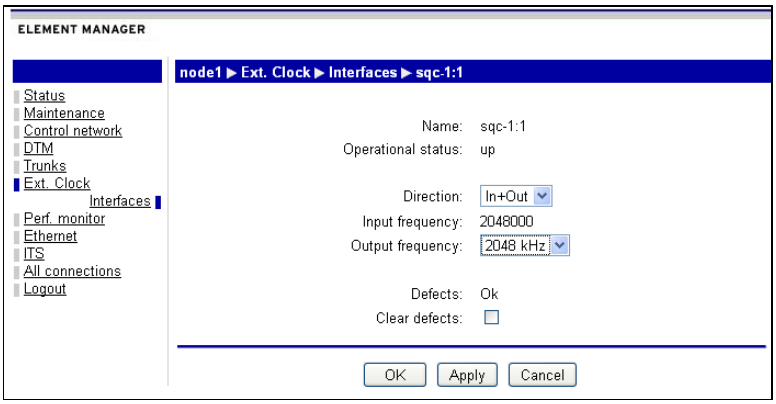


Figure 152. Configuration of the clock interface sqc-1:1 in Nimbra One.

11.5.2.2.2 Nimbra 340

In Nimbra 340 nodes, one external sync interface is available. The external clock source is attached to the front of the node with an BNC connector (75 Ω). This is the only available clock interface for Nimbra 340. In the web interface, the clock is configured.

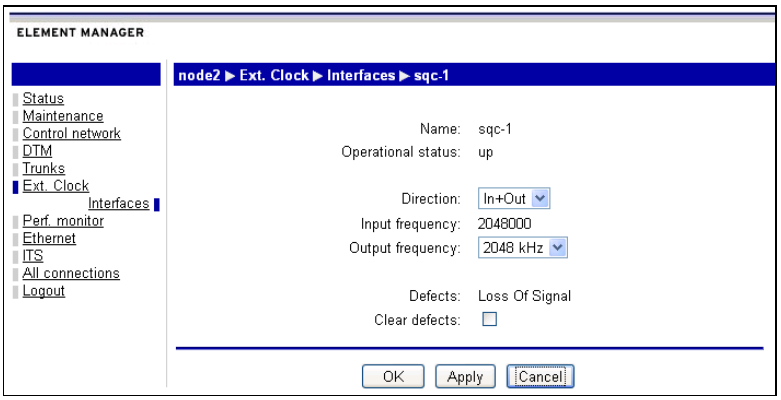


Figure 153. Configuration of sqc-1 in Nimbra 340.

The parameters for Nimbra One and Nimbra 340 are:

11.5.2.2.2.1 Direction

Default value: In + Out

Type: One of In + Out, In, Out

Range: In + Out, In, Out

Description: Active direction for the external synchronization clocks. In + Out means that both in- and output interfaces are enabled, In means that only the input interface is enabled and Out means that only the output interface is enabled.

11.5.2.2.2.2 Output frequency

Default value: 2048 kHz

Type: One of 8 kHz, 1544 kHz and 2048 kHz.

Range: 8 kHz, 1544 kHz or 2048 kHz

Description: This is the frequency delivered to the external sync output.

11.5.2.2.2.3 Clear defects

Default value: Unticked

Type: Checkbox

Range: Ticked, unticked

Description: Ticking this box and clicking on OK or Apply clears the presented defect(s).

11.5.2.2.3 Nimbra 360

In Nimbra 360 nodes, there are two different external clock interfaces, sqc-1 and sqc-2. On the physical node, they can be found at the lower right side, with notations TSI-1 (sqc-1) and TSI-2 (sqc-2).

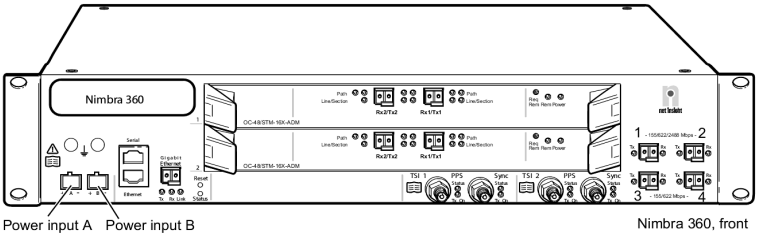


Figure 154. Nimbra 360 front. The sync interfaces are found at the lower right side.

Configuration of TSI-1/sqc-1 includes one parameter, time dual frequency mode, with possible values ‘none ‘or ‘PPS + 10 MHz’. With the parameter set to none, the port is transformed to a regular external clock interface of the same type as on Nimbra 340/Nimbra One.

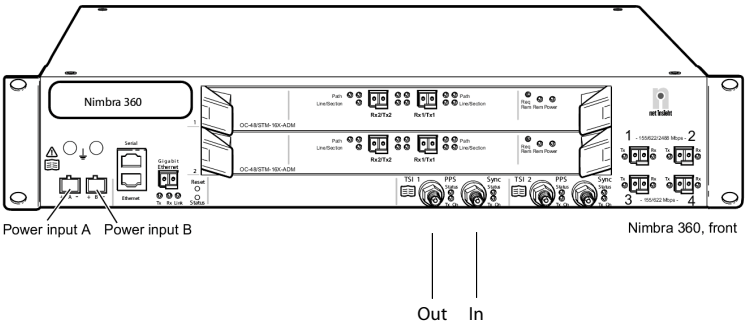


Figure 155. Nimbra 360 with TSI-1/sqc-1 configured with Time Dual Frequency Mode equal to ‘None’.

The sqc-1 interface for Nimbra 360 looks a bit different from the corresponding interface in Nimbra One/340. There are some additional parameters to configure.

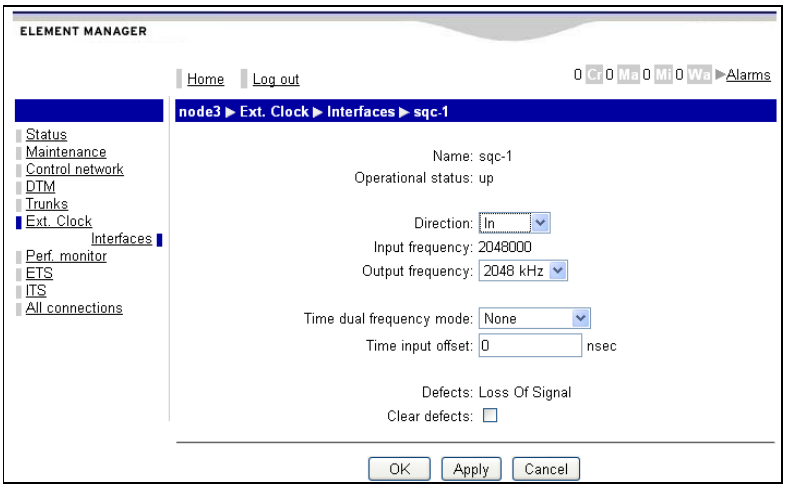


Figure 156. Configuration of sqc-1/TSI-1 of Nimbra 360.

When Time Dual Frequency Mode is set to 'none', the parameters to configure are the same as for the Nimbra One/340 case plus 'Time input offset'. Time input offset is a calibration factor for the time it takes for the clock signal (from its source) to reach the Nimbra 360 node, but it is only relevant for Time Dual Frequency Mode set to PPS + 10 MHz, described in next section.

When Time Dual Frequency Mode is set to PPS + 10 MHz, TSI-1 expects to receive two signals: one PPS (pulse per second) on the PPS port and one 10 MHz signal on the Sync port if the Direction parameter is set to In. If the parameter is set to 'Out' the pulses are extracted on the interfaces. Selecting the clear defects box and clicking on OK or Apply clears the presented defect(s) as for Nimbra One/340.

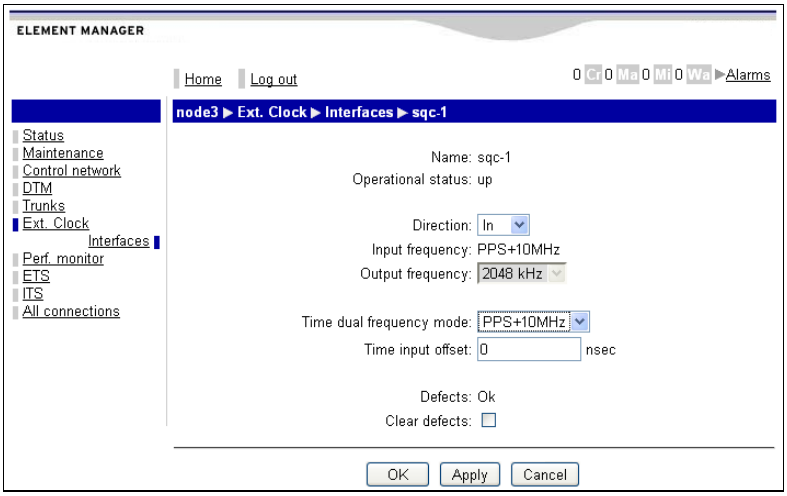


Figure 157. Configuration of sqc-1/TSI-1 of Nimbra 360 with Time dual frequency mode set to PPS+10 MHz. Note that as the direction is 'In', the parameter Output frequency is not used.

The one remaining parameter to configure is Time input offset. This parameter is the time from source to Nimbra 360 of the PPS signal.

Input frequency (MHz)	Defects	Interpretation
0	Loss of signal	Both PPS+10MHz are faulty
10	Loss of Signal	PPS is faulty, but 10 MHz is OK
PPS	Loss Of Signal	PPS is OK, but 10 MHz is faulty
PPS+10Mhz	OK	Both PPS+10Mhz are OK

Figure 158. The four different combinations of PPS and 10 MHz. Under normal time transfer operation, PPS should always be attached.

The other interface on Nimbra 360, TSI-2/sqc-2, can be used as an output interface with time dual frequency mode set to PPS+10 MHz.

If one or both expected signals are missing or of poor quality, it can be deducted from the web interface where the problem is. It is sufficient to look at Input frequency and Defects.

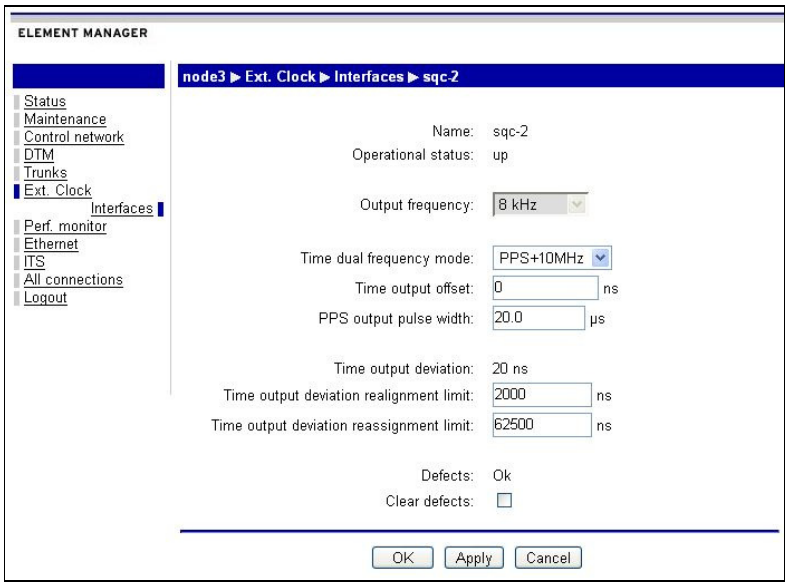


Figure 159. Configuration of sqc-2/TSI-2 of Nimbra 360 with Time dual frequency mode set to PPS+10 MHz.

The parameters to configure, in addition to time dual frequency mode, are:

11.5.2.2.3.1 Output frequency (kHz)

Default value: 2048 kHz

Type: one of three values, real

Range: 8 kHz, 1544kHz, 2048 kHz

Description: This is the frequency delivered to the Out port when the interface is in sync mode. The parameter can be set independently on both configurable ports.

11.5.2.2.3.2 Time output offset

Default value: 0 ns

Type: real value, unit ns

Range: -999999999 to +999999999

Description: This is delay from the Nimbra 360 to the destination of the sync signal. If this is another Nimbra 360, the compensation can also be done on the input of that node.

11.5.2.2.3.3 PPS output pulse width

Default value: 20 µs

Type: real value, unit µs

Range: 0.1-999999.9

Description: This is pulse width of the PPS output pulse, configurable in steps of 0.1 µs.

11.5.2.2.3.4 Time output deviation realignment limit

Default value: 2000 ns

Type: real value, unit ns

Range: 0-999999999

Description: This is deviation value where the sync jumps back to its nominal value. This action causes a temporary loss of sync.

11.5.2.2.3.5 Time output deviation reassignment limit

Default value: 62500 ns

Type: real value, unit ns

Range: 0-999999999

Description: This is deviation value where an alarm is generated.

11.5.3 Trunk interface configurations

Different trunk interfaces has different capabilities with respect to SDH/SONET synchronization. In this section, the various interfaces are discussed and recommended settings are given. Below is a table that summarizes capabilities and recommended settings.

Trunk interface	Capabilities	Choices	Default	Recomm.	Comments
Nimbra One/300 series					
4 x OC-3/STM-1 Trunk (-X/3S31)	Transmit sync source	Interface Loop	Interface	Interface	As discussed in this document
4 x OC-3/STM-1 Access	Transmit sync source	Internal Loop	Loop	Loop	Internal = Interface
	Synchronization Status message (SSM)	0..15	15	15	15 = DNU (see OC-48 above)
4 x DS3/E3 Trunk	Receive sync (RX_FSYNC) source	Line FSP	Line	Line FSP (if Time transfer is used)	DS3: Line = synchronized to line signal FSP = synchronized to Frame Start Pattern
OC-12/STM-4 Trunk	Transmit sync source	Interface Loop	Interface	Interface	As discussed in this document
OC-3/STM-1 Trunk	Transmit sync source	Interface Loop	Interface	Interface	As discussed in this document
3 x IP/Ethernet Trunk	Enable sync recovery	Checked Unchecked	Checked	Depending on use case	As discussed in this document
Nimbra 600 series					
4 x OC-3/12/48 / STM-1/4/16 Trunk	None	N/A	N/A	N/A	Uses Network timing mode
OC-192 / STM-64 Trunk	None	N/A	N/A	N/A	Uses Network timing mode

Figure 160. Capabilities of Nimbra trunks

11.5.3.1 Trunks for Nimbra One/300

11.5.3.1.1 OC-48/STM-16 X-ADM, 2 x OC-12/STM-4 Trunk and 4 x OC-3/STM-1 Trunk Module (NPS0009-X/3S32)

These trunks only support Network sync mode, so there is no timing mode to configure. Note that it is important that the network frequency is kept within ±4.6 ppm in order to comply with SDH/SONET standards (see 11.5.1). The on-board clock quality is of SEC/Stratum 3.

11.5.3.1.2 OC-12/STM-4 Trunk, 4 x OC-3/STM-1 Trunk/Access (NPS0009-X/3S31) and OC-3/STM-1 Trunk Module

These nodes support interface and loop timing modes. Default is interface timing mode and this is also the recommended mode. Loop timing mode may be used when the trunk interface is connected to SDH/SONET network that sources timing. When two OC-12 trunks are directly connected via a fiber or wavelength the following combinations exists:

Interface <-> Interface	OK
Interface <-> Loop	OK
Loop <-> Interface	OK
Loop <-> Loop	Not OK

The last combination would lead to a timing loop and possibly a fault.

The 4 x OC-3/STM-1 Trunk/Access Modules have SEC/Stratum 3 quality clocks, the others is of Stratum 4 quality.

11.5.3.1.3 4 x DS3/E3 Trunk/Access Module

This module is always slaved to the network frequency and thus it has no timing configuration options. The same external synchronization condition that applies to the OC-48/STM-16 X-ADM also applies for this board.

FSP (Frame Sync Pattern) is required when the Time Transfer is used.

11.5.3.1.4 IP/Ethernet Trunk for Nimbra One/300 and built-in ports on Nimbra 360

This module has one option, Enable sync recovery, which is by default enabled. The option may be disabled in for example the following cases:

Interconnection of two Nimbra networks via an IP/MPLS/Ethernet link:

If each of the two Nimbra networks is synchronized via a centralized external synchronization source, it may be beneficial not to not transport the sync from one network to the other over the IP connection but rather use two synchronization sources for the two sections of the network. This requires that both external references are synchronized (for example both references are tied to GPS clocks) to avoid slips.[3]

[3] In the initial IP/Ethernet trunk release GX4.5 it is not recommended to use the recovered sync from an IP trunk to synchronize downstream nodes, but rather use the method described in this paragraph. This is due to a long settling time that may affect downstream nodes.

Single Frequency networks (SFN). When feeding transmitter sites with the IP/Ethernet trunks in a SFN use case, GPS clocks are needed to provide the time synchronization for SFN operation, since the IP/Ethernet trunk does not support the Time Transfer functionality. Then the GPS can be used to synchronize the Nimbra switch also.

11.5.3.1.5 All trunks for the Nimbra 600 series

No synchronization options exist for these boards. They all use Network timing mode.

11.5.4 Nimbra 680 with redundant switch planes

DSYP handles redundant switch planes in Nimbra 680 transparently to the operator. Both switch planes will lock in to the selected synchronization reference signal and deliver a node synchronization signal in phase with each other. At fail-over, the standby switch module becomes active and sources node synchronization.

There is, however, one operational aspect of having redundant switch planes in a Nimbra 680. If the Nimbra 680 receives an external synchronization signal, this signal must be delivered to both switch planes, i.e. the signal must be split by a passive splitter or a distribution amplifier and connected to both switch planes. It must be ensured that the physical signal is of adequate quality after splitting/distribution.

If only the active switch plane is connected to the external synchronization source, the node does not use this synchronization source after a fail over as no incoming synchronization source is impinging on the now active module (that previously was standby). The node searches for another synchronization source according to the rules of the DSYP protocol, but this search does not include the source connected to the now standby switch module.

Nimbra 680 accepts 8 kHz, 1544 kHz or 2048 kHz synchronization signals. They are attached to the front of the switch modules.

In a mixed Nimbra network, this potential problem can be overcome by just using Nimbra One/300 as input interface for external synchronization.

11.6 Monitoring synchronization performance

11.6.1 Slip Seconds

The single most important tool for monitoring the synchronization performance is to inspect the Slip Seconds (SS) performance counters. These counters indicate if there have been one or more DTM frame slips during a second. This could hypothetically happen if node sync, for some faulty reason, is not synchronized to a trunk interface that is part of the synchronization spanning tree. Then it will pace out frames at another frequency than the network frequency. This should never happen. The counters are found in the Web GUI under

Perf. Monitor → Trunks

These should always indicate “0”. Anything else indicates a serious problem. During extreme conditions, such as changing to a new reference source with

another frequency, or if there has been very many sync changes (due to many intermittent topology changes for example) the slip counter may step one count. In former case due to that all phase relations are altered when the network frequency changes. In the latter case due to accumulated residual phase errors in the synchronization source change process. However, in steady state there should be no slips if the network synchronization works alright.

It is also possible to trigger an alarm, by enabling a threshold crossing alarm. Use a threshold of "1" in order to be sure to catch a single slip.

11.6.2 Pointer Justification Events

Pointer Justification Events (PJE) at SDH/SONET interfaces are also available for monitoring. There are counters for

TX PJE +
TX PJE -
RX PJE +
RX PJE -

on Trunks → Interfaces web page. These counters are reset each time the web page is accessed. (Note that if several users are logged in, it may be reset of another user accessing the page). These counters give information about the difference between the line rate of the interface and the DTM network frequency. For interfaces in Network timing mode the TX counters should be zero. In the RX direction an intermediate SDH/SONET network could introduce pointer justifications also when in Network timing mode.

11.7 IP/Ethernet Trunk

The synchronization performance of the IP/Ethernet trunk is affected by the quality of the IP connection. The more packet jitter, the more jitter/wander on the recovered sync signal. The quality of the IP/Ethernet trunk can be monitored by inspecting the Synchronization Signal Status. This Status has three values[4]

Normal – Recovered node sync is of G.813 quality, i.e. of the same quality as given by a SDH/Sonet equipment clock (ADM).

Degraded – Recovered sync is not of G.813 quality, due to packet delay variations outside what can be handled, but is still used. Performance degradation can be expected.

Failed – Recovered sync is not usable, the node selects another synchronization source as decided by the DSYP protocol. Frame slips can be expected.

Other performance indicators related to the synchronization signal recovery are available in the Web GUI:

Packet jitter delay variation

Peak-to-peak packet jitter (to be implemented)

[4] The limits (i.e. when to make a transition from state to another) in the initial GX4.5 release are can be considered temporary and will be adjusted after feedback from use in real networks, since lab networks and network simulators may not provide the same typical packet jitter distributions as in real networks.

99.99% percentile packet delay variation (to be implemented)

11.8 Time Transfer

Time transfer is an optional software feature, which requires Nimbra 360 and/or 600 Series hardware.

Time transfer is based on node clocks and network synchronization available in all DTM networks. The Time Transfer functionality distributes absolute time to all participating nodes of a Nimbra Network. This is useful for many applications. For example, in DTT networks a technique called Single Frequency Networks is used for transmitter sites to simultaneously broadcast programs on the same frequency such that a receiver gets a stronger signal and the operator gets a simpler network/frequency plan.

With Time Transfer, Time delay between two neighboring nodes is constantly measured and communicated between the nodes. This allows the nodes to calculate absolute time with great accuracy, with all intrinsic, static and dynamic time delay constantly taken into account.

Time transfer specific information is sent between nodes on dedicated, automatically set-up time transfer channels. They can be listed from the link All connections → Channels or from Nimbra Vision.

The time transfer function utilizes DSYP to find the shortest path for time distribution and to find an alternative path in case of node or link failure. The time transfer accuracy is better than ± 1.5 µs for ten consecutive node hops.

Time transfer is available from the DTM → Time transfer link.

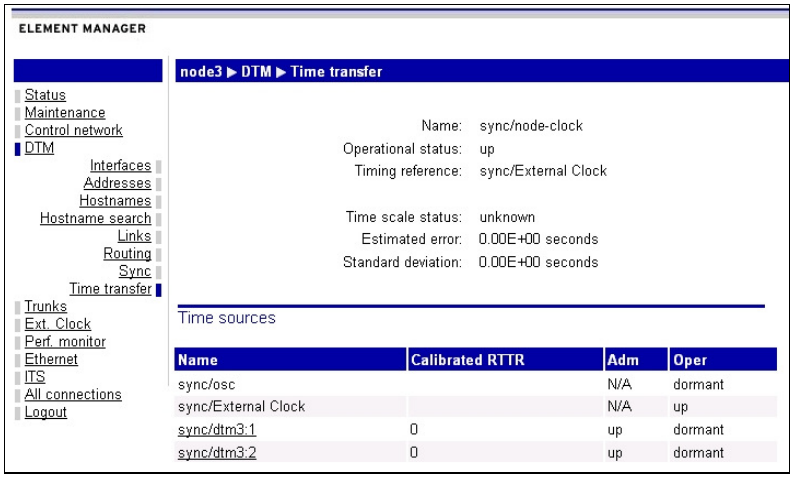


Figure 161. Time transfer configuration web page.

Operational status is 'Up' when time transfer is active. The timing reference for time transfer is identical to the DTM synchronization reference (as seen above).

The remaining three listed variables; time scale status, estimated error and standard deviation (of the PPS signal) describe the status of the time scale, the current estimated error of the measurement and the standard deviation of the PPS value. Currently, this is not implemented.

Time Transfer is enabled on a per link basis, which requires that interfaces on both ends of the link has Time Transfer enabled.

Clicking on the link to the available synchronization sources takes the user to the interface configuration page.

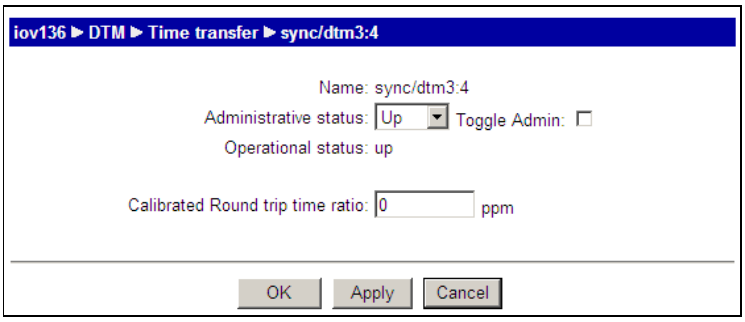


Figure 162. Time transfer configuration web page for a specific interface.

On this page, the administrative status can be set. The administrative status is set to 'Down' for all trunks by default. In order to enable time transfer, the administrative status must be set to 'Up' on at least one trunk interface. In order to let the system handle selection of a suitable synchronization source, it is strongly recommended to set the administrative status on all trunk interfaces to 'Up' when using the time transfer feature.

Setting the administrative status to 'Down' on an interface with operational status 'Up' forces the operational status to state 'Down' and disables the time transfer function. No warning is given to nodes further down in the synchronization chain, but an event is generated in the event log. **This setting is strongly discouraged.**

The parameter 'Calibrated Round trip ratio' is the difference between the ratio of the trip ratio from the far end to the node and the round trip time and ½. Observe that it is the time going in to the node that counts, not vice verse. The parameter is expressed in ppm and is in the range -499999 to 499999.

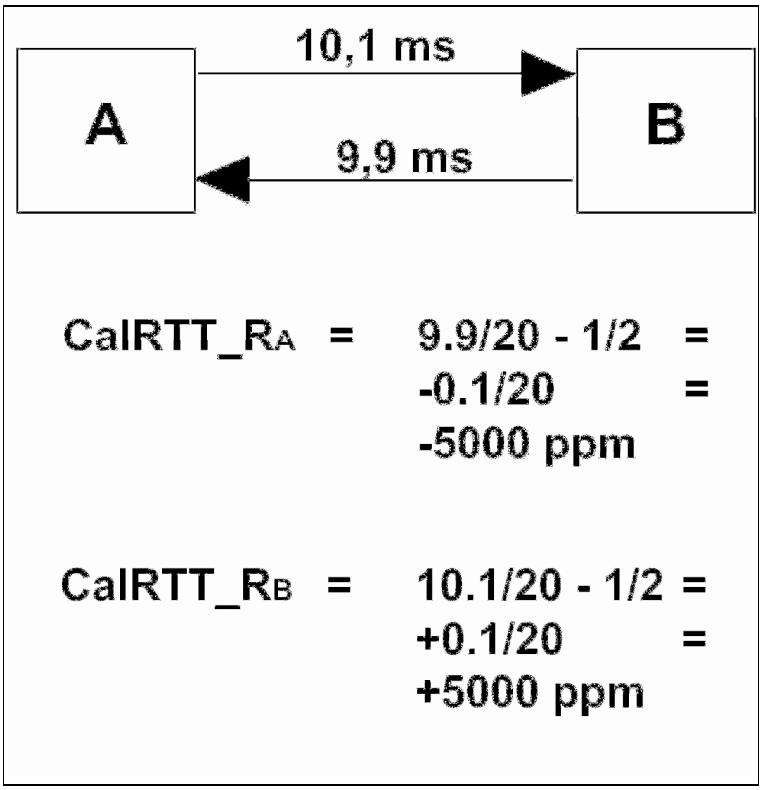


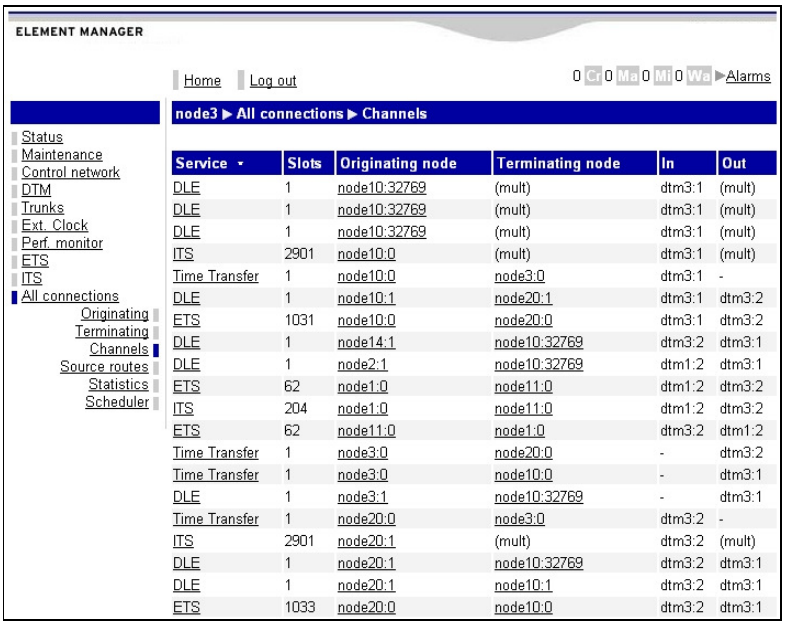
Figure 163. Definition of calibrated round trip ratio.

11.8.1 Time transfer distribution

Time transfer is distributed according to a spanning tree configuration.

11.8.2 Listing of time transfer channels

The time transfer channels are seen in the link All Connections → Channels are listed.



Service	Slots	Originating node	Terminating node	In	Out
DLE	1	node10:32769	(mult)	dtm3:1	(mult)
DLE	1	node10:32769	(mult)	dtm3:1	(mult)
DLE	1	node10:32769	(mult)	dtm3:1	(mult)
ITS	2901	node10:0	(mult)	dtm3:1	(mult)
Time Transfer	1	node10:0	node3:0	dtm3:1	-
DLE	1	node10:1	node20:1	dtm3:1	dtm3:2
ETS	1031	node10:0	node20:0	dtm3:1	dtm3:2
DLE	1	node14:1	node10:32769	dtm3:2	dtm3:1
DLE	1	node2:1	node10:32769	dtm1:2	dtm3:1
ETS	62	node1:0	node11:0	dtm1:2	dtm3:2
ITS	204	node1:0	node11:0	dtm1:2	dtm3:2
ETS	62	node11:0	node1:0	dtm3:2	dtm1:2
Time Transfer	1	node3:0	node20:0	-	dtm3:2
Time Transfer	1	node3:0	node10:0	-	dtm3:1
DLE	1	node3:1	node10:32769	-	dtm3:1
Time Transfer	1	node20:0	node3:0	dtm3:2	-
ITS	2901	node20:1	(mult)	dtm3:2	(mult)
DLE	1	node20:1	node10:32769	dtm3:2	dtm3:1
DLE	1	node20:1	node10:1	dtm3:2	dtm3:1
ETS	1033	node20:0	node10:0	dtm3:2	dtm3:1

Figure 164. All Channels listed, including all Time Transfer channels.

12 Performance Monitoring

12.1 Overview

The Performance management function performs collection of measurement data to allow a network operator to base the planning of network reconfiguration and maintenance on statistics reports on the performance of network resources.

All monitoring points are sampled every second. If a parameter cannot be calculated, e.g. because a sample is unavailable or a sample is outside the value range of the measurement point, the performance interval is declared invalid. New performance calculations are started every even 15 minutes (hh:00, hh:15, hh:30, hh:45) and 24 h (00:00), respectively. All monitoring points are then reset.

Performance reports are issued at the end of the measurement intervals. The performance reports are logged. The size of the PM log is configurable to store up to 96 latest 15 min reports and 30 latest 24 h reports. The PM function is scalable according to the number of circuits/interfaces provisioned in the switch.

A threshold can be defined for each performance parameter: An alarm is issued when a threshold is crossed. Threshold crossing alarms are reset after a complete measuring period where the threshold value has not been exceeded.

The system also generates real-time Degraded Signal (DEG) alarms. It is possible to select the degraded threshold for the DEG alarm.

The Nimbra platform supports performance management to ITU-T G.826 based on SONET/SDH, DTM and access performance primitives. The overall purpose is to support monitoring in all parts of the network as illustrated in the figure below, but without providing redundant information at multiple layers. Monitoring is available for:

Trunk interfaces

Access interfaces

ITS services (end-to-end)

12.2 General

Navigate to the **Perf. Monitor** menu. The view below appears.

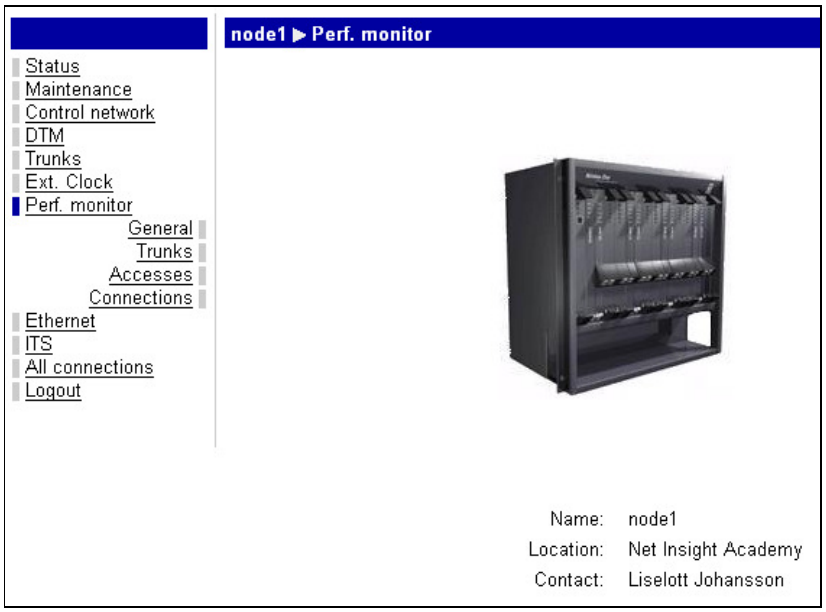


Figure 165. Performance Monitoring main menu

The sub-sections are General, Trunks, Accesses and Connections.

From the link General, the sizes of the logs and the maximum number of small and large history logs (15 minutes and 24 hours) reports are set. The default number of stored reports per node is four large and 128 small.

From the link Trunks, an overview of current performance monitoring reports for relevant trunk interfaces is presented. Performance monitoring of the interfaces is configured from this web page. Blocks (for bit error detection) are 125 µs long.

In the same way, Accesses and Connections display performance monitoring reports for relevant access interfaces/service connections. Blocks (for bit error detection) are 1 ms long.

The following performance parameters are monitored:

Parameter (G.826)	Description
Suspect	If the parameter value is yes, this gives an indication that all counter values may be erroneous. This parameter is seen on an interface basis by clicking on the interface name in the Perf. Monitor/Trunks.
ZS	Zero suppression counters, i.e. number of periods without error before current period.
ES	Error Second is a second of available time with one or more BBE (see below).
SES	Severely Error Second (Subset of ES) is a second of seriously faulty available time. One second of available time containing ≥30% EB or at least one defect. Ten consecutive SES seconds begin UAT state while ten consecutive non-SES seconds end UAT.
BBE	Background Block Error is the number of error blocks found during one second of available time that is not part of SES.
UAS	Unavailable Second is the number of seconds of unavailability of a service access point (SAP) during its up time.
SS	Slip Second is one second containing one or more Slips, which is Applicable for trunk modules. Clicking on the interface name in the Perf. Monitor/Trunks make this parameter visible.

Figure 166. Performance Monitoring, monitored parameters

12.3 Set-up of Performance Monitoring

Under the sub-menu **General**, system resources are allocated for the specified number of performance monitoring history logs.

Select the **General** sub-menu to set-up the maximum number of the small and the large history log. The view below appears.

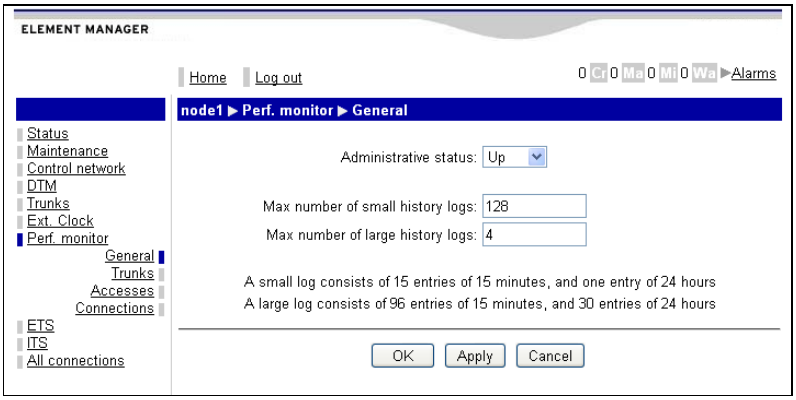


Figure 167. Performance Monitoring, General set up

Set the Administration status drop-down menu to **Up**.

Enter the number of small and large history logs.

Parameter	Description
Admin status	The administrative status of all performance monitoring in the node. Setting it to 'Up' enables performance monitoring while setting it to 'Down' disables performance monitoring in the node.
Small history	Consist of 15 entries of 15 minute and 1 entry of 24 hrs. Allocated system resources for the small history log.
Large history	Consist of 96 entries of 15 minute and 30 entries of 24 hrs. Allocated system resources for the large history log.

Figure 168. Performance monitoring, general configuration settings

Store the configuration by clicking on the **OK** or **Apply** button.

12.3.1 Set-up Performance monitoring for Trunk Links

The monitored trunk links have to be configured and the administrative status of the trunk interfaces must be set to '**Up'** before the start of performance monitoring.

Navigate to the **Perf. Monitoring** and click on the **Trunks** menu. The view below appears:

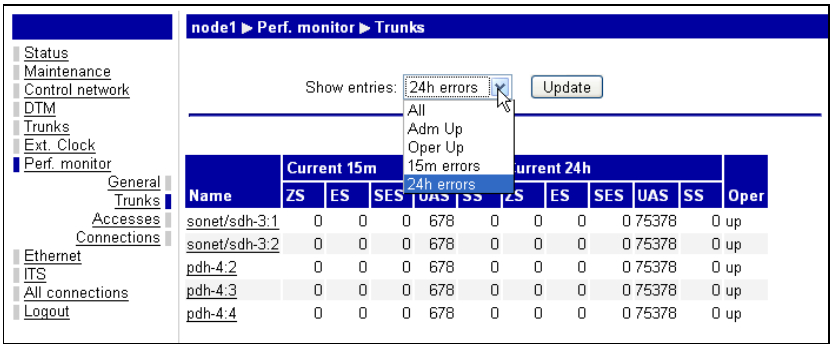


Figure 169. Performance Monitoring, Trunks

All trunks interfaces are presented under **Name**. Performance Monitoring events are accumulated as counter values in intervals 15-minutes (Current 15m) and 24-hours (Current 24h). **Oper** (status) up/down indicates if performance monitoring is running (up) or not (down) on the interface. On top of the page, there is a parameter, 'Show entries', which can be set to 'all', 'Adm Up', 'Oper Up', 15m errors' or '24h errors'. This will limit the list to those entries with Adm' status or Oper status set to 'Up' alternatively with entries different than zero for 15 m or 24h errors.

Click on the link to the particular interface to access details about Performance Monitoring. The view below appears:

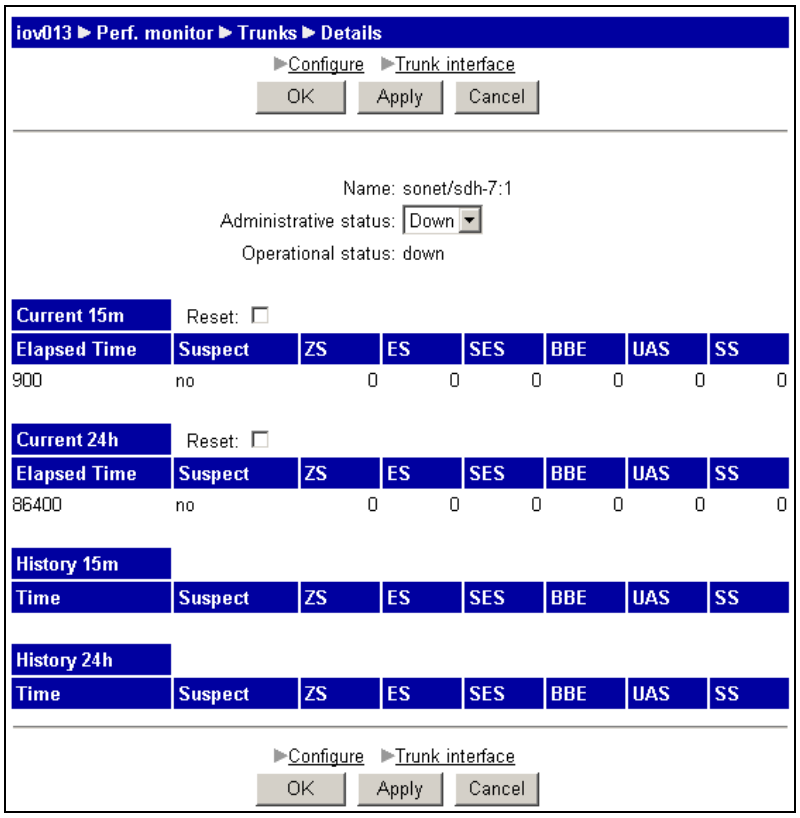


Figure 170. Set the Administrative Status

The configurable parameters are:

Parameter name	Description
Administrative status	The administrative status of the interface enables (‘Up’) or disables (‘Down’) performance monitoring on the interface.
Reset	Tick the relevant Reset checkbox (or boxes) and click on the ‘Apply’ button to clear current logs. All entries are reset to zero and any (if any) threshold crossing alarms are cleared.

Figure 171. Configurable parameters, performance monitoring

The **Read-only** parameters are:

Current 15 minutes

The switch collects data in the current 15 minutes interval.

Current 24 hours

The switch collects data in the current 24 hours interval.

History 15 minutes

The switch collects data in intervals of 15 minutes from the 15 minutes current register and produces events and history records. After collection,

counters in the 15 minutes current register are reset to zero and a new 15 minutes interval starts.

History 24 hours
The switch collects data in intervals of 24 hours from the 24 hours current register and produces events and history records. After collection, counters in the 24 hours current register are reset to zero and a new 24 hours interval starts.

To configure a particular interface, proceed as follows:

Set the **Administrative Status** to '**Up'** by selecting it from the drop-down list and clicking on the **'Apply'** button.

Click on **Configure** at the top or bottom of the page. The view below appears.

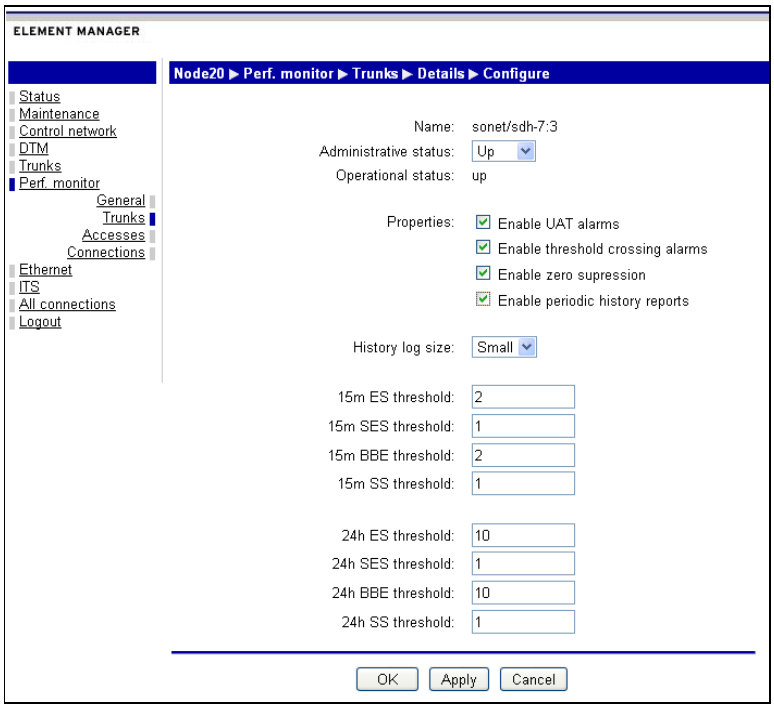


Figure 172. Threshold parameters

The configurable parameters are:

Parameter	Description
Admin status	The administrative status of the interface enables or disables performance monitoring on the interface.
Properties	The tick boxes must be selected for alarms to be sent. UAT Unavailable time alarms UAS (UnAvailable Seconds) alarm is sent Threshold crossing alarms Each 15m and 24h current register counter can optionally be assigned a threshold value. When this value is exceeded, a threshold crossing (TC) alarm will be raised. Enable zero suppression: Log entries with all zeros, i.e. periods with no errors are not logged. Instead, the zero counter is increased by one. When a period containing errors is logged, the zero counter (i.e. the number of consecutive fault free periods immediately preceding the errored period) is stored with the error data. By default, this parameter is enabled. Enable periodic history reports: Without this tick box selected, no history logs are stored. Only current values are available.
History log size	None: No history log will be used. Small: Small history log will be used. Large: Large size of history log will be used.
Configured parameters to generate threshold alarms	
15m ES threshold	0 disabled; 1-900 enabled
15m SES threshold	0 disabled; 1-900 enabled
15m BBE threshold	0 disabled; 1-(2^{32}-1) enabled. Depends on the technology, differs between SDI and ASI etc.
15m SS threshold	0 disabled; 1-900 enabled
24h ES threshold	0 disabled; 1-86400 enabled
24h SES threshold	0 disabled; 1-86400 enabled
24h BBE threshold	0 disabled; 1-(2^{32}-1) enabled. Depends on the technology, differs between SDI and ASI etc.
24h SS threshold	0 disabled; 1-86400 enabled

Figure 173. Performance monitoring, configurable parameters

12.3.1.1 Threshold

Each 15 minutes and 24 hours current register counter can optionally be assigned a threshold value. When crossed, a threshold crossing (TC) alarm is raised if the alarm is enabled and the interval suspect flag is not set. Raised alarms are cleared at end of a following fault free interval i.e. one with all interval counter values below their threshold values, no interval suspect flag raised and without UAT. Only one TC alarm per interval can be raised, regardless of how many thresholds have been crossed.

Set the **Administrative Status** to '**Up'** by changing the value in the drop-down menu.

Edit the parameters for Performance Monitoring for the connection and click **OK** or **Apply** button to set the changes.

12.3.2 Set-up of Performance Monitoring for ITS Connections

Navigate to the **Perf. Monitor, Connections**. The view below appears.

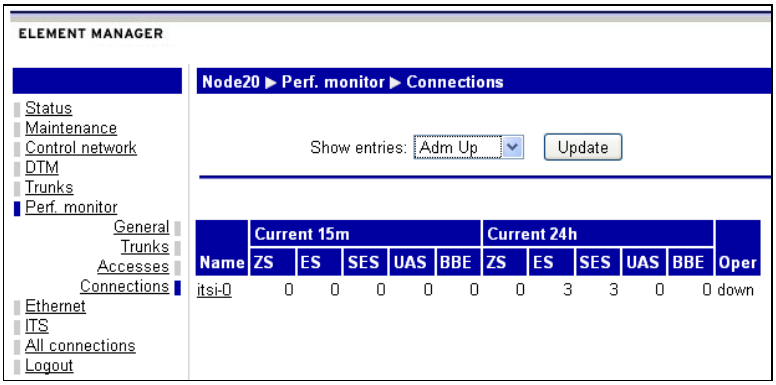


Figure 174. Performance Monitoring, Connections

Parameter PM events are accumulated as counter values in intervals 15-minutes (15m) and 24-hours (24h).

Click on the connection to start the Performance Monitoring.
The view below appears.

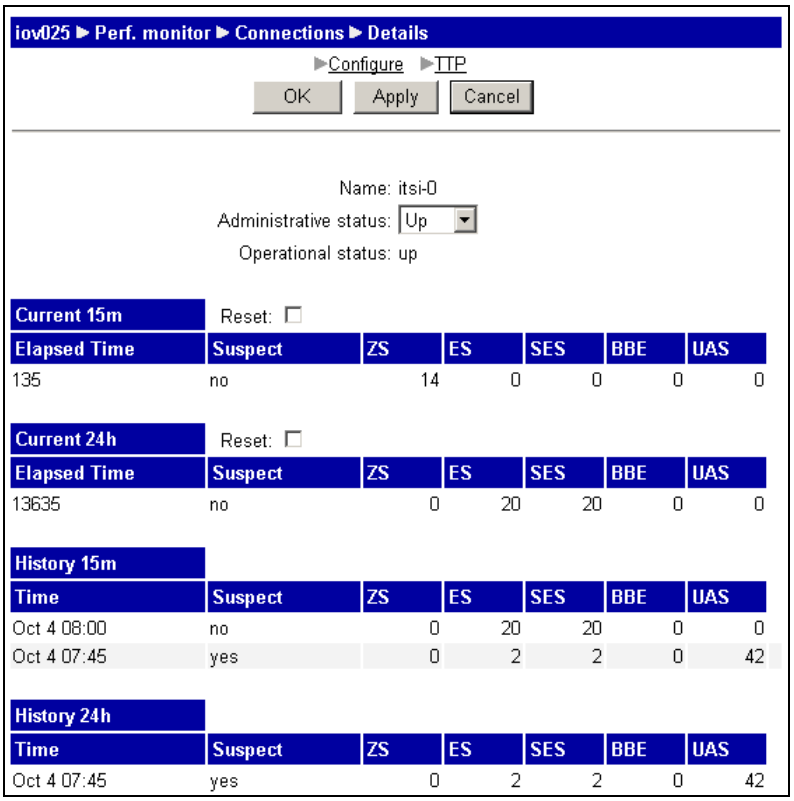


Figure 175. The Administrative Status is set

The **configurable** parameters are:

Parameter name	Description
Administrative status	The administrative status of the connection enables (‘Up’) or disables (‘Down’) performance monitoring on the connection.
Reset	Tick the Reset check-box and click on the ‘Apply’ button to clear the current logs.

Figure 176. Configurable parameters

The **Read-only** parameters are:

Current 15 minutes/24 hours

The switch collects data in the current 15 minutes/24 hours interval.

History 15 minutes/24 hours

The switch collects data in intervals of 15 minutes/24 hours from the 15 minutes/24 hours current register and produces events and history records. After collection, counters in the 15 minutes/24 hours current register are reset to zero and a new 15 minutes/24 hours interval starts.

Set the **Administrative Status** to ‘**Up’** by changing the drop-down list to **Up.**

Click on **Configure** at the top of the page. The view below appears.

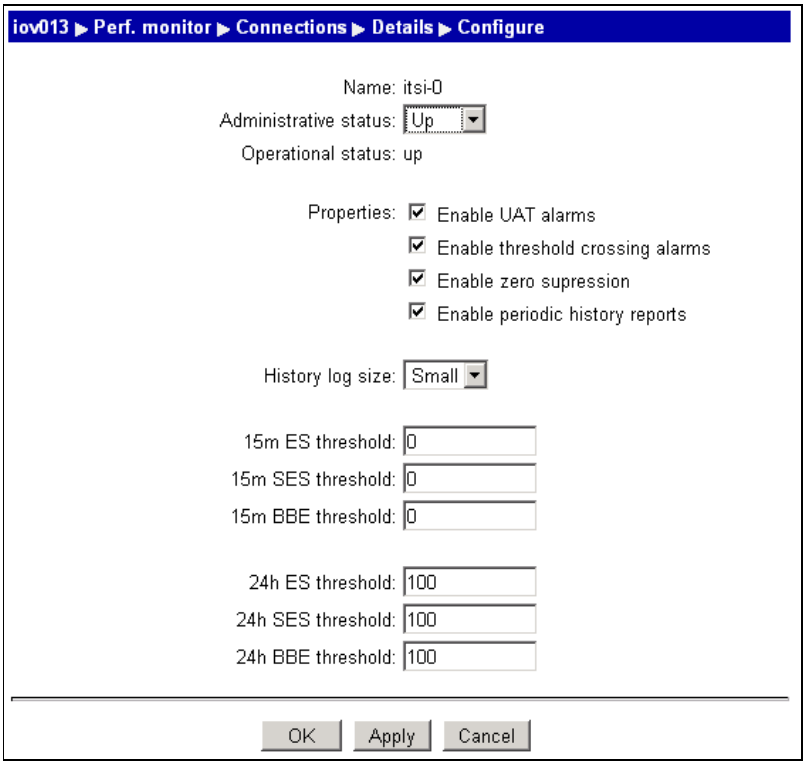


Figure 177. Parameters to configure

The **configurable** parameters are:

Parameter name	Description
Admin status	The administrative status of the interface enables or disables performance monitoring on the interface.
Properties	The tick boxes must be selected for alarms to be sent. UAT Unavailable time alarms UAS (UnAvailable Seconds) alarm is sent Threshold crossing alarms Each 15m and 24h current register counter can optionally be assigned a threshold value. When this value is exceeded, a threshold crossing (TC) alarm will be raised. Enable zero suppression: Log entries with all zeros, i.e. periods with no errors are not logged. Instead, the zero counter is increased by one. When a period containing errors is logged, the zero counter (i.e. the number of consecutive fault free periods immediately preceding the errored period) is stored with the error data. By default, this parameter is enabled. Enable periodic history reports: Without this tick box selected, no history logs are stored. Only current values are available.

History log size	None: No history log will be used. Small: Small history log will be used. Large: Large size of history log will be used.
Configured parameters to generate threshold alarms	
15m ES threshold	0 disabled; 1-900 enabled
15m SES threshold	0 disabled; 1-900 enabled
15m BBE threshold	0 disabled; 1-(2^{32}-1) enabled. Depends on the technology, differs between SDI and ASI etc.
24h ES threshold	0 disabled; 1-86400 enabled
24h SES threshold	0 disabled; 1-86400 enabled
24h BBE threshold	0 disabled; 1-(2^{32}-1) enabled. Depends on the technology, differs between SDI and ASI etc.

Figure 178. Configurable parameters

12.3.2.1 Threshold

Each 15 minutes or 24 hours current register counter can have a user defined threshold value. When this level is exceeded, a threshold crossing (TC) alarm is raised. Raised alarms are cleared at end of a following fault free period i.e. one with all counter values below their threshold values, no interval suspect flag raised and without UAT. Only one TC alarm per interval can be raised, regardless of how many thresholds have been crossed.

Set the Administrative Status to Up by changing the value in the drop-down menu.

Edit the parameters for Performance Monitoring for the connection and click OK or Apply button to set the changes.

To start Performance Monitoring for other connections, accesses or trunks, repeat the steps above.

12.3.3 Set-up Performance Monitoring for ITS Access Interfaces

The monitored access interfaces have to be configured and the administrative status of them must be set to '**Up'** before the start of performance monitoring.

Navigate to the **Perf. Monitoring** and click on the **Accesses** menu. The view below appears:

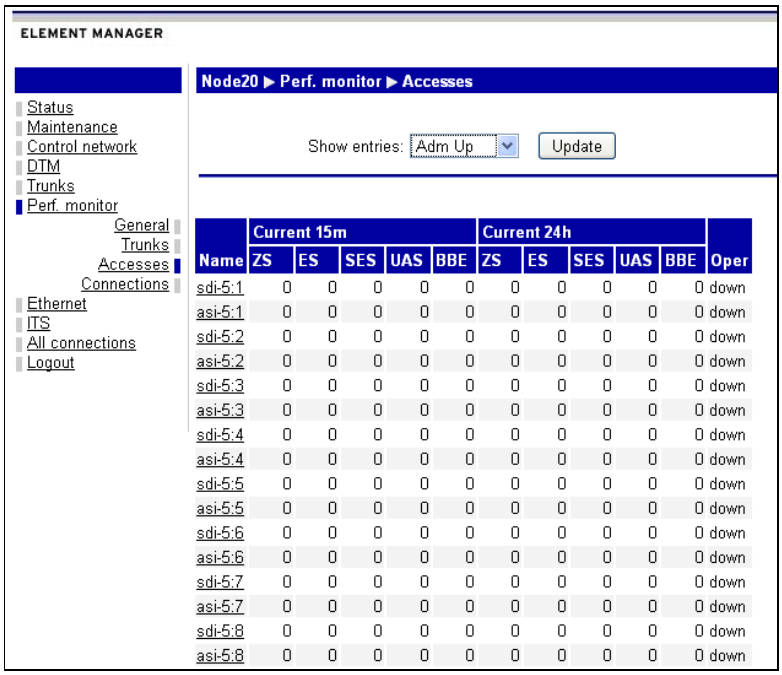


Figure 179. Performance Monitoring, Accesses

The interfaces of the combined 8 x Video Access Module can be configured as either ASI or HD/SD SDI, so e.g. only one of sdi-4:1 and asi-4:1 can be configured.

All access interfaces are presented under **Name**. Performance Monitoring events are accumulated as counter values in intervals 15-minutes (Current 15m) and 24-hours (Current 24h). **Oper** (status) up/down indicates if performance monitoring is running (up) or not (down) on the interface. On top of the page, the listings can be restricted to entries with Adm status or Oper Status 'Up' or with non-zero entries in the 15m or 24h error log.

Click on the link to the particular interface to access details about Performance Monitoring. The view below appears:

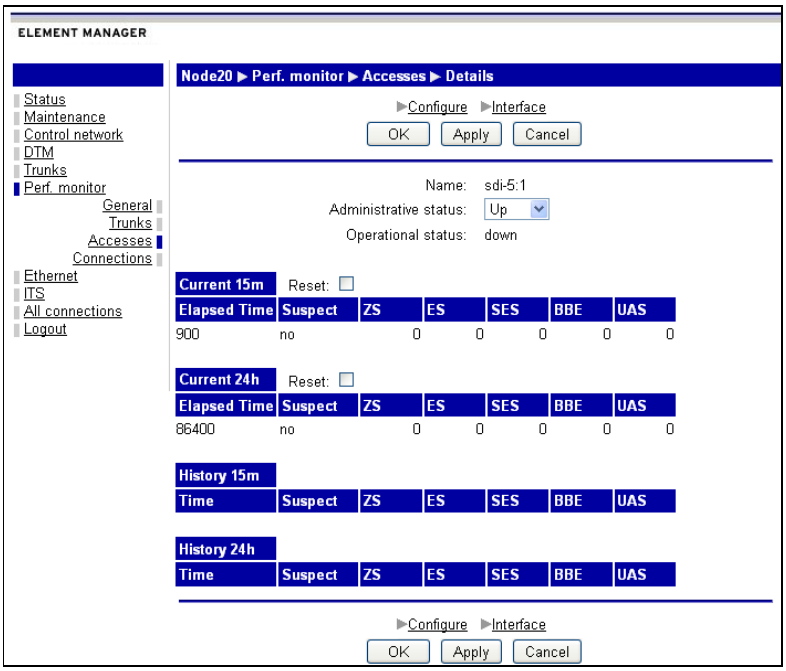


Figure 180. Set the Administrative Status

The configurable parameters are:

Parameter name	Description
Administrative status	The administrative status of the interface enables (‘Up’) or disables (‘Down’) performance monitoring on the interface.
Reset	Tick the relevant Reset checkbox (or boxes) and click on the ‘Apply’ button to clear current logs. All entries are reset to zero and any (if any) threshold crossing alarms are cleared.

Figure 181. Configurable parameters

The **Read-only** parameters are:

Current 15 minutes//24 hours

The switch collects data in the current 15 minutes/24 hours interval.

History 15 minutes/24 hours

The switch collects data in intervals of 15 minutes/24 hours from the 15 minutes/24 hours current register and produces events and history records. After collection, counters in the 15 minutes/24 hours current register are reset to zero and a new 15 minutes/24 hours interval starts.

To configure a particular interface, proceed as follows:

Set the **Administrative Status** to ‘**Up’** by selecting it from the drop-down list and clicking on the **‘Apply’** button.

Click on **Configure** at the top or bottom of the page. The view below appears.

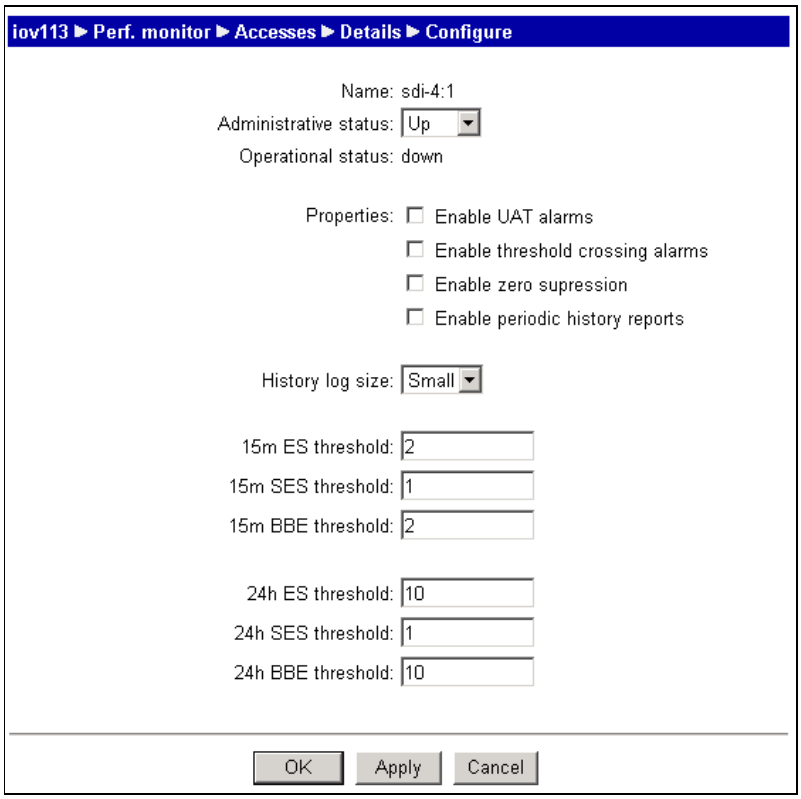


Figure 182. Threshold parameters

The configurable parameters are:

Parameter	Description
Admin status	The administrative status of the interface enables or disables performance monitoring on the interface.
Properties	The tick boxes must be selected for alarms to be sent. UAT Unavailable time alarms UAS (UnAvailable Seconds) alarm is sent Threshold crossing alarms Each 15m and 24h current register counter can optionally be assigned a threshold value. When this value is exceeded, a threshold crossing (TC) alarm will be raised. Enable zero suppression: Log entries with all zeros, i.e. periods with no errors are not logged. Instead, the zero counter is increased by one. When a period containing errors is logged, the zero counter (i.e. the number of consecutive fault free periods immediately preceding the errored period) is stored with the error data. By default, zero suppression is enabled. Enable periodic history reports: Without this tick box selected, no history logs are stored. Only current values are available.
History log size	None: No history log will be used.

	Small: Small history log will be used. Large: Large size of history log will be used.
Configured parameters to generate threshold alarms	
15m ES threshold	0 disabled; 1-900 enabled
15m SES threshold	0 disabled; 1-900 enabled
15m BBE threshold	0 disabled; 1-(2^{32}-1) enabled. Depends on the technology, differs between SDI and ASI etc.
15m SS threshold	0 disabled; 1-900 enabled
24h ES threshold	0 disabled; 1-86400 enabled
24h SES threshold	0 disabled; 1-86400 enabled
24h BBE threshold	0 disabled; 1-(2^{32}-1) enabled. Depends on the technology, differs between SDI and ASI etc.
24h SS threshold	0 disabled; 1-86400 enabled

Figure 183. Configurable parameters to generate threshold alarms

12.3.3.1 Threshold

Each 15 minutes and 24 hours current register counter can optionally be assigned a threshold value. When crossed, a threshold crossing (TC) alarm is raised if the alarm is enabled and the interval suspect flag is not set. Raised alarms are cleared at end of a following fault free interval i.e. one with all interval counter values below their threshold values, no interval suspect flag raised and without UAT. Only one TC alarm per interval can be raised, regardless of how many thresholds have been crossed.

Set the **Administrative Status** to '**Up'** by changing the value in the drop-down menu. Edit the parameters for Performance Monitoring for the connection and click **OK** or **Apply** button to set the changes.

13 Access Modules

13.1 Access Module types

Access Modules can be of two different types in Nimbra nodes, ITS (Isochronous Transport Service) or Ethernet. Currently, all modules are ITS modules except the Fast Ethernet Access Module and Gigabit Ethernet Access Module for Nimbra One and 8 x Gigabit Ethernet Access Module for Nimbra 600.

Configurable parameters of the modules are described under the ITS or Ethernet sections.

13.2 Overview

The access interfaces are used to feed the network with various kinds of traffic. A wide range of interfaces allowing access modules interacting of most kinds of data, voice and video equipment or external network are available. For Nimbra One, some of the interfaces are available in type A and B versions but most of the modules are turnable, i.e. they can be inserted in all slots.

Access modules without specified hardware are available in Nimbra One and Nimbra 300 versions.

Access Modules	Data
E1 Access Module	Switched E1 service with on-board 1+1 APS 8 port, RJ48 120 Ohm, E1 ITU-T G.703 Framing: E1: ITU-G.704 and unframed Power consumption <12W
T1 Access Module	Switched T1 service with on-board 1+1 APS 8 port, RJ48 120 Ohm, T1 ANSI T1.102 Framing: T1: ANSI T1.403 and unframed Power consumption <12W
4 x DS3/E3 Trunk/Access module	4 PDH interfaces (In and Out), 75 ohm BNC, ITS service Power consumption < 10 W

Fast Ethernet Access Module	Ethernet Transport Service 8 port, RJ 45 10/100 Mbps, full duplex autosensing On every FEC there could be 4094 VLANs and on each FEC The VLANs must be unique; VLAN Range: 1-4094 MAC addresses: 8k; Frame Storage: 4 MB IEEE 802.3- 2002, 802.1Q, 802.1D; ETSI ES 201 803-7 Power consumption <20W
Gigabit Ethernet Access Module	Ethernet Transport Service; 1 port, SFP optical module 1 Gbps; full duplex VLAN Range: 1-4094 MAC addresses: 8k; Frame Storage: 4 MB IEEE 802.3- 2002, 802.1Q, 802.1D; ETSI ES 201 803-7 Power consumption <25W 1000 Base SX MM: 850nm, reach 500 m 1000 Base LX SM: 1310nm, reach 10 km 1000 Base LX SM: 1550nm, reach 70 km 1000 Base T Electrical, UTP, Cat 5, reach 100 m Framing: SFP optical module SX, LX, ZX
4 x OC-3/STM-1 Access Module	4 x OC-3/STM-1 Access, 4 port, SFP LC SR-1/I:1310nm, MM, 2km IR-1/S-1.1:1310nm,SM, 10km LR-1/L-1.1:1310nm, SM, 40km LR-2/L-1.2: 1550nm, SM, 80km Framing: OC-3:STS-3c; ANSI T1.105 STM-1 ITU-T Recommendation G.707 Mapping: SONET:STS-3c SPE/(STS-1 SPE) SDH: VC-4/(VC-3) Power consumption <20W
SDI Video Access Module	Switched 270 Mbps SDI streaming video 4 ports (2 in, 2 out); 2 monitoring ports, BNC ITU-R (BT.601 and BT.656) Power consumption <25W
ASI Transport Access Module	Switched DVB/ASI transport; 2 Mbps to 200 Mbps 4 port (2 in, 2 out) 2 monitoring ports, BNC Comply to CENELEC EN 50083-9 and ITU requirements for professional video equipment Power consumption <20W
8 x ASI Transport Access Module	Switched DVB/ASI transport; 2 Mbps to 200 Mbps 8 ports (In or Out), 1 monitoring port, BNC Comply to CENELEC EN 50083-9 and ITU requirements for professional video equipment Power consumption <20W
8 x AES/EBU Access Module	AES/EBU (AES3) Digital audio signals with various sampling rates (32 – 176.4 kHz) 8 ports (In or Out), 1 monitoring port, BNC 75 Ohms Power consumption <15W

8 x Video Access Module (Nimbra 680)	HD-SDI (1.485 or 1.485/1.001 Gbps video) SD-SDI (270 Mbps video) Switched DVB/ASI transport (2 to 212 Mbps) 8 ports (configurable as HD/SD/ASI and In/Out/Monitor) with some restrictions, BNC 75 Ohms Comply to CENELEC EN 50083-9 and ITU requirements for professional video equipment (ASI) Power consumption <40W
8 x 3Gbps Video Access Module (Nimbra 680)	3G SDI (2.97 or 2.97/1.001 Gbps Video) HD-SDI (1.485 or 1.485/1.001 Gbps video) SD-SDI (270 Mbps video) 8 ports (configurable as 3G/HD/SD SDI and In/Out/Monitor) with some restrictions, BNC 75 Ohms Power consumption <40W
8 x Gigabit Ethernet Access Module (Nimbra 680)	Ethernet Transport Service 8 port, RJ-45 electrical interface 1 Gbps; full duplex VLAN Range: 1-4094 MAC addresses: 8k; Frame Storage: 4 MB IEEE 802.3- 2002, 802.1Q, 802.1D; ETSI ES 201 803-7 Power consumption <25W 1000 Base SX MM: 850nm, reach 500 m 1000 Base LX SM: 1310nm, reach 10 km 1000 Base LX SM: 1550nm, reach 70 km 1000 Base T Electrical, UTP, Cat 5, reach 100 m Framing: SFP optical module SX, LX, ZX

Figure 184. Access module overview

13.3 OC3 /STM-1 Access Interface – web example

Configuration of STM – 1 Access Interfaces is shown as an example of web configuration of interfaces. The configuration web page is shown below:

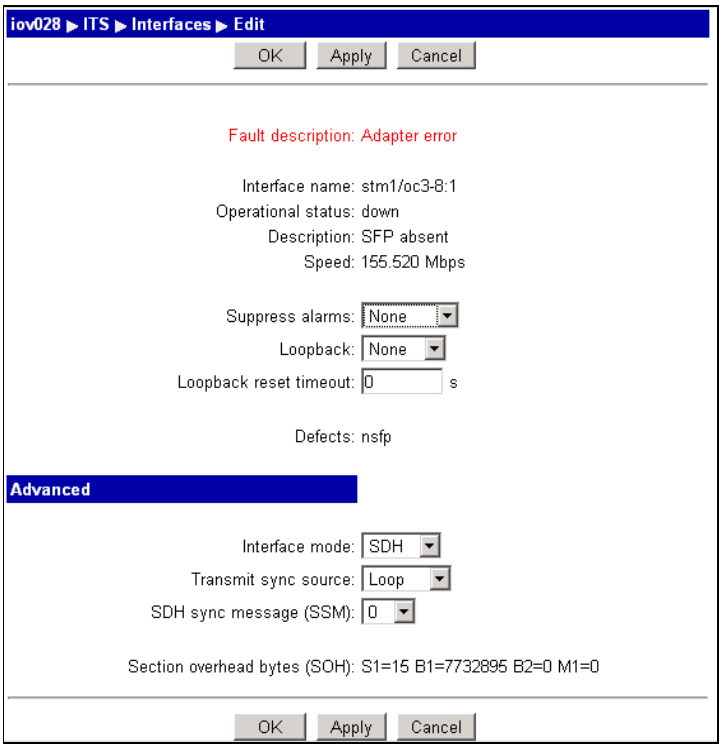


Figure 185. Parameters to configure

The displayed variables are:

Parameter	Description
Interface name	The name of the interface, STM1/OC-3-8:1
Operational status	The operational status of the board: Up, Down or Absent
Description	A description of the card (e.g. if the XFP/SFP is absent)
Speed	The capacity of the access interface, 155.520 Mbps.
Defects	Presents the defect status of the module; e.g. if the SFP is absent, the defect status is NSFP (No SFP)

Figure 186. Read-only parameters

The **configurable** parameters for the module are:

Parameter name	Description
Suppress Alarms	When the service is up and running as intended, alarms are by default suppressed. In order to enable the alarms, the suppress alarms parameter must be set to 'none'. Other possible parameter values are: All: When marked, all alarms are suppressed. Warning: Suppresses all active alarms with severity warning
Loopback	The loopback parameter can have three values; None, line or DTM None means that loopback is disabled Line means that the signal is looped back on the line side, i.e. that a signal that comes from an external equipment is sent back to that equipment directly at the interface. DTM means that the incoming signal from the DTM network is looped back to the DTM network. See chapter 19 Loopback for a more detailed discussion.
Loopback reset	Loopback is automatically disabled after the loopback reset timeout, given in seconds. A parameter value of 0 disables the function, i.e. loopback is enabled until the parameter value is changed.

Figure 187. Configurable parameters

The **Advanced** parameters for the module are:

Parameter	Description
Interface mode	This parameter determines if the interface works in SDH or Sonet mode.
Transmit sync source	This parameter determines which clock is used for the outgoing signal from the interface. If Transmit sync source is set to 'Loop', the clock from the incoming signal on the interface is extracted and used as clock for the outgoing signal. If Transmit sync source is set to 'Internal', the node internal clock is used as clock for the outgoing signal.
SDH sync message (SSM)	Synchronization Status Message Should be 11 if Transmit sync source is set to Internal. The default value is 15 (Do Not Use).
Performance monitoring counters	B1 Section overhead B2 Line overhead B3 Path overhead M1 Remote indication of B1 G1 Remote indication of B3 Overhead bytes: SS=2 C2=255

Figure 188. Advanced parameters

13.4 DS3 /E3 Access Interface – web example #2

Configuration of the DS3/E3 Access Interface is shown below as another example of web configuration of interfaces.

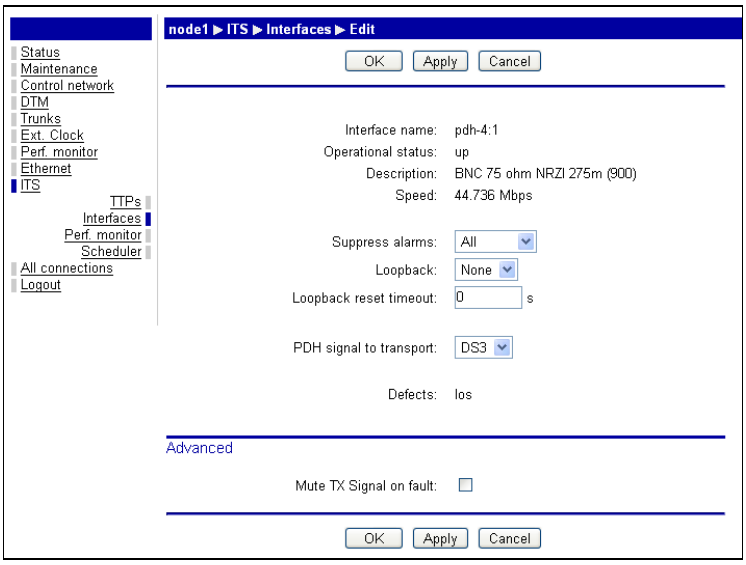


Figure 189. Configuration/edit web page of a DS3/E3 access interface.

The displayed variables are:

Parameter	Description
Interface name	The name of the interface, STM1/OC-3-8:1
Operational status	The operational status of the board: Up, Down or Absent
Description	A description of the card (e.g. if the XFP/SFP is absent)
Speed	The capacity of the access interface, 44.736 Mbps, with a DS3 configuration
Defects	Defect(s) on the interface are presented here

Figure 190. Read-only parameters

The **configurable** parameters for the module are:

Parameter	Description
Suppress Alarms	When the service is up and running as intended, alarms are by default suppressed. In order to enable the alarms, the suppress alarms parameter must be set to 'none'. Other possible parameter values are: All: When marked, all alarms are suppressed. Warning: Suppresses all active alarms with severity warning

Loopback	The loopback parameter can have three values; None, line or DTM None means that loopback is disabled Line means that the signal is looped back on the line side, i.e. that a signal that comes from an external equipment is sent back to that equipment directly at the interface. DTM means that the incoming signal from the DTM network is looped back to the DTM network. See chapter 19 Loopback for a more detailed discussion.
Loopback reset timeout (s)	The Loopback functionality is automatically disabled after the loopback reset timeout period. A parameter value of '0' disables the loopback reset timeout function, i.e. loopback is enabled until the loopback parameter value is changed or the loopback setting itself is removed.
PDH signal to transport	Type of PDH signal is configured here. DS3 (default) and E3 are the available options.
Mute Tx signal on fault	Could be ticked or Unticked, which is interpreted as 'yes' and 'no' to the action defined by the parameter.

Figure 191. Configurable parameters

14 Ethernet Transport Service (Ethernet)

14.1 General

Net Insight offers a flexible Ethernet Transport Service, usable for implementing Ethernet networks on top of the DTM network. The main feature offered is VLAN enabled Ethernet bridging (Ethernet switching).

14.2 Basic concepts

14.2.1 Terminology

In this text, an item which fits into a slot in a node and is connected to the node via connectors to the backplane is called module. Likewise, anything that serves as an end-point of an Ethernet connection is called interface. An interface may be a physical Ethernet port or a virtual port of an Ethernet Transport Service (ETS) through the Nimbra Network. The latter may in other contexts be called a TTP (Trail Termination Point), a term that is also used for other services (Isochronous Transport Services, ITS) in the Nimbra Network.

The physical Ethernet interface on the module is labeled after the slot occupied by the module in the node and secondly, the interface number on the module. An example is eth3:6, for physical interface number six (from the left) on the module occupying slot number three.

The virtual Ethernet interfaces (ETSes) are also labeled after the slot occupied by the module on which the ETS is defined. Secondly, this type of interface is assigned an integer at its creation. An example is ets5:9, for a defined ETS on the module occupying slot number five of the node.

The cornerstone of the Ethernet configuration model, the Forwarding Function (FF), is labeled after the module on which it is defined and is assigned an integer to keep it unique (starting with one). An example is ff7:2, the second defined FF on the module that is occupying slot number seven.

14.2.2 Unicast

A schematic picture of an ETS connection is shown below. It consists of two channels, one in each direction. These channels are used to send packets arriving on the Ethernet port at X to the Ethernet port at Y and vice versa.

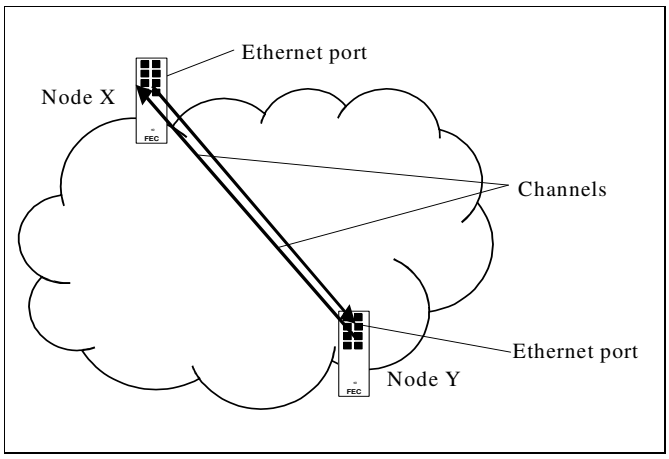


Figure 192. A bidirectional ETS service, using two connections between two Ethernet ports.

14.2.2.1 Unicast TTP

Note:	A unicast ETS TTP provides a duplex point-to-point connection to another ETS TTP!

Two unicast ETS TTPs are connected using one connection and one channel in each direction, providing the same service as a full duplex Ethernet link.

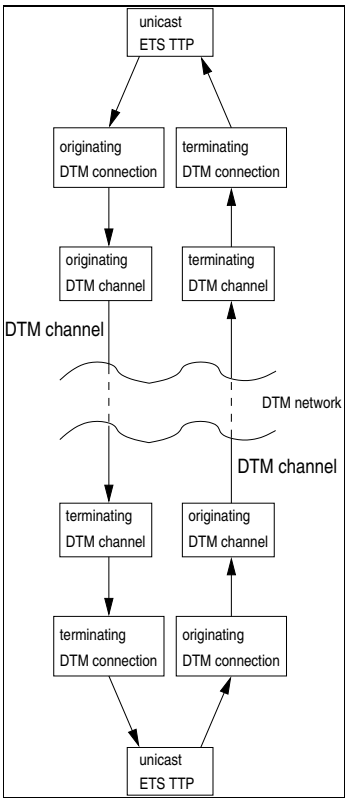


Figure 193. A bidirectional ETS service, using two connections between two Ethernet ports.

14.2.3 Multicast

An Ethernet transport service (ETS) multicast connection, connecting several TTPs (Trail Termination Point/s) to one source.

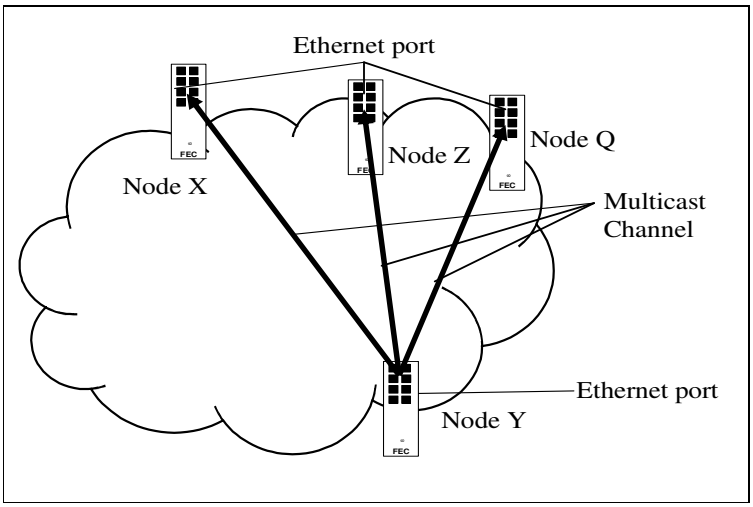


Figure 194. A multicast ETS connection

14.2.3.1 Multicast TTP

> ***Note:***
>
> A multicast ETS TTP provides a uni- or bidirectional connection to zero, one or several other ETS TTPs

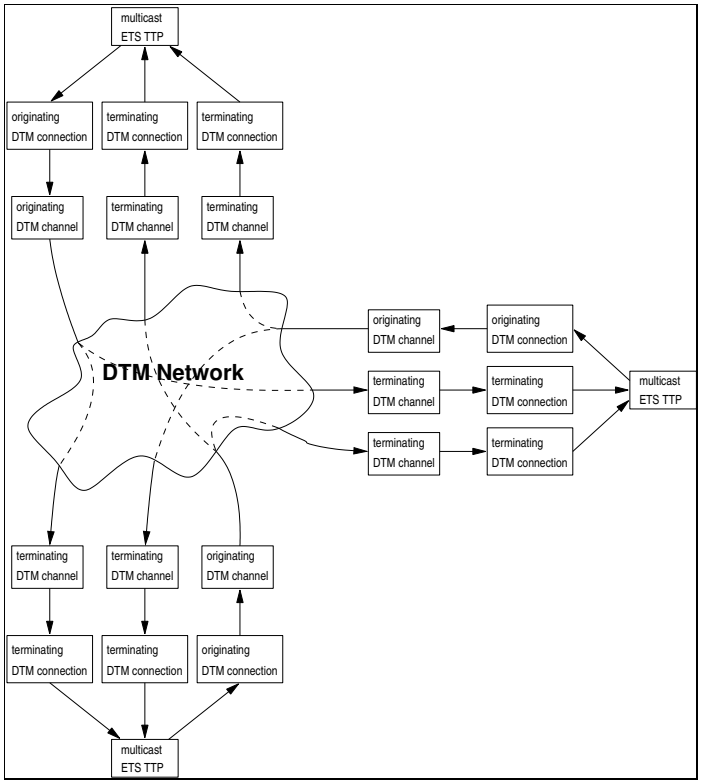


Figure 195. A multicast ETS connection, a hub between three TTPs

14.2.4 Forwarding Function

A Forwarding Function (FF) is a virtual Ethernet switch defined on a module.

The FF is created and deleted by the user. The first time an 8 x Gigabit Ethernet Access Module is detected, no FFs exist on the module. In order to use the module, at least one Forwarding Function must be created.

The configuration model for Ethernet switching consists of multiple objects, which sometimes must and sometimes may be created and configured. The relationship between these objects is exemplified below, where two ETS endpoints of a DTM channel are connected to different forwarding functions.

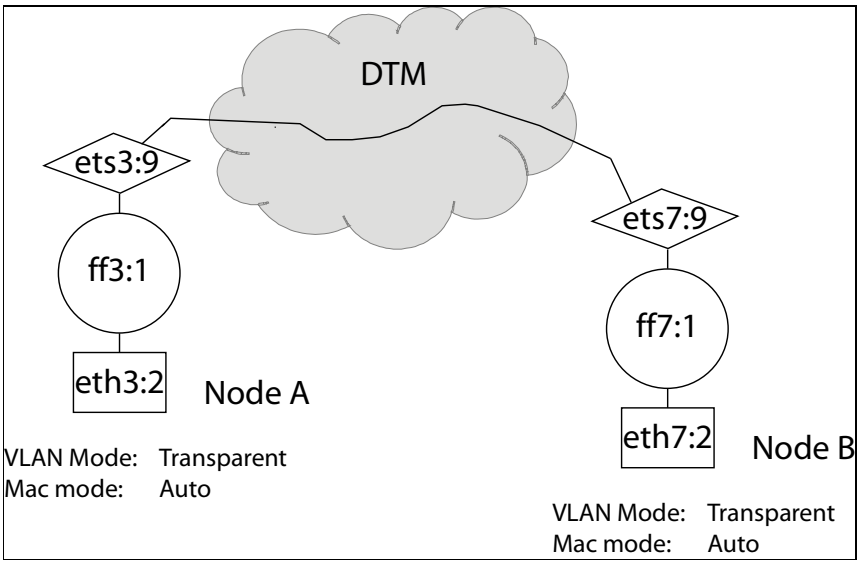


Figure 196. The relationship between different fundamental concepts in Ethernet switching is shown.

Each Forwarding Function is associated with a number of Ethernet (ETH) and ETS interfaces. All Ethernet and ETS interfaces associated with a specific FF must be defined on the same module as the Forwarding Function itself is defined.

The basic configurable parameters for a forwarding function are: VLAN Mode, MAC Mode, MAC Aging Time, Jumbo Frames and Spanning Tree. In addition, a ‘Customer ID’ and a ‘Purpose’ may be associated with the FF.

A Forwarding Function can currently be set in two different VLAN modes.

MAC mode → VLAN mode ↓	Nomac	MAC
Transparent	Transparent mode Forwards all incoming packets to the interfaces belonging to the same FF.	Bridged MAC mode VLAN transparent Switching mode IEEE802.1D
Customer	Customer mode Forwarding based on customer VLAN only. Forwards incoming packets to the interfaces belonging to the same FF and (customer) VLAN. Only mode supported in Nimbra One/300 products	Bridged VLAN/MAC mode VLAN aware Switching mode IEEE802.1Q

Figure 197. The table shows available VLAN and MAC mode settings of Forwarding Functions. The operation of the FF is lined out for the different cases.

In VLAN transparent mode, the frames are forwarded unchanged. The Forwarding Function (FF) ignores any VLAN tag that may be included in the incoming data frame. No tag is added to or removed from the frame in the FF and the frame is forwarded as-is, i.e. an included incoming tag is forwarded with the frame but no tag is added in untagged frames.

No VLAN configuration is possible with VLAN mode equal to transparent. The selections are grayed out in the web interface.

VLAN-handling is in accordance with IEEE 802.1Q. All frames belong to a VLAN, either from a tag present in the header or from a default tag added by the Ethernet/ETS interface in case no VLAN tag is included in the incoming frame. The old configuration model uses this mode and in all Nimbra One/300 nodes VLAN mode is preconfigured to Customer and unchangeable

Independently of VLAN mode, there is another key parameter of FF configuration, the ‘MAC mode’. This parameter can assume values ‘MAC’ and ‘Nomac’, in addition to the value ‘Auto’.

In MAC mode ‘Auto’, MAC mode ‘Nomac’ is used when only two Ethernet/ETS interfaces are associated with a specific FF (since the packets are always forwarded to the interface that they didn’t arrive on) and MAC mode ‘MAC’ is used for all FFs that have more than two associated Ethernet/ETS interfaces. Auto is the default mode. For MAC mode ‘Auto’, the actual, employed MAC mode is shown listed in the web browser.

In MAC mode ‘MAC’, the FF performs MAC based forwarding and learning (i.e. traditional Ethernet switching). This requires the connections to be defined with the parameter ‘Learning’ set to ‘On’.

In MAC mode ‘Nomac’, the FF never looks at the source/destination MAC address of forwarded packets. It only forwards all frames according to the settings of VLAN mode.

In the table below, the impact of VLAN and MAC mode settings are summarized.

There are some additional parameters to configure. In MAC mode, the parameter ‘MAC aging time’ defines how long time the stored MAC addresses remain listed before they are removed from the list. The function can be disabled.

One well known problem with Ethernet switching is that packets can travel in loops, never to reach a final destination. In some topologies, their number can be multiplied per loop and eventually all available bandwidth is used. The “Spanning Tree Protocol” is used to resolve such problems. The configurable parameter ‘Spanning Tree’ defines how BPDU packets are handled by the Forwarding Function. BPDU stands for Bridge Protocol Data Unit. These frames are exchanged between adjacent Ethernet Switches and carry STP information. The ‘Spanning Tree’ parameter can assume values ‘Auto’, ‘Forward’, ‘Drop’ and ‘Process’.

‘Forward’ means that all incoming BPDU packets are forwarded by the FF. ’Drop’ means that all incoming BPDU packets are dropped by the FF. ‘Process’ means that the FF processes incoming BPDU frames. ‘Auto’ results in different settings depending on the value of VLAN mode and the capability of the particular module. If VLAN mode is transparent, ‘auto’ results in ‘process’ if the board support it; otherwise ‘forward’. If VLAN mode is not transparent, ‘auto’ results in ‘drop’ if the board supports it, otherwise ‘forward.’ is used.

The parameter ‘Jumbo Frames’ is used to configure the FF to accept oversized Ethernet packets, i.e. packets that are larger than standard size Ethernet packets. The parameter ‘Jumbo frames’ must be set to ‘On’, if these packets are to be accepted. In case the parameter is set to ‘Off’ only standard size frames are forwarded and all other frames are dropped. The default setting of the parameter is ‘On’.

The parameters ‘Customer ID’ and ‘Purpose’ are also configurable on a FF level, as well as on the ETS/ETH interfaces themselves (as different instances of the parameters). These parameters are described under the ‘Interface’ heading.

In addition to the ‘Basic Settings’ of a Forwarding Function, there are Diffserv, Spanning Tree and Statistics links on the FF configuration web page.

Diffserv is done according to IETF RFC 2998. Since there are numerous code group to flow point mappings to be made, this configuration is made on a separate web page. A description of Diffserv is given in the Configuration section.

Configuration of the spanning tree function is made from the forwarding function link, as well as from a similar link from the interface web page.

From the Statistics link, a summary of basic statistics for all interfaces associated with the Forwarding Function are shown. There are links to the specific interfaces, for additional and more specific interface statistics.

14.2.5 Interfaces

Ethernet switching has two separate interface types that in all important aspects are configured the same way. They are physical interfaces (Eth) and

virtual Ethernet Transport Service (ETS) interfaces, i.e. end points of Ethernet transport in the DTM network. In the illustration below, the two types of interfaces are tied together with a forwarding function.

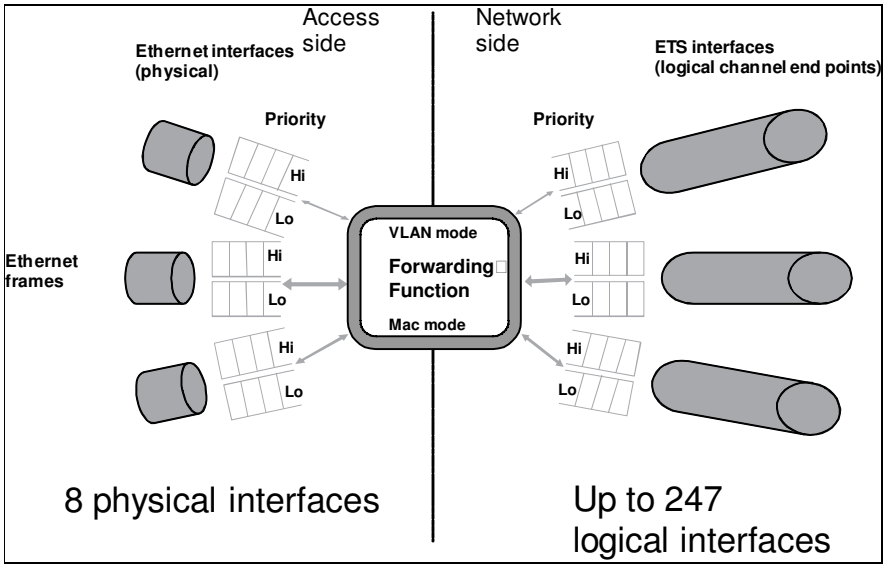


Figure 198. Illustration of the two types of interfaces, connected with each other through a forwarding function.

14.2.5.1 *Configurable interface parameters*

On all different interfaces, both physical Ethernet and virtual ETS, most common features are configured in the same way. There is a drop-down menu for Forwarding Function, with all available FFs. Default is that no FF is selected (i.e. the interface is disabled), which means that the user has to associate the interface with the forwarding function before the switch is enabled. This default setting is necessary, as different associations give the Ethernet switch different properties.

Each interface has a default VLAN, which is assigned to all untagged received frames before they are forwarded. If the Forwarding Function is set to VLAN mode customer, then the default VLAN is interpreted as an IEEE 802.1Q VLAN tag. If the Forwarding Function is set to VLAN mode transparent, the default VLAN is ignored.

The parameter ‘Acceptable Frame Type’ can be set to the values ‘Admit only VLAN-tagged frames’, ‘Admit only untagged and priority-tagged frames’ or ‘Admit all frames’. The default setting of the parameter is ‘Admit all frames’.

With the parameter set to ‘Admit only VLAN-tagged frames’, presented as ‘Tagged’ in the web, all untagged or priority tagged packets are dropped at the interface. The parameter value ‘Admit only untagged and priority tagged frames’, presented in the web as ‘Untagged’ causes all VLAN tagged frames to be dropped.

The implementation is made as required by IEEE 802.1Q, section 8.4.3

All interfaces have a default VLAN parameter, which is an integer. The default value for the parameter ‘default VLAN’ is 1. In case the FF is configured as transparent, this setting is irrelevant as VLAN tags are ignored in this case.

The parameter ‘Transmitted Frame Type’ controls if the outgoing frames are tagged or untagged. Value ‘Tagged’ adds a tag to all untagged frames before

they are forwarded. The value 'Untagged' removes any tags from the frames before they are forwarded. This parameter is relevant only if the FF is set to VLAN mode customer, as nothing is done to the packets in case VLAN mode is set to transparent.

VLAN mode 'Legacy' means that Ethernet frames are sent unmodified, but that information about the VLAN ID is sent in the ETS header. The ETS header is terminated on the ETS TTP in the terminating node. The VLAN ID information is used for VLAN assignment in the terminating node.

Other common interface parameters are:

Parameter	Default value	Possible values	Explanation
Administrative status (Admin status)	Down	Down Up	The interface is disabled The interface is enabled
Customer ID	0	Integer	This is an integer value, which works as an ID label in the range 0-4294967295 ($2^{32} - 1$)
Purpose	Empty text string	Text string	This is a text string of 255 or less characters

Figure 199. Additional common interface parameters.

There are some common advanced settings for all ETH/ETS interfaces:

Parameter	Default	Possible values	Explanation
MAC Learning	On	On, Off	Upon reception of a packet, the association between source MAC address and the interface is learnt. Subsequent frames are only distributed to relevant interfaces. MAC Learning disabled.
Default Ethernet priority	0	Integer, 0-7 Selectable from a drop-down menu	The Default Ethernet priority is a field in the header of incoming packets. If it is not filled out in an incoming packet, it is filled with the default value.
Priority mode	Ethernet	Ethernet Diffserv	Priority according to Ethernet Priority according to Diffserv
Default traffic class	0	0 1	All packets, not specifically prioritized, have lowest priority All packets, not specifically prioritized, have highest priority
Flow Group to Traffic Class mapping, flow groups 0 to 7	0	0 1	All packets in the flow group have lowest priority (traffic class 0) All packets in the flow group have highest priority (traffic class 1)

Figure 200. Advanced common interface parameters.

14.2.5.2 Ethernet interface (Eth)

Each Ethernet interface belongs to a single Forwarding Function. If two customers share a single interface, then the customers share a single Forwarding Function. To separate the customers in this case, the FF has to be set up in VLAN mode customer and the different customers must belong to different VLANs and use different VLAN tags.

If the Forwarding Function is set to VLAN mode transparent, all packets are transmitted exactly as they were received, without addition or removal of any VLAN tags.

There are some specific Ethernet interface parameters to be configured, in addition to the auto-negotiation protocol described later.

Parameter	Default	Possible values	Explanation
'Force VLANs tagged'	None	Integer, or a combination and range of integers.	VLANs included in this field are tagged, despite the general setting of Transmitted frame type 'Untagged'
'Force VLANs untagged'	None	Integer, or a combination and range of integers.	VLANs included in this field are not tagged, despite the general setting of Transmitted frame type 'Tagged'

Figure 201. Specific Ethernet Interface parameters.

Auto-negotiation of interface rate, protocols etc is either made with the Auto-negotiation feature at the Ethernet interface or not at all.

The settings of the auto-negotiation features are:

Parameter	Default	Possible values	Explanation
Auto negotiate	On	On	The standardized auto-negotiate feature (Nway) is enabled
		Off	The standardized auto-negotiate feature (Nway) is disabled
Advertised speed	Auto	Auto	All HW supported speeds (by module and SFP) are advertised. Recommended
		1000 Mbps	Only 1 Gbps is advertised
		100 Mbps	Only 100 Mbps is advertised
		10 Mbps	Only 10 Mbps is advertised
		100,10 Mbps	100 and 10 Mbps are advertised
		1000,100 Mbps	1000 and 100 Mbps are advertised
		1000,100,10 Mbps	1000, 100 and 10 Mbps are advertised
Advertised duplex	Auto	Auto	All supported duplex forms are advertised. Recommended
		Full	Only full duplex is advertised
		Half	Only half duplex is advertised
Advertised flow-control	Auto	Auto	All supported flow-control forms are advertised.
		PAUSE	PAUSE flow-control is advertised
		ASM_DIR	ASM_DIR flow-control is advertised
		PAUES, ASM_DIR	PAUSE and ASM_DIR are advertised. For a description, see IEEE802.3-2005 Section Two.

Figure 202. Auto negotiation parameters for Ethernet interfaces.

14.2.5.3 ETS interface

An ETS interface behaves much in the same way as a physical Ethernet interface: In addition to the common parameters, the following parameters are needed specifically for ETS interfaces:

Parameter	Default value	Possible values	Explanation
Local DSTI (DTM Service Type Instance)	Lowest unused integer, starting with 0.	Integers between 0 and 32767	Must be unique in the node.
Destination node	None	DTM address or Hostname	
Destination DSTI	Lowest unused integer, starting with 0.	Integers between 0 and 32767	Must match the local DSTI of the ETS unicast or multicast termination defined in the destination node.
Requested capacity (Mbps)	0.485 Mbps	Values between 0 and the trunk capacity	

Figure 203. Specific interface parameters for virtual ETS interfaces.

14.2.5.4 VLAN

The configurable parameters for VLAN settings are very basic:

Parameter	Default value	Possible values	Explanation
VLAN set	Empty	Integer or a List of integers in the range 1-4094	Allowed VLAN(s); Example: 1,3-18,47,62-68, 4092-4094
Customer ID	0	Integer	Integer identifier
Purpose	Empty string	Text string	Text string identifier

Figure 204. Auto negotiation parameters for Ethernet interfaces.

A VLAN id is always interpreted in context of the VLAN mode set for the FF that the VLAN is associated to. If the FF is in VLAN mode Customer, then the VLAN id is identical to an IEEE 802.1Q tag.

If 'VLAN Mode' of the FF is set to transparent, there is no need to define a VLAN as the FF ignores the VLAN tag.

14.2.6 Ethernet Configuration

Ethernet Configuration, starts from the link Ethernet in the left column. Additional links pop up: Devices; Forwarding Functions; Ethernet Interfaces and ETS Interfaces. To continue, follow the Devices link.

14.2.6.1 Devices

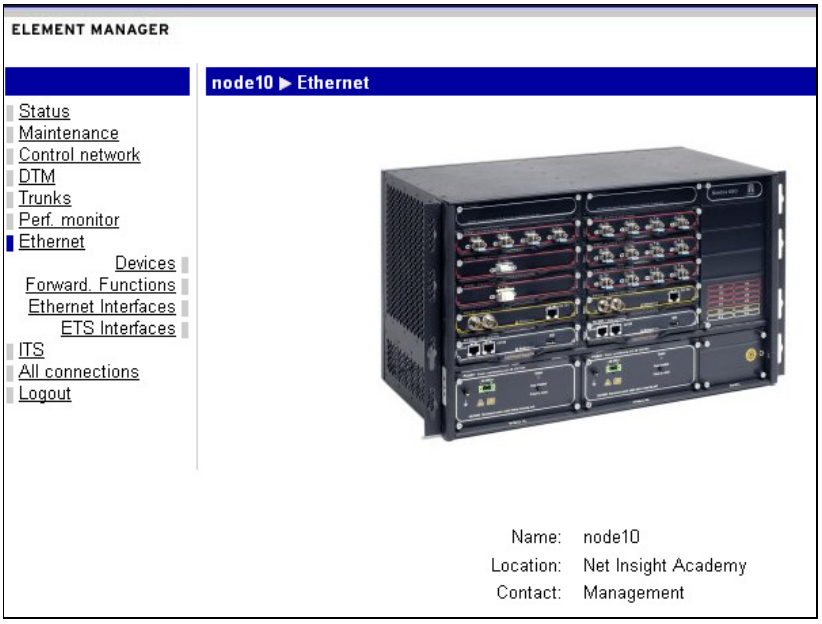


Figure 205. The first configuration page for Ethernet.

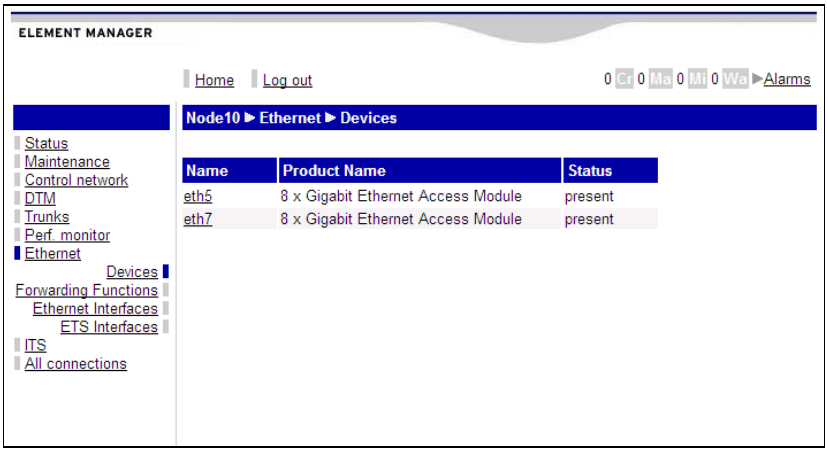


Figure 206. The configuration page obtained by clicking on the Devices link.

The starting point for configuration of Forwarding Functions and ETS Uni- and Multicast connection interfaces is found by clicking on the name of the particular device to be configured.

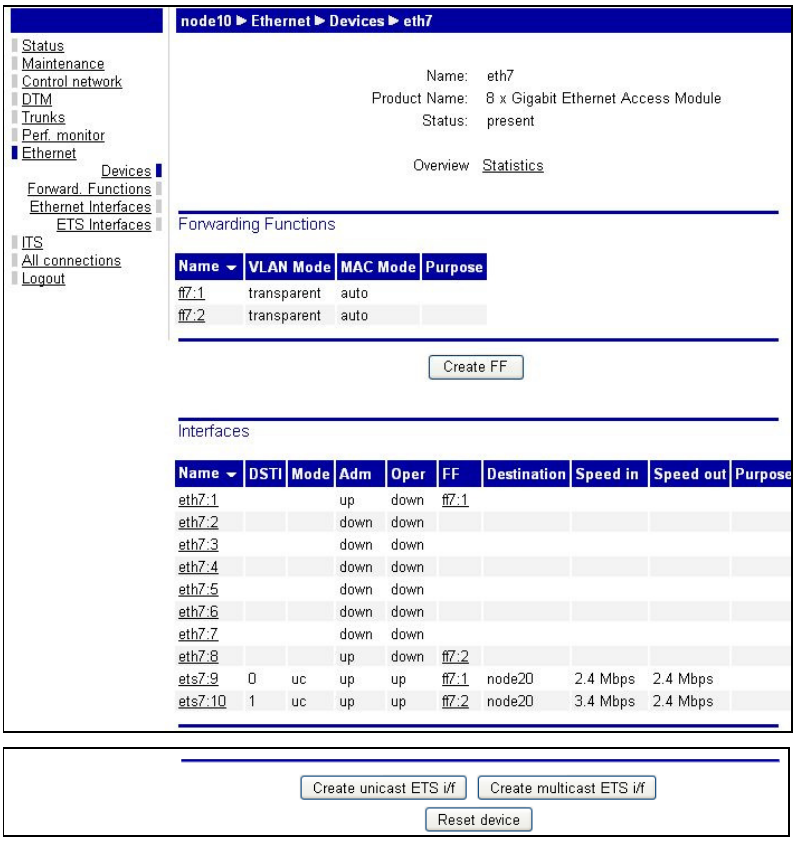


Figure 207. The configuration page for a particular Ethernet device (i.e. module) is found in this example when the link (name) eth7 is used

14.2.6.2 *Configuration of Forwarding Function*

In order to configure the basic parameters of the forwarding function, the button 'Create FF' on the previous web page is clicked. This configuration page appears:

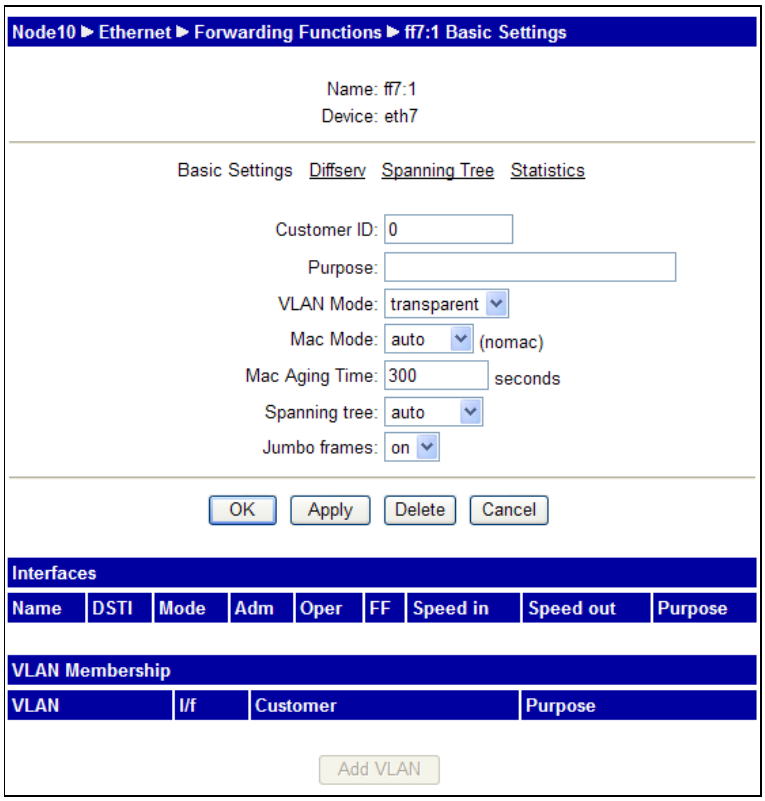


Figure 208. Configuration of a forwarding function, basic settings.

Customer ID is an integer between 0 and 4294967295 ($2^{32} - 1$). Purpose is a character string, up to 255 characters long.

VLAN mode can be set to Transparent or customer.

MAC mode can be set to Auto, MAC or Nomac. The actual MAC mode is presented.

MAC Aging time is the time an entry remains in the MAC address table. The default value is 300 seconds. It can be set to values in the range 0-65500 seconds, where 0 has a special meaning. 0 means that the look up table is never cleared.

Spanning tree: All values supported by the hardware are presented in the drop-down menu. Currently values 'Auto', 'Forward', 'Drop' or 'Process' are available for Nimbra 680/688 nodes and 'Auto' and 'Forward' for other nodes.

Jumbo frames, i.e. oversized frames, may be allowed (the parameter is set to 'on'; default) or disallowed (the parameter is set to 'off').

Clicking on the Diffserv link, gives the user access to all Diffserv configuration settings. Diffserv is configurable on a per interface basis.

Clicking on the Spanning Tree link gives the user access to spanning tree configuration when this is supported by the hardware. Currently, this feature is available on Nimbra 680/688.

Clicking on the Statistics link gives the user access to statistics, on an overview page as well as links to statistics pages of particular interfaces.

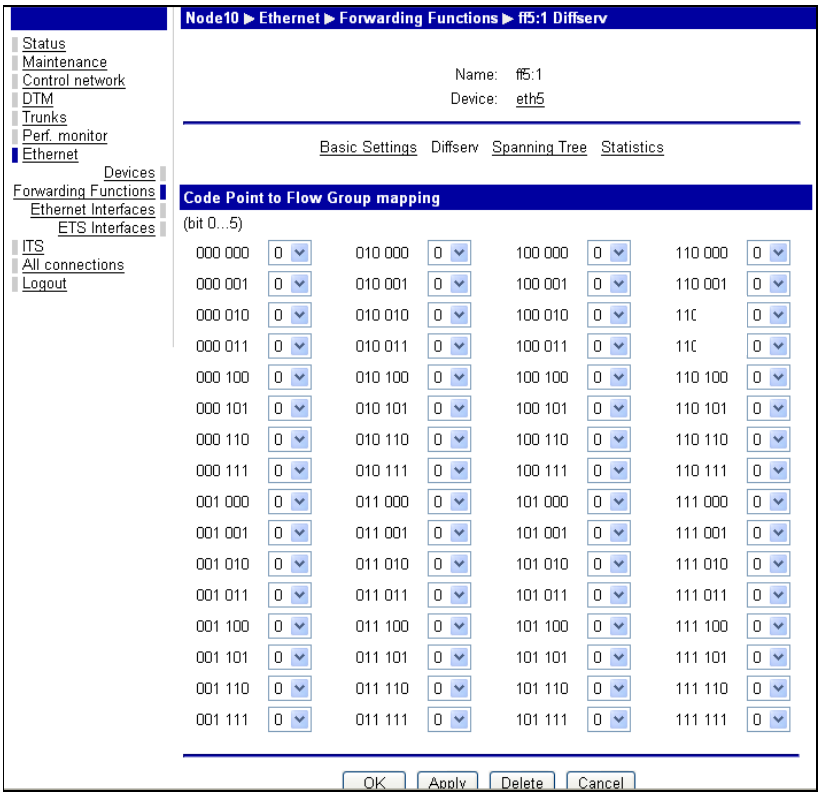


Figure 209. The diffserv configuration.

14.2.6.3 *Diffserv priority configuration*

In the IP header, as discussed in IETF RFC2474, there is a Differentiated Services Code Point (DSCP) defined as a six bit long value. Each DSCP value has to have a defined per-hop-behavior, which is determined by the defined Flow Group. On the Diffserv configuration page, all of these settings have to be made. Flow Group is defined as an integer in the range 0-7. Diffserv configuration is applied per forwarding function, but for each interface there is an option to select Ethernet or Diffserv prioritization. Hence a Forwarding Function may have some interfaces with Diffserv and some with Ethernet prioritization.

In the interface configuration, there is a mapping of the Flow Groups to Traffic Classes, 0 or 1. The Traffic Class is a strict priority function, where all packets in Traffic Class 1 are handled before any packets in Traffic Class 0 are handled. In other words, dual queues are used.

14.2.6.4 *Ethernet priority configuration*

Ethernet user priority is a standard for prioritizing Ethernet frames (IEEE 802.3 and IEEE 802.1D) based on the Ethernet user priority field, which only exists in tagged Ethernet frames.

Each ETS or Ethernet interface supports two out-queues, 0 and 1 with different levels of priority. Frames in queue 1 are strictly prioritized over frames in queue 0.

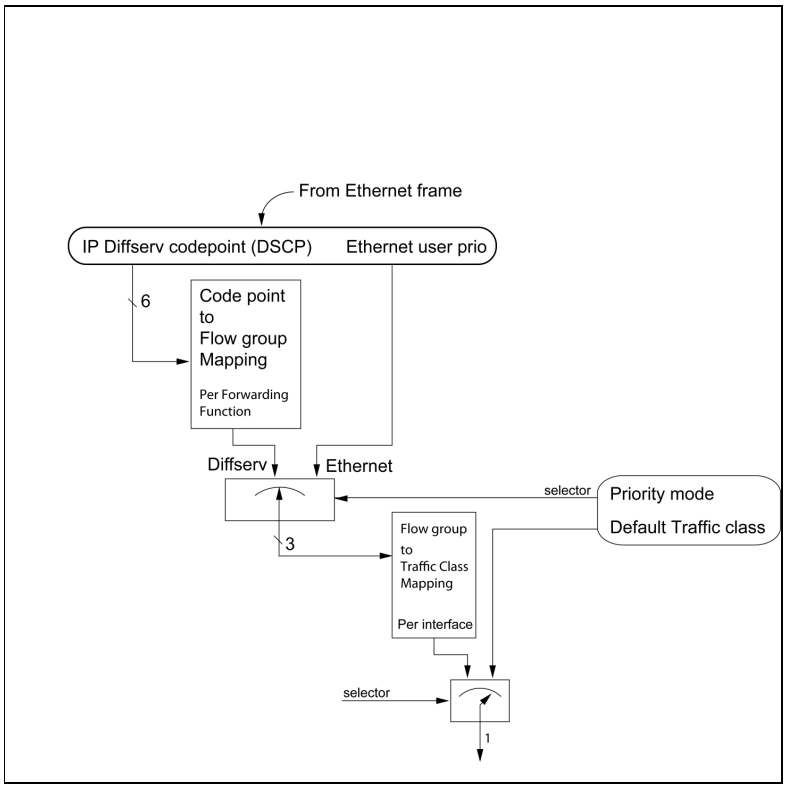


Figure 210. Priority selection: Two priority modes are allowed (Diffserv and Ethernet) on a per-Interface basis. Traffic class mapping leads to two queues.

14.2.7 Spanning tree configuration

The spanning tree functionality is by default disabled. Spanning tree is enabled on the configuration page of the forwarding function by setting the value of the parameter ‘Spanning Tree’ to ‘process’. Spanning tree for the forwarding function is configured from a link on the forwarding function basic configuration page. In the illustration below, the FF spanning tree configuration page is shown.

Some spanning tree settings are made on the interface configuration page. This configuration page is identical for ETH and ETS interfaces.

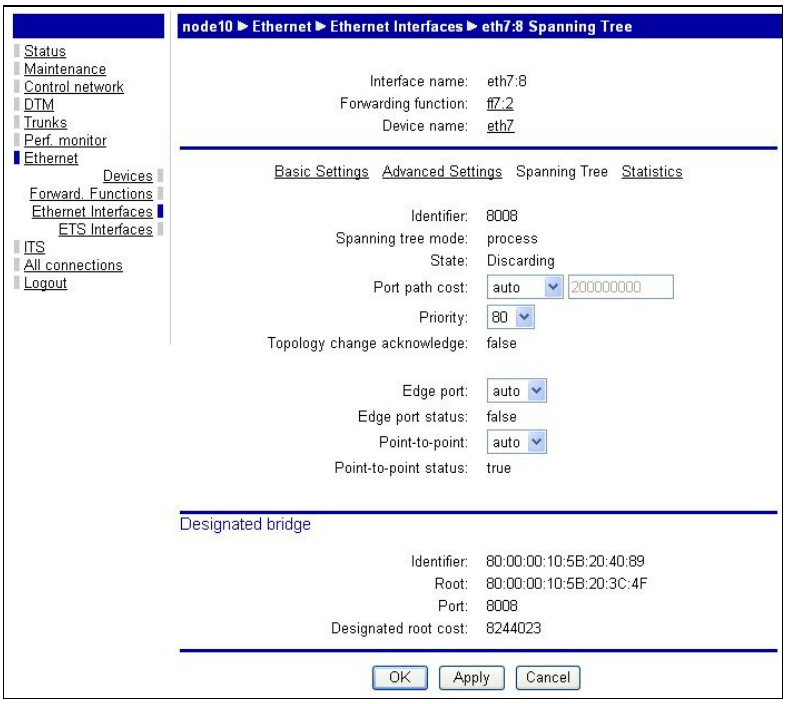


Figure 211. Spanning tree configuration (Forwarding Function), part one.

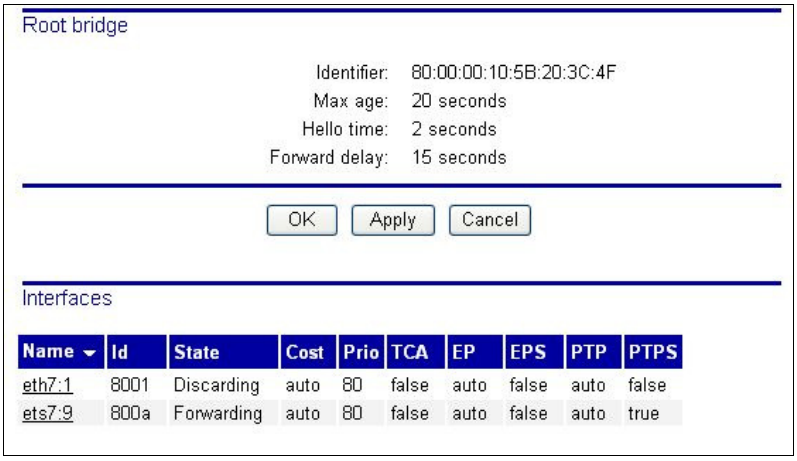


Figure 212. Spanning tree configuration (Forwarding Function), part two.

Spanning tree is specified in IEEE 802.1D from 2004. Net Insight adheres to the specification. The parameters are:

Parameter	Default	Range	Type	Comment
STP version	RSTP	STP, RSTP	IEEE 802.1D	
Priority	8000	0000-F000	Hexadecimal	Drop-down menu
Max age	20	6-40	Integer	seconds
Hello time	1	1-2	Integer	seconds
Forward delay	15	4-30	Integer	seconds
Transmit hold count	6	1-10	Integer	

Figure 213. Configurable spanning tree parameters for a forwarding function.

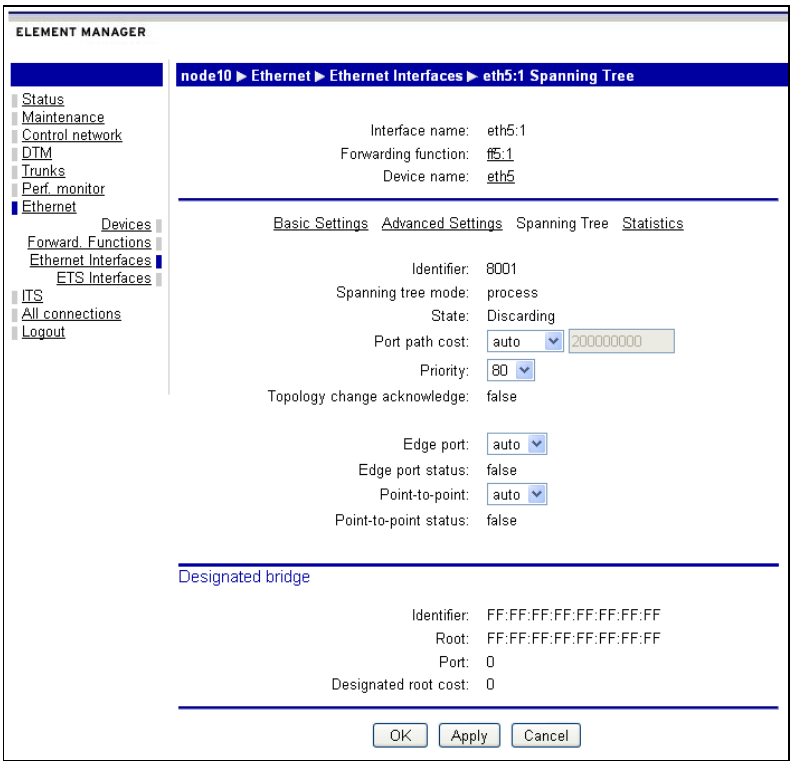


Figure 214. Spanning tree example configuration (ETS/ETH Interface).

The configurable spanning tree parameters on the interfaces are ‘Port path cost’, ‘priority’, ‘edge port’ and ‘point-to-point’. The parameters are explained in the table below:

Parameter	Default	Range	Type	Comment
Port path cost	Auto	Auto, Manual	Auto or Integer (manual)	Manual enables an input field
Priority	80	00-F0	Two hexadecimal digits	Drop-down menu
Edge port	Auto	Auto, True, False	Boolean variable	Drop-down menu
Point-to-point	Auto	Auto, True, False	Boolean variable	Drop-down menu

Figure 215. Configurable spanning tree parameters for an ETS/ETH interface.

Port path cost defines a cost associated with the particular port(interface). If two or more interfaces are available for a connection to a particular node, the spanning tree algorithm ensures that only the low-cost interface is used.

Priority defines the priority of the particular interface. The two hexadecimal digits are added as a prefix on the MAC address of the interface to create the identifier. The lowest identifier interface is used, in case there are two interfaces with equal cost.

Edge port is a Boolean variable used to signal if the interface is connected to equipment not part of the DTM Ethernet universe. Auto means that auto detection is used.

Point-to-point is a Boolean variable used to signal if the interface is connected to a link and a node with a point-to-point connection. Auto means that auto detection is used.

14.2.8 Unicast connection (ETS interface)

The configuration page of an ETS interface is created from the button ‘Create unicast ETS i/f’ found from the ETS interfaces link under the Ethernet link.

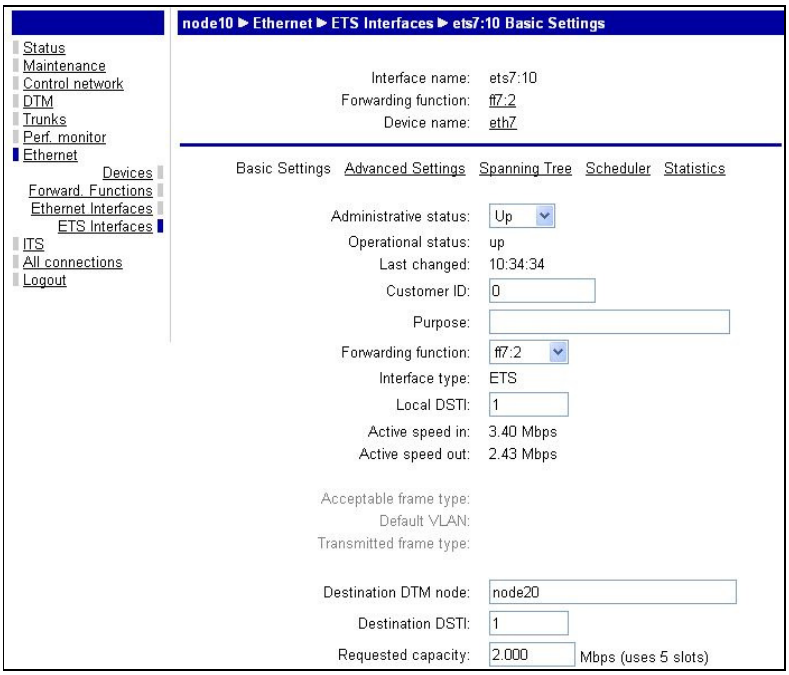


Figure 216. Configuration of an ETS unicast interface, upper part.

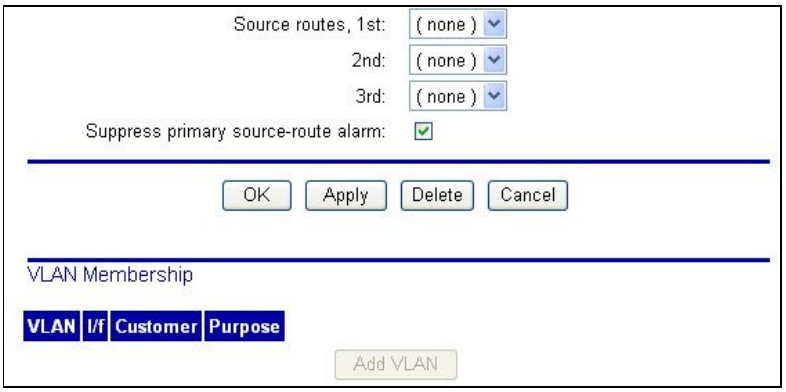


Figure 217. Configuration of an ETS unicast interface, lower part.

'Administrative status' can be 'Up' or 'Down', but is as default set to 'Down'. 'Customer ID' is an identification number of the interface, an integer between 0 and 4294967295 ($2^{32} - 1$). 'Purpose' is an arbitrary character string, up to 255 characters long that also can be used as an identifier.

Forwarding function: From this drop-down menu, all available FFs plus the option 'none' are available.

Local DSTI: The local DSTI is the local DTM Service Type Instance, an identification number of the channel.

Acceptable frame type can be 'All', 'tagged' or 'untagged'.

Default VLAN: If VLAN mode is set to 'Customer', untagged packets are tagged with the default VLAN tag (if they are transmitted as tagged; see below) and tagged packets are unaffected. Transmitted frame type can be tagged' or 'untagged'.

Destination DTM node is the DTM address or hostname of the destination. Destination DSTI is the DSTI number in the destination node for the terminating ETS.

Requested capacity for the connection is given in Mbps.

Source routes: 1st, 2nd and 3rd. Here source routes can be selected. They are defined under the All connections link. First source-route alarms can also be suppressed, if so selected. The used source route is indicated with the text 'currently used' within parenthesis.

14.2.8.1 VLAN

Click on the 'Add VLAN' button on the basic configuration page for ETS uni- or multicast interfaces to create a VLAN association. Observe that for VLAN mode transparent, this setting is grayed out.

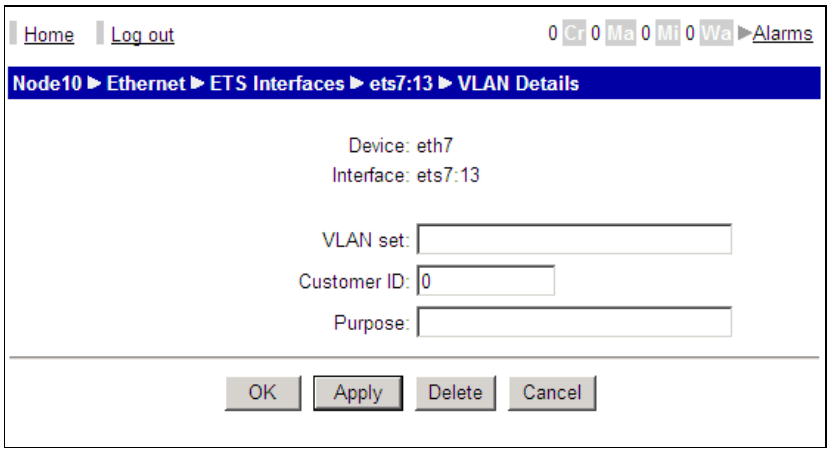


Figure 218. VLAN configuration.

The configurable parameters are:

'VLAN set' is the ID number of a VLAN, an integer in the range 1-4094, or a comma separated list of ID numbers or ranges of ID numbers. All VLANs included in this list are allowed to pass the interface. Example of such a list is 1,3,17-29,54,4002,4091

Customer ID is an identification number of the interface, an integer in the range 0-4294967295 ($2^{32} - 1$). The default value is 0.

'Purpose' is a Character string, up to 255 characters long. The default value is the empty string.

14.2.8.2 ETS Advanced settings

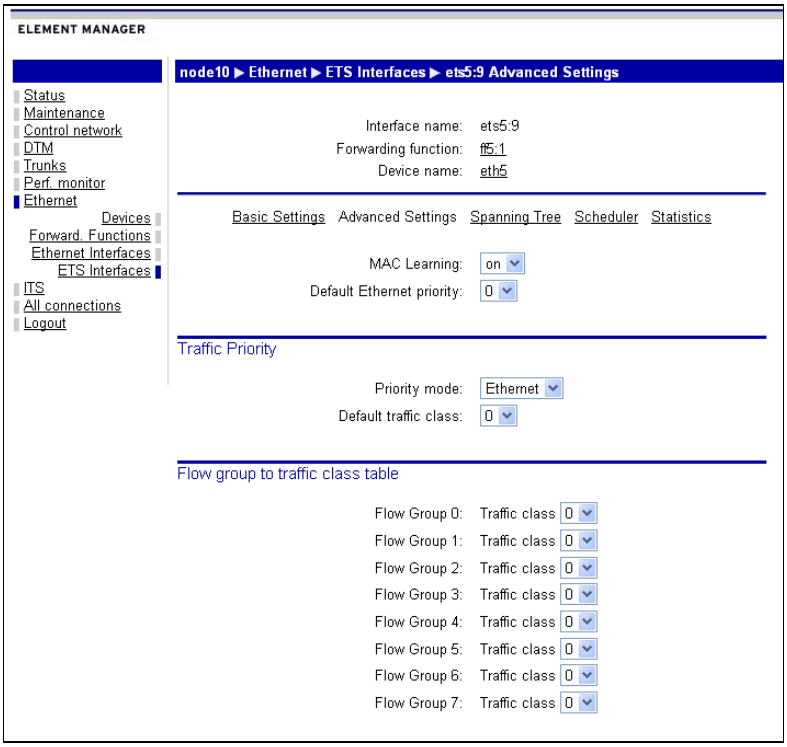


Figure 219. The picture illustrates the 'Advanced configuration' settings for unicast and multicast ETS creation, part one. For multicast (not shown here), there is an extra link for Destinations.

The parameter 'MAC Learning' means if a cross-reference table between MAC addresses and interfaces should be created or not. It is typically set to 'On' in MAC mode 'MAC' and to 'Off' in MAC mode 'Nomac'.

Default Ethernet priority can be set to any integer between 0 and 7 from the drop-down menu.

Priority mode is set to either Ethernet or Diffserv

The link Spanning Tree takes the user to the Spanning Tree menu.

The link Scheduler takes the user to the scheduler menu, under All connections.

Under the 'Flow group to Traffic Class Table', different Flow Groups (0 to 7) can be associated to different Traffic Classes (0 or 1).

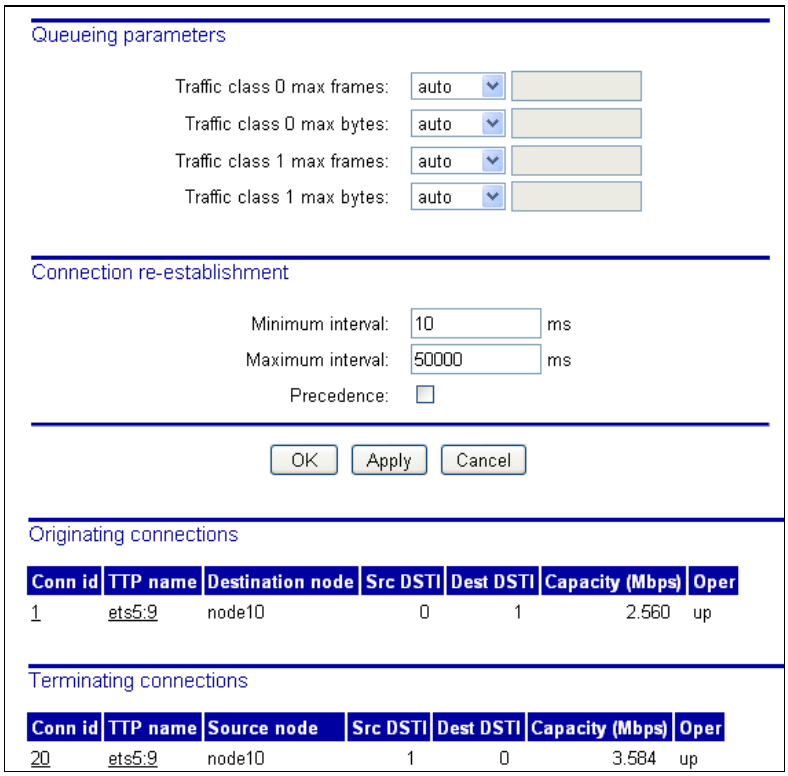


Figure 220. Advanced configuration settings for unicast and multicast creation, part two.

It is strongly recommended that the Queueing parameters are left with their respective default values. Setting these parameters manually requires skill and experience. Setting max frames to disable means effectively that all packets are dropped as the queue is turned off. Setting them to manual and a number controls the maximum number of frames in the queue and the total number of bytes in those frames. Contact Net Insight for more information.

Under the 'Connection re-establishment' header, the parameters of the exponential back-off algorithm and the reconnect time out can be set. Also, the connection can be defined as having "Precedence", which means that in case an intermediary node goes down, this particular connection is taken down with priority, which also means that a replacement connection is typically set up with priority (i.e. it has precedence over other connections).

Minimum interval: The starting value of the back-off algorithm is in this case 10 ms. When a connection is torn down, a first connection re-establishment attempt is made immediately; if the attempt fails, another attempt is made after the minimum interval of the back-off algorithm. The default setting is 10 ms.

Maximum interval: The end value of the algorithm, 50000 ms. The re-establish mechanism will wait no longer than 50000 ms to re-establish a channel.

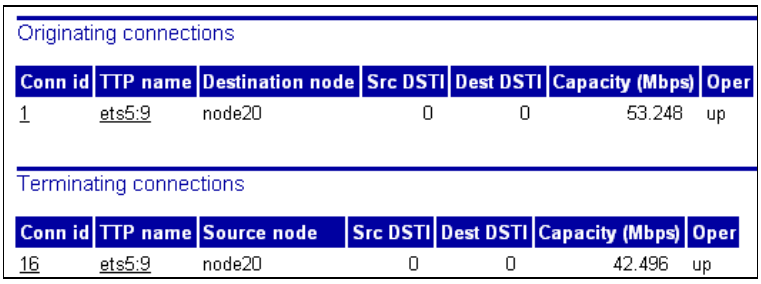


Figure 221. Listing of originating and terminating connections on ETS advanced configuration page.

14.2.8.3 ETH Advanced settings

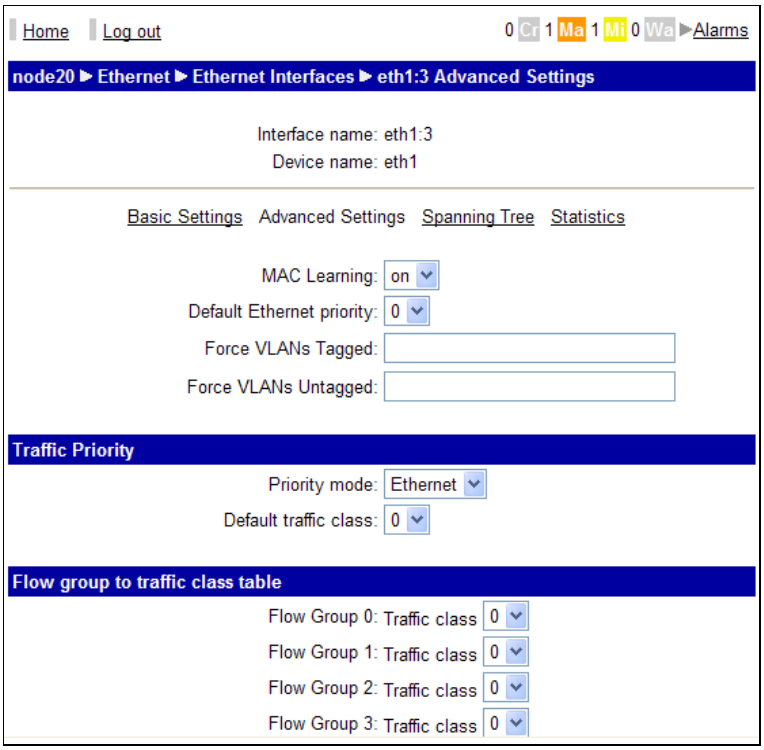


Figure 222. The picture illustrates the Advanced configuration settings for unicast and multicast eth creation, part one.

The parameters are configured as for ETS interfaces, except for the parameters ‘Force VLANs tagged’ and ‘Force VLANs untagged’. These parameters, with a list as argument like 1,2,5-8,16 (meaning VLANs 1,2,5 to 8 and 16 are affected), are exceptions to the general rule set under Transmitted frame type in ‘Basic Settings’.

For example, if ‘Transmitted Frame Types’ is set to ‘Untagged’ the value (list) stated above forces tags on VLANs 1,2, 5 to 8 and 16. The ‘Force VLANs untagged’ parameter has the opposite effect, i.e. no tags are set for VLANs listed here despite the ‘Tagged’ value of the parameter ‘Transmitted Frame Types’.

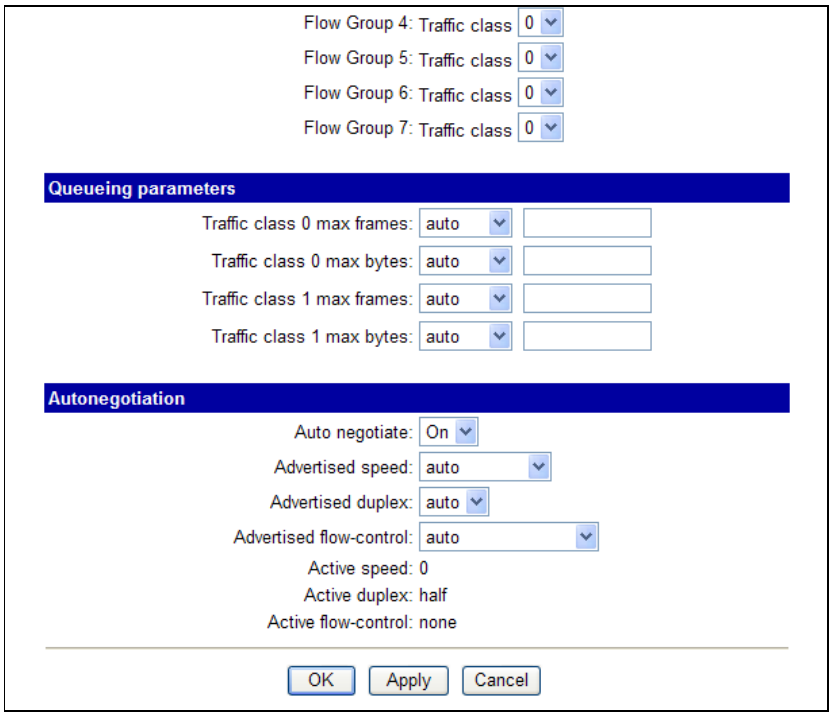


Figure 223. The picture illustrates the Advanced configuration settings for unicast and multicast eth creation, part two.

14.2.9 Multicast connection (ETS interface)

In addition to all settings links of a unicast connection, there is a Destinations link for multicast connections.

To add a destination, click on the 'Add Destinations' button and define:

Administrative status: Up or Down

Destination DTM node: DTM address or hostname of the destination node

Destination DSTI: DSTI of the connection at the destination node. Observe that this parameter is different for different destinations.

Add source routes as needed. New source routes are defined under All connections -> Source routes.

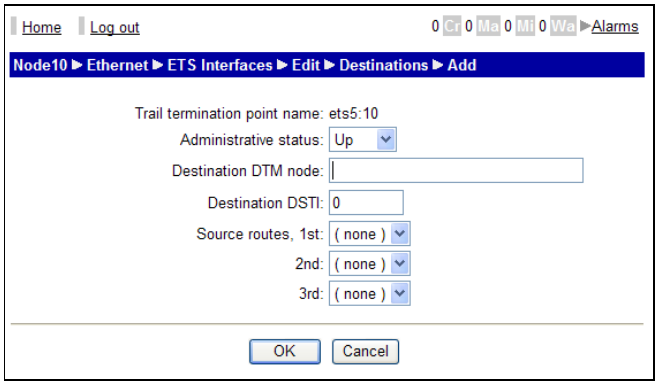


Figure 224. 'Add destinations' submenu for multicast ETS and ETH interfaces. Used source routes are indicated to the right of the drop-down menu.

14.2.10 Unicast connection on Eth interface

Configuration of Ethernet (ETH) and ETS interfaces are very similar. They are both tied to a forwarding function with essentially the same configurable parameters. In addition to all ETS parameters, there are two additional parameters under advanced settings (‘Forced VLANs tagged’ and ‘Forced VLANs untagged’).

In addition, auto negotiation with connected Ethernet equipment is defined for Ethernet interfaces. In order to use the auto negotiate feature, select ‘On’ in the roll-down menu for Auto negotiate (‘On’ and ‘Off’ are the two possible values). In addition, there are four roll-down menus for ‘Advertised speed’ (Auto, 1000&100&10 Mbps, 100 Mbps or 10 Mbps) and two drop-down menus for ‘Advertised duplex’ (Auto, full) and ‘Advertised flow control’ (‘Auto’, ‘PAUSE’, ’PAUSE,ASM_DIR’, ‘ASM_DIR’ is available). See IEEE 802.3-2005 for details of these settings.

Following the Statistics link, there is a page displaying Ethernet counter statistics for the specific interface.

14.3 Configuration examples

14.3.1 DTM network as extension cable

It is possible to configure the DTM network to act as an Ethernet extension cable, where the signal on a physical Ethernet interface is transported transparently through the DTM network from one endpoint to another.

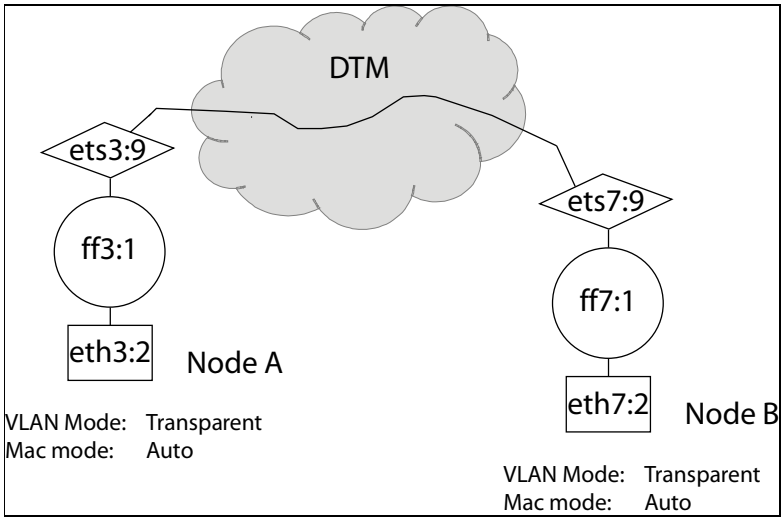


Figure 225. A unicast connection between two Ethernet interfaces.

The Forwarding Functions ff3:1 and ff7:1 must be configured the same way:

VLAN Mode	Transparent
MAC Mode	Auto (recommended) or Nomac
MAC Aging Time	Any allowed value works
Spanning Tree	Forward
Jumbo Frames	On is recommended

The Ethernet interfaces (eth3:2 and eth7:2) must be tied to their respective Forwarding Function (ff3:1 and ff7:1). In ETS unicast connection between ets3:9 and ets7:9, set up on two separated web pages, the local DSTI number must match the destination DSTI set up on the other ETS configuration page.).

14.3.2 ETS Multicast replication in the DTM layer

Multicast Ethernet, where traffic originates on one ingress interface and leaves the DTM network for further distribution on several egress interfaces, is illustrated below. This traffic pattern is typical for IP multicast distribution in applications like IP-TV.

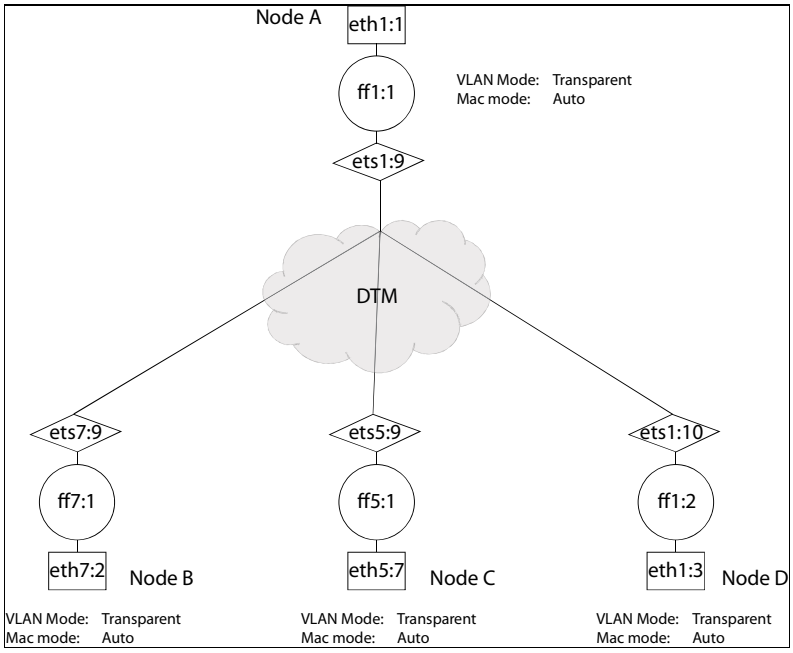


Figure 226. A multicast connection between one originating and three terminating interfaces.

All Forwarding Functions can be defined with VLAN mode transparent and MAC mode auto. MAC Aging Time can be chosen as the default, 300 s, and Jumbo Frames set to 'On' if oversized Ethernet packets are used in the application. In ff1:1, an ETS multicast connection is set up with three destinations. In the terminating ETS interfaces, a multicast ETS connection is defined. Make sure the used local DSTI matches the destination DSTI entered in the originating ETS interface. No destinations should be entered at the egress sites.

In this case, Ethernet capacity is reserved from the ingress interface at the top to the three egress interfaces at the bottom, but no capacity is reserved in the other direction.

The respective Forwarding Functions need to be connected to relevant Ethernet interfaces. VLAN settings may be Acceptable Frame Type: All, Default VLAN: 1 and Transmitted Frame Type: Tagged.

14.3.3 Ethernet Switching

Ethernet switching can be configured by connecting multiple ETS unicast channels to one common Forwarding Function. In the illustration below, one node is configured as hub node and three as spoke nodes. Three unicast ETS connections are defined between node A and nodes B, C and D respectively. These ETS interfaces are all associated to one forwarding function, which also is associated with node A. All nodes should have VLAN Mode set to 'Transparent' and MAC mode set to Auto'.

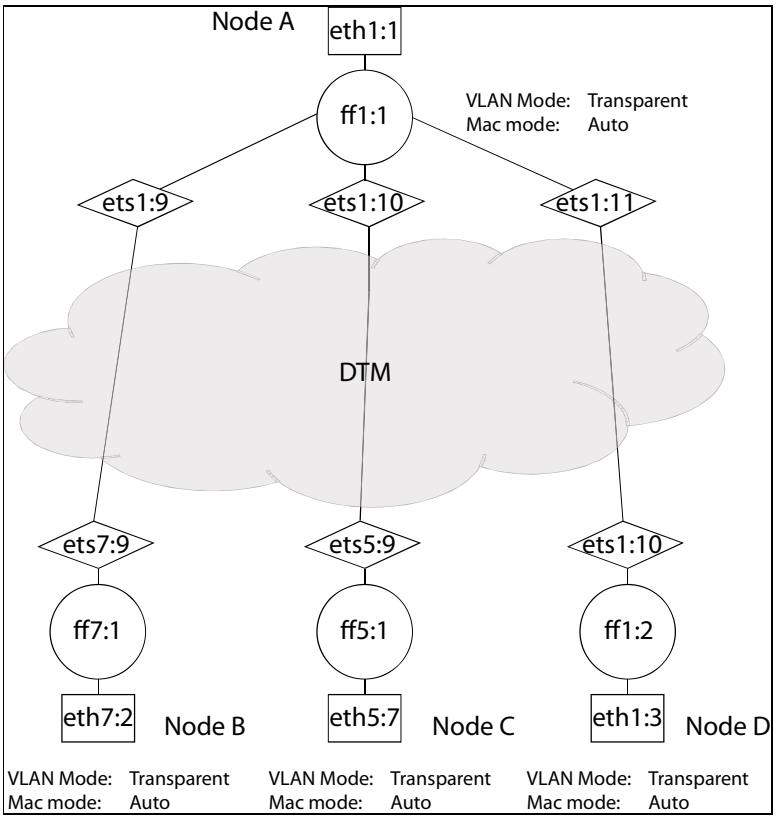


Figure 227. Ethernet switching with one switch and three more nodes.

14.3.4 Ethernet switch and VLAN tagging

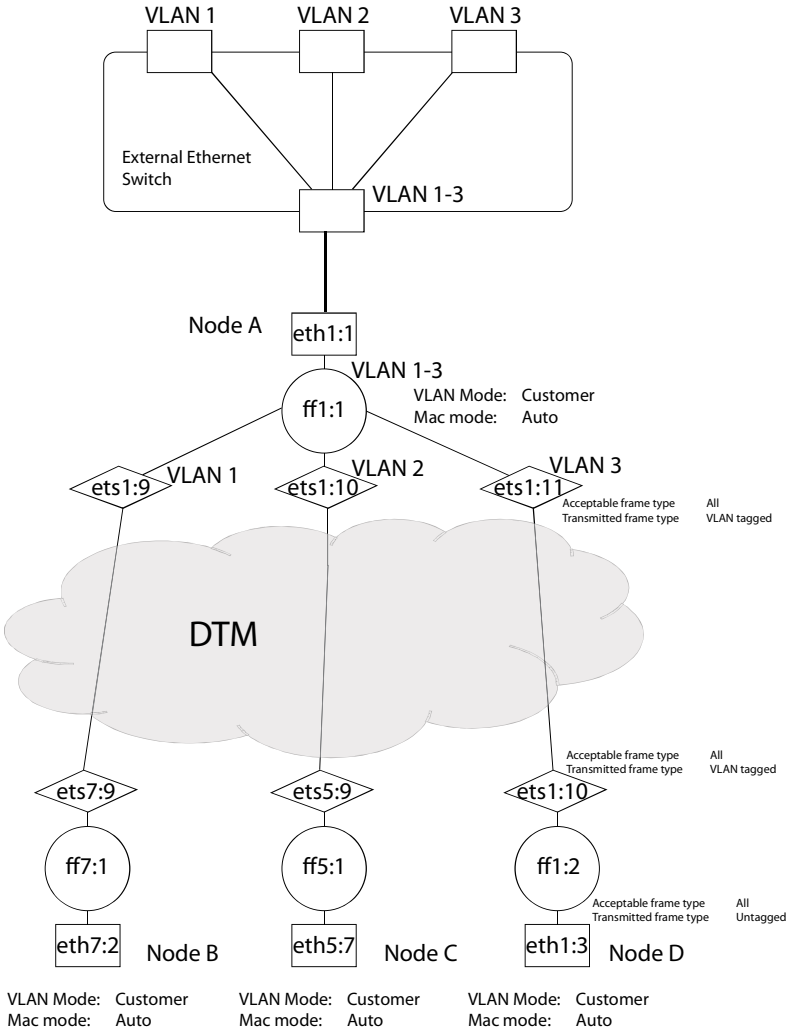


Figure 228. An external Ethernet switch with aggregated traffic from three separate VLANs has its traffic separated on three different Ethernet interfaces.

Different customers can share one common Ethernet interface in the Nimbra network. VLAN tagging makes it possible to separate the different VLANs in a Forwarding Function (in this case ff1:1) to three different virtual ETS interfaces. On the outgoing Ethernet interfaces, typically the tags are removed, which makes the entire DTM network transparent.

14.3.5 Auto-negotiation protocol (Nway)

Flow control enables flow control for Ethernet.

Auto-negotiation protocol (Nway):
The enableNway setting controls whether the interface uses the NWAY auto negotiation protocol or not. If the resource is set to yes then there is an exchange of information between the interface and its link partner. Each interface sends an announce message containing its capabilities regarding

speed and duplex. Each interface also expects to receive such an announcement. If it does receive capabilities form its link partner then the highest common speed and duplex is selected and the interface is configured to use these settings.

In the case that the interface does not receive capabilities from its link partner then a process called parallel detection is used to determine the settings. This process listens to the link heartbeats and symbol rates to determine the speed that the link partner is using. The duplex mode cannot be determined and half-duplex is always selected.
If `enableNway` is set to off then no exchange of capabilities will take place and the interface is statically configured. Observe that the settings of both link partners must match exactly.

The capabilities to announce and static selection is selected by modifying `currentSpeed` and `currentDuplex` in the interface table

Selected Speed; the speed for the interface is configured here.

If enableNway is on and the interface type is 100Base-TX then:

Autoselect announces 10 Mbps and 100Mbps speed capabilities.

100 announces 100Mbps speed capability only.

10 announces 10Mbps speed capability only.

If enableNway is off and the interface type is 100Base-TX then:

Autoselect results in 100Mbps speed.

100 results in 100Mbps.

10 results in 10Mbps speed.

If enableNway is on and the interface type is 1000Base-[SX|LX|ZX|T]

Autoselect announces 1000 Mbps speed capability.

1000 announces 1000 Mbps speed capability.

If enableNway is off and the interface type is 1000Base-[SX|LX|ZX|T]

Autoselect results in 1000 Mbps speed.

1000 results in 1000 Mbps speed.

Selected Duplex; the duplex for the interface is configured here.

If enableNway is on and the interface type is 100Base-TX

Autoselect announces full- and half-duplex capabilities.

Full-duplex announces full-duplex capability only.

Half-duplex announces half-duplex capability only.

If enableNway is off and the interface type is 100Base-TX

Autoselect results in full-duplex operation

full-duplex results in full-duplex operation

half-duplex results in half-duplex operation

If enableNway is on and the interface type is 1000Base-[SX|LX|ZX|T]

Autoselect announces full-duplex capability.

Full-duplex announces full-duplex capability.

Half-duplex announces half-duplex capability.

If enableNway is off and the interface type is 1000Base-[SX|LX|ZX|T]

Autoselect results full-duplex.

Full-duplex results in full-duplex.

Half-duplex results in half-duplex.

Active speed presents the current speed of the interface.

Active duplex presents the present duplex of the interface.

Default VLAN the VLAN is selected from the drop down list.

Drop untagged packets

The capabilities to announce and static selection is selected by modifying currentSpeed and currentDuplex, the most common setting is presented in the table below.

100Base-TX									
	Local interface				Link partner				Result
Comment	Speed	Duplex	Flow	Nway	Speed	Duplex	Flow	Nway	spd/dpx/an
auto	auto	auto	off	on	auto	auto	on	on	100/full/off
auto	100	auto	off	on	auto	auto	on	on	10/full/off
auto	10	auto	off	on	auto	auto	on	on	100/full/off
auto	auto	full	off	on	auto	auto	on	on	100/full/off
auto	100	full	off	on	auto	auto	on	on	10/full/off
auto	10	full	off	on	auto	auto	on	on	100/half/off
auto	auto	half	off	on	auto	auto	on	on	100/half/off
auto	100	half	off	on	auto	auto	on	on	10/half/off
auto	10	half	off	on	auto	auto	on	on	100/full/on
auto	auto	auto	on	on	auto	auto	on	on	100/full/on
auto	100	auto	on	on	auto	auto	on	on	10/full/on
auto	10	auto	on	on	auto	auto	on	on	100/full/on
auto	auto	full	on	on	auto	auto	on	on	100/full/on
auto	100	full	on	on	auto	auto	on	on	10/full/on
auto	10	full	on	on	auto	auto	on	on	100/half/on
auto	auto	half	on	on	auto	auto	on	on	100/half/on
auto	100	half	on	on	auto	auto	on	on	10/half/on
auto	10	half	on	off	100	full	off	off	100/full/off
static	100	full	off	off	10	full	off	off	10/full/off
static	10	full	off	off	100	half	off	off	100/half/off
static	100	half	off	off	10	half	off	off	10/half/off
static	10	half	off	off	100	full	on	off	100/full/on
static	100	full	on	off	10	full	on	off	10/full/on
static	10	full	on	off	100	half	on	off	100/half/on
static	100	half	on	off	100	half	on	off	100/half/on
static	10	half	on	off	10	half	on	off	10/half/on

Fault examples

fault	100	full	off	off	100	half	off	off	incompatible
fault	100	any	any	any	10	any	any	any	incompatible
fault	any	any	off	off	any	any	on	off	incompatible

Figure 229. Configuration with Nway enabled.

If enableNway is off and the interface type is 1000Base-[SX|LX|ZX|T]

1000Base-[SX|LX|ZX|T]									
	Local interface				Link partner				Result
Comment	Speed	Duplex	Flow	Nway	Speed	Duplex	Flow	Nway	spd/dpx/an
auto	auto	auto	off	on	auto	auto	on	on	1000/full/off
auto	1000	auto	off	on	auto	auto	on	on	1000/full/off
auto	auto	full	off	on	auto	auto	on	on	1000/full/off
auto	1000	full	off	on	auto	auto	on	on	1000/full/off
auto	auto	auto	on	on	auto	auto	on	on	1000/full/on
auto	1000	auto	on	on	auto	auto	on	on	1000/full/on
auto	auto	full	on	on	auto	auto	on	on	1000/full/on
auto	1000	full	on	on	auto	auto	on	on	1000/full/on
static	1000	full	on	off	1000	full	on	off	1000/full/on
static	1000	full	off	off	1000	full	off	off	1000/full/off
Fault example									
fault	any	any	off	off	any	any	on	off	incompatible

Figure 230. Configuration with Nway disabled and a 1000 Mbps interface

To make changes for an interface, mark the **Toggle Admin** selection, make the changes and click on **OK** or **Apply** button.

When all parameters are entered click the **OK** button.

The **Edit Device** page reappears.

14.4 Priority

Prioritization is performed on traffic within the ETS channel, which makes it possible to provide a differentiated service to the customers. For customers utilizing equipment with or without VLAN-tagging, diffserv prioritization can be used to prioritize the traffic.

Diffserv user priority is supported according to the standard for prioritizing IP-packets based on information in the IP DSCP field, RFC2474 and RFC2475.

Ethernet user priority is supported according to the standard for prioritizing Ethernet frames based on information in the Ethernet user priority field, IEEE 802.3-2002 and IEEE 802.1D.

Please note that this function is only supported in the new Fast Ethernet Module (article number NPS0017-X001) and the Gigabit Ethernet Module.

14.4.1 Diffserv and Ethernet user priority

Support for two ways of prioritizing Ethernet frames is provided:

Diffserv: Differentiated services, a standard for prioritizing IP packets based on the DSCP-field in the IP-header. Specified in [RFC2474] and [RFC2475].

Ethernet: Ethernet user priority, a standard for prioritizing Ethernet frames based on the Ethernet user priority field. This field only exists in tagged Ethernet frames and is standardized by IEEE in [802.3] and [802.1D]. This mechanism is also known as (the now obsolete) 802.1p.

Each virtual port, ETS TTP or physical Ethernet port, supports two out-queues, 0 and 1 with different levels of priority. Frames in queue 1 are strictly prioritized over frames in queue 0.

Traffic class

Each frame arriving to a GEC- or FEC-board is assigned a traffic class (TC). The TC is used for selecting out-queue on the virtual port. The TC is always assigned based on configuration on the TTP or physical Ethernet port the frame arrived on to the GEC or FEC.

The traffic classes local to each GEC or FEC. It is not propagated over the network.

14.4.2 Assignment of Traffic class

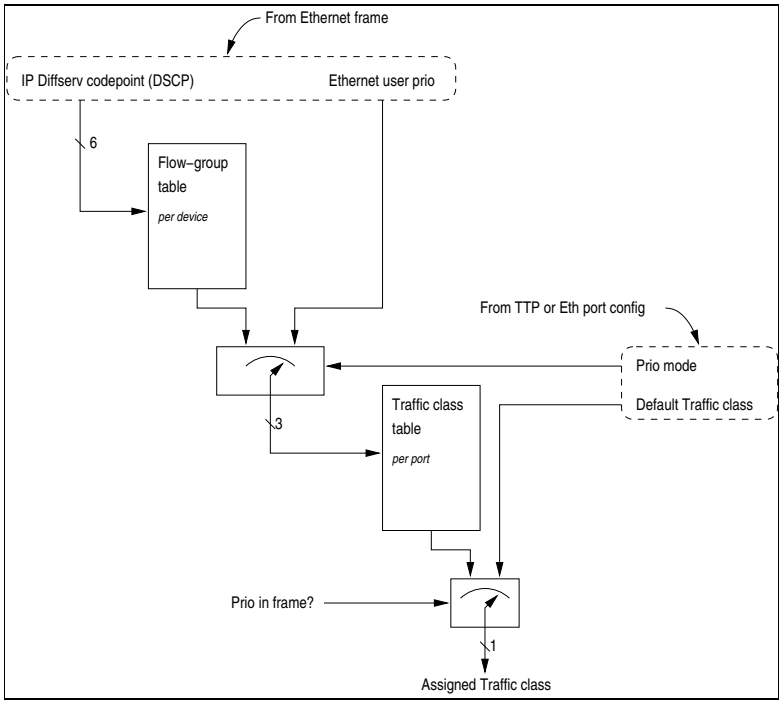


Figure 231. Assignment of Traffic class

The assignment of Traffic Class is performed as illustrated.

Priority mode can either be set to either of:

Diffserv

Index the device-global flow-group table with the DSCP-field from the IP-header to get the flow-group.

Index the virtual port-local traffic class (TC) table with the flow-group to get the TC.

Index the virtual port-local traffic class table with the Ethernet user priority from the Ethernet frame to get the TC.

Check if the frame contains priority (Ipv4- or Ipv6-header in the case priority mode = Diffserv and tagged frame in the case priority mode = Ethernet user priority). If it does, use the traffic class assigned **Diffserv** above. Otherwise, use the virtual-port configured default traffic class.

15 Isochronous Transport Service (ITS)

15.1 Overview

The ITS menu handles configuration of all Isochronous Transport Services (ITS). These services are used to create HD/SD-SDI, ASI, AES/EBU, PDH and Sonet/SDH tunnels through the DTM network.

The services can be of two different types, unicast or multicast. Unicast ITS services transport a stream through the network from one originating interface to one terminating node. Multicast ITS services transport a stream from an ingress interface to multiple egress interfaces.

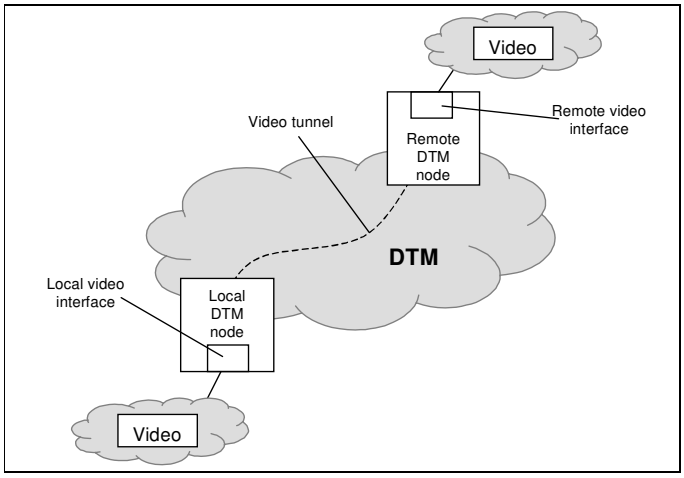


Figure 232. Video tunnel through the DTM network, unicast

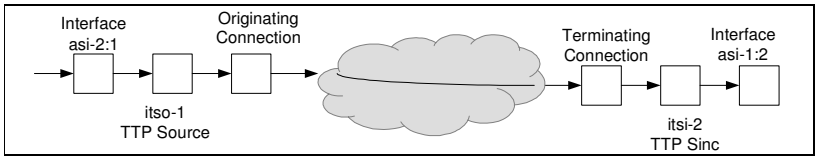


Figure 233. ASI,TTP connection, unicast

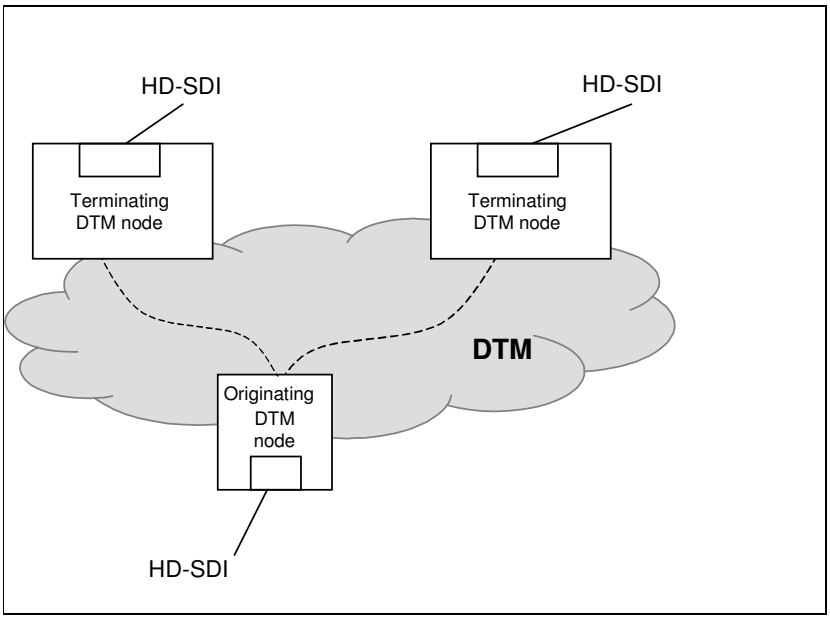


Figure 234. Multicast HD-SDI tunnel through the DTM network

This chapter describes how to configure ITS services, both uni- and multicast. The main web page for ITS is shown below.

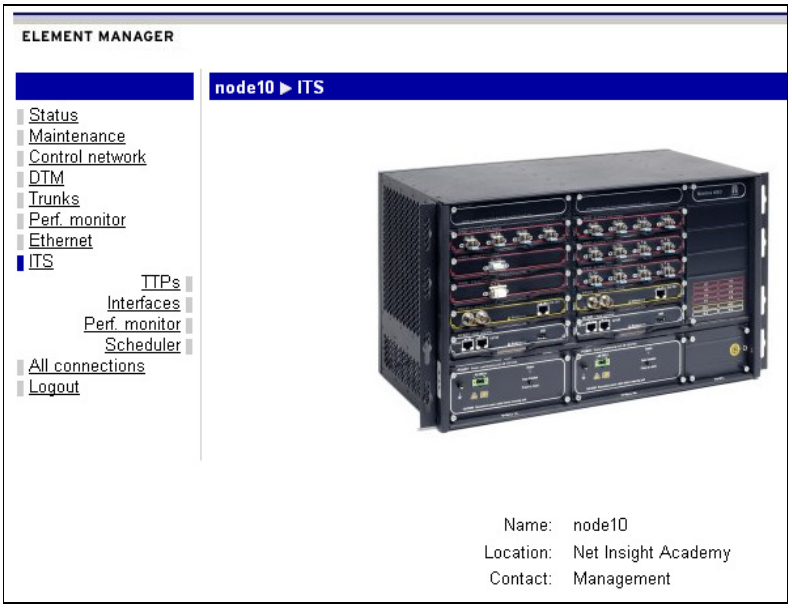


Figure 235. ITS main page

The sub-sections of the Isochronous Transport Services (ITS) are:

TTPs**:** Configuration and editing of ITS TTPs (Trail Termination Points).

Interface**:** Configuration and editing of the interfaces.

Perf. monitor**:** Shortcut to the Performance monitoring menu, which is seen in chapter *Performance monitoring*.

Scheduler**:** Configuration and editing of scheduler of the connections.

To configure ITS services, start with creating TTPs with destinations (i.e. ITS sources). Continue with matching TTPs at the various ITS destinations (one or multiple). After finishing the configuration, all ITS channels should be set up if the required bandwidth is available.

15.2 Interface settings for Access Module

The configurable settings for the access cards are found either under ITS or ETS headings in the web browser interface. The interface settings of ITS services are found under **ITS** → **Interfaces** web page, described below.

15.2.1 Configurable interface parameters

15.2.1.1 Mute TX Signal on fault

Default value: Unchecked

Type: Binary

Range: Checked, Unchecked

Description: If checked, the module's TX port is muted upon reception of a defect indication such as AIS. If not checked, the port transmits IDLE bytes (ASI) / Undefined (other boards) during defect intervals. The muting function may speed up fail-over switching time when using external fail-over switches.

15.2.1.2 Ignore TS-packet synchronization errors

Default value: Unchecked

Type: Binary

Range: Checked, Unchecked

Description: If checked, synchronization errors in the Transport Stream packets are ignored. This option will allow the Nimbra equipment to accept ASI streams which do not comply with accepted international standards. The robustness of the transport stream cannot be guaranteed in this mode and it should be seen as a customer specific workaround for deficiencies in equipment from other vendors. The setting should be made on the receive side of the connection.

15.2.1.3 Output mode

Default value: Auto

Type: One of Auto, Spread, Burst

Range: Auto, Spread, Burst

Description: Determines how MPEG TS packet bytes are transmitted from the ASI TX port.
In Burst mode, all bytes of a TS packet are sent back-to-back in one burst. IDLE bytes are sent between bursts to adapt the bit stream.

In Spread (spread-byte) mode, TS packet bytes are spread out as evenly as possible, with IDLE stuffing between TS packets as well as between bytes within a TS packet.

In Auto mode, Burst or Spread mode is automatically selected to be the same as detected on the corresponding ASI RX port.
In general, Spread mode is the preferred mode.

15.2.1.4 Suppress alarms

Default value: None

Type: one value in range

Range: None, Warning, All

Description: None does not suppress any alarms; Warning suppresses only alarms with severity warning and All suppress all alarms.

15.2.1.5 Loopback

Default value: None

Type: one of None, Line or DTM

Range: None, Line, DTM

Description: None sets No loopback; Line sets Line side traffic is in loopback mode, i.e. traffic arriving at the Rx interface is sent back on the associated Tx interface; DTM sets DTM side traffic in loopback mode, i.e. traffic exiting on a Tx interface is looped as closed to the interface and returned on the corresponding Rx interface. Some modules may not have all capabilities.

15.2.1.6 Loopback reset timeout (s)

Default value: 0

Type: integer

Range: ≥ 0

Description: This parameter is the time the parameter Loopback has a value different from None. A loopback reset timeout value of 0 disables the function and makes the loopback permanent. Observe that with Loopback set to Line, Loopback reset timeout to 0 and no other communication links open to the node, the node becomes isolated.

15.2.1.7 Interface mode

Default value: SDH

Type: One of SDH, Sonet

Range: SDH, Sonet

Description: This parameter determines if the interface works in SDH or Sonet mode.

15.2.1.8 Transmit sync source

Default value: Loop

Type: one of Loop, Internal

Range: Loop, Internal

Description: This parameter determines which clock is used for the outgoing signal from the interface. When Transmit sync source is set to Loop, the clock from the incoming signal on the interface is extracted and used as clock for the outgoing signal. When Transmit sync source is set to Internal, the node internal clock is used as clock for the outgoing signal.

15.2.1.9 SDH Sync message

Default value: 15

Type: Integer, 0-15

Range: 0-15

Description: Sets the outgoing Synchronization Status Message (SSM) in byte S1. The default value is 15. (Do not use for synchronization!)

If Transmit sync source is set to Internal, the value 11 should be set (G.813 Option I)

15.2.1.10 Interface to monitor

Default value: None

Type: interface

Range: None, sdi-1:1-1:8

Description: This parameter describes which interface is monitored, i.e. which incoming or outgoing video stream that is duplicated and sent to the configured interface.

15.2.1.11 PDH signal to transport

Default value: DS3

Type: one of DS3, E3

Range: DS3, E3

Description: PDH type to transport, configurable per interface.

In the cross-reference table below, it is shown on which modules/fixed interfaces the different configurable parameters are found.

Configurable parameter	E1 or T1 Access Module	DS3/E3 Access Module	4 x OC-3/STM-1 Access Module	SDI Video Access Module	ASI Transport Access Module	8 x ASI Transport Access Module	8 x AES/EBU Access Module	Fixed ASI interface (Nimbra 340)	Fixed HD-SDI i/f (Nimbra 340-HD)	8 x or 8 x 3Gbps Video Access Module, HD/SD or 3G –SDI configured interface (Nimbra 600)	8 x Video Access Module, ASI configured interface (Nimbra 600)	8 x Video Access Module, monitor configured interface (Nimbra 600)
Mute TX Signal on fault	x	x		x	x	x	x	x	x	x	x	
Output mode						x					x	
Ignore TS-packet synchronization errors											x	
Suppress alarms	x	x	x	x	x	x	x	x	x	x	x	
Loopback	x	x	x	x	x			x	x			
Loopback reset timeout (s)	x	x	x	x	x			x	x			
Interface mode			x									
Transmit sync source			x									
Synchronization Status Message (SSM)			x									
Interface to monitor												x
PDH signal to transport			x									

Figure 236. Cross-table Configuration parameters vs. Access Module

15.3 Setting up a unicast ITS tunnel

Tip:

Configure the terminating connections before the originating connections, when doing so the establish time will be 5 ms compared to 50 ms. Only works for unicast connections.

15.3.1 Terminating Connection

Follow the ITS → TTPs link; a page appears like the page below.

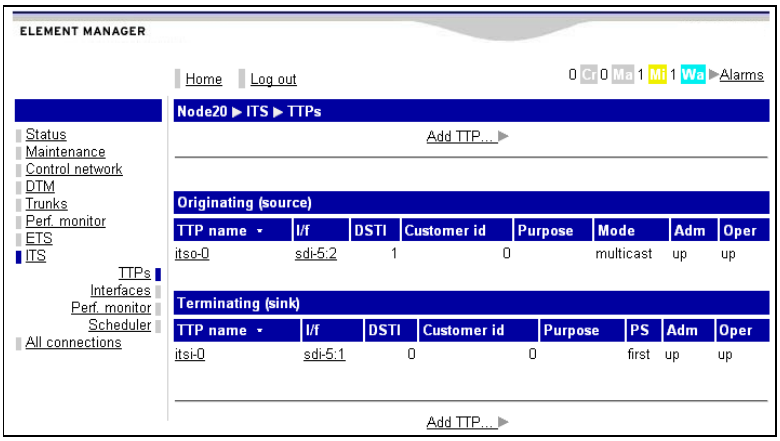


Figure 237. ITS setup TTPs main terminating page

Click on Add TTP … to configure the Termination; see figure below.

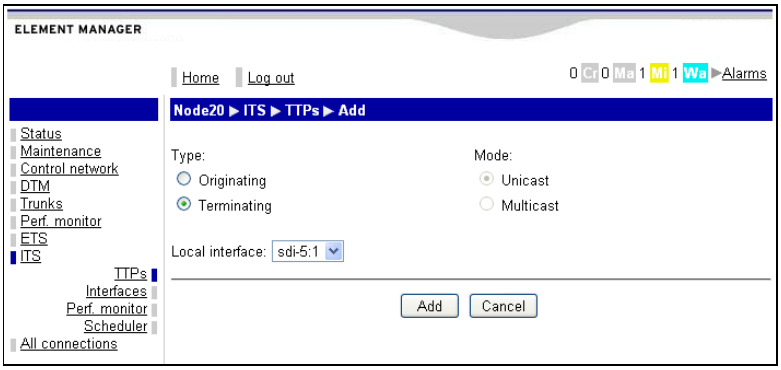


Figure 238. ITS, TTPs, Add page

On this web page, type can be set to originating (source) and terminating (sink). Mode can also be set, either to unicast or multicast. As soon as terminating type is set, the options for mode becomes irrelevant and the setting can no longer be made.

The local interface drop down menu lists all possible available options for the local interface. The selected interface is tied to the connection and TTP.

When the add button is selected, the terminating TTP is configured/defined in a web page.

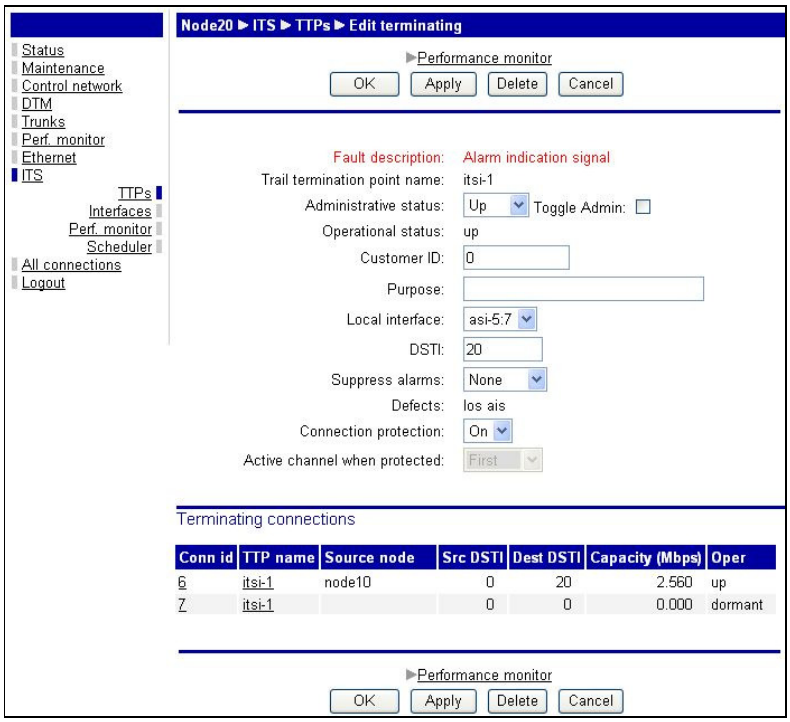


Figure 239. Configuration of terminating TTP of an ITS unicast channel.

Reference information

Administrative status is either Down (when the TTP is disabled) or Up (when attempts to establish a channel to this TTP is made). Customer ID (integer) and Purpose are freely configurable fields. In the local interface drop down menu, all available interfaces are listed. DSTI is the DTM Service Type Instance, a unique number per service type and node. A default DSTI is selected by the system but it can be user modified. The DSTIs don't have to be consecutive.

Suppress alarms can have valued none, warning or all. Active channel when protected can be set to first or second. This is the defined channel. It is grayed out if it cannot be set.

Note that there are two terminating connections connected to one single TTP. This is because of the open ended 1+1 protection feature, described in chapter Source Routing.

When finished; Click **'OK'** or **'Apply'**.

15.3.2 Originating Unicast Connection

Note:	Even if there are 2 in + 2 out connectors on the 340-HD for HD-SDI, there are only one HD-SDI in and one out stream that can be configured. One of the two in or out connectors can be used at a time! The preferred in and out HD-SDI streams should be configured via the web. Both out ports can be used for a multicast HD-SDI stream.

Follow the ITS → TTPs link; a page appears like the page below.

Click on Add TTP … to enter the setup page. A page similar to the page below will appear.

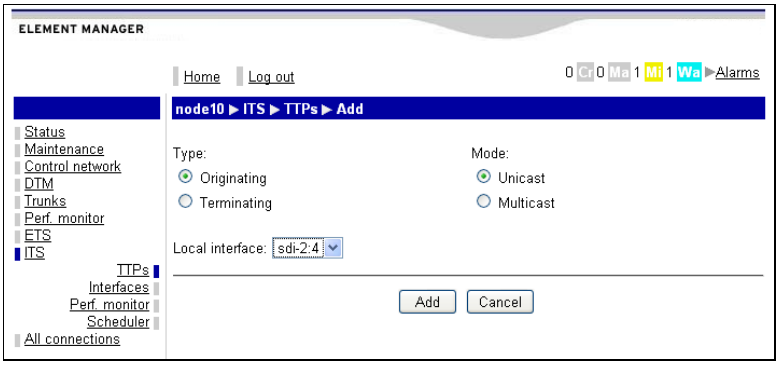
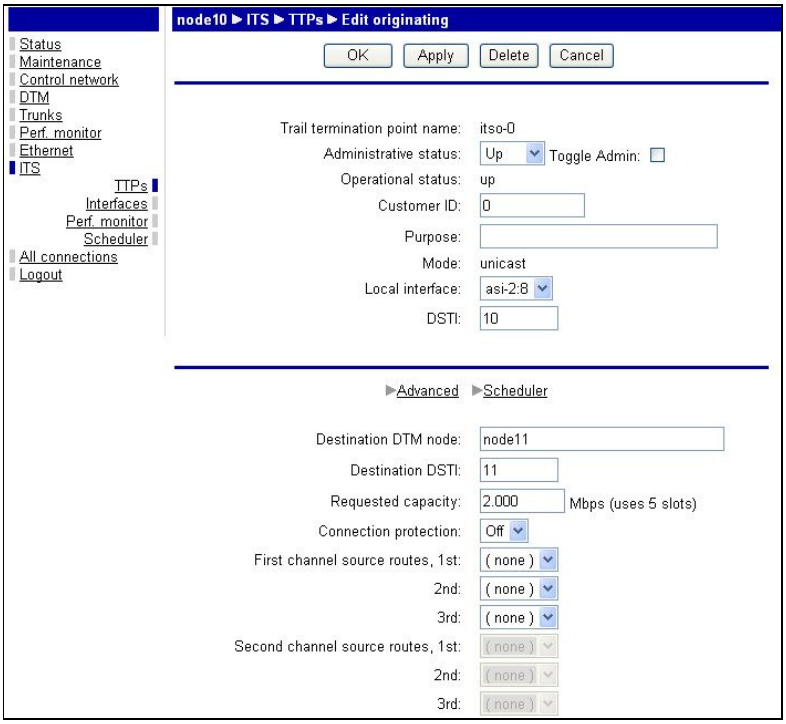


Figure 240. Definition of the originating ITS TTP.

In the web page, the same settings as for the terminating TTP can be made.

Make the settings required (Originating/Unicast), use the drop-down menu to set the local interface and click on the **Add** button.



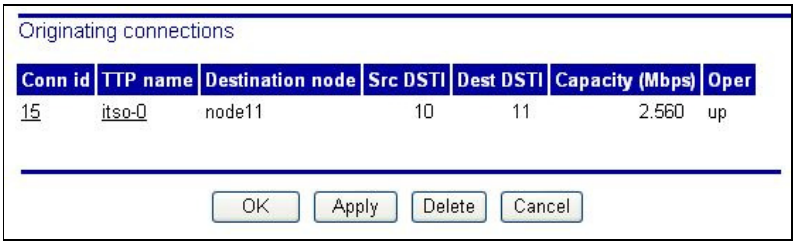


Figure 241. ITS, TTPs, create connection page

In addition to the settings made for the termination, in the originating node the destination DTM node with associated destination DSTI are needed. The required capacity must be specified, either as a bandwidth (2-212 Mbps) for ASI or SDI (270 Mbps), SDI compatible (from Nimbra 600 to Nimbra One/300) HD-SDI (1.485 Gbps) or 1.485/1.001 Gbps.

We must also specify if we use protection and the source route(s) we use (if any). If a source route is used, this is indicated on the web page with the text 'currently used' within parenthesis to the right of the source route itself.

See chapter Source Routing for additional information on how to setup a source route.

Once both terminating and originating nodes are configured, the channel should be established if enough transport bandwidth is available.

Note:	The lower part Destination DSTI is the terminating unit DSTI number. Note the DSTI number for the unit you are logged in to.

15.4 Setting up a multicast ITS tunnel

A multicast ITS tunnel is a channel from one ingress interface to multiple egress interfaces. The channel is unidirectional, i.e. traffic only flows from the source to the destination. No traffic is transmitted in the back direction.

In our example, an HD-SDI channel is set up between node10 and node20. The channel is terminated on several interfaces in node20.

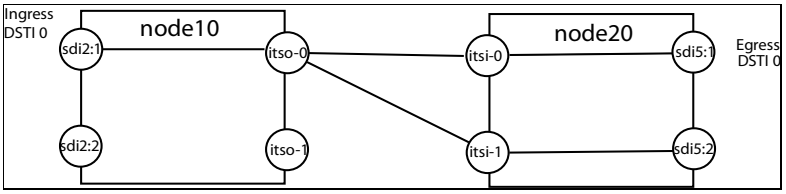


Figure 242. Setup of Multicast Channel.

15.4.1 Originating Multicast Connection

Follow the ITS → TTPs link and the link Add TTP … ; a page appears like the page below.

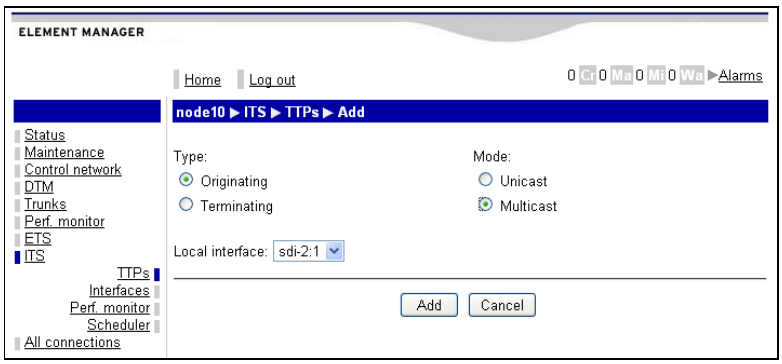


Figure 243. ITS setup TTPs page main

Chose the type of interface (originating) and type of mode (unicast/multicast). Use the pull-down menu to set the local interface. Click on the Add button.

A webpage similar to page below will appear.

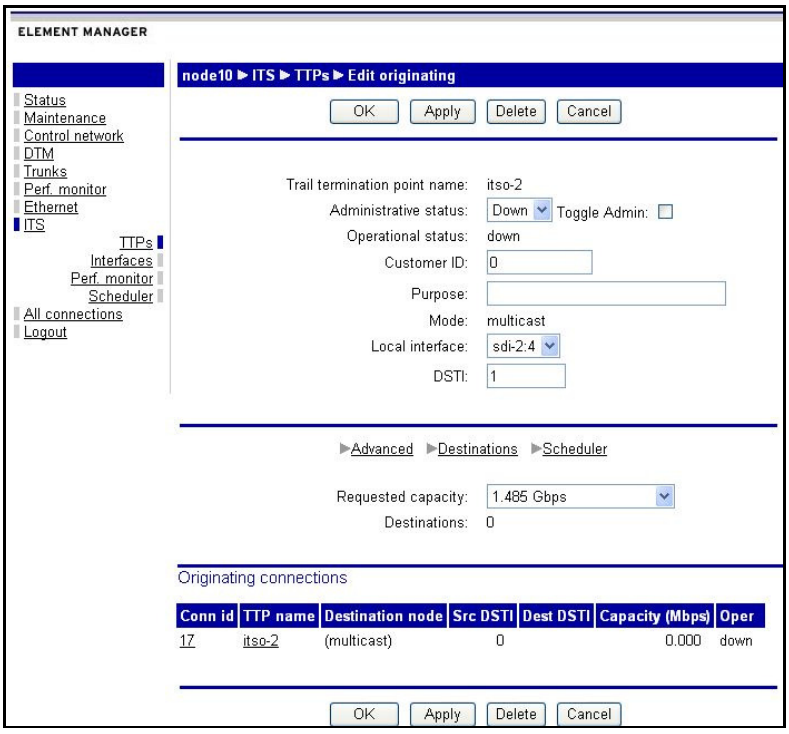


Figure 244. ITS TTPs create Multicast page

In addition to common parameters with the unicast case, there is an extra link to Destinations, where the details about the various destinations are entered.

Click on the Destinations in the middle of the page, to set the multicast destinations for the originating connection. This page shows the nodes that are configured in this connection.

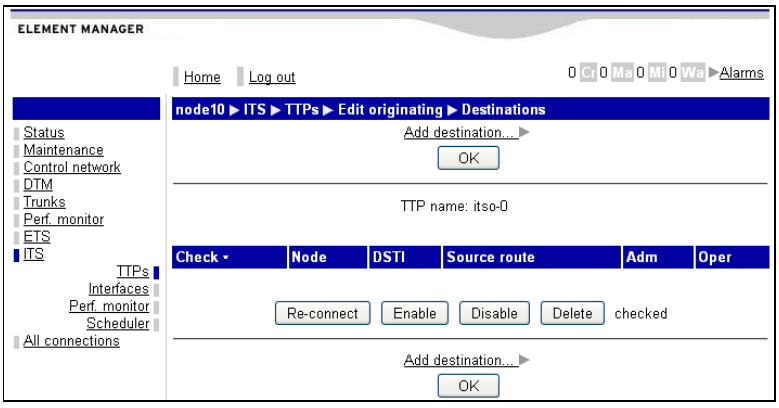


Figure 245. ITS Add destination page. No destinations are listed here.

In order to define the destinations, click on the link Add destination… and enter the parameters for the terminating TTPs. In the following figures, the two destinations of our example are shown.

Click on the **Add destination** to add a new node.

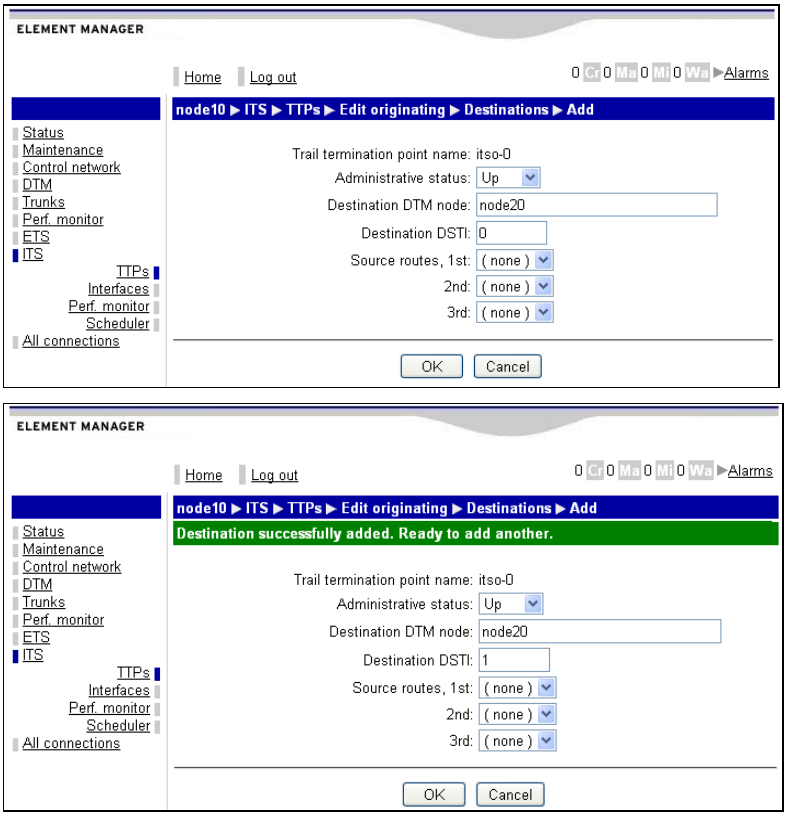


Figure 246. Destinations to an ITS TTPs are defined.

Set Administrative status to 'Up', Destination DTM to node20 and destination DSTI to 0 and 1 for the two different cases. The destinations have now been added. In this case, we have not used source routes.

When all the nodes are added click on the **Cancel** button, a list of the destinations is shown in the Destination page. As the terminating side is not yet defined, the destinations are listed as down.

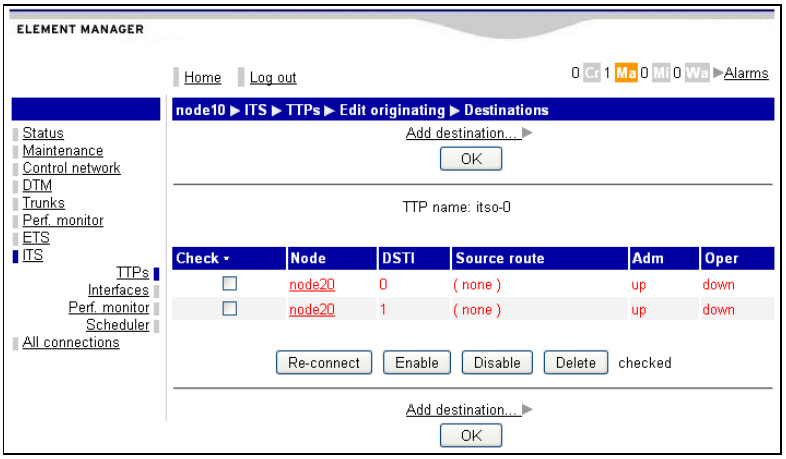


Figure 247. Destinations defined in the originating TTP.

15.4.2 Terminating Multicast Connection

Follow the ITS → TTPs link and the link Add TTP … ; a page appears like the page below.

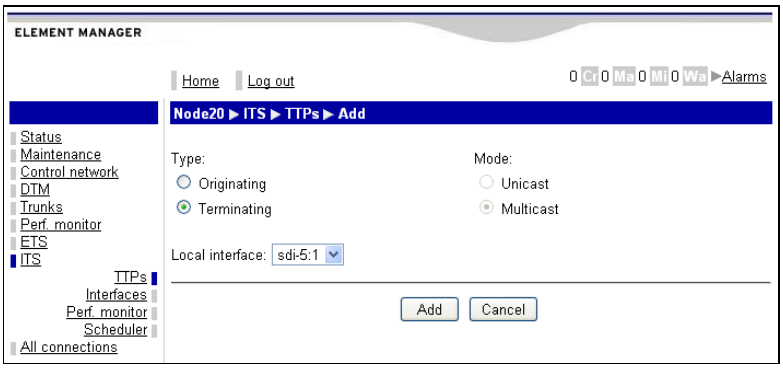


Figure 248. ITS TTPs create Multicast page

Select the type to Terminating and use the pull-down menu to set the local interface.

Click on the **Add** button. Repeat for all destinations.

15.5 Editing/deleting Connections

Follow the ITS → TTPs link and the link Add TTP … ; a page appears like the page below.

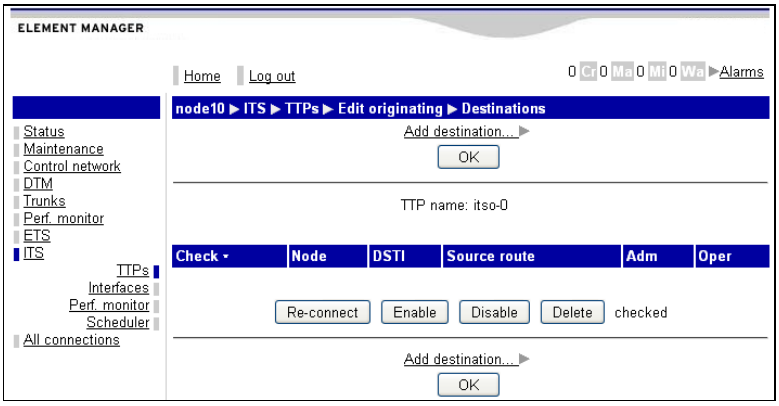


Figure 249. ITS setup TTPs page main

To edit the originating or terminating connection, click on the TTP name in the table.

To be able to delete the connection set the Administrative status to Down and click Apply.

Edit the connection or delete the connection. To delete, click on the Delete button.

15.6 Advanced settings

> ***Note:*** Before changing the max and min settings in a production network please consult Net Insight support services first.

Follow the ITS → TTPs link, open an originating TTP by following the TTP name link, open the Advanced link; a page appears like the page below.

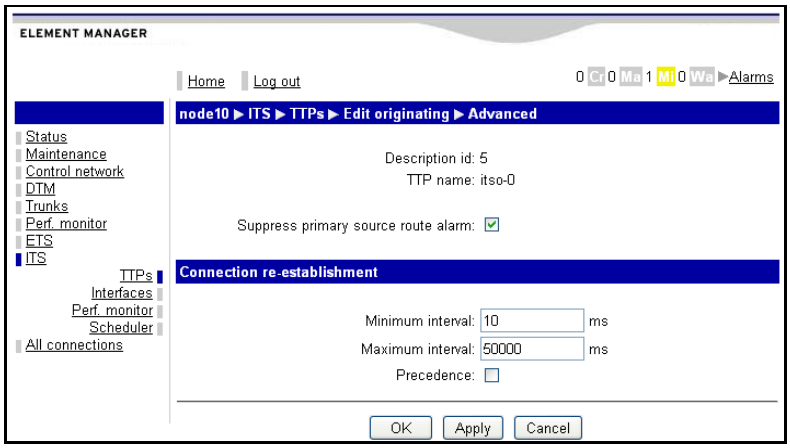


Figure 250. Edit ITS Unicast Advanced

This menu controls the parameters of the exponential back-off algorithm, including the re-connect time out.

Suppress primary source route alarm: This tick box is selected by default. In case it is not selected, an alarm with severity warning is raised when the primary source route is not used.

Minimum interval: 10 ms. The starting value of the back-off algorithm. After a tear down of the connection, the system tries to re-establish the connection immediately. If unsuccessful, after a wait of 10 ms a second attempt is made. A third attempt is made after a longer time according to the algorithm.

Maximum interval: 50000 ms. The end value of the algorithm. The re-establish mechanism will wait not longer than 50000 ms to re-establish a channel.

Precedence: This tick box determines if the connection has precedence or not, i.e. if it is torn down fast (and is re-established fast). Maximum 5 per node.

If required, back up the configuration changes; see chapter *Maintenance*, section *Configuration handling* for details.

15.6.1 Embedded ASI in HD-SDI channels

A feature of release GX4.4 and later is that ASI channels can be embedded in HD-SDI channels. These channels use all the reserved bandwidth of an HD-SDI channel (1.485 Gbps) in the network at all times, but the feature enables mixing of video formats.

To set up an embedded ASI channel in an HD-SDI channel, start with the HD-SDI channel and reserve 1.485 Gbps capacity. Below is an illustration of the ITS -> TTPs -> Edit originating web page.

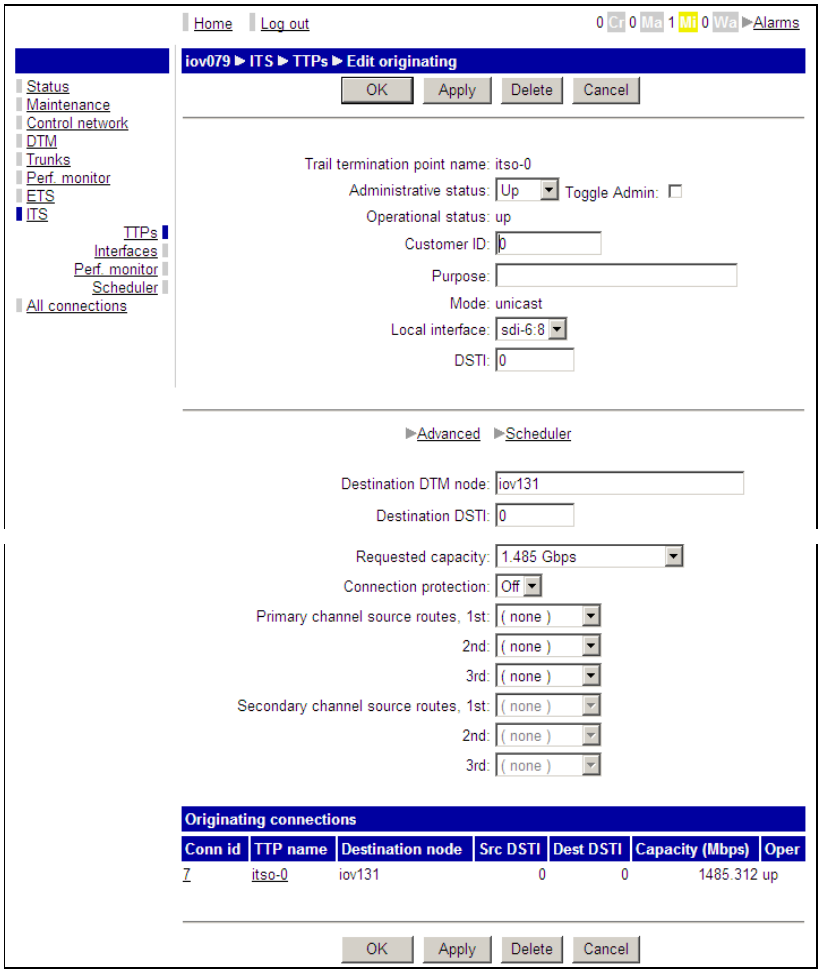


Figure 251. Configuration of the HD-SDI channel that is used for transportation of an ASI-signal. Requested capacity is 1.485 Gbps.

After configuration of the HD-SDI channel, the ASI stream is simply attached to the proper port. A look on the ITS -> interface web page of the interface then shows the bandwidth used by the ASI stream.

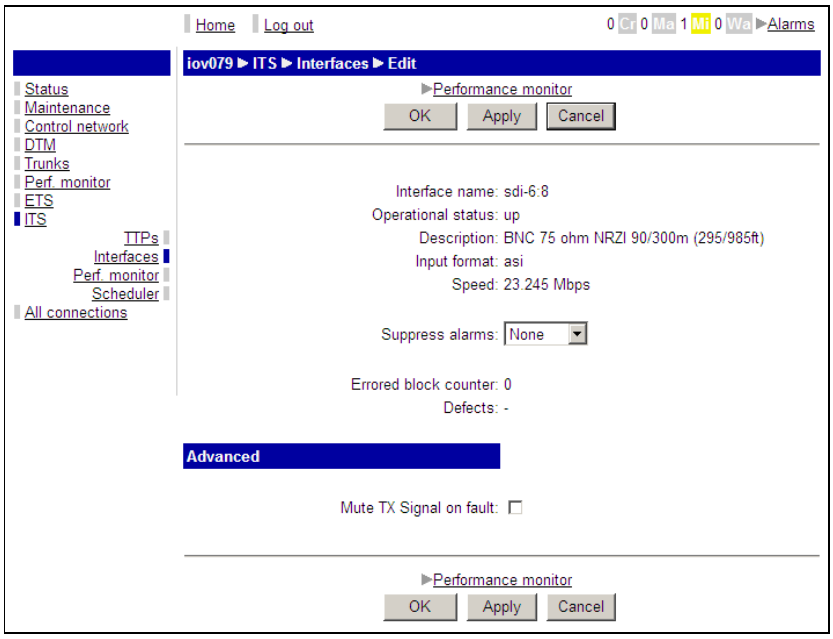


Figure 252. ITS → Interfaces web page of the inserted ASI stream.

16 Channel Persistence

16.1 General

Given a large network, it is inevitable that failures occur from time to time. These failures can affect transmission links as well as switching nodes. When an error occurs somewhere in a DTM network, the default action is to tear down all channels that are affected by the error. The reason for this is that the network can hopefully find another path through the network for the channel and restore the service quickly.

Tearing down the channels is however not always the best course of action. In some situations, channels can continue to forward data even though a node-controller has stopped working or a link has become unidirectional. In other situations, it might be appropriate to let a channel remain established even though a link that it is running over has failed. This will lead to faster recovery when the link is repaired. The Channel Persistence functionality allows the operator to configure the behavior of the network when failures occur. Three main types of failures are handled:

A node-controller that restarts due to a software or hardware error.

A node-controller that fails completely due to a hardware failure.

A link that fails in one or both directions.

16.2 Persistence Configuration

The main configuration parameter for channel persistence is the Link Class for each interface. The Link Class decides how a node shall behave if it detects that the neighboring node stops responding or the link fails. It is configured on a per-interface basis on the DTM->Interfaces->Edit page. The link class must be configured with the same value at both ends of a link.

16.2.1 Link Class Normal

Link Class Normal means that the node will consider the link as Down if it detects an error with the link (Signal Failure) or if the node at the other end of the link fails to respond to the periodic supervision messages. When a link is considered Down, all channels utilizing that link are immediately torn down. . This means that as soon as an error is detected, all channels affected by the error are torn down. Link Class Normal is the default for all interfaces.

An interface configured with link class Normal will never have status NoControl or DownKeep. It will go directly to status Down instead.

16.2.2 Link Class Persistent

> ***Warning:*** This option is for advanced use only. Used inappropriately, the option may cause multiple problems. It is strongly suggested that the user should understand the feature properly before employing it.

With Link Class Persistent, the node will not tear down channels if the neighboring node stops responding. Instead, it will classify the link as NoControl and leave all existing channels in place, but deny any new channels from being established via the interface to the peering node that has stopped responding. Furthermore, if a node has one or more links configured as Persistent, the node will by default enter a NoControl mode if the node-controller restarts. In the NoControl mode, the node will not run the normal DTM protocol stack and instead leave the hardware configured as-is. This means that all existing channels will continue to forward data, but it will not be possible to supervise the links and channels or setup any new channels.

If an interface is configured with Link Class Persistent and the node receives an indication that the link on that interface has failed completely (e.g. a Signal Failure condition), it will tear down all channels over that link.

Persistent links are useful to protect end-nodes that are single points of failure for a service. An interface configured with link-class Persistent will never have status DownKeep, it will go to status Down instead.

16.2.3 Link Class Nailed

> ***Warning:*** This option is for advanced use only. Used inappropriately, the option may cause multiple problems. It is strongly suggested that the user should understand the feature properly before employing it.

With Link Class Nailed, the node will never tear down channels unless the operator sets the administrative status of the interface to down or if the channel is removed via the management interface. This means that the node will leave channels in place even if it knows that the channels cannot forward any data since there is a loss-of-signal situation on the interface.

If the neighboring node stops responding or if the link to or from the neighboring node fails, the node will leave all existing channels in place, but deny any new channels from being established via the interface to the peering node. Furthermore, if a node has one or more links configured as Nailed, the node will by default enter a NoControl mode if the node-controller restarts. In the NoControl mode, the node will not run the normal DTM protocol stack and instead leave the hardware configured as-is. This means that all existing channels will continue to forward data, but it will not be possible to supervise the links and channels or setup any new channels.

Nailed links are useful since they allow links that break in one direction to continue forwarding data in the other direction. They also allow faster

recovery after the link has been restored again, since all channels are already established.

16.2.4 Restart On Error

If a node is configured with at least one interface with a link class of either Persistent or Nailed, the node will by default enter node status NoControl if the local node controller restarts. See the section on “Node Status NoControl” for an explanation of the consequences of this.

The “Restart on error” setting allows the operator to tell the node that it shall always go directly to Up mode and tear down all existing channels if the node controller restarts. This means that the only time the node stops in NoControl is if the node-controlled fails and needs to be replaced.

The Restart on error setting can be found on the Maintenance->System page.

16.2.5 Redundant DLE Servers

If persistent channels are used in a DTM network, it is strongly recommended to configure all nodes with access to two redundant DLE servers. Otherwise, it may happen in an error situation that a node looses contact with the DLE server and becomes impossible to reach via the in-band management network.

It is also important to place the DLE servers in nodes that can be reached via in-band-management without passing through the DLE segment that the DLE server handles. Otherwise, if a DLE server fails for some reason, then it becomes impossible to reconfigure the DLE server since to reach the node with the DLE server, we need to use the DLE segment that just failed. One possible location for the DLE server is in the gateway to the DLE segment in question. The backup DLE server can be placed in a node connected to a different DLE segment.

16.3 Handling an Error Situation

When the Persistent Channel functionality is used (i.e. when at least one interface in the network is configured with link-class Persistent or Nailed), the network will try to tolerate some types of failures without tearing down all affected channels. If such an error occurs in the network, the network will run in a somewhat degraded state. This section describes how to diagnose a network in such a degraded state, the behavior that can be expected from the network in the degraded state and how the network can be repaired.

16.3.1 The DTM->Links Page

The DTM->Links web page displays the status of communication with all neighboring nodes. It shows a list of all local DTM trunks with the administrative status set to Up. For each interface it shows the status of the RX interface followed by the status of the TX interface. Since a DTM network only requires bi-directional connectivity between a pair of nodes and not bi-directional links, it is possible for the status of an RX interface to be different from the status of the corresponding TX-interface. It is even possible (but not recommended) for the RX and TX interfaces to be connected to different nodes.

The status of a TX interface can be

Down – No peering node has been detected.

Up – Full, bi-directional communication with the peering node is possible.

NoControl – The communication with the peering node has been Up, but the peering node has now stopped responding. This indicates that the peering node-controller has either entered the NoControl state or it has failed completely and needs to be replaced.

DownKeep – The communication with the peering node is still Up, but an error has been detected on the trunk to or from the peer.

An RX-interface can have the same statuses as a TX-interface plus

Pending – A node has been detected at the other end of the link, but it has not been possible to establish full communication with the node. This indicates that we only have uni-directional communication (from the peer to this node) with the peering node.

Loopback – The RX-interface is connected to a TX-interface in this node.

In status Pending and Loopback, only the interface-address of the peer is known and displayed. In status Up, NoControl and DownKeep, the node-address and DTM address of the peer is also shown.

In normal operation, all interfaces with attached fibers shall show a status of Up. If you suspect that a node has entered a NoControl state and you cannot reach the node directly, look at the DTM Links page in a neighboring node to determine what the neighbor thinks about the node.

If any link has status NoControl, the node will raise a Major alarm with cause “Response time excessive” and description “Peering node is in state NoControl or is not responding”.

If any link has status DownKeep, the node will raise a Major alarm with cause “Communication subsystem failure” and description “Link is in state DownKeep”.

Note that unless we have several links between two nodes, both the RX and TX direction of the link will get status NoControl or DownKeep at the same time. This means that two alarms will be raised in each node, one for each direction.

16.4 Node Status NoControl

If a node is configured with one or more links with link-class Persistent or Nailed and the node-controller restarts, the node will by default enter a state called NoControl. In this state, the node will not run with the DTM protocol stack disabled and it will thus not communicate with its neighbors. It will however retain all existing channels, both to, from and via the node.

Since the DTM protocol stack is disabled, it is not possible to contact the node via the in-band management network (DLE). If the node is contacted via outband management, it will show a very limited view of the node and it will not display any information about the status of the hardware or services. The only meaningful action in this state is that the node can be restarted. When this is done, the node will activate the DTM protocol stack, tear down any existing channels and try to reestablish them from the beginning.

The idea behind the NoControl state is that if an error occurs, the node tries very hard not to disrupt any existing traffic. It is then up to the operator to

choose when he wants to tear down the channels and restore the node to full working condition.

16.5 Restarting a node in NoControl

A node in NoControl state can be brought into full working state ("Up") in three different ways:

Via outband management

Via serial console

From a neighboring node

16.5.1 Restarting via Outband Management

To restart the node via outband management, you can either use the "Resume full operation" button on the Maintenance->System web page or the CLI-command "node-restart local".

16.5.2 Restarting via Serial Console

To restart the node via serial console, use the CLI-command "node-restart local".

16.5.3 Restarting from a Neighboring Node

To restart a neighboring node, look at the DTM → Links page. It will show the status of all its neighbors. If any neighbor appears to be in status NoControl, click on the interface name for the row that displays NoControl. It will take you to the DTM Interface page for that interface. From that page, you can send a restart command to the node connected to the TX-part of the interface. This is done with the Restart Neighbor button. Note that a node will only respond to the Restart Neighbor command if the node has status NoControl. If the node is already up and running, the Restart Neighbor button will have no effect.

It is also possible to send the same restart command to a neighbor via the CLI using the command "node-restart dtm3: 1".

16.6 Link Errors

If a link configured as Nailed reports an error such as Signal Failure, all channels will remain established over that link. To force the system to tear down the channels, set the administrative status of the interface to Down or reconfigure the link-class as Normal. This must be done on both nodes connected to the link in question.

16.7 Channels with broken control-paths

If a link configured as Nailed fails, or if a node-controller enters the NoControl state, all channels running over that link or to, from, and via that node have broken control paths. This means that the network will preserve the channels, but it will have limited control over them. Depending on the

type of error that has occurred, channels with broken control-paths may or may not continue to forward data.

The best way to get rid of the broken control-path is to resolve the underlying problem, i.e. to restart or replace the node-controller that is in NoControl state or repair the broken link. Alternatively, the operator can also choose to disable the broken link by setting the administrative status of the link to Down in both nodes connected to the link. All these measures will however affect traffic if only the control-path is broken but the data-path is actually working.

Another alternative is to selectively tear down and reestablish channels. This gives exact control over which channels will be affected, but is more complex to perform. This is because it is generally not possible to send control messages all the way from the source to the destination for a channel. Control messages will only reach the node before the error and there they will be buffered, waiting for the error to be resolved. Therefore, special measures are sometimes needed to resolve the situation.

The rest of this chapter describes how to tear down or reestablish different types of channels when the channels have broken control-paths.

16.7.1 Tearing down a unicast channel

To tear down a unicast channel with a broken control path, it is necessary to tear it down from both sending and receiving side. This can be done by setting the administrative status for the service to Down at both ends. If this is only done at the sending side, the receiving side will show that it is still receiving the channel, but the sending side will show that the channel has been torn down.

16.7.2 Reestablishing a unicast channel

By reestablishing a unicast channel, we can force the network to find an alternate route through the network that avoids the error. To force a channel to be reestablished, open the webpage for the TTP at the sending side and click the connection id (Conn id) that you want to reestablish under “Originating connections”. On the displayed page, click the button labeled “Re-connect channel”.

In some (rare) circumstances, the channel must be torn down at the receiving side before it can be reestablished. If the channel is not reestablished properly, go to the TTP at the receiving side and click on the connection id under “Terminating connections”. Then use the button labeled “Delete” to tear down the channel from the terminating side as well.

16.7.3 Re-establishing a multicast channel

If a multicast channel is affected by a broken control-path, there are two different ways to reestablish the channel to the affected destinations. The easiest way is to reestablish the entire multicast tree by toggling the administrative status of the originating TTP. This will tear down the entire multicast tree and replace it with an entirely new channel. This of course affects all destinations and not just the destinations that are affected by the broken control-path. Note that since the control-path is broken, it may take slightly more than one minute to tear down the old multicast tree.

If it isn't possible to reestablish the entire multicast tree, you can also choose to tear down and reestablish only the affected destinations. To do this, it is necessary to perform two different tear downs:

First, we want to tear down the channel downstream from the break in the control path. To do this, we first need to find out the channel identifier for the channel. This id consists of the source DTM address for the channel and a numerical identifier. To find the channel identifier, go to the webpage for the originating TTP and click on the number in the column "Conn Id" for the failed originating multicast channel. This will display the "Connection Details" page for the connection. The Channel id can be found on that page. Write down the Channel id or copy it by selecting it and pressing Ctrl-C.

Now, we need to find the node directly after the break in the control-path for the channel. If the error is a link in DownKeep state, then it is the node connected directly downstream from that link. If the error is a node in NoControl state, then it is the node connected directly downstream from that node.

Log in to the node in question via the CLI. Use the "dcp list" command to verify that you have found a node that the channel passes through. This can be done by issuing the command "dcp list <channel id>" (e.g. "dcp list 02.00.00.00.00.00.00.41 65538"). If the node answers with a lot of output, then the channel exists. If the node answers "No such channel", then the channel does not exist in this node.

If the channel exists, you can tear it down using the command "dcp remove <channel id>" (e.g. "dcp list 02.00.00.00.00.00.00.41 65538"). This will tear down all multicast destinations in this node and any downstream nodes.

Second, we need to remove the destinations from the source to the point where the control path is broken. If the control path wasn't broken, you would have torn down the channel from the source to all downstream nodes in the first step. However, since the control path is broken, the source application still thinks that the destinations are properly established. To fix this, locate the originating TTP for the channel. Click on the "Destinations" link to see all destinations for this TTP. Put a checkbox before the destinations that you tore down in the previous step and click the button "Re-connect checked". Note that since the control-path is broken, it will take approximately one minute before the destinations are torn down and can be reestablished along an alternate path.

16.7.4 DLE

DLE will automatically tear down and reestablish channels to maintain functionality as long as there is an available path for control signaling. It is however very important to have two redundant DLE servers for each DLE segment, since it may happen that a DLE server is unable to reestablish a channel to a DLE client that has been affected by an error. This will be resolved automatically when the DLE client decides to move to the other DLE server since the first one is non-functional.

However, there are some situations when channels between DLE clients cannot be reestablished automatically. The symptoms of this is that there does not seem to be anything wrong with the node judging from the DTM Links page on its neighbors, but it is impossible to reach the node via DLE from some node(s). The easiest way to fix this situation is to force the DLE server that the failing node is attached to re-establish the channel to all the DLE clients. This is done from the page for the In-band server (Control network->In-band servers, click on the relevant server id, e.g. dles0). On that page, click on the connection id of the only entry under the heading

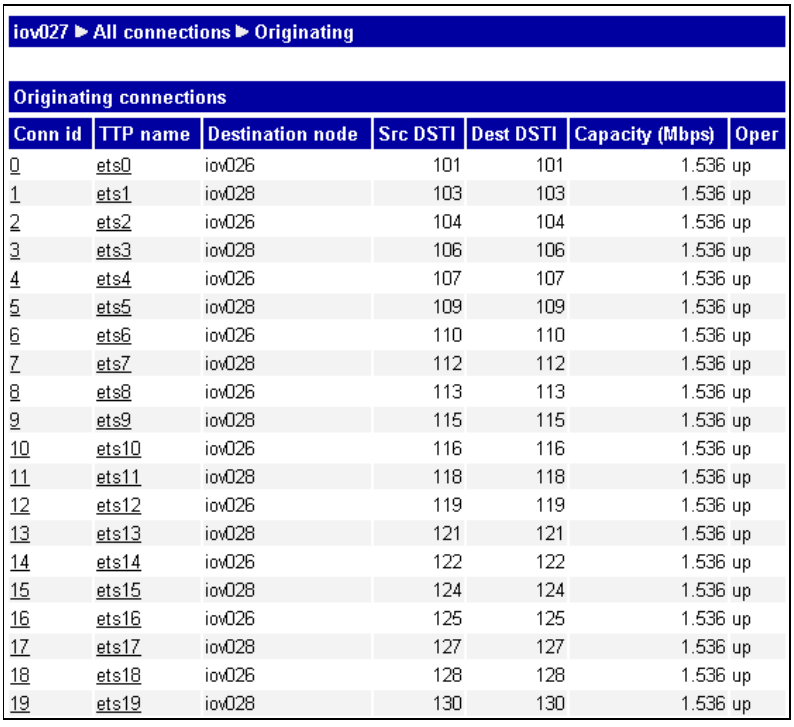
“Originating client connections” and then click Re-connect channel on the resulting page. This forces the DLE server to re-establish the channel to all DLE clients.

17 Connection and channel lists

17.1 Overview

In the web interface, information about originating and terminating connections is available, as well as information about originating, terminating and pass-through channels.

These listings are informational only.



iov027 ▶ All connections ▶ Originating

Originating connections

Conn id	TTP name	Destination node	Src DSTI	Dest DSTI	Capacity (Mbps)	Oper
0	ets0	iov026	101	101	1.536	up
1	ets1	iov028	103	103	1.536	up
2	ets2	iov026	104	104	1.536	up
3	ets3	iov028	106	106	1.536	up
4	ets4	iov026	107	107	1.536	up
5	ets5	iov028	109	109	1.536	up
6	ets6	iov026	110	110	1.536	up
7	ets7	iov028	112	112	1.536	up
8	ets8	iov026	113	113	1.536	up
9	ets9	iov028	115	115	1.536	up
10	ets10	iov026	116	116	1.536	up
11	ets11	iov028	118	118	1.536	up
12	ets12	iov026	119	119	1.536	up
13	ets13	iov028	121	121	1.536	up
14	ets14	iov026	122	122	1.536	up
15	ets15	iov028	124	124	1.536	up
16	ets16	iov026	125	125	1.536	up
17	ets17	iov028	127	127	1.536	up
18	ets18	iov026	128	128	1.536	up
19	ets19	iov028	130	130	1.536	up

Figure 253. List of originating connections

iov027 ▶ All connections ▶ Terminating

Terminating connections

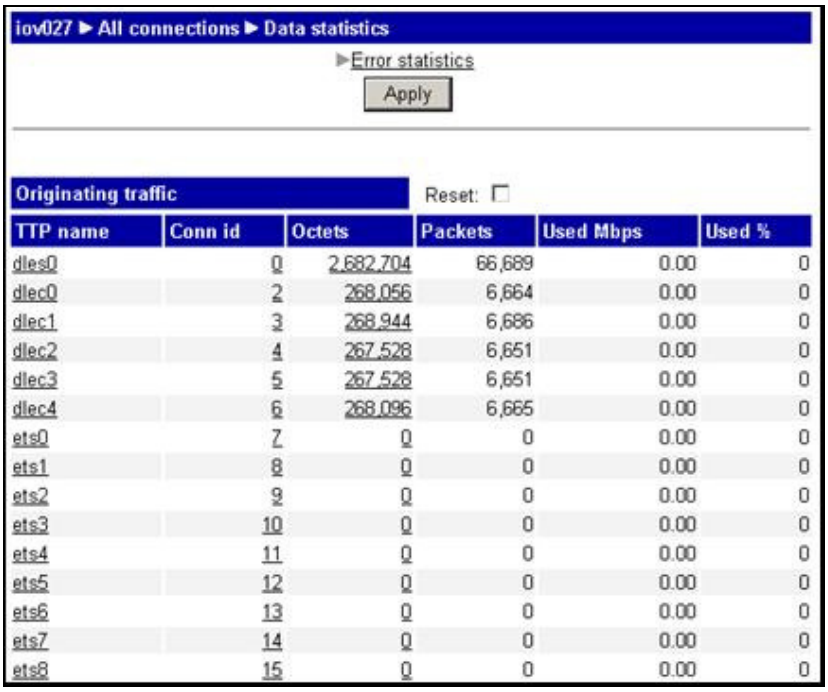
Conn id	TTP name	Source node	Src DSTI	Dest DSTI	Capacity (Mbps)	Oper
0	itsi-0	iov095	701	701	35.840	up
1	itsi-1	iov026	701	702	35.840	up
2	itsi-2	iov029	901	901	2.560	up
3	itsi-3	iov029	902	902	2.560	up
4	itsi-4	iov029	903	903	2.560	up
5	itsi-5	iov029	904	904	2.560	up
6	itsi-6	iov029	905	905	2.560	up
7	itsi-7	iov029	906	906	2.560	up
8	itsi-8	iov029	907	907	2.560	up
9	itsi-9	iov029	908	908	2.560	up
10	dles0	iov027	3	32769	0.512	up
11	dlec1	iov027	32769	3	0.512	up
12	dles0	iov054	3	32769	0.512	up
13	dles0	iov025	3	32769	0.512	up
14	dles0	iov029	3	32769	0.512	up
15	ets66	iov025	207	207	1.536	up
16	ets70	iov028	213	213	1.536	up
17	dles0	iov095	3	32769	0.512	up
18	ets41	iov028	169	169	1.536	up
19	ets19	iov028	130	130	1.536	up
20	ets37	iov028	160	160	1.536	up

Figure 254. List of terminating connections

iov027 ▶ All connections ▶ Channels

Service	Slots	Originating node	Terminating node	In	Out
DLE	1	iov098:3	iov027:32769	dtm7:1	-
ETS	3	iov098:199	(mult)	dtm7:1	(mult)
ETS	3	iov098:200	(mult)	dtm7:1	(mult)
ETS	3	iov098:201	(mult)	dtm7:1	(mult)
ETS	3	iov098:202	(mult)	dtm7:1	(mult)
ETS	3	iov098:205	(mult)	dtm7:1	(mult)
ETS	3	iov098:206	(mult)	dtm7:1	(mult)
ETS	3	iov098:207	(mult)	dtm7:1	(mult)
ETS	3	iov098:208	(mult)	dtm7:1	(mult)
ETS	3	iov098:211	(mult)	dtm7:1	(mult)
ETS	3	iov098:212	(mult)	dtm7:1	(mult)
ETS	3	iov098:213	(mult)	dtm7:1	(mult)
ETS	3	iov098:214	(mult)	dtm7:1	(mult)
DLE	1	iov095:32769	(mult)	dtm7:1	(mult)
ITS	70	iov095:701	(mult)	dtm7:1	(mult)
DLE	1	iov095:3	iov027:32769	dtm7:1	-
ETS	3	iov095:199	(mult)	dtm7:1	(mult)
ETS	3	iov095:200	(mult)	dtm7:1	(mult)
ETS	3	iov095:201	(mult)	dtm7:1	(mult)
ETS	3	iov095:202	(mult)	dtm7:1	(mult)
ETS	3	iov095:205	(mult)	dtm7:1	(mult)
ETS	3	iov095:206	(mult)	dtm7:1	(mult)

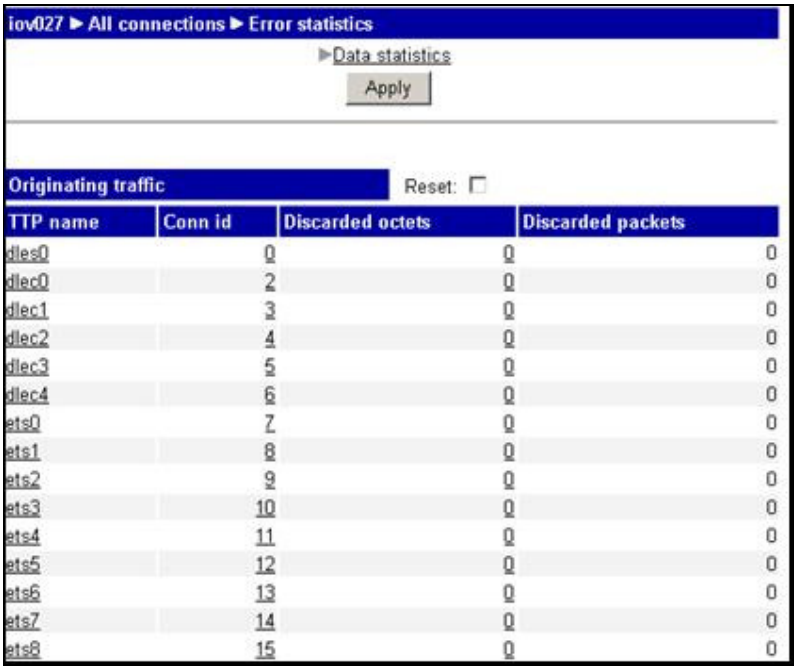
Figure 255. List of channels to, from and via the node



TTP name	Conn id	Octets	Packets	Used Mbps	Used %
dles0	0	2,682,704	66,689	0.00	0
dlec0	2	268,056	6,664	0.00	0
dlec1	3	268,944	6,686	0.00	0
dlec2	4	267,528	6,651	0.00	0
dlec3	5	267,528	6,651	0.00	0
dlec4	6	268,096	6,665	0.00	0
ets0	7	0	0	0.00	0
ets1	8	0	0	0.00	0
ets2	9	0	0	0.00	0
ets3	10	0	0	0.00	0
ets4	11	0	0	0.00	0
ets5	12	0	0	0.00	0
ets6	13	0	0	0.00	0
ets7	14	0	0	0.00	0
ets8	15	0	0	0.00	0

Figure 256. List of data statistics

Selecting All connections, Statistics provides data statistics of all connections since the last reset. Furthermore, on the data statistics page information about errors (error statistics) is also retrievable



TTP name	Conn id	Discarded octets	Discarded packets
dles0	0	0	0
dlec0	2	0	0
dlec1	3	0	0
dlec2	4	0	0
dlec3	5	0	0
dlec4	6	0	0
ets0	7	0	0
ets1	8	0	0
ets2	9	0	0
ets3	10	0	0
ets4	11	0	0
ets5	12	0	0
ets6	13	0	0
ets7	14	0	0
ets8	15	0	0

Figure 257. List of error statistics

18 Source Routing

18.1 Overview

When establishing a connection between two (or more for multicast) endpoints at the rim of the network, it is usually not important to know exactly which path the connection takes through the network.

The default routing method is therefore to let the network itself decide the best (shortest and most efficient on transmission resources) path via hop-by-hop routing.

An obvious exception to this is when 1+1 protection is used to improve the reliability of a service. It is then vital to ensure that the two channels that make up the connection take different paths from the source to the destination. This means that if a link or a node in the network should fail for some reason, then only one of the channels shall be affected.

There are other situations when it may be of interest to specify explicit paths, e.g. in order to avoid a certain link that is scheduled for maintenance.

The tool for accomplishing this is called source-routing. Using source-routing, it is possible to specify the exact path that a channel takes through the network. The path is specified by pinpointing the nodes that the channel passes on its way from the source to the destination and in some cases also the outgoing interface on the originating node. A source-route is specified in the source node for a connection.

It is possible to configure three different source-routes for a single channel. If more than one source-route is configured for a single channel, it means that the channel is allowed to follow any of the specified source-routes through the network. The specified source-routes will be tried in order until one of them succeeds.

If no source-route is configured, then the channel will be established along the shortest path from source to destination.

It is possible to let several channels use the same source-route. This is often very useful, especially in conjunction with loose source-routing.

18.1.1 Loose and strict source-routes

It is possible to select whether a source-route shall be strict or loose:

For a strict source route, every node along the way to the destination must be specified. Optionally, the interfaces can also be specified.

For a loose source route, only nodes that are required to be traversed are specified; the path between the specified nodes is found via hop-by-hop routing (i.e. by DRP).

18.1.2 Configuration

Source-routing is configured in two steps. The first step is to create a source-route in the source node and give it a descriptive name. The second step is to configure a TTP to use the specified source-route.

These steps are described in detail in the following example.

18.2 Example

Consider the network below. We want to establish a 1+1-protected tunnel from node node1 to node node11. The first channel, route A, passes through nodes node2, node3, node20 and node14. The second channel passes through nodes node4, node10, node13 and node12.

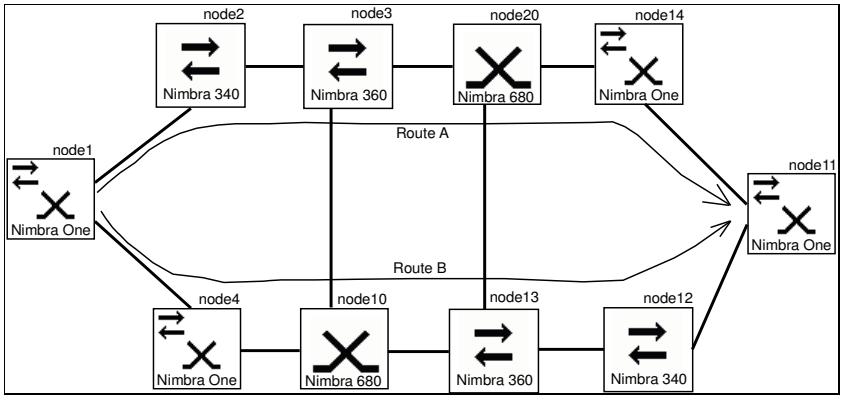


Figure 258. Example network to illustrate source routing. The two source routes are Route A and Route B.

18.2.1 Strict source-route

We can force the channels to take the desired paths through the network by using two different source-routes, routes A and B. Both of these source-routes are "strict", since we specify all nodes on the path from the source to the destination.

Navigate to the menu **All connection|Source routes** and click **Create**. This brings up the web-page shown in the picture below.

Each source-route is specified as a list of all the nodes that the source-route passes through. Each node is written on a separate line and it can be represented either by its node name (if it has been configured in the list of hosts under **DTM|Host names**) or by its DTM address directly.

Click the **OK** or **Apply** button to set the route, and create the second Source-route by selecting the *Create* button.

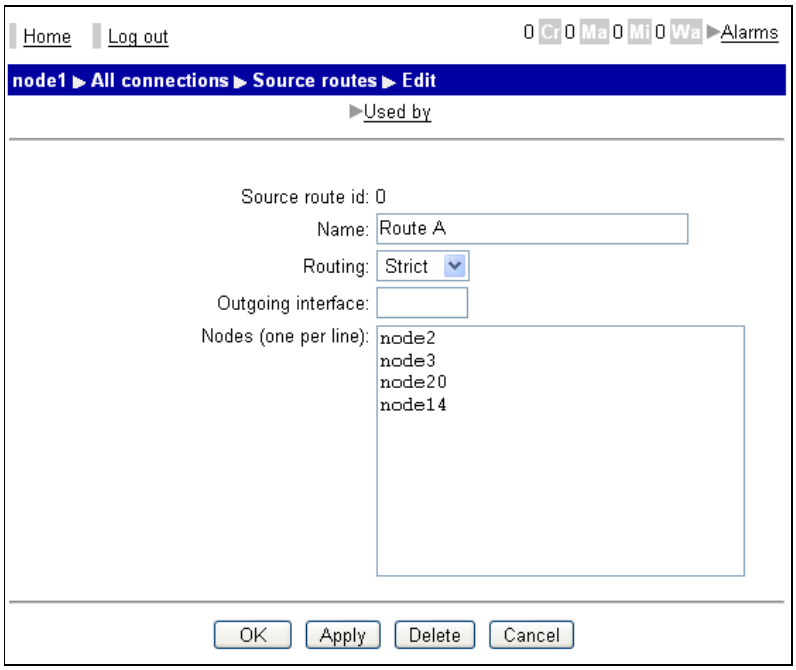


Figure 259. Specification of the primary source-route

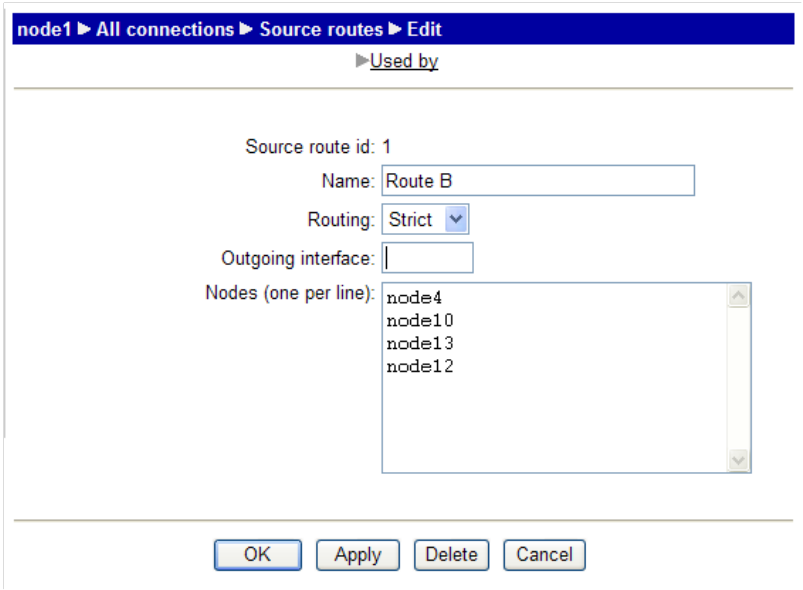


Figure 260. Specification of the second source-route

From the **Connection|Source routes** page it is also possible to view, edit and delete a specific source-route by clicking on the source-route id in the list of all configured source-routes and edit or delete.

18.2.2 Loose source-route

The operator may be tempted to use loose-source routing instead of strict source-routing, since loose source-routing is easier to configure. The source-route “first-to-node11” could then be specified as containing only node20 and “second-to-node11” containing only node10. This means that the first

channel is allowed to take any available path to the destination as long as it passes through node20 on the way.

18.2.3 Specifying interfaces

Sometimes there are several trunks available between two nodes. It is then possible to specify which of these interfaces are to be used in a source-route. This can be important when you have fibers running in several different fiber ducts and you want to make sure that you use two fibers that are running in different ducts. It is done by specifying the outgoing interface that shall be used on a node. If no interface is specified, then the node is free to choose any of the available interfaces.

Each trunk interface has an interface identifier associated with it. The interface identifier for a node can be found by looking at the list of DTM interfaces in the web manager (accessible by clicking DTM and then Interfaces). Each interface has a name (for example dtm3:1) and the interface identifier is the same as the name but with the "DTM" part omitted (i.e. 3:1).

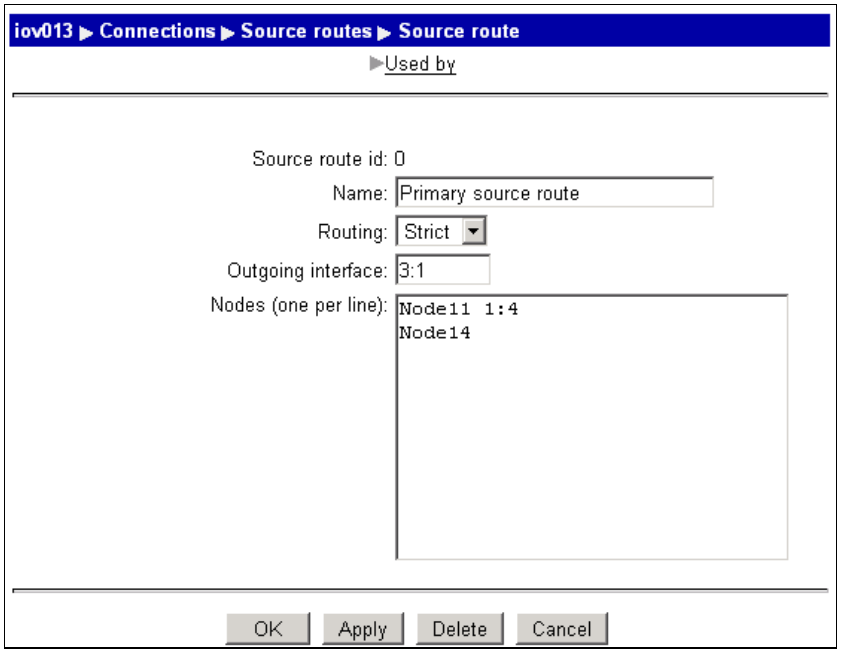


Figure 261. A source-route with explicit interface specifications

To specify which outgoing interface should be used in an intermediate node, enter the interface identifier after the name/DTM address of the intermediate node.

To specify which outgoing interface should be used from the source node, enter the interface identifier in the field labeled "Outgoing interface".

18.2.4 Using a source-route in a TTP

After creating a source-route, you must also tell the TTP to use the source-route when it establishes the channel. This is done in the configuration for the TTP.

Source-routing can be used for all TTPs, regardless of if they are 1+1-protected or not.

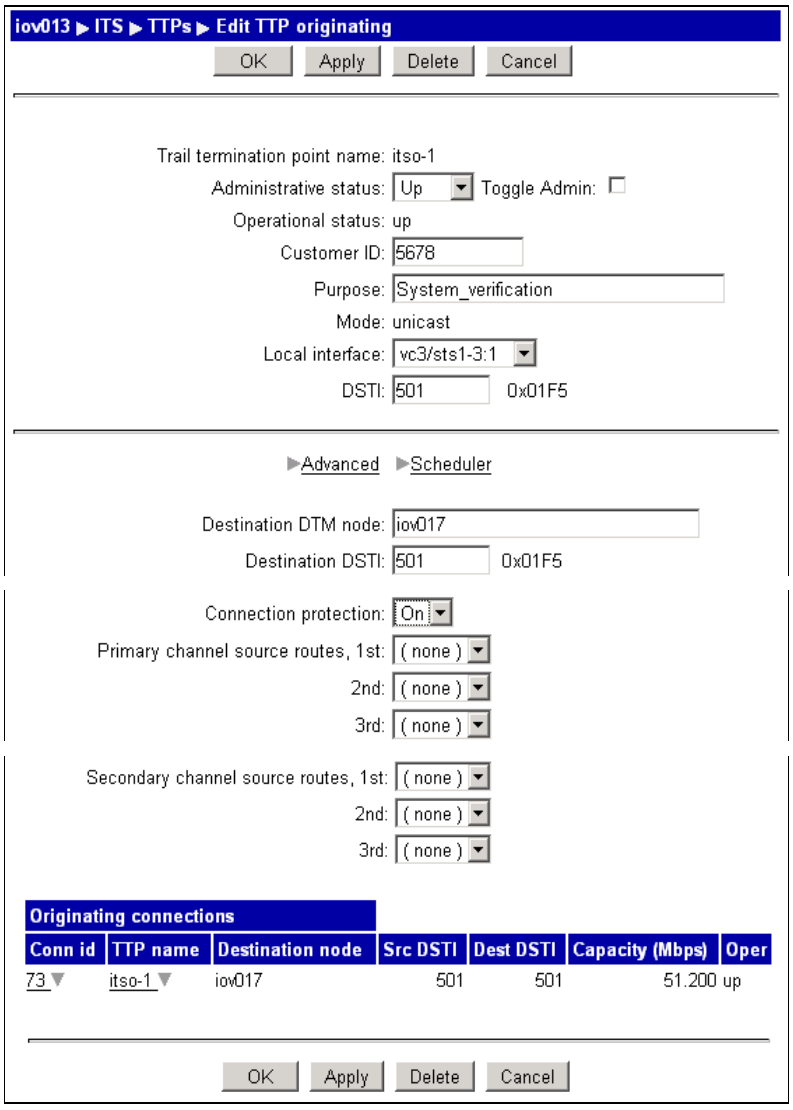


Figure 262. Source-routes for an 1+1-protected TTP

Note:	It is also possible to use source-routing for multicast connections. The source-routing information is then specified for each destination separately in the same dialog where you add or change the destination for the TTP.

18.2.5 Updating a source-route

Note: 	It is possible to update a source-route that is currently configured in a TTP or even actually used by an established channel. If you update a source-route that is used by an established channel, then the channel will be torn down and then re-established along the new source-route.

It is also possible to change which source-route a TTP shall use. If the change means that any of the channels currently established for the TTP are no longer valid according to the new configuration (i.e. they were established via a source-route that is no longer used for this TTP or if the channel was established in hop-by-hop routing mode and you add a source-route configuration), then these channels will be torn down and re-established.

18.2.6 Deleting a source-route

Before you can delete a source-route entry, you must make sure that the source-route is not used by any TTP. This is easy to check by clicking on the link “Used by” in the page describing the path for the source-route. If you try to delete a source-route that is currently in use, the node will return an error message and refuse to delete it.

18.2.7 Practical example one – Original 1+1 protection

One 1+1 type of protection existing in the GX software is defined with two unicast connections, both source routed (different source routes) through the network. As the modules on both sides of the connection are the same, no protection of end-node failure is given in this example.

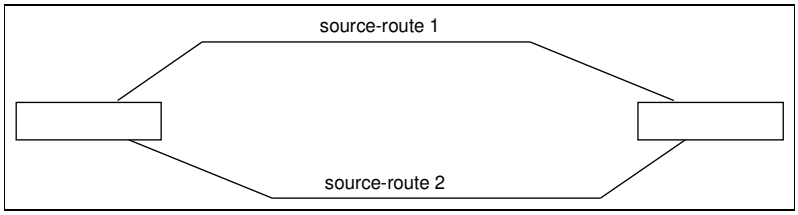


Figure 263. Setup of strict source-routes in a network. The ITS service is set up as a unicast 1+1 protected channel.

18.2.8 Configuration of original 1+1 unicast protection

To set up a 1+1 source routed connection, configure a regular ITS channel.

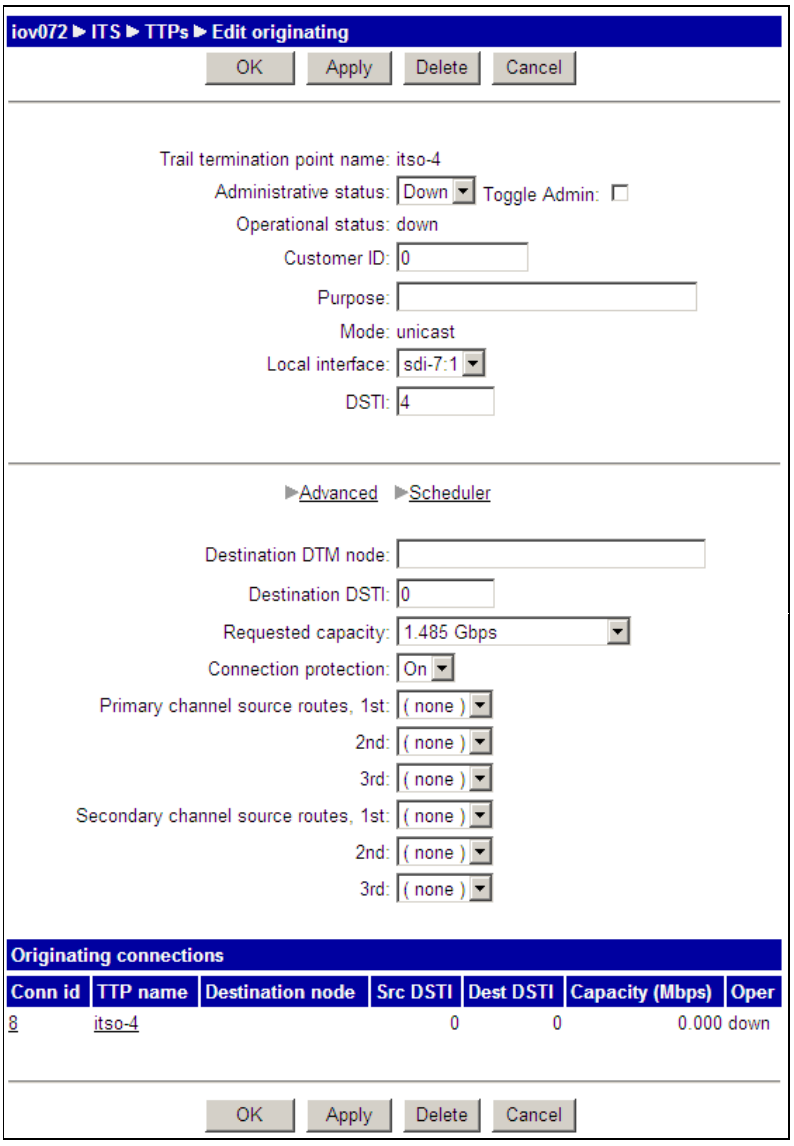


Figure 264. Setup of 1+1 connection protection. Make sure to set 'connection protection' to 'On' and select suitable source routes. The ITS services are set up as a unicast 1+1 protected channel. The used route is indicated to the right of the drop down menu with the text 'currently used' within parenthesis.

18.2.9 Practical example two – 1+1 open ended protection for Multicast ITS services

A new feature of GX4.4 is that it allows for an additional form of 1+1 protection, namely 1+1 protection for multicast ITS services. This new form of 1+1 does not change the web interface in any way, but what is new is that the terminating TTPs can be associated to two separate multicast ITS streams.

A common ingress signal is split at the head end and the two identical streams are connected to separate modules. At the receiving side (both

nodes), only one of the streams are used. In this way we get head end protection, network protection and egress node protection.

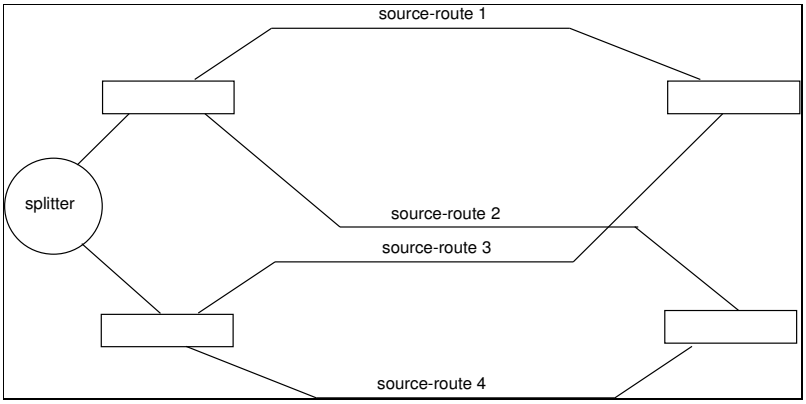


Figure 265. Setup of 1+1 multicast protection. The split signal is transported through two separate multicast channels, which both in turn use different source routes. Make sure to set 'connection protection' to 'On' and select suitable source routes.

In the practical configuration example, we let two multicast channels start from node10 and node20. The channel set up from node10 is terminated in node10 and node 20. The channel set up from node20 is terminated in node10 and node20. In the illustration below, the set-up is explained.

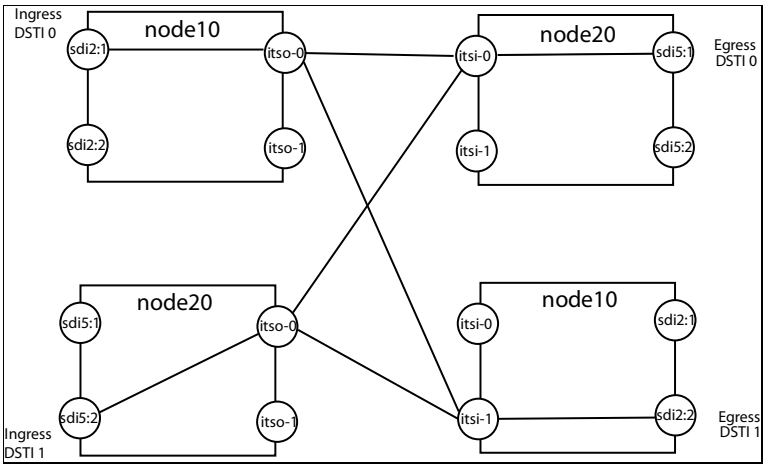


Figure 266. Practical configuration example of a 1+1 protected multicast channel.

Note that the terminating TTP accepts two separate video streams.

Start with defining a multicast ITS service from node10.

Follow the ITS → TTPs link and click on Add TTP… . Define an originating, multicast connection from interface sdi2:1. Set the administrative status to up and then follow the link Destinations to define the two destinations in node10 (DSTI1) and node20 (DSTI0).

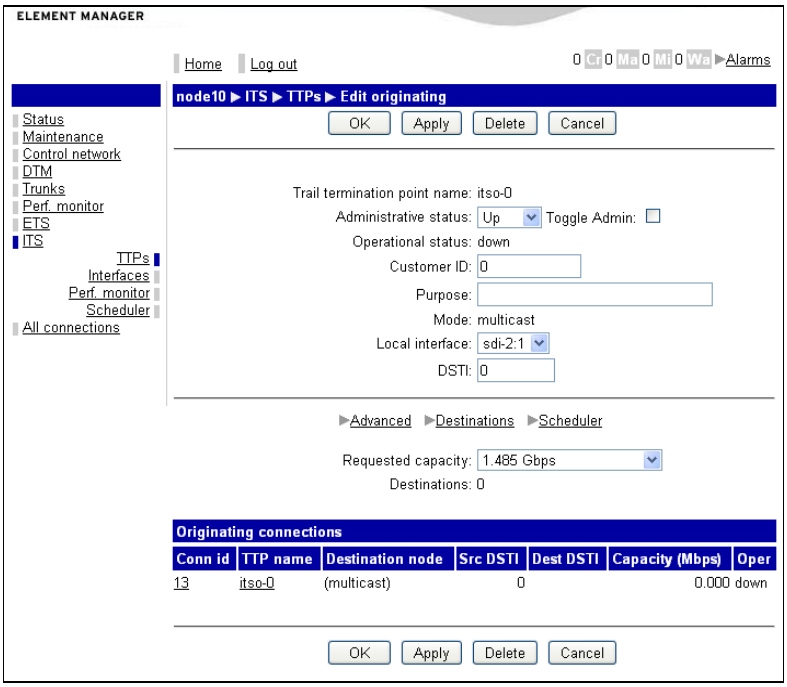


Figure 267. The originating multicast configuration in node10.

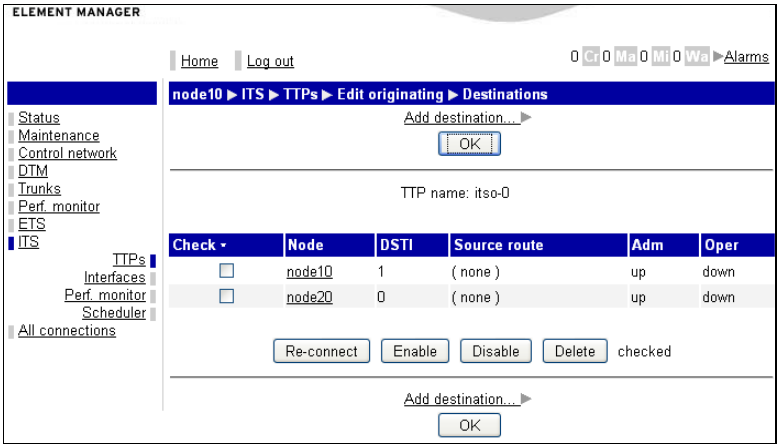


Figure 268. Destinations for the first multicast.

After the originating TTP is defined, turn to the terminating side and create terminating TTPs for both destinations. Note that these TTPs accept two separate, incoming ITS streams each. This feature can be disabled on the ITS → TTPs → Edit terminating web page.

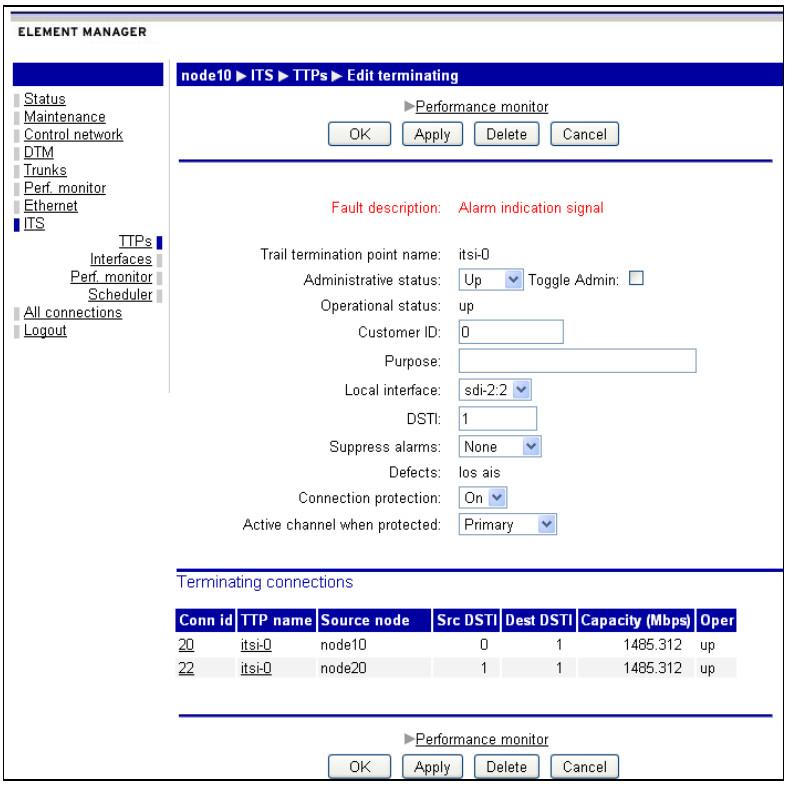


Figure 269. Definition of the terminating TTPs. Note the disabling feature for the second connection (by setting Connection Protection to 'Off'). In this picture, both terminating connections are defined.

After the first multicast is defined, it is time to turn to the second multicast. Define the originating TTP in the same manner, but for node20/DSTI 1. The destinations are in this case the very same destinations as for the first multicast, namely node20/DSTI 0 and node10/DSTI 1.

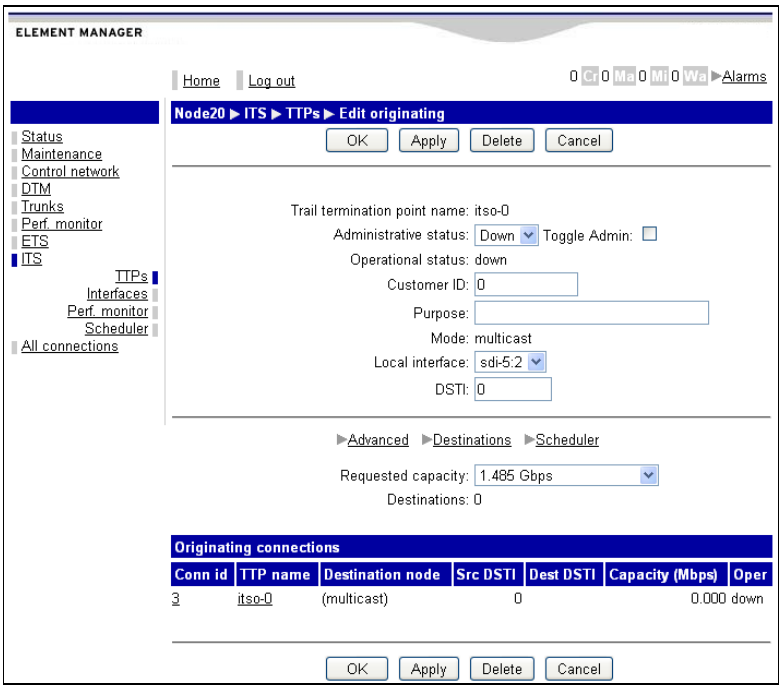


Figure 270. Second multicast defined in node20. The destinations are the same as for the first multicast.

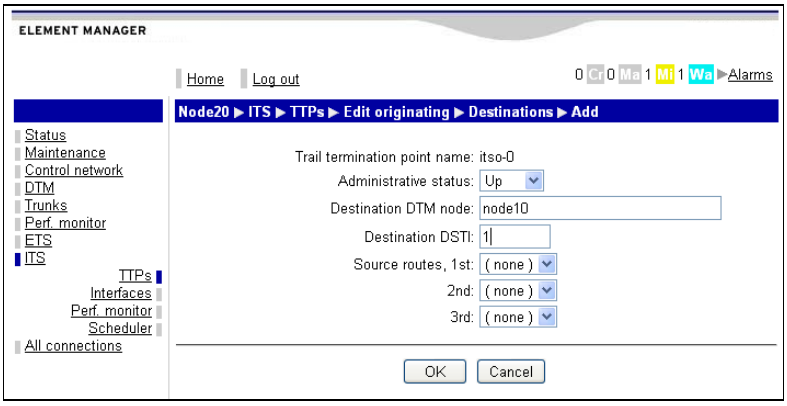


Figure 271. Definition of the multicast destination in node10.

19 Loopback

19.1 General

Loopback is a function that makes it possible to loop the incoming signal on an interface (Rx port) to the outgoing port on the same interface (Tx port) or to loop the signal destined for the outgoing Tx port on an interface back to the Rx port on the same interface. The first type of loopback is called line loopback and the second type DTM loopback in this document, as well as in the web interface of the Nimbra nodes.

19.1.1 Line loopback

Line loopback is illustrated below. It is currently implemented explicitly on the ASI Transport Access Module for Nimbra One and 300, as well as on the fixed interfaces of Nimbra 340.

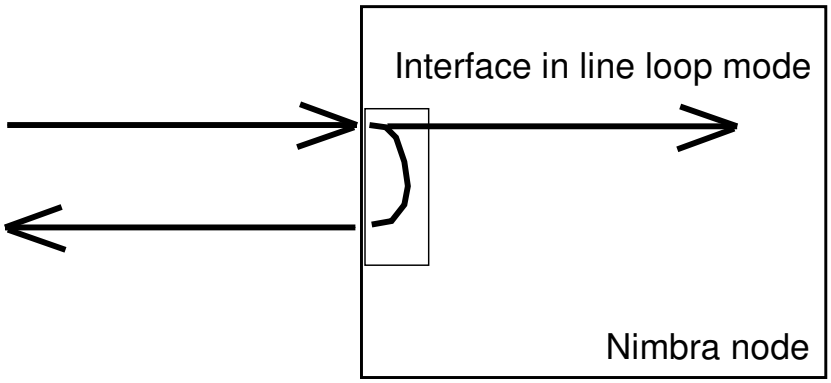


Figure 272. Schematic illustration of line loopback.

To explicitly configure the interface in line loopback mode, proceed as follows:

Follow the link ITS -> Interfaces -> Name of the interface to be configured, like asi-3:1

The following web page should be opened:

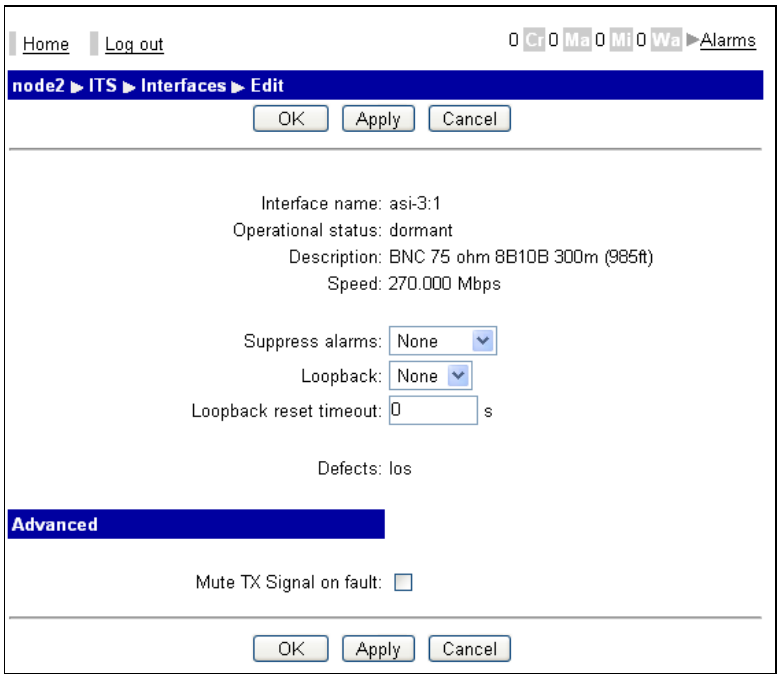


Figure 273. Configuration of loopback.

To configure the interface in line loopback mode, set the value of the parameter Loopback to Line from the drop-down menu. The signal reaching the Rx port on the interface should now be directly returned to the Tx port, in addition to being sent along the regular path of an incoming signal.

It is possible to reset the loopback condition with the loopback reset timeout. This parameter, a time given in seconds, determines how long the loopback condition is active. The value zero has a special meaning, namely that the loopback condition remains in place until removed.

19.1.2 DTM Loopback

DTM loopback is a way to send a signal, destined for a Tx interface, back to the path of the Rx signal on the very same interface. The signal is split at the interface and sent out on the Tx interface as well. To configure the ASI ports described above in this manner, set the parameter Loopback to DTM.

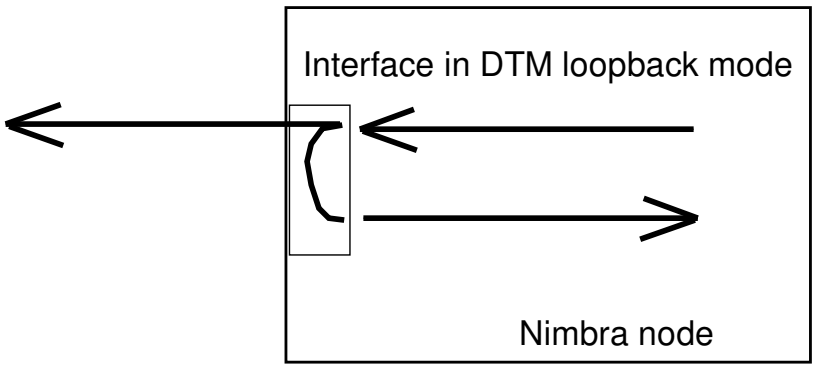


Figure 274. DTM loopback mode. The signal is copied to the Rx port on the same interface before being sent out on the Tx port.

19.2 Behaviorally equivalent configurations

Strict implementation of DTM and line loopback, with a loop very close to the actual interface, is only found in the ASI Transport Module and the ASI ports of Nimbra 300. However, an equivalent system behavior can be configured in some other ways.

19.2.1 Loopback from the line side in 8 x ASI Transport Module for Nimbra One/300

In 8 x ASI Transport Module, the monitoring port (the ninth port) can be used for loopback. In this case, the monitor port copies the incoming signal on a port and sends the copy back towards the line.

The loopback is set up by creating an ITS from one node to another. In our case, it is made between node1 and node11.

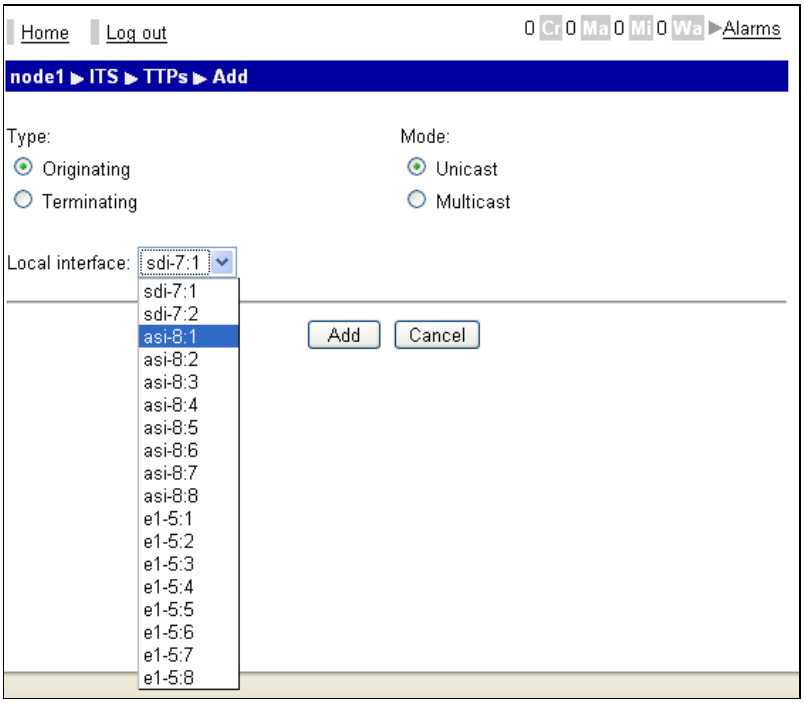


Figure 275. Configuration of an ITS unicast.

The monitor port on the module in node 1 is set to listen to this local interface (asi-8:1), which is used as an Rx port. To configure the monitor port, select Interfaces from the ITS link after the ITS unicast service is set up between nodes1 and node11. The ITS unicast is configured as a regular ITS unicast. If in doubt, see the specific description of ITS configuration.

Select interface asi-8:1 to be monitored and connect the return cable to the external ASI player. The ASI signal now enters the module on interface asi-8:1 and leaves the module from the monitor interface. The loopback is complete.

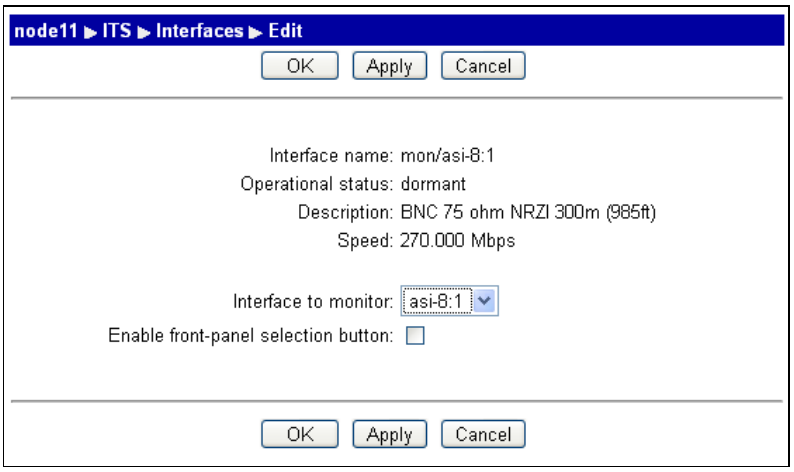


Figure 276. Configuration of the monitor interface.

The front panel selection button makes it possible to disable the output directly from the hardware.

Configuration of DTM side loopback is made in an analogous fashion as for the 8 x Video Access Module for Nimbra 600 described below.

19.2.2 Loopback from the line side in 8 x Video Access Module for Nimbra 600

In an 8 x Video Access Module or an 8 x 3Gbps Video Access Module, one of the eight ports can be used as a monitor port and configured in the same manner as the 8 x ASI Transport Module for Nimbra One/300 described in the previous section. The physical port will be busy in this configuration and only seven ports of the modules can be actively used.

First, an ITS unicast is defined. Another port is selected as monitor port from the ITS -> Interface link. The original port is selected as 'Interface to monitor'.

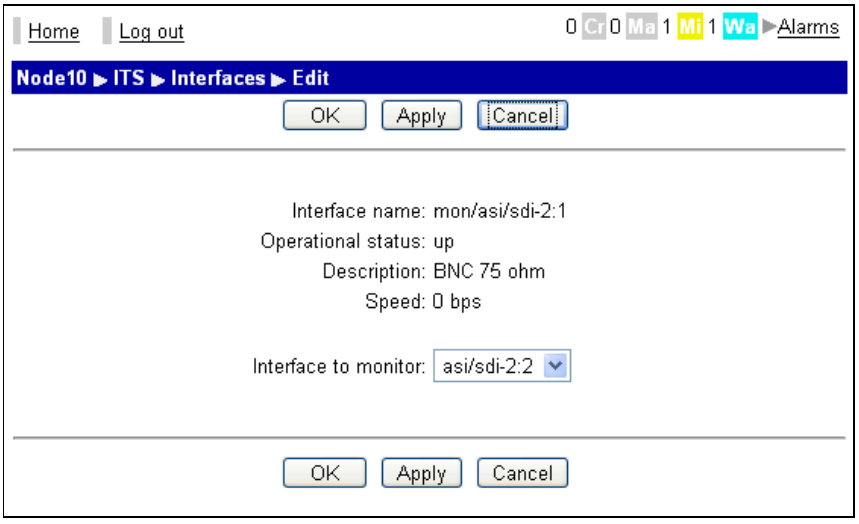


Figure 277. Configuration of line type loopback on an 8 x Video Access Module on Nimbra 680/688.

Click on the ‘OK’ or ‘Apply’ button and the configuration is made.

19.2.3 Loopback from the DTM side in 8 x Video Access Module for Nimbra 600

In order to configure this module for a DTM type of loopback, the port/interface already configured as an end point of an ITS unicast can be used as an originating port/interface of another ITS unicast. In this manner, the outgoing signal is both sent out from the port/interface towards the line and returned towards the DTM side and the terminating port/interface of the second ITS unicast. The principle is illustrated below.

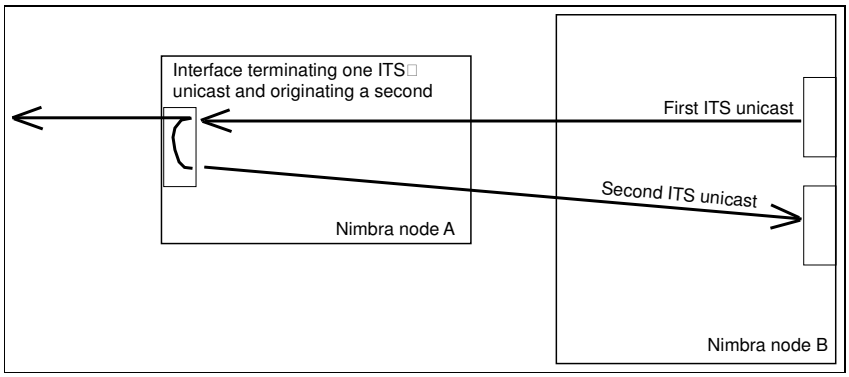


Figure 278. Loopback from the DTM side in 8 x Video Access Module for Nimbra 680.

The ITS unicast services are configured as regular ITS unicast services.

Analogous loopbacks can be made on the 8 x ASI Transport Module for Nimbra One and 300.

20 Scheduler

20.1 Scheduling of connections

Although the mechanisms for provisioning and re-configuration of connections for the ITS and ETS services are easy and fast to use, they normally require manual operations at the actual time when the change is supposed to occur.

The scheduling function makes this less of a problem as it allows the operator to schedule the creation/removal/change of a certain connection to a future point in time

Schedule any of these operations to occur regularly on daily or weekly basis

For example, this can be used to provide a high-speed connection for file-transfer between a newspaper publisher and their printing facilities only during the times it is actually required, which usually would be in the middle of the night.
Another example is to provision a SDI connection from an arena to a central studio during a few hours on a weekend without actually requiring the operator to have personnel working during the weekend to perform the operation.

An important aspect to note is that a scheduled connection will be denied if there is a lack of capacity in the network at the actual time when the operation is performed.

Reliable scheduling does therefore require good planning and control of resources and utilization in the network.

20.1.1 Set-up of Scheduling

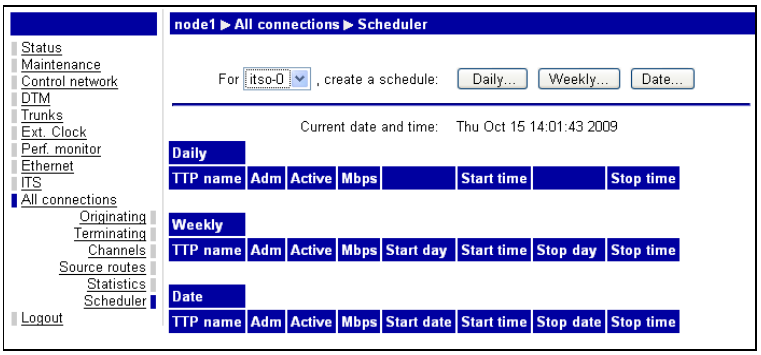


Figure 279. Scheduler menu for all connection types

The scheduler function can be reached from the following menus:

ETS → Scheduler
Lists all schedules for ETS connections and allows creation of new ETS schedules

ITS → Scheduler
Lists all schedules for ITS connections and allows creation of new ITS schedules

Connections → Scheduler
Lists all scheduled connections in the node and allows creation of schedules for all types of connections

It is also possible to configure scheduling for a specific TTP by clicking on the Scheduler link directly in an Edit TTP page.

20.1.2 Create a new scheduling entry

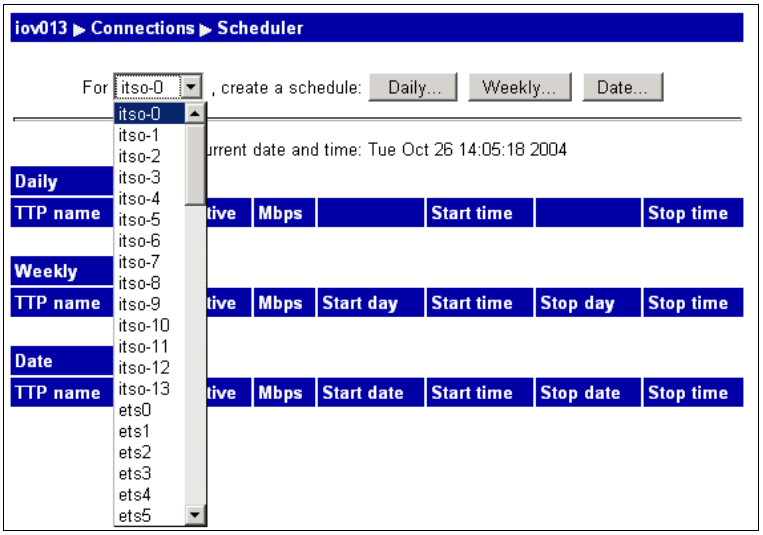


Figure 280. Selecting a TTP

A scheduling entry is always connected to an originating TTP (Trail Termination Point). An existing TTP must be chosen from the drop-down list in the scheduler menu. The creation of TTPs is described in the ETS and ITS chapters.

It is then possible to create scheduling entries on the selected TTP that will be active on a Daily, Weekly or One shot basis

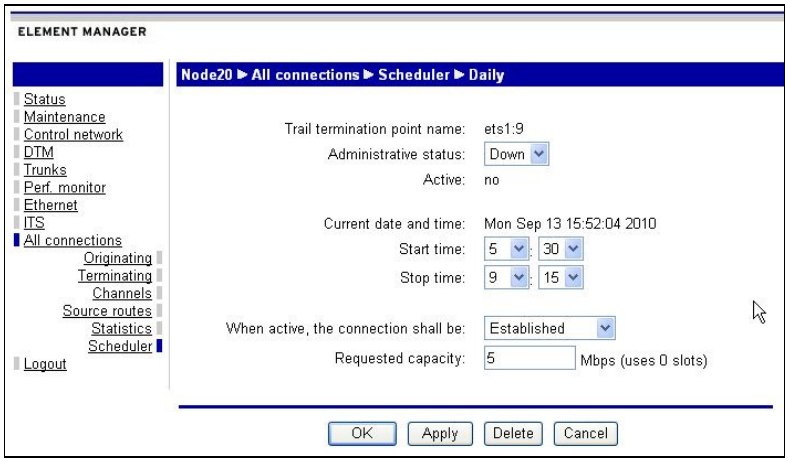


Figure 281. Setup a daily scheduling

The administrative status in the scheduling entry must be set to '**Up'** in order to activate the scheduling mechanism. If administrative status is "down", the entry will be visible in the scheduler list, but no scheduling activities will occur.

The start-time and stop-time parameters in the entry allow specification of the time-interval when the entry shall be active. A status field, indicating whether the current time is within the "active" interval is also available in the entry.

Finally, the operator must also choose whether the connection from the TTP shall be "Established" or "Not Established" during the active scheduling interval (see scheduling activities for an explanation of this). For variable bit-rate services (Ethernet and ASI transport), choosing "established" also implies choosing the capacity for the connection during the established period.

20.1.3 Automatic scheduling activities

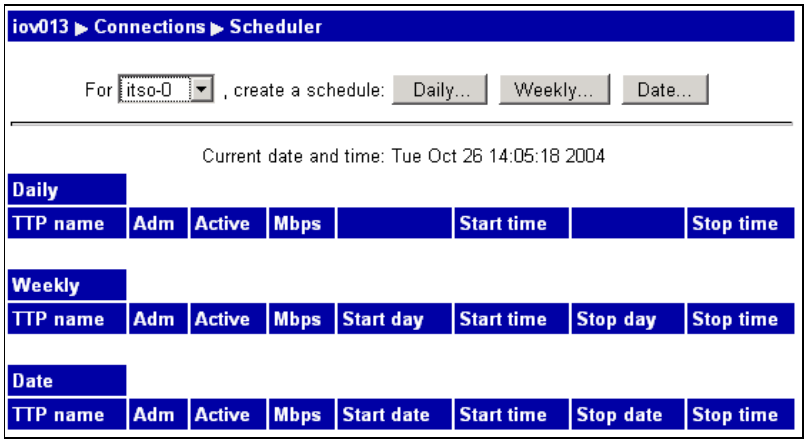


Figure 282. Overview of entries in the scheduler

All entries in scheduler with administrative status “up” will trigger an action when the current time reaches the “active” period specified in the entry. The action will consist in changing the default connection state configured on the TTP to the connection state defined in the scheduler entry (“Established” or “Not Established”). For variable bit-rate services, the default connection capacity will also be adjusted to the value defined in the scheduler entry.

When the “active” period has passed, connection state and connection capacity will be adjusted back to the default values configured on the TTP (or the values defined in another scheduler entry for the TTP that may become active at that time).

Note: 	It is possible that one daily, one weekly and one one-shot entry are activated at the same time for a certain TTP. In that case the one-shot entry has highest priority, followed by the weekly entry.

21 Redundancy for Nimbra 600

21.1 General

Redundancy is available with the Nimbra 600 Series and software NimOS GX 4.1.0 and later versions. In order to keep the node operating normally or with a minimal interruption upon module failure or degradation, Node Controllers and Switch Modules can be duplicated. A failure of an active module causes an automatic switchover to a standby module with minimal or no loss of traffic. In order to understand how the duplicated modules operate, three module specific state variables (AdminStatus, OperStatus and RedundancyRole) are important and described.

AdminStatus is set by the user to either Up or Down on each module. Down implies that the module is not intended to take an active role as Node Controller or Switch Module.

OperStatus can be one of Up, Degraded, Starting, down or Absent. OperStatus Up means that the module is working properly. Note that this does not imply that the module is active, only that it may be. State variable RedundancyRole (see below) determines if it actually is. OperStatus Degraded means that an error has been detected on the module, but it may be able to function anyway. Starting (a transient state) means that the module is starting up. Down means that the administrative status for the module is set to Down, or that the module has suffered a serious failure and cannot take over control of the node. Absent means that there is no module physically present.

RedundancyRole can be one of Active, Standby or None. Active means that the module is operational. Only one of the two duplicated modules can be active at a given time. Standby means that the module is prepared to immediately take over the critical tasks and become active. None indicate that the module is unable to take over as active for the moment.

LEDs on the module front display current status of OperStatus (Status LED) and RedundancyRole (Redundancy LED).

Another state variable, nodeStatus, is tied to the node, not individual modules. Normally, it has value ‘Up’. In case persistent channels are set up and the Node Controller reboots for some reason, the persistent channels are kept and the nodeStatus variable takes the value NoControl. No traffic interruption is seen on these persistent channels during the reboot, but the Node Controller lacks proper control of node hardware afterwards. In order

to complete the reset, nodeStatus is set to Up by the user. At this point, traffic disturbance follows on the persistent channels.

21.2 Node Controller redundancy

The key idea in order to have a properly working node at all times is to replicate (copy) any changes in software or configuration on the active Node Controller as soon as they occur to the other Node Controller and reboot this (standby) Node Controller as a last step in the replication process. In this manner, the standby Node Controller will always have the latest software and configuration and, after the reboot is completed, will be ready to take over.

The replication procedure is initiated by the active Node Controller. It updates software and configuration on the standby Node Controller to match its own settings. After successful completion of the replication procedure, the Standby Node Controller is rebooted.

Replication takes place when the Node Controller is promoted to active or when the state variable OperStatus on the other Node Controller is changed to Up or Degraded. Replication also takes place when software has been upgraded or the configuration has changed on the active Node Controller.

Upon failure or restart of the active Node Controller, the standby Node Controller takes over as active Node Controller (i.e. its RedundancyRole state variable changes from Standby to Active) immediately if the value of its OperStatus state variable is Up. In case this value is Degraded, the standby Node Controller waits for the (previously) active Node Controller to restart before taking any actions. If the OperStatus state variable of the latter Node Controller is Up after restart, it becomes active again and continues to run the node and the standby Node Controller remains standby. If the (previously) active Node Controller comes up with an OperStatus state variable value of Degraded, Down or Absent after reboot, the Standby node-controller is promoted to Active, even though its OperState state variable value is Degraded. It is not recommended to run the node in this way for any prolonged period of time.

When the operator restarts the node, only the active Node Controller is restarted. As a consequence, this means that if both Node Controllers have their OperStatus state variable value equal to ‘Up’, a restart makes the standby Node Controller take over as active Node Controller immediately.

In order to maintain changes in the Standby Node Controller’s state variable AdminStatus upon soft or hard reboot, it is essential to save any altered configuration on the active Node Controller and have it replicate the changes to the Standby Node Controller.

In order to maintain changes in the Active Node Controller’s state variable AdminStatus upon soft or hard reboot, it is essential to save any altered configuration on the active Node Controller and to reboot the active Node Controller.

The node should be configured from the serial port of the active Node Controller. The active Node Controller is identified from its green Redundancy LED, whereas the Redundancy LED of a standby Node Controller is amber. Once the initial IP configuration has been made, it is suggested that an Ethernet switch be introduced before the two Node Controllers. In this way, the user sees the node as one entity with one IP address irrespective of which Node Controller is active.

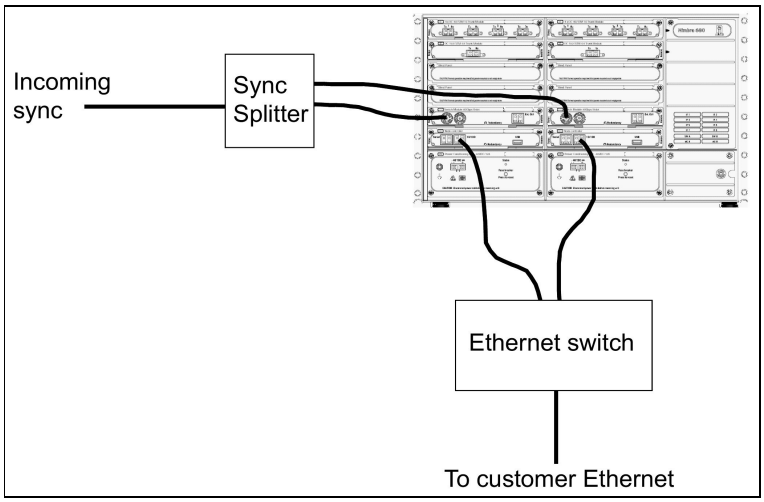


Figure 283. Hardware configuration of redundant Node Controllers and Switch Modules.

It should be observed that the Node IP address is associated with different hardware (different MAC addresses) depending on which Node Controller is active.

In the web based user interface, it looks like the user manages the node and not the node controllers. The user needs not be concerned about which Node Controller is active, only to manage the Node. The Node Controllers manage the node collectively.

21.3 Switch Module redundancy

From a user perspective, switch mode redundancy works transparently. Plug in one Switch Module and there is no redundancy; plug in two Switch Modules and there is redundancy. There is no problem to power the switch with dual Switch Modules mounted; in fact that is the suggested way to work if redundancy is planned from the start.

Internally, as long as the active Switch Module has OperStatus Up, it continues to be active. If its OperStatus value for some reason changes to Degraded, negotiation with the standby Switch Module begins and as a result its RedundancyRole state variable changes to Standby and the RedundancyRole variable of the previously Standby Switch Module changes to Active.

The Node takes its synchronization signal from the active switch module. For this reason, an external synchronization signal has to be split before the interface to the switch modules. The signal is distributed to the modules. Make sure the connecting cables from the splitter to the switch modules are as identical as possible. In this manner it is ascertained that the same synchronization signal reaches both Switch Modules and it does not matter which module is active.

On the Status/Equipment page in the web interface, the active module can be found (shown below).

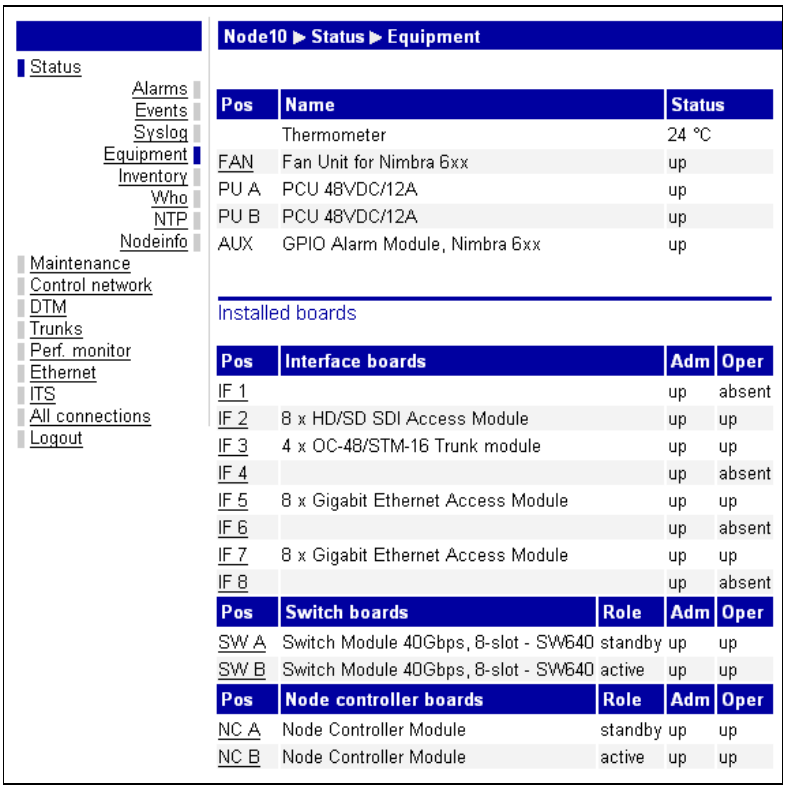


Figure 284. Status/Equipment web page of a system with duplicated Node Controllers.

22 Module installation

22.1 General

There are a few things to consider when modules are added to a node installed in a network in full operation. It is critical to have complete nodes aligned to a system release software and the delivered new module(s) may have different system release software than the node.

In order to make sure that the system release software running on the node is downloaded to the new module and the module is properly aligned, it is very important to follow the procedure described in this chapter when installing new or replacement modules.

The system release software should be stored in a so called repository on a computer or server with connectivity to the Nimbra node where the new module is installed. The repository is a collection of files stored in a directory with the name of the system release. An example is shown below:

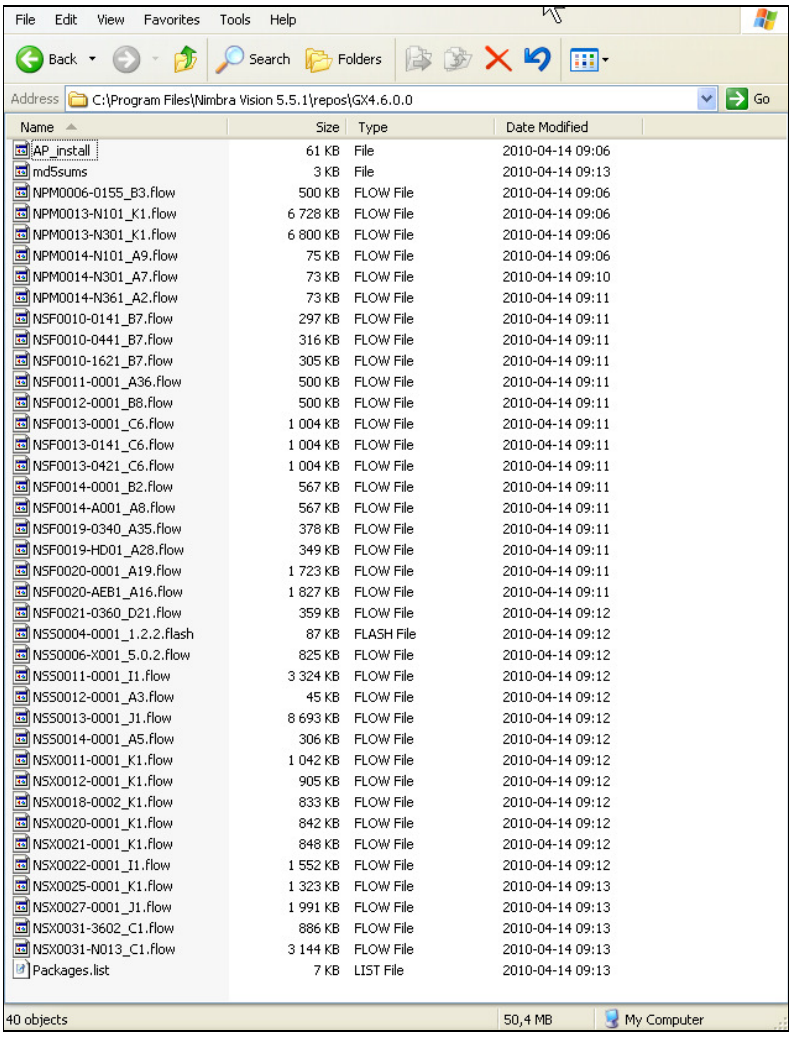


Figure 285. The repository, here for GX4.6.0.0, is shown.

22.2 Differences Nimbra One/300 vs Nimbra 600

Implementation of administrative status is different on Nimbra One/300 and Nimbra 600. If a module has administrative status set to 'Down' on a Nimbra One/300 node, power is shut down to the module. Hence, the module is incommunicado and no software realignment is possible. For this reason, all software realignment on Nimbra One/300 must be made with admin status 'Up'. Otherwise, the procedure outlined below can be followed. Make sure to click on the 'Bring new image into service' at the end of the procedure and 'OK' in the confirmation window irrespective of the misleading confirmation window.

The procedure below describes how to realign a Nimbra 600 node

22.3 Addition of new modules to existing nodes

Before new modules are inserted in existing nodes, it is crucial that the administrative status of the slot position is set to down in the Nimbra 600. If it is not, the module comes up direct, which may cause various problems if the system release software is not aligned.

Connect to the node via the web interface. Log in to the node and follow the link System → Equipment. Click on the interface link (IF1 – IF8) of the slot(s), which will receive the new module(s). In the drop-down menu, select Down as value for Administrative status, then click the 'Apply' button.

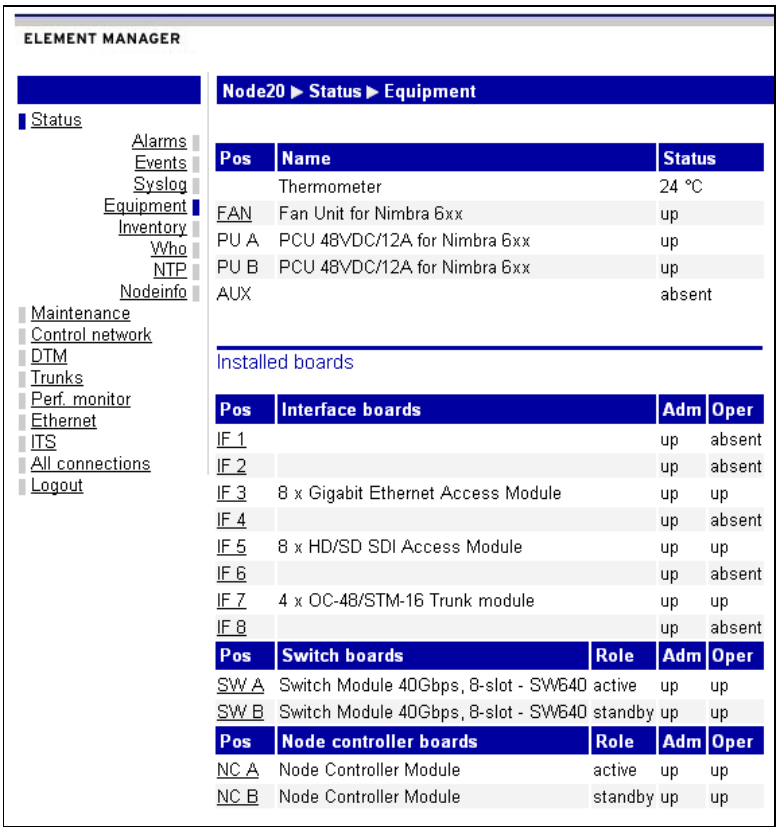


Figure 286. Status equipment page, with administrative status of all interface slots set to up.

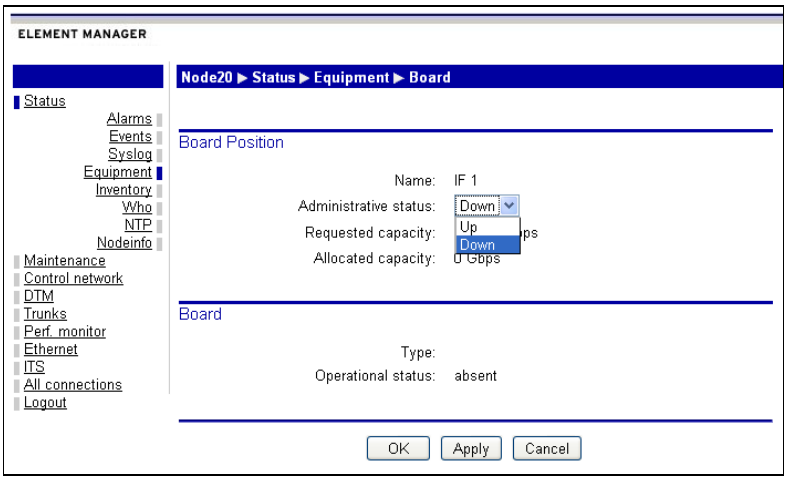


Figure 287. Administrative status of IF1 is set to down.

After the administrative status of the slot/module has been set to down (Figure 287), the new module may be inserted in the slot. While the administrative status is still down, alignment of the system release software of the node and the module is made.

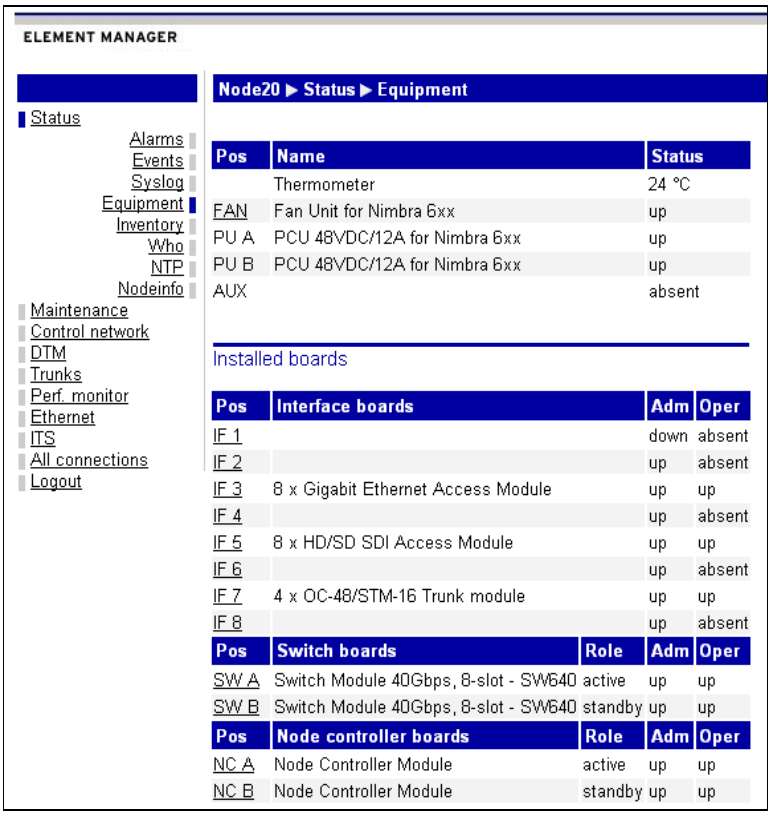


Figure 288. Status equipment page, with administrative status of all interface slots set to up, except slot IF1 which is intended for the new module.

To check if the new module already is aligned with the rest of the node, click on the link Maintenance → Software. If the system alignment status parameter has value ‘full’, no alignment is needed. In this case, all that remain is to change the value of the administrative status parameter to ‘Up’ on the new interface.

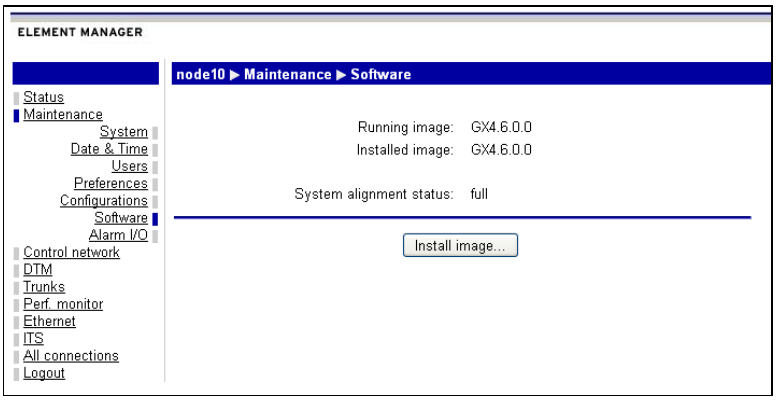


Figure 289. A node with full system alignment status after the new module is inserted does not need additional software alignment. All that remain is to set the administrative status of the new module to ‘Up’.

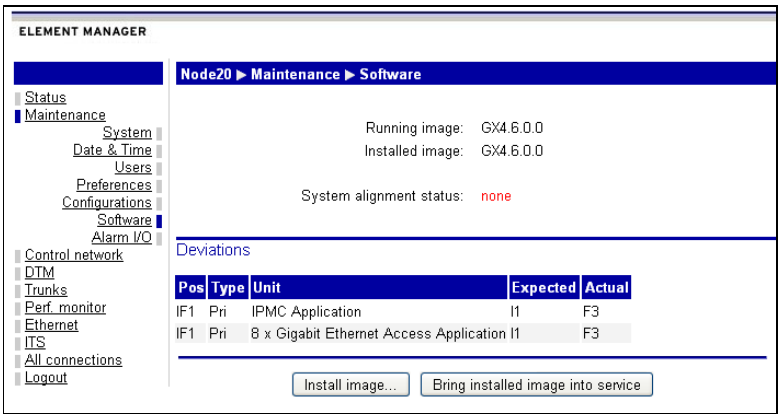


Figure 290. A node with other system alignment status than ‘full’ needs realignment between the new module and the node. This process is described below.

In order to align node and module system releases, the repository of the node system release software is stored on an http or ftp server. Follow the link Maintenance → Software and click on the button ‘Install image’. The page below appears on the screen.

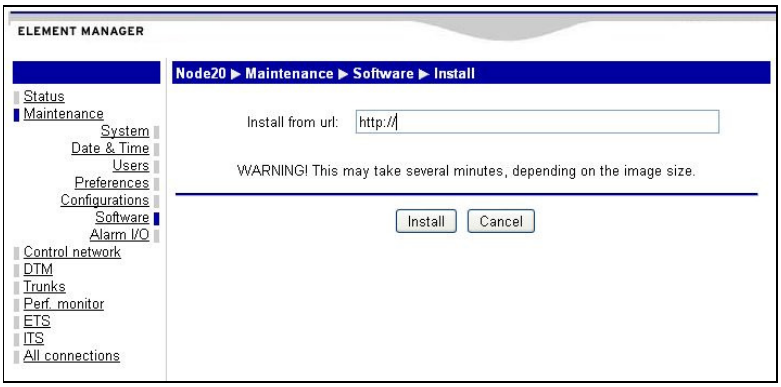


Figure 291. Install image web page.

Type the URL to the http or ftp server. The syntax below gives two examples, one for http and one for an ftp server.

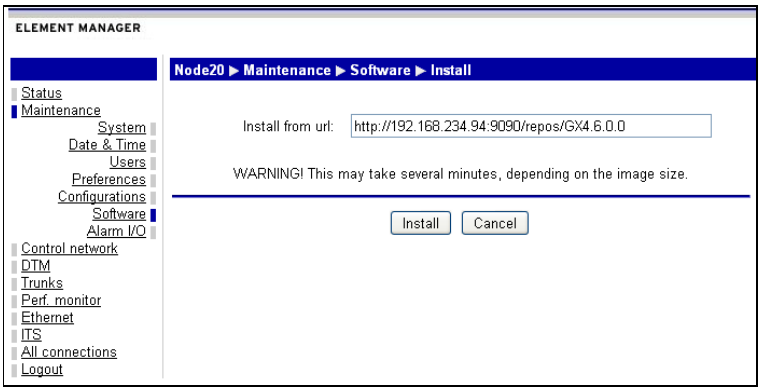


Figure 292. Example of an http server. The repository of system release software GX4.6.0.0 is found under directory /repos of the http server.

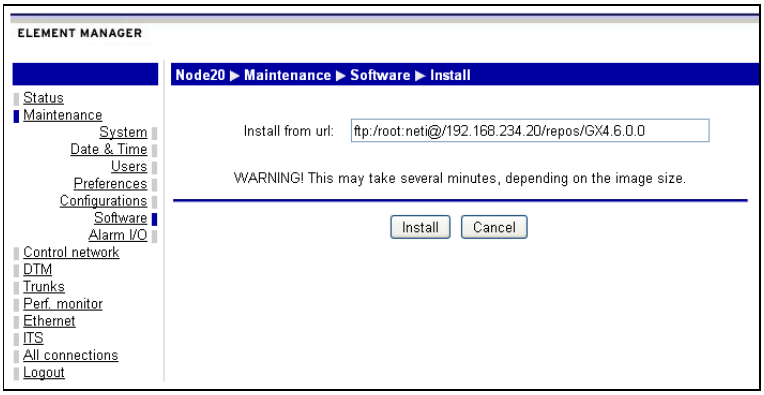


Figure 293. Example of an ftp server, with user root and password neti. The repository of system release software GX4.6.0.0 is found under directory /repos of the http server.

Clicking on the install button starts the alignment process to the repository system release software version, i.e. the installation of the system release software to the entire node including the parts with administrative status down. After a brief interruption, a progress report is generated.

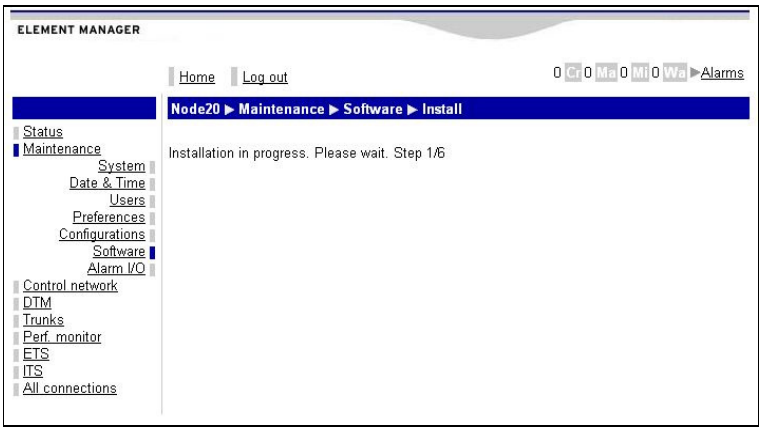


Figure 294. Progress report of installation.

When the installation is complete, the web interface communicates this.

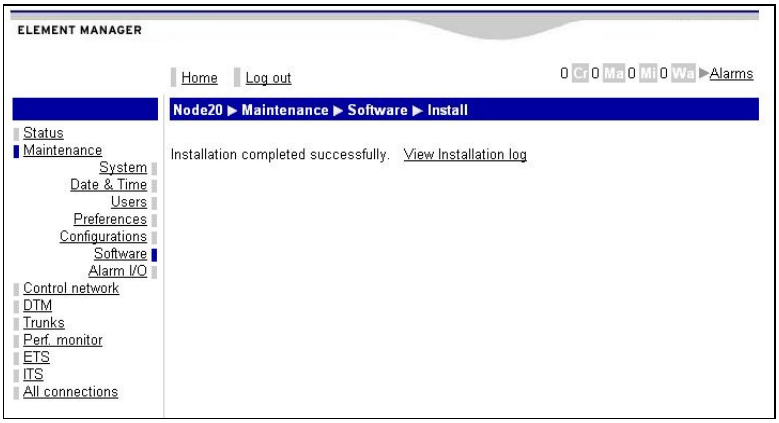


Figure 295. Message of complete installation.

For details, the installation log can be viewed.

Click on the link Maintenance → Software. If alignment exists, the system alignment status parameter has value full. In this case, just change the administrative status of the module to 'Up'. Then the system is aligned and operational.

Otherwise, the inserted module must have its ipmc software restarted (this software is never automatically rebooted). To manually reset this process,; follow the link Maintenance → Software. Click on the 'Bring installed image into service' button.

If this step is required, click on the 'Bring installed image into service' after saving the configuration. A general confirmation window pops up, asking if the user wants to restart the node controller. However, the installation software ensures that only software that needs to be restarted is restarted. If this procedure has been followed, there is no need for a restart of the node controller and no such restart will occur. In order to align software, confirmation must be given in the confirmation window (i.e. the question must be answered with 'OK', not 'Cancel').

After this set is completed, just set the administrative status to 'Up' and the module is operational and the node is fully aligned.

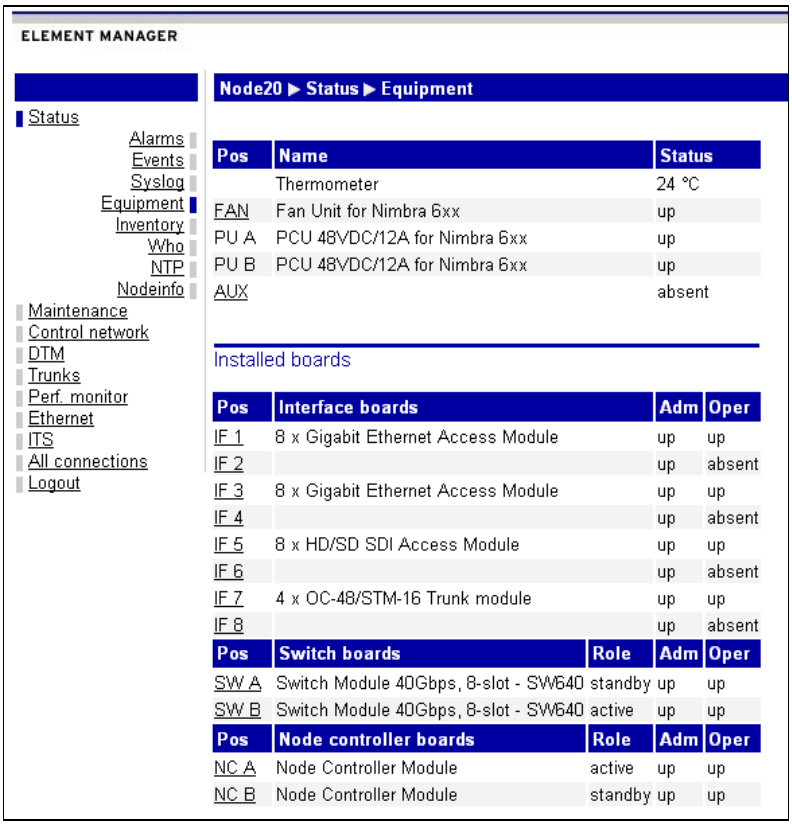


Figure 296. Status equipment page of the aligned node/module, with all nodules having admin status set to ‘Up’.

23 Up- and Downgrading

23.1 General

Changing system release software, i.e. a defined collection of soft- and firmware modules, can be made to a higher or lower system release. In addition, an enhanced software/firmware feature, requiring a separate software license, can be added without modifying the system release.

In this chapter, the regular up/downgrading procedure is described first. Addition of enhanced features without altering system release is described later in this chapter, on a case-by-case basis. Currently, there are three cases of enhanced features; addition of FEC on a 4 x OC-3/STM-1 Trunk Module; changing of trunk speed on Nimbra 360 and change of mode on the DS3/E3 Trunk/Access Module.

The regular up/downgrading procedure is described on a node basis, using the Command Line Interface (CLI). Changing the system release in a Nimbra network is conveniently handled in the Nimbra Vision software. Using this software, checks are made that proper software and firmware are loaded in all places where they are needed.

23.2 Up/downgrading GX version from CLI

Note: 	The CLI commands given below shall be executed on one line in the shell of the node, despite that the format of this manual sometimes splits the command on two or more lines. Upgrading is more conveniently done from Nimbra Vision.

In GX4.1.2 and all later system releases, software and embedded software modules (i.e. application packages) are delivered in a release "repository" file. This file is a compressed file with a directory and an internal file structure. It is imperative that it is used "as is". The procedure below outlines the up/downgrade of the node in just a few simple steps.

This upgrading procedure requires that the files of the repository are unpacked and properly stored in a location, which can be reached from the node. A repository is preferably set up on a common http or ftp server that all nodes in the network can reach. Alternatively, on a Nimbra 600 series node, the repository can be downloaded (as a "tgz" file) to the node, be unpacked and the node can be upgraded (using CLI). In the web interface, the repository must be unpacked (manually) before upgrading takes place. In a

Nimbra One/300 node, the repository must reside on an external disk, as the repository structure is too large for available memory on the Nimbra One/300.

23.2.1 Saving the current configuration

Before any up- or downgrade is started, the current configuration should be saved and preferably labeled with current system release version. If a downgrade should be needed, a saved configuration file from the previous release should be restored before the downgrade is carried out. A configuration name of 'Config_for_GX4.4.0.2' or similar (for the appropriate system release) is suitable to keep track of the system release under which the configuration file was generated.

23.2.2 Creating the repository directory

In order to create a release repository, the repository file must be obtained. Provided that a proper license agreement exists, the repository file can be downloaded from a Net Insight ftp server. The release repository file for release GX4.4.0.2 is called "GX4.4.0.2.tgz" and analogously for other system releases.

Unpack the .tgz file on an ftp or http server, accessible from the nodes that shall be upgraded. In the example below, the ".tgz" file is unpacked in the `<target-dir>` directory. The sub-directory GX4.4.0.2 is created in the process.

On a Linux server, proceed as follows (from the directory `<target-dir>`

```
# tar xzf GX4.4.0.2.tgz
```

This will unpack the GX4.4.0.2 repository to the directory

`<target-dir>/GX4.4.0.2/`

On a Windows server, if the tar/gzip commands are not available, the file can be unpacked with a file decompression utility like 7-zip or Winrar. **Note that WinZip does not decompress all files correctly!** For that reason it cannot be used.

The unpacked repository contains all the files that constitute the new GX release. To check the integrity of the repository directory, go to the directory and run (Linux):

```
# md5sum -c md5sums
```

If the "`md5sum`" command does not give any error output the repository is correctly set-up and ready to be used.

23.2.3 Using "`node-install`" to up-/downgrade a node

Up/downgrading of software and firmware of systems running software versions GX 4.4.0.2 or higher is now made with a simple CLI command for any type of node. Proceed as follows:

Save the current configuration according to the process previously described.

Start a telnet session with the node that is to be upgraded.

Log in as root (root/neti is the default user/password combination)

At the node prompt, write

```
node-install http://192.168.234.20:9090/repos/GX4.4.0.2
```

`repos/GX4.4.0.2` is a repository for the system release to be installed. Alternatively, if the repository is installed on an ftp server, use the following command:

```
node-install
ftp://user:pass@192.168.234.20:port/repos/GX4.4.0.2
```

where `192.168.234.20:port` denotes the IP address and port of the http/ftp server of the repository, and `user:pass` is the login and password for the ftp account. Note that if DNS is not enabled on the node, the numerical IP address has to be given.

The `node-install` command checks the new release and compares it with installed hardware. All relevant software and firmware images are retrieved from the repository and installed at appropriate locations in the node.

After downloading, proceed with (for an http repository):

```
node-install --restart
http://192.168.234.20:port/repos/GX4.4.0.2
```

or (for an ftp repository):

```
node-install --restart
ftp://user:pass@192.168.234.20:port/repos/GX4.4.0.2
```

at a suitable service window.

It is essential to include the URL to the repository, as the command checks that the node is indeed upgraded to the right GX release and restarts (only) modules with new software and firmware. Default is that no reboot is needed.

All activity of the "node-install" command is logged by syslog to the file `/var/log/messages`, which can be inspected for anomalies after an upgrade.

The "`node-install`" command can just as easily be used for downgrades as for upgrades. The only thing determining what release is uploaded to the node is the repository, which defines the version.

It is recommended that caution is used in downgrading GX software as testing on this point has been limited. If needed to downgrade, contact Net Insight for the availability of repositories for older releases.

23.2.4 How to upgrade pre-GX4.1.2 nodes

Upgrade for Nimbra 680 from GX4.1.1.X to GX4.1.2 and for Nimbra One/300 from GX3.3.3.0 can also be done using "`node-install`". In this case the "`node-install`" command must be fetched to the node via ftp or wget; it must get executive rights and it must be executed.

Fetch the command from a Net Insight ftp server. Store the command on /flash/root and execute (as root, once, to set execute rights for root):

```
/flash/root # chmod u+x node-install
```

To install the release, use the procedure as described above but in this case the "`node-install`" command must be pre-pended with a "`./`"

```
/flash/root # ./node-install
```

since the command is not in the system path. After a first upgrade, the node-install command is installed in the right place and it is no longer necessary to use the pre-pended "`./`".

This procedure can only be used to upgrade to system release GX.4.1.3.4. For upgrades to higher releases (i.e. newer releases) the upgrade must be made in two steps. After a successful installation of GX4.1.3.4, node install can be used once more to install a newer system release. In this second step, a new repository must be used.

For upgrades from versions prior to GX4.1.1.X (Nimbra 600 series) or GX3.3.3.0 (Nimbra One/300 series), this procedure does not work. In case you have such needs, please contact Net Insight.

23.3 Addition of functional enhancement

Note: 	All functional enhancements described in this section require a separate software license. This license should be obtained before the upgrade procedure.

23.3.1 FEC to the 4 x OC-3/STM-1 Trunk Module from CLI

Adding FEC to the 4 x OC-3/STM-1 Trunk Module can be made with the `node-install` command. An additional option, `--replace`, tells the script that it is not a question of system upgrade but rather an enhancement upgrade.

The syntax is (for Nimbra One):

For an http-server

```
node-install -d <module #> --replace ,NPM0006-0155
http:// 192.168.234.20:port/repos/GX4.4.0.2
```

and for an ftp-server

```
node-install -d <module #> --replace ,NPM0006-0155
ftp://user:pass@192.168.234.20:port/repos/GX4.4.0.2
```

Corresponding syntax for Nimbra 300 series is:

for an http-server

```
node-install -d <module #> --replace ,NPM0006-0155
http://192.168.234.20:port /<target-dir>/GX4.4
```

and for an ftp-server

```
node-install -d <module #> --replace ,NPM0006-0155
ftp://user:pass@x.x.x.x:port/<target-dir>/GX4.4
```

23.3.2 Changing fixed trunks interfaces on Nimbra 360

> ***Note:*** This procedure should only be executed with a separate data network. Using in-band DLE causes a loss of contact with the node upon reboot of the node.

The functionality (supported trunk rate) for the fixed trunks of a Nimbra 360 can now be changed from both from CLI and the web interface. Note that changing the default setting of 4 STM-1/OC-3 trunks requires additional licenses.

To change firmware from the web interface, follow the link Maintenance → Software. On this page, click on the button 'Install onboard image …'.

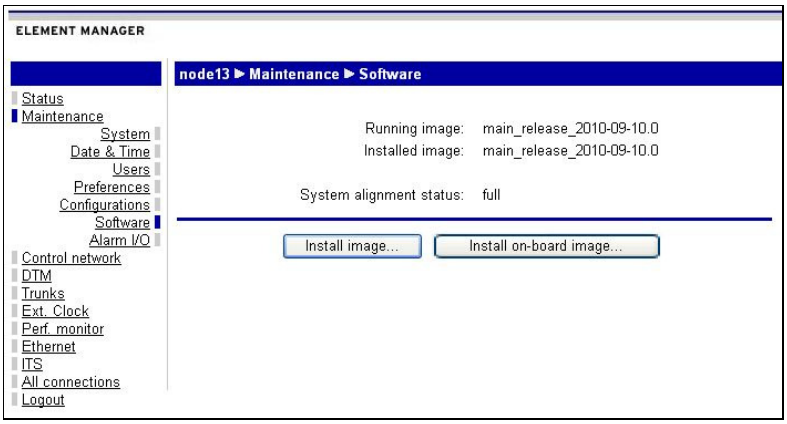


Figure 297. Web page for replacement of the factory default setting of four STM-1/OC-3 trunks on the fixed interfaces of a Nimbra 360.

For Nimbra 360, a new page appears, Maintenance → Software → Install. Here a repository with the required files is needed, and it is only possible to install trunk firmware OC-3/STM-1, OC-12/STM-4 and OC-48/STM-16 from the web interface. Installation of IP/Ethernet trunk firmware is currently not possible.

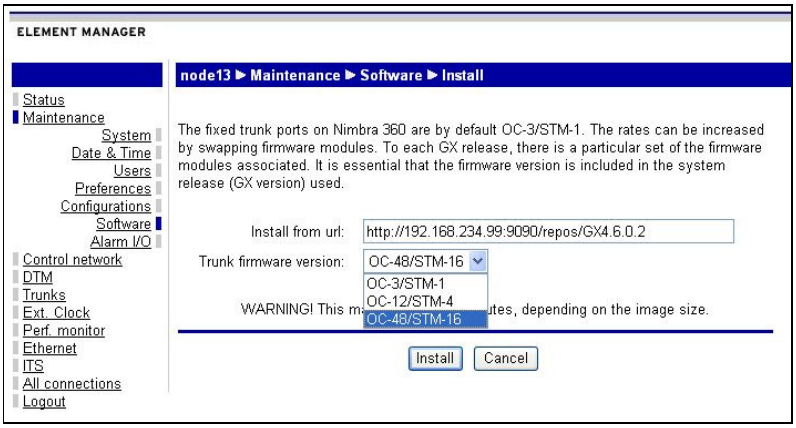


Figure 298. Selection of fixed trunk firmware on a Nimbra 360.

Select the required firmware and click on install. To later activate the new firmware, go back to Maintenance → Software. Click on Bring installed image into service makes the new firmware with new rates active.

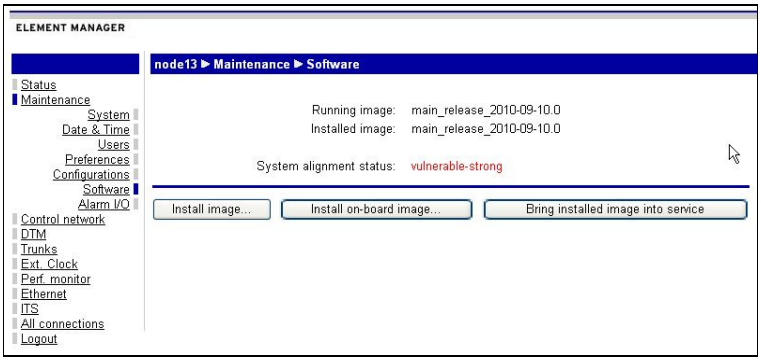


Figure 299. Activation of the new firmware is made by clicking on the 'Bring installed image into service' button.

23.3.3 Changing fixed trunks interfaces on Nimbra 360 by CLI

Note:

This procedure should only be executed with a separate data network. Using in-band DLE causes a loss of contact with the node upon reboot of the node.

The fixed trunk ports on Nimbra 360 are by default OC-3/STM-1, running embedded software `NSF0010-0141`. The rates can be increased by swapping firmware module. To each GX release, there is a particular set of the firmware modules associated. It is essential that the correct firmware version is installed, a version that is included in the system release (GX version) used.

Installation of four OC-12/STM-4 ports requires firmware `NSF0010-0441`, installation of two OC-48/STM-16 ports require `NSF0010-1621` and installation of two IP/Ethernet trunk ports require `NSX0031-3602`.

To install the enhancement, proceed as follows (e.g. for OC-48/STM-16):

Log on to the node. Save the configuration file just prior to enhancement installation with:

```
registry backup -n name_of_conf -c comments
```

To see the version currently running, the command

```
inventory -s 3
```

can be used.

Run the script node-install. Note the absence of spaces between the two NSF product numbers:

```
node-install -d 3 --replace NSF0010-0141,NSF0010-0441
http://x.x.x.x:port/<target-dir>/GX4.6.0.2
```

for an upgrade to STM-4 on an http-server and

```
node-install -d 3 --replace NSF0010-0141,NSF0010-1621
ftp://user:pass@x.x.x.x:port/<target-dir>/GX4.6.0.2
```

for an upgrade to STM-16 from an ftp-server. Upgrading to the IP/Ethernet trunk requires the following script settings from an http server:

```
node-install -d 3 --replace NSF0010-0141,NSX0031-3602
http://x.x.x.x:port/<target-dir>/GX4.6.0.2
```

Observe that in all cases when the firmware has been replaced, the old DTM interfaces remain with operational status absent. If the user doesn't intend to go back to previous interface rates, these interfaces can be deleted.

The structure of the node-install script is described below.

By extension, upgrading from STM-4 to STM-16 becomes:

```
node-install -d 3 --replace NSF0010-0441,NSF0010-1621
http://x.x.x.x:port/<target-dir>/GX4.6.0.2
```

and upgrading from STM-4 to IP/Ethernet trunk:

```
node-install -d 3 --replace NSF0010-0441,NSX0031-3602
http://x.x.x.x:port/<target-dir>/GX4.6.0.2
```

Finally, the upgrade from STM-16 to IP/Ethernet trunk becomes:

```
node-install -d 3 --replace NSF0010-1621,NSX0031-3602
http://x.x.x.x:port/<target-dir>/GX4.6.0.2
```

23.3.4 Setting modes for 4 x DS3/E3 Trunk/Access Modules

> ***Note:***
>
> 
>
> This procedure should only be executed with a separate data network. Using in-band DLE causes a loss of contact with the node upon reboot of the node.

The 4 x DS3/E3 trunk/access module can be set to operate either in trunk or in access configuration. The hardware is common; the difference in the two cases is the firmware placed on the module. It is fairly easy to reconfigure the trunk mode to the access mode and vice verse. Firmware for trunk mode is called `NSF0014-0001` and firmware for access mode is `NSF0014-A001`.

To install the access mode firmware on a module configured as a trunk module, proceed as follows:

Log on to the node. Save the configuration file just prior to enhancement installation with:

```
registry backup -n name_of_conf -c comments
```

Run the script node-install:

```
node-install -d <slot #> --replace ,NSF0014-0001
http://192.168.234.20:port/<target-dir>/GX4.4.0.2
```

to download the trunk module firmware on a module in access mode from an http-server. To change a module in trunk mode to operate in access mode, use the command

```
node-install -d <slot #> --replace ,NSF0014-A001
ftp://user:pass@192.168.234.20:port/repos/GX4.4.0.2
```

for an upgrade from an ftp-server. Note the comma in front of the firmware module we want to upgrade to.

When the download is finished, save the configuration once more and reboot the node. The node should restart running the installed firmware.

Note that an Access mode feature license is needed to enable/use a 4 x DS3/E3 Trunk/Access Module with access functionality if it has been purchased for trunk use, and that a Trunk mode feature license is needed to enable/use a 4 x DS3/E3 Access/Trunk Module with trunk functionality if it has been purchased for access use.

23.4 Functional Description of upgrade functionality

On the network element, "`node-install`" issues a command to download the installation program to the network element from the repository. The program is stored on a temporary folder on a volatile disk. The installation program is then started on the network element. The installation program examines what is already installed as primary and secondary software and firmware images. All images that do not match the contents (article number and version) in the repository are downloaded and installed as secondary image. When the installation is confirmed successful, it swaps the secondary and primary images, making the primary image the just installed image. It then downloads and installs the image again as secondary. This means that when complete, the primary and secondary images are identical, matching the contents of the repository.

The "`node-install`" command accepts a number of options. Some of them control what will be done and some influence the presentation of the result.

Usage:

```
./AP_install [options] <repo>


<repo> = AP repository:  URL to repo or full path to repo
(packed or unpacked)

( URL example:  http://10.100.0.53/pub/GX4.1.1.4 )


Options:


-w <what> | --what <what>

<what> = BOOT | MGMT | PAYLOAD | ALL(=BOOT+MGMT+PAYLOAD),
default ALL

MANAGEMENT is a synonym for MGMT

PAYLOAD and MANAGEMENT can be shortened down to 3 chars

-d <dest> | --dest <dest>

<dest> = pos to load if not all, optional
(nca,ncb,swa,…), default ALL

-h | --help

print usage info (this text)

-n | --sim [ <node description file> ]

no action, just print what would be done.

The <node description file> can be used when not running
on an NC, it shall be the output from the 'swap' command
with some extra markers

--restart

restart all boards that are updated (after successful
installation)

--verify

check that all boards are loaded with images from the
currently installed

system release (or the specified repository if given).

Can not be combined with any other options.

-s | --silent

print limited progress info: m/N (N/N when finished)

--pri-only

install new images as primary images and leave secondary
images as backup

--warnings

print more info

--no-warnings

suppress some info

--replace [<art-no-from>,]<art-no-to>

When a product (AP) <art-no-from> is found it shall be
replaced with product <art-no-to>. If <art-no-from> is
not specified <art-no-to> will be loaded wherever
possible. This option may be repeated to specify more
than one replacements. N.B. Both products must be
loadable on the same board(s).

The following mnemonics are available as product names:

4xSTM1 = NSF0010-0141
```

```
4xSTM4 = NSF0010-0441

2xSTM16 = NSF0010-1621

--exclude <art-no>[,<art-no>]…

don't upgrade boards or Aps with article number starting
with <art-no>

--force

ignore errors, useful if a node contains a board that
refuses to upgrade

-x

debug script by 'set -bx'
```