Element Manager, overview

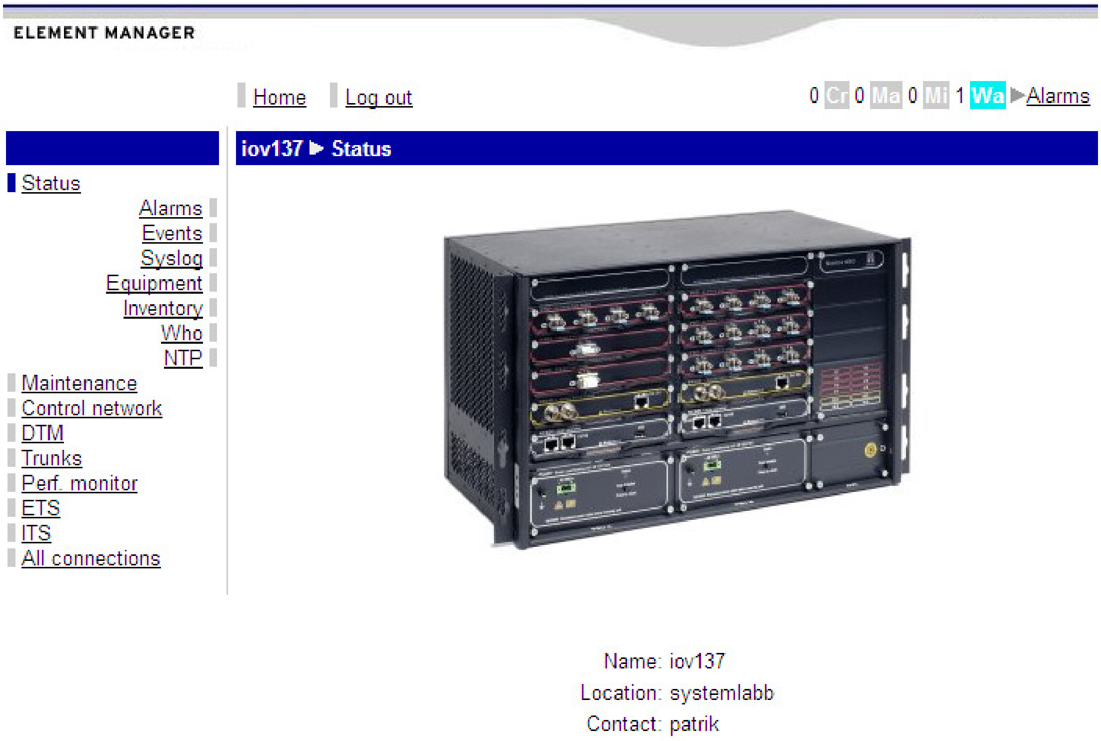
February 2009

Description

This page is intentionally blank.

Web browser (Element Manager)

Status menu



Name: iov137
Location: systemlabb
Contact: patrik

Figure 1. Status menu in the web browser.

Status – Alarms, Events and Syslog

The link Alarms in the Status menu shows all active and cleared alarms in the node.

The link Events in the Status menu shows all events that occurred in the node.

The link Syslog in the Status menu sends the user to additional links. For a Nimbra 680/688 with dual node controller modules, four different system logs are available: Active node controller, latest log; Active node controller, older log; Other node controller, latest log or Other node controller, older log. Other nodes have two links, Active node controller, latest log and Active node controller, older log.

Status – Equipment, Inventory and Who

The link Equipment shows the installed modules in the chassis, as well as some basic information about the chassis. It shows status of the power modules, the fan unit module and all installed card.

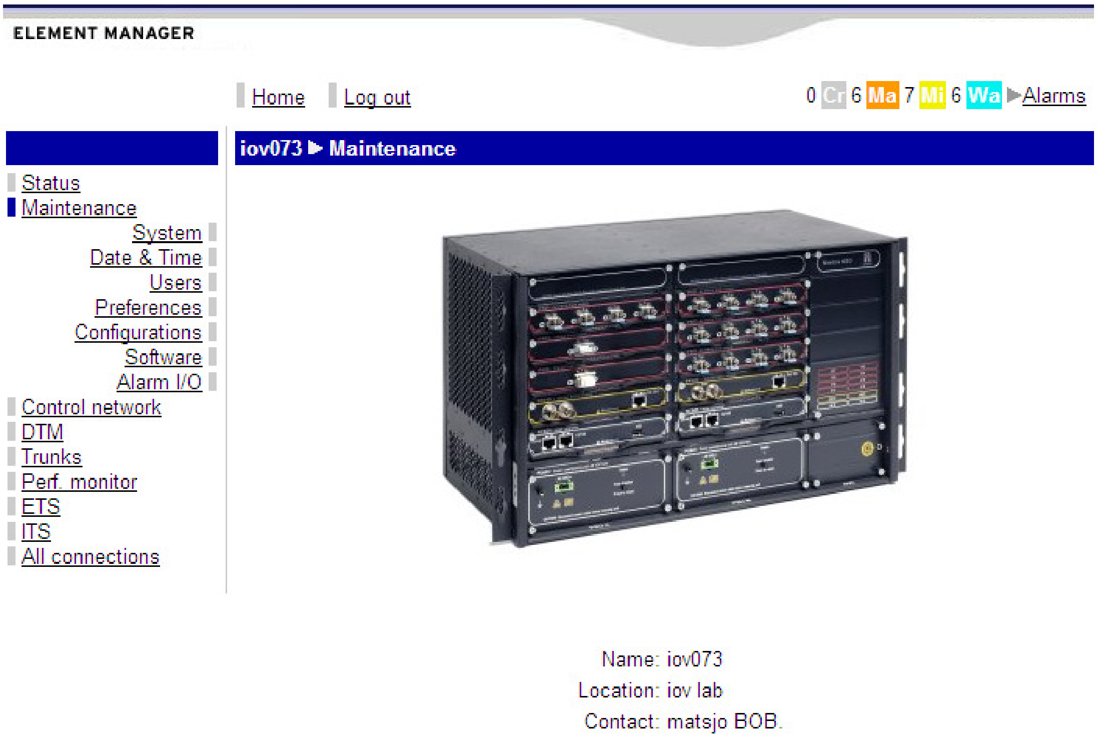
The link Inventory gives a detailed listing of soft- and firmware modules, as well as the hardware modules they are running on. It also provides hardware specific parameters, name, article, serial number and version etc.

The link Who displays all users logged on to the unit.

Status – NTP (Network Timing Protocol)

The link NTP displays all Network Timing Protocols available for the node. The listing with the lowest stratum clock level is used in the node.

Maintenance menu



Name: iov073
Location: iov lab
Contact: matsjo BOB.

Figure 2. Maintenance menu in the web browser.

Maintenance - System

Navigate to **Maintenance | System**. Here you can set a number of administrative parameters. You can enter system name, contact person, and location of the node. You can configure an (IP) name server and a NTP (Network Time Protocol) server. You'll also select which events and alarms should be logged and set the maximum number of logged events and alarms. You'll reboot or halt the node here, by clicking on the Reboot or halt system link (just below the heading) and then either type "restart" and click on the 'Restart' button or type "halt" and click on the 'Halt' button. The node performs the requested action.

Clicking on the 'Resume full operation' button, which is only available when the node is in state 'NoControl', reboots the node. Ticking the 'Restart on error' tick box before clicking the button overrides any persistent or nailed links previously defined in the node.

Maintenance – date and time

Here you'll set and reset the internal date and time clock of the unit. You can also select a time zone, but note that you need to set the time zone before you set the time, as otherwise the time adjusts automatically to the new time zone.

Maintenance – users/preferences

Here, all logged on users are listed. In addition, new users may be added. Click on Add user … and enter username and password (twice). Also, the user access mode (privilege level) must be defined as one of 'Full access' or 'Read-only access'.

From the Maintenance – Preferences menu, it is possible to select which events and alarms that are shown and how many events from the log file that should be presented in the web browser.

Maintenance – Configuration

Here you'll back up your configuration by clicking on the 'Save configuration …' button. You are also able to upload a configuration to the node, provided it is stored in such a way that it is available from the computer communicating with the node.

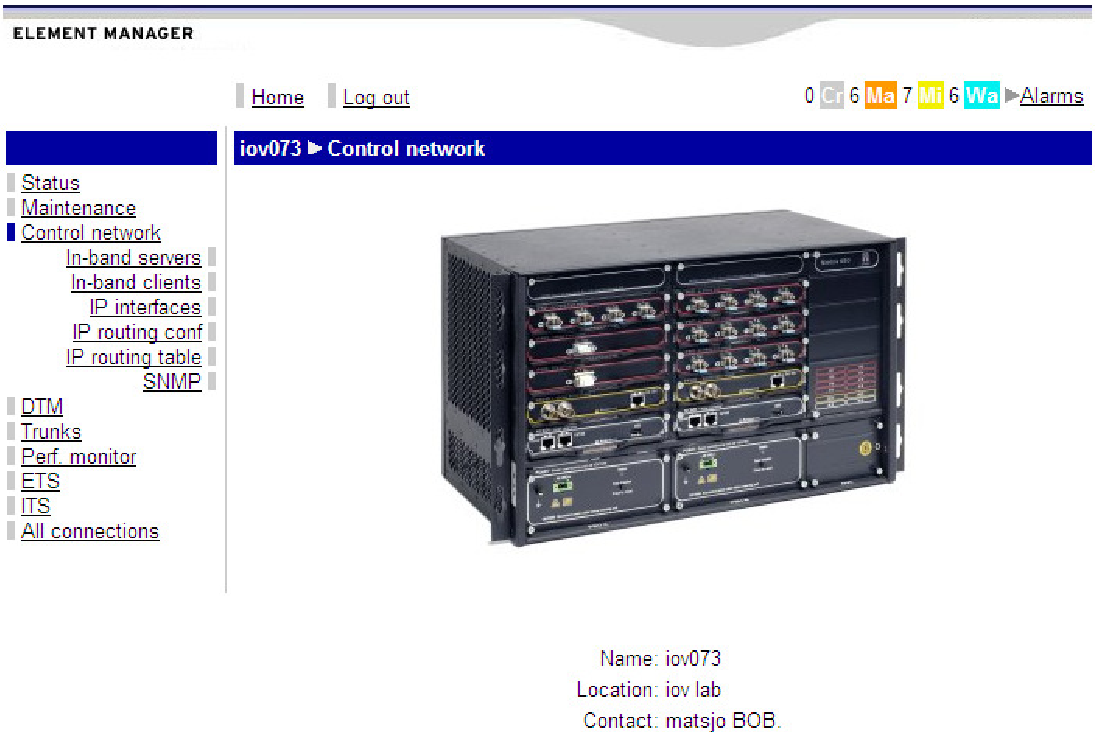
Maintenance – Software and Alarm I/O

Clicking on the Software link displays two software images, which here is synonymous to two system releases (GX-releases). The running image is active and is so until node reboot. The installed image is the image that is used during reboot and it becomes the active image after a reboot. The installed image can be replaced by clicking on the 'Install image …' button. The web browser now asks for a URL. This URL is the repository, i.e. the top directory of the set of files constituting the system release. This repository must be accessible from the node. Installing an image may take several minute.

In order to activate the installed image, the node must be rebooted. This is easily done from the System link in the Maintenance menu.

From the Alarm I/O link, the GPIO Alarm Module of Nimbra 680/688 and the Alarm ports of Nimbra 340 can be configured.

Control network menu



Name: iov073
Location: iov lab
Contact: matsjo BOB.

Figure 3. ‘Control network’ menu in the web browser.

Clicking on the Control network link, displays its structure (above). The subsections are In-band servers, In-band clients, IP interfaces, IP routing conf(iguration), IP routing table, SNMP.

Control network – In-band servers

Following the In-band servers link, you’ll be able to configure the in-band servers, which are needed in at least one of the units of the training network. To add a DLE server click on the ‘Add’ button. Set the **Administrative status** in the drop-down menu to value ‘**Up’** and select the recommended DSTI (as long as it is unique in the network).It is suggested to use a backup server, in case communication with the regular server is lost or degraded. Add proper DSTI (DTM service type instance) numbers throughout the network. This identifies service, port and interface.

Click *Apply* if you want to do more changes or *OK* if you are done.

The Advanced link takes the user to a page, from where the parameters of the exponential back-off algorithm are controlled. Reconnect time out has a **Minimum interval** of 10 ms; the starting value of the algorithm. After a tear down of the connection, the node tries to re-establish the connection immediately. In case of failure, it waits 10 ms before retrying. **Maximum interval** (default value 50000 ms = 50 s) is the end value of the algorithm, and can be set from here. The re-establish mechanism then waits no longer than 50000 ms to re-establish a channel.

Selecting the Precedence tickbox before clicking on the ‘Apply’ button makes this connection prioritized in case of node shutdown. It is removed early and reconnected early from another node. Obviously, there must be a backup In-band server in this case.

The Destinations link goes to peering DLE servers, i.e. DLE servers on the same hierarchical level, used for redundant multiple DLE servers.

Control network – In-band clients

An In-band client must be configured on every node in the DLE segment, including any node(s) with In-band server. Click on the In-band Clients link and subsequently on the ‘Add’ button. The Administrative status can be set in the roll down menu to ‘Up’. Also set (client) DSTI, Server DTM address and (server) DSTI. If a backup server is installed it too must be configured with Server DTM address and (server) DSTI as well. In addition to these parameters, the time of idleness before an unused connection is torn down as well as the client-to-client and client-to-server capacity must be specified. To activate the settings, click on either of the ‘Apply’ or the ‘OK’ button.

The Advanced link takes the user to a page, from where the parameters of the exponential back-off algorithm are controlled. Reconnect time out has a **Minimum interval** of 10 ms; the starting value of the algorithm. After a tear down of the connection, the node tries to re-establish the connection immediately. In case of failure, it waits 10 ms before retrying. **Maximum interval** (default value 50000 ms = 50 s) is the end value of the algorithm, and can be set from here. The re-establish mechanism then waits no longer than 50000 ms to re-establish a channel.

Selecting the Precedence tickbox before clicking on the ‘Apply’ button makes this connection prioritized in case of node shutdown. It is removed early and reconnected early from another server node. Obviously, there must be a backup In-band server in this case.

Control network – IP interfaces

Following the link IP interfaces, the physical Ethernet address of the node interface, **eth0** and the added DLE client, **dlec1** are presented. To set or modify the address, click on the interface Id of the interface that should be modified. Click on the ‘Add address …’ button and enter the IP address and the netmask. Click on the ‘OK’ button.

Control network – IP routing configuration and table

Following the link IP routing conf**,** IP gateways can be set.

Destination: is the destination IP network that the route will use.
Netmask: is the network mask to apply for the destination network.
Gateway: is the IP address of the node that is connected to the other network.

In order to enable routing outside an In-band segment, routes have to be configured. Some default routes are always configured in a node, e.g. to the subnet of a configured Ethernet interface, and to the loopback interface. To set up a route for all other traffic, click on the Add route … link. Enter **Destination** IP address, **Netmask** and the IP address of the **Gateway**. Click **OK**.

A click on the link IP routing table display all defined IP routes.

Control network - SNMP

Configuration of SNMP (Simple Network Management Protocol) parameters is made from the SNMP link.

The **Read-only** community name is the community name for SNMPv1/v2c read (i.e. get) operations. If this name is defined, then get operations using this community name is accepted, while write (i.e.

set) operations are not accepted.

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

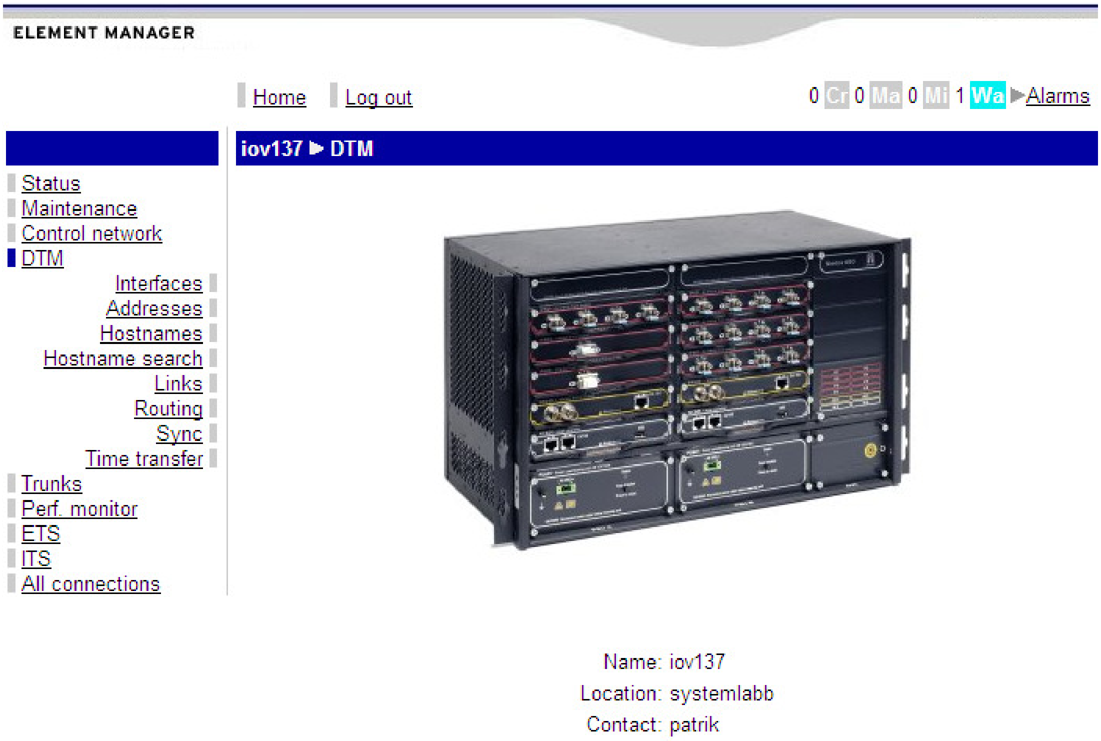
The **Notification** (trap) community name is the community name used when notification are sent. If this name is defined, notifications are sent as SNMPv2 traps with this community name.

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

Authentication key is the password used for SNMPv3 authentication of the SNMPv3 user. If empty, then the authentication check is disabled, e.g. the security level is set to 'noAuthNoPriv'. If it is defined, without a defined Privacy key, then only the authentication check is done, not encryption, e.g. the security level is set to 'authNoPriv'. If both Authentication and Privacy keys are set, then an authentication check is done and the data is encrypted, e.g. the security level is 'authPriv'.

IP address: Shows the IP address of all configured SNMP trap subscribers. To add additional trap subscribers, use the 'Add SNMP notification receiver …' button.

DTM menu



Name: iov137
Location: systemlabb
Contact: patrik

Figure 4. DTM menu in web browser.

Setting the DTM address

Please click on the DTM link to the left and then on the Addresses link.
Here you can set the DTM address for the node. To define a new address, click on the link Add addresses... above the address table. When you specify the DTM address, select 'Yes' from the Primary address roll down menu, if you want this address to be the widely used DTM address of the node in the DTM network.

When the DTM address is defined, save the configuration and reboot the node. You must reboot the node as otherwise the other nodes are unaware of its existence. As you can see there is also a predefined Loopback address (00.00.00.00.00.00.00.01), which goes to the backplane. This address can be compared to the IP address 127.0.0.1 (IP loopback address).

Defining the link

Click on the (DTM) Interfaces link to the left. To define the interface, click on the interface Name link**,** e.g. dtm:2:1. Here you can set up the link class of the link.

Link class is set to one of:
Normal: All channels are torn down if the link fails or the neighboring node stops responding (default choice).

Persistent: When the neighboring NC stops responding, all existing channels to and from that NC will be preserved. If the link fails in either direction, all channels in both directions will be torn down.

Nailed: When the neighboring NC stops responding, all existing channels to and from that NC are preserved. If the link fails in either direction, all channels in both directions will be preserved.

The control channel capacity is normally set to 0. Regardless of this setting, the control channel always use slot 0 in the DTM link. The number entered is the additional control channel capacity requested.

You could also set the interface metric (Metric = Cost to use this interface) for DRP (dynamic routing protocol) here. To activate the dynamic routing protocol (DRP) the 'Enable' tick box must be selected.

In the advanced settings section, the first and last slot of the link can be defined. Normally, they should be one and one less than the transmit capacity of the link.

After making all configurations and changes, the Administrative status should be set to up. Clicking on the 'Apply' button now makes the configuration active. Note that changes can only be made with Administrative status set to down. To modify a made setting, rather than doing it in two steps, the 'Toggle admin' tick box can be selected before either of the 'Apply' or 'OK' buttons are selected.

Restart Neighbor button: This button can be used when the link is set to Persistent. A click on this button sends a signal to the neighboring node on the other side of the DTM link, telling it to resume to normal operation if it is in Operational state NoControl. In this case, all the channels are torn down in the node. If the Operational state is 'Up' in the neighboring node, the restart command is ignored.

There are two alarms shown on this page:

Failure on underlying interface alarm: An error reported by the underlying trunk interface (LOF, loss of frame.).

Reduced control capacity alarm: The control capacity (bandwidth) requested cannot be allocated by the network.

Link overview

To get an overview of all links from the node, click on the Links link on the left side.
Here all links to and from the node are presented.

Id: dtm3:1/rx and dtm3:1/tx , is the Id given to the interface. The first number identifies the slot position, the second number identifies the port position on the module and rx or tx identifies if it is a receiver or a transmitter.

I/F MAC addr: Lists the MAC (Media Access Control) address of the DTM interface.

Node MAC addr: Lists the MAC address of the node.

Node addr: Shows the DTM address or the host name of the node.

Oper: Shows the operational state of the interface.

Last changed: Shows when the operational state of the interface was last changed.

Routing overview – static routes

Click on the Routing link. This displays all defined Static routes and additional ones can be entered here. In addition, this is where DRP is turned on or off.

Static routes: To add a static route, click on the ‘Add route’ button. Fill in the following entries:

Adm: The administrative status is ‘Up’ when the route is set to be active, and ‘Down’ if the operator wants the route deactivated, e.g. when testing.

Type: Static is typically selected for static routes. Link prefix and Area prefix routes are used for static routes in border nodes between areas, and are only needed in large networks. They are a bit intricate, and not described in detail in this document. Usage of link prefix routes is discouraged.

Destination: The address or name of the remote node or network.

Prefix: Number of significant bits (0-64 bits).
E.g. Prefix 56 = FF.FF.FF.FF.FF.FF.FF.00

Next hop: DTM address of neighboring node.

Metric: The cost associated with passage through the node (node metric), by this route. This cost is distributed in the network, together with the route, and used by the dynamic routing protocol for establishment of further channels. The lowest cost alternative route is selected, if several routes are available.

Routing overview - Dynamic routing

To turn on the dynamic routing protocol, click on the Dynamic routing config link.

Variables Node Metric and Interface Metric must be entered for all interfaces.

Node Metric is the cost associated with passing through the particular node.

Interface Metric is the cost associated with passing through a specific DTM interface.

These costs are added by the network when routes are selected and channels established. The lowest cost route is used for freshly set up channels.

Under the heading ‘Advanced’ some additional settings are made:

The node has to be set as either a **Switch node** or an **End node**. Normal usage is switch node, and end node usage is discouraged if the node is connected to more than one other node directly (or if such usage is planned). End node usage can be employed if a node is attached to the rest of the network with a single point-to-point link. It then doesn’t need a complete routing table, only a single routing entry to the peer on the point-to-point link.

In addition, the following variables can be set:

Area number: A large network can be configured as several areas, with different area numbers. Routing information is then only distributed within an area, not between areas. In order to connect nodes in different areas, static routes between the areas must be set up.

Detect from neighbors: Ticking this box (and the ‘Apply’ button) causes the node to find its area identity from the peer of the DTM link. In a network without defined areas (when all nodes belong to the same area), this can be used. In all other cases, this usage is discouraged.

When choosing a node as End node, one additional option is available.

Detect default gateway: A default gateway is found by the node automatically. This option is only relevant for end-nodes, but is ticked and grayed out for switch nodes.

DTM synchronization

Click on the Sync link**.** The sync page is used to monitor the synchronization of the DTM unit and to modify external clock settings. A list of the interfaces displays all available clocks, current sync source and current backup.

Prio (Priority) 15 is used for the internal clock and Prio 0-14 is used for external synchronization. The lower the number is, the higher the priority it has.

DTM Hostnames and hostname search

Click on the Hostnames link. DTM addresses can be translated to host names for easier recognition on this page. Click on the Add entry … link and enter DTM address and the chosen host name. Observe that in order to work, the entry has to be made in all nodes.

It is suggested that the hostnames have a structure similar to IP addresses, like node10.academy.netinsight.se.

The link Hostname search … allows you to define suffixes to hostnames, so that an unrecognized host name is looked for by adding the suffix to the name. For example, if the previously defined node (node10.academy.netinsight.se) is called node10 when a route is defined, this is initially not recognized by the system. If, in the hostname search list, an entry of ‘academy.netinsight.se’ has been made, the system looks for node10.academy.netinsight.se when it doesn’t find node10.

Note:	The host names of the nodes must be entered in all the nodes! The hostname search list must be entered in all nodes!

DTM Time Transfer

This function requires a separate firmware license and is currently only available in Nimbra 360 and Nimbra 680/688 nodes.

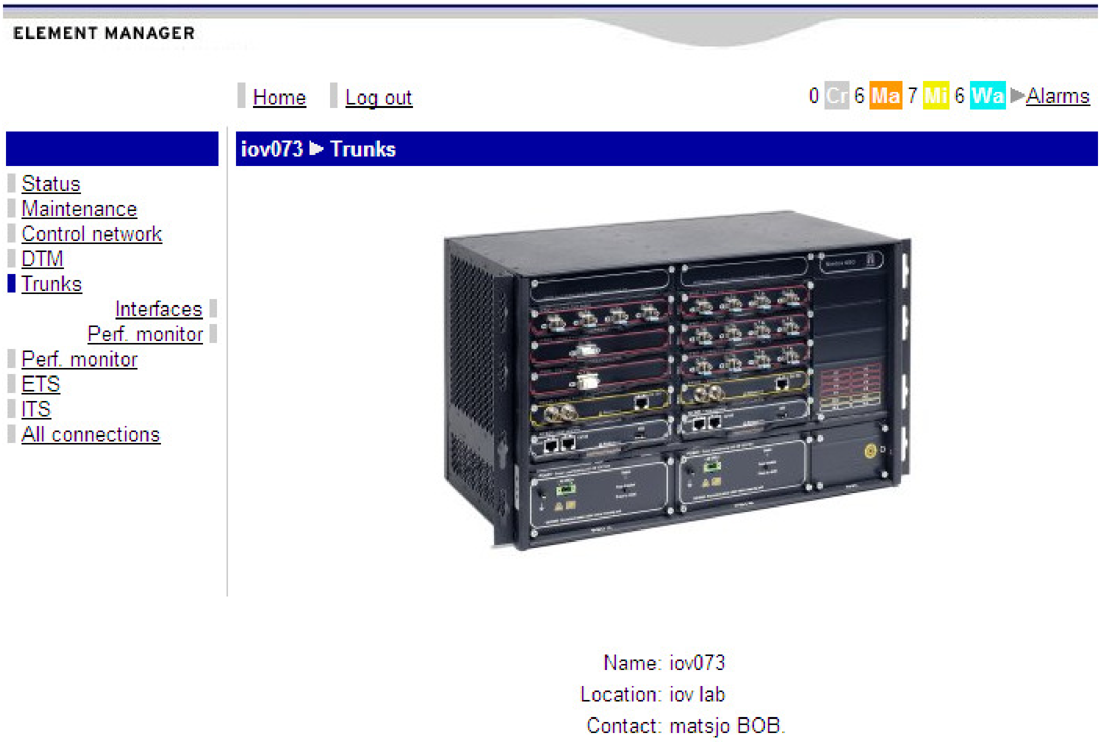
Click on the Time transfer link. A list of available time sources and their operational status is shown. The time source currently used for the time transfer function is shown with operational status up. A time source with admin status down or lacking a channel is shown as down. A time source that is potentially useable as time transfer source for the node is shown as dormant. Such a source is potentially used by other nodes as time transfer sources. Finally, a source where the DTM link or other higher level function has administrative status down or a source which is lacking a higher level resource, gets operational status ‘LowerLayerDown’.

The selection of active source is made by the network and can’t be set by the operator.

Trunks menu

Trunks - interfaces

Click on the Trunks link, followed by the Interfaces link. Here all the physical interfaces are presented. The trunk interface manager supports 8b10b and SONET/SDH class of interfaces.



Name: iov073
Location: iov lab
Contact: matsjo BOB.

Figure 5. Trunks menu in the web browser.

The main functional areas covered by the manager are: Trunk interface configuration, Trunk interface alarm administration and PMM support for trunk interfaces.

Name: The physical name of the module. Sonet/sdh-5:1, 8b10b-3:1.
Mode: Shows the mode of the interface.
Capacity: The capacity of the module 2488.320 Mbit/s, 1000.000 Mbit/s
Oper: Operational state of the interface; Up or down.

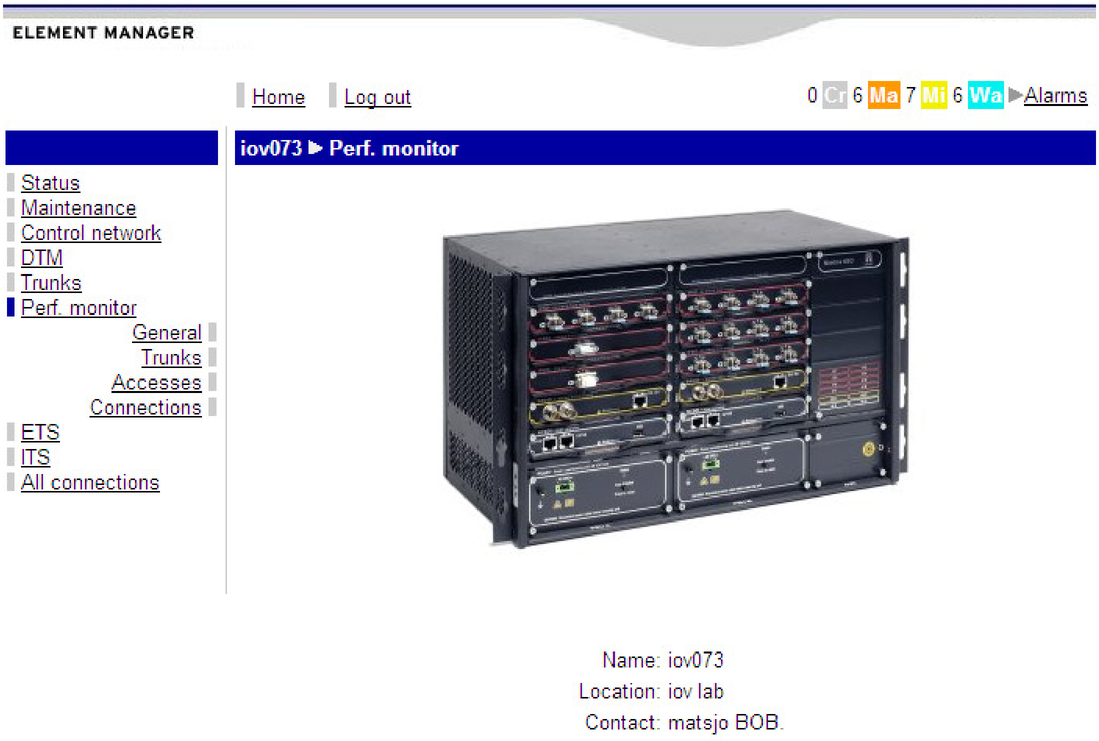
Click first on the link to the **Name** of the interface (e.g. sonet/sdh-5:3). Continue by configuring the alarms. Suppress alarms (all, AIS, RDI) as desired. Set advanced SONET/SDH parameters according to the table below:

Parameter name	Description
H1 SS bits	Differences between Sonet and SDH. Sets value of the SS bits in the H1 byte in the Sonet/SDH section overhead. Older Sonet/SDH equipment may require other value than the default : 00 Sonet, 10 SDH
POH C2 byte:	Path overhead C2 = DTM (Type of network ATM/DTM.)
Signal failure filter period	Delay time for 1+1. The time that the nodes waits for underlying network (SDH/SONET/WDM) to re-establish connection, in order to avoid a switch over. This parameter can also be used to allow certain amount of errors without tearing down channels or a certain trunk.
Degraded defect (DEG) period	Configuration parameters for the “Degraded” alarm, according to ITU G.806 for the interface. Period, default 5 sec.
Degraded defect (DEG) threshold	Configuration parameters for the “Degraded” alarm, according to ITU G.806 for the interface. Number of block errors. Default 1200.

On 8B/10B trunks, configuration is much simpler. All alarms can be suppressed and the signal failure filter time can be set.

The link Perf. monitor, in the Trunks menu, is identical to the link Trunks in the Perf. Monitoring menu, and is described with all other performance monitoring below.

Performance monitoring menu



Name: iov073
Location: iov lab
Contact: matsjo BOB.

Figure 6. Performance monitoring menu in the web browser.

A contract between an end-user and an operator regarding a service in a telecom network often contains some kind of service level agreement (SLA). The SLA may for example state a minimum level of quality in terms of transmission characteristics and availability on a leased connection.

The process of actively checking these and other parameters in a telecom network is called performance monitoring. The measured parameters and measurement intervals are modeled after the ITU-T standard G.826. This includes the collection of parameters describing both small anomalies as well as periods of unavailability. It also allows the possibility to collect performance data for both short and long intervals.

It is only the connections across the DTM network that are monitored If an end user has a problem with the signal in the end-equipment, the PM function can be used to isolate the problem to be either within the DTM network or outside it.

Following the General link, the user may set the size of the small and large history log.

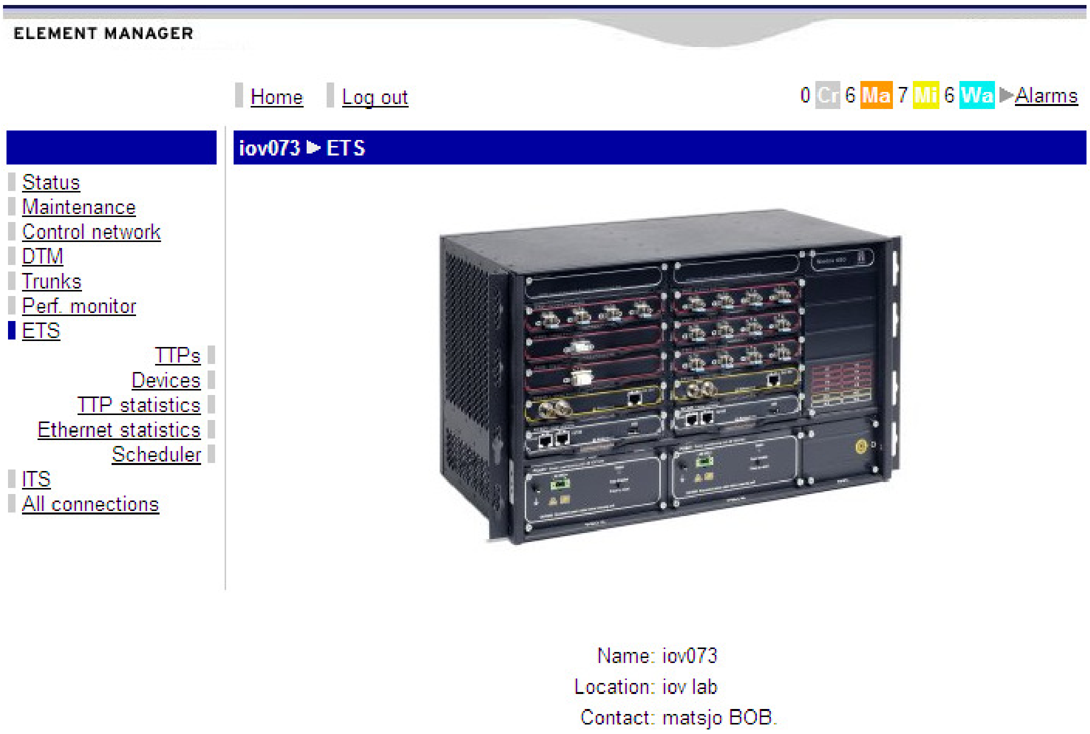
Following the Trunks link, the user is presented with a table of available trunks and their respective performance values. Performance monitoring can be configured by clicking on the link for a particular trunk and then clicking on the link Configuration.

Following the Accesses link, the user is presented with a table of available accesses and their respective performance values.

Following the Connections link, the user is presented with performance data on all links terminating in the node. Configuration is made in the same way as for trunks.

ETS (Ethernet Tunneling Service) menu

From the ETS menu, both unicast and multicast services can be configured.



Name: iov073
Location: iov lab
Contact: matsjo BOB.

Figure 7. ETS menu in web interface.

Unicast

A schematic picture of an ETS tunnel is shown below. It consists of two DTM channels, one in each direction. These channels are used for sending packets between the Ethernet ports at node X and node Y.

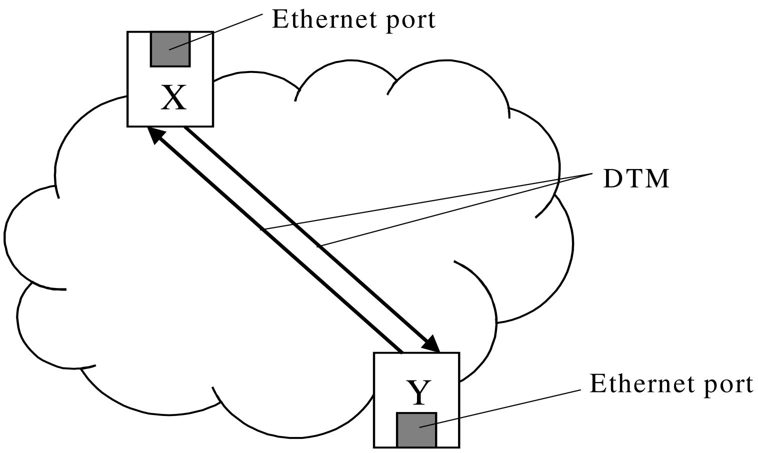


Figure 8. An illustration of an Ethernet tunnel through a DTM network.

The unicast connection is set up in several steps. First the TTP is configured, then the VLAN is configured and then the device is configured.

In order to set up an Ethernet tunnel, links ETS and subsequently TTPs should be used. From the TTPs menu, you can create either unicast or multicast connections. The menus are described under separate headings.

For a unicast connection, the configuration must be done at both nodes of the connection.

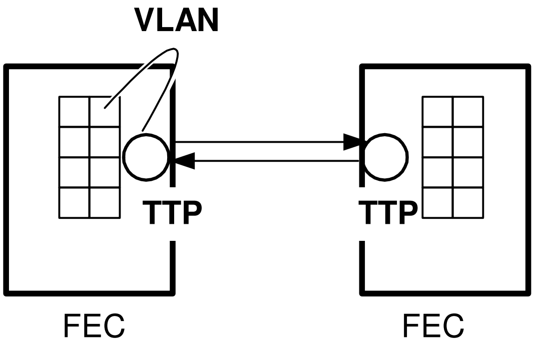


Figure 9. Creation of a virtual LAN between two 10/100 Ethernet ports.

The following links are available from the ETS menu.

TTPs (Trail Terminating Points): This link gives the user a list of all defined TTPs, as well as a starting point to define new ones.

Devices**:** Modules to be configured (FEC or GEC).

TTP Statistics**:** Statistics of the originating and terminating connections regarding traffic and used bandwidth of the connections.

Ethernet statistics**:** Ethernet statistics on the device, separated on the different interfaces.

Scheduler: Scheduler of the ETS, described under All connections, scheduler.

In order to set up a unicast connection, proceed as follows:

Navigate to the TTPs link and click on the ‘Create Unicast’ button. Here you enter the DSTI (DTM Service Type Instance) and the requested capacity for the transport. Fill in the DTM address to the destination node and its DSTI (It’s a good idea to choose the same DSTI for destination node and source.).

Example of a configuration:

Administrative Status: Up
Customer ID: 100
Purpose: VLAN
DSTI: 100
Destination DTM node: 00.00.00.00.00.01.10.80
Destination DSTI: 100
Connection shall as default be: Established
Requested capacity: 10 (May be asymmetric)
Select **Source routes**, if such are chosen.

To configure the device, click on the link Device. Proceed with the link to the specific device, e.g. 4**.** First, you create the VLAN. Click on the ‘Add VLAN...’ button at the bottom of the page. Fill in the entries.

Example:

TTP name: 1 (Will Show TTP name ets1)
Customer: 100
Purpose: Unicast VLAN
VLAN id: 1

Select the interface on the device that the packets are using for this particular VLAN. Also, select if the packets should be tagged or not and click on the ‘OK’ button. The VLAN is now defined.

To finalize the connection configuration, click on link to the specific interface (like eth6:1). Here you can set the interface parameters.

Example

Administrative status: **Up**
Flow control enables flow control for Ethernet. Tick as appropriate.
Tick **Auto-negotiation protocol (NWay)** if selected.
This setting determines if the interface uses the NWay auto negotiation protocol or not. If it is set to yes, there is an exchange of information between the interface and its link partner. The highest common speed and duplex (preferred to half duplex, which in turn is preferred to simplex) is selected and the interface is configured to use these settings.
Selected Speed: Autoselect is automatically chosen if NWay is enabled.
Selected Duplex: Autoselect is automatically chosen if NWay is enabled.
Default VLAN: You can also choose default on VLAN, the VLAN to which untagged packets go. Alternatively, the “Drop untagged packets” tick box may be selected. Click on the ‘OK’ button.

Multicast

An ETS-multicast connection is connecting several TTPs (Trail Termination Points) to one source.

A multicast connection is most conveniently set up starting with the source. Click on the TTPs link. Click on the 'Create multicast …' button. Here you enter the DTM Service Type Instance (DSTI) and the requested capacity for the transport.

Example:

Customer ID: 150
Purpose: Multicast VLAN
DSTI: 150
Connection shall as default be: Established
Requested capacity: 0.400 Mbps
Click on the 'Apply' or 'OK' button.

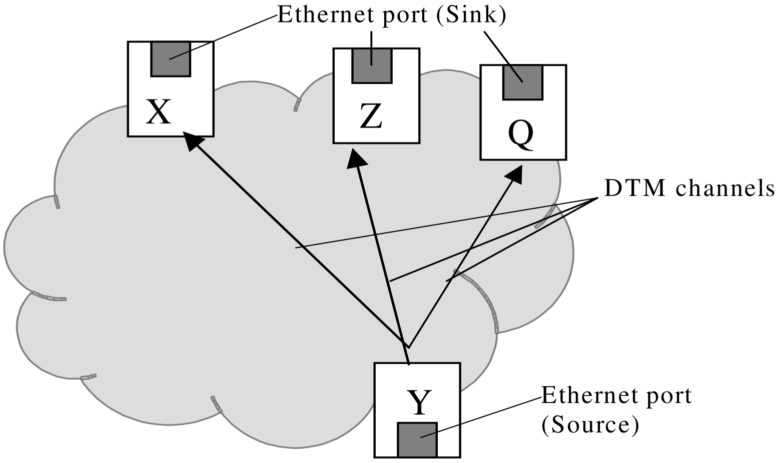


Figure 10. ETS multicast

To add a destination, click on the link Destinations and then on the link Add Destinations… . Here you'll be able to add destination nodes.

Destination DTM node: 00.00.00.00.00.01.10.80
Destination DSTI: 150
Select Source routes, if such are wanted. Using source routes makes it possible to specify all or some of the nodes employed by the connection. See the description under the 'All connections menu' section.

Click on the 'OK' button if no more destinations are needed or on the 'Apply' button to select another destination.

In order to define the VLAN used, click on the Devices link. Click on the specific Device. Here you can create a VLAN. Click on the 'Add VLAN …' button. Fill in the entries.

Example:

TTP name: 0, 1, 2 (Shows up with TTP name ets0, ets1, ets2...)
Customer: 150
Purpose: Multicast VLAN

VLAN tag: 5

“Interface Packets leaving interface are”, means from which interface port on the module the packets of this particular VLAN passes. Select the appropriate interface and if the packets should be tagged or not. Click the ‘OK’ button to make the setting.

Diffserv

Diffserv user priority is supported according to the standard for prioritizing IP-packets based on information in the IP DSCP field, RFC2474 and RFC2475. If diffserv is used, a Flow Group mapping must be specified with values between 0 and 7 for all flow groups. Note that configuration of priority should only be performed if it is used in the network. The default settings is to force traffic class = 0 for all frames.

The Advanced link
Before changing max and min settings in the advanced link in a production network, please consult Net Insight support.

Navigate to the TTPs link in the ETS menu and click on one of the TTPs on the middle of the page. Continue by clicking on the ‘Advanced’ link. The settings are:

Minimum interval: The start value of the algorithm (Default10 ms). After a tear down of the connection, the network tries immediately to re-establish the connection; if it fails it retries after 10 ms.

Maximum interval: The end value of the algorithm. The re-establish mechanism waits no longer than this value (in ms) to re-establish a channel. The default value is 50000 ms.

Precedence: A tick in the precedence tick box gives the connection priority over other channels. They are torn down faster and should be reestablished sooner in case of node failure. At the most five per node are recommended.

The Priority link

From the TTPs link, click on one of the TTPs. Continue and click on the mid-page Priority link. Here diffserv (described above) or Ethernet priority can be selected. 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.

ITS (Isochronous Transport Services) menu

General

The ITS link handles all Isochronous Transport Services i.e. ASI, SD-SDI and HD-SDI transport service, PDH transport service and AES/EBU audio transport service. ITS can be used to create various types of tunnel over the DTM network.

The illustration below shows a video tunnel.

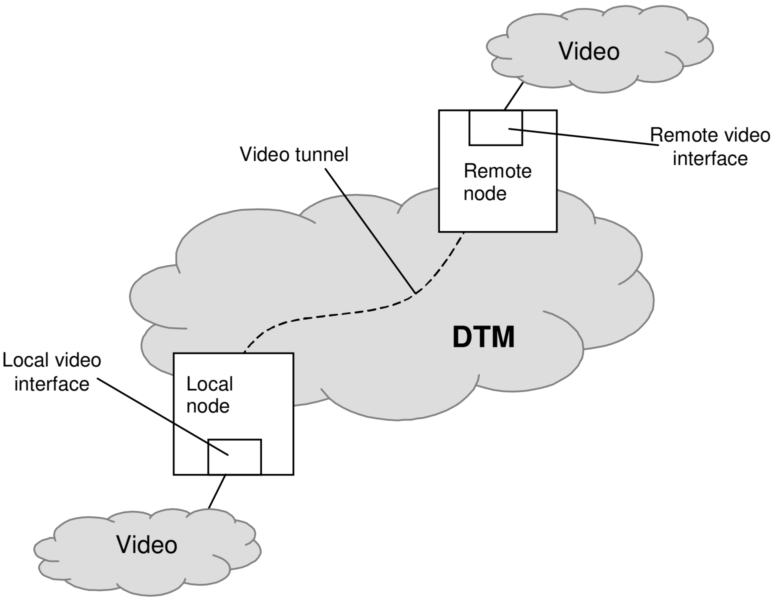
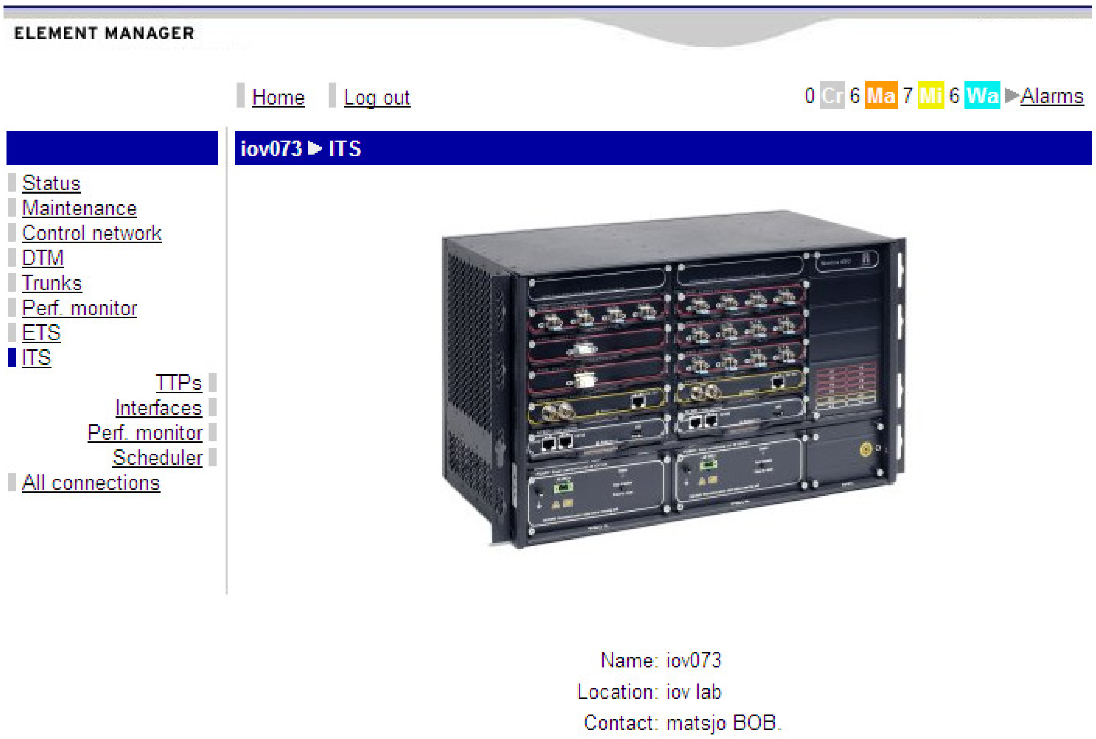


Figure 11. A video tunnel through a DTM network.



Name: iov073
Location: iov lab
Contact: matsjo BOB.

Figure 12. The ITS menu.

To create any type of ITS connection, click on the ITS link, followed by the TTPs link. Here you'll be able to define the connection as Originating or Terminating as well as the connection mode (Unicast or Multicast).

Unicast

To create a unicast service, click on the ‘Add TTP …’ button and fill in the entries and click on either the ‘Apply’ or the ‘OK’ button. Example:

Type: Can be selected as either originating (source) or terminating (drain)
Local interface: All available services for the local interface ports are shown in the roll-down menu.
Mode: Can be selected as either Unicast or Multicast.
Click on the ‘Add’ button to complete the setting.

For an SD-SDI interface, fill in the parameters:

Administrative status: Up
Customer ID: 2
Purpose: SDI unicast
Local Interface: sdi-3:1
DSTI: 15
Destination DTM node: 00.00.00.00.00.01.10.80
Destination DSTI: 2
Connection shall as default be: Established (Available choices are shown)
Requested capacity: 270 Mbps (Available choices are shown)

Click on the “Apply” or “OK” button to make the setting.
Repeat this interface definition on the terminating node as both interfaces must be defined.

Multicast

To create an ASI, SD-SDI, HD-SDI, AES/EBU or other multicast connection, click on the TTPs link. Here you’ll be able to define the connection type as either originating or terminating and the connection mode to Unicast or Multicast. Select originating connection type and multicast mode. Select an appropriate port and click on the ‘Add’ button.

Set the **Administrative status** to Up and enter additional parameters, like:

Customer ID: 3
Purpose: ASI
Local Interface: ASI 5:1
DSTI: 3
Connection shall as default be: Established (Available choices are shown)
Requested capacity: 270 Mbps (Available choices are shown)

Click on the “Apply” or “OK” button to make the setting of the originating node.

In order to configure the destination interfaces, click on the Destinations link and subsequently on the ‘Add destination …’ link. Enter node data, like

Administrative status: Up
Destination DTM Node: 00.00.00.00.00.01.10.80
Destination DSTI: 3

Use source-routes if needed. Typically, such static routes should be avoided.

Add the remaining nodes in the Multicast connection.

Click on the ‘OK’ button until you can see all the originating and terminating nodes.

Following the link TTPs from the ITS menu, the user sees all originating and terminating ITS connections in the node. The headings shown are:

TTP name: A name of the TTP that you have decided.
I/F name: A structured interface name, including type of interface, slot position and port position on the module.
DSTI: 3 (DTM Service Type Instance, a number chosen by you.)
Customer ID: A unique customer number, like 3
Purpose: String entered by the user
Mode: Uc (Unicast) or Mc (Multicast).
Admin: Administrative status, can have values ‘up’ or ‘down’
Oper: Operational status, can have values ‘up’, ‘down’ or ‘dormant’ (no incoming physical interface exists)

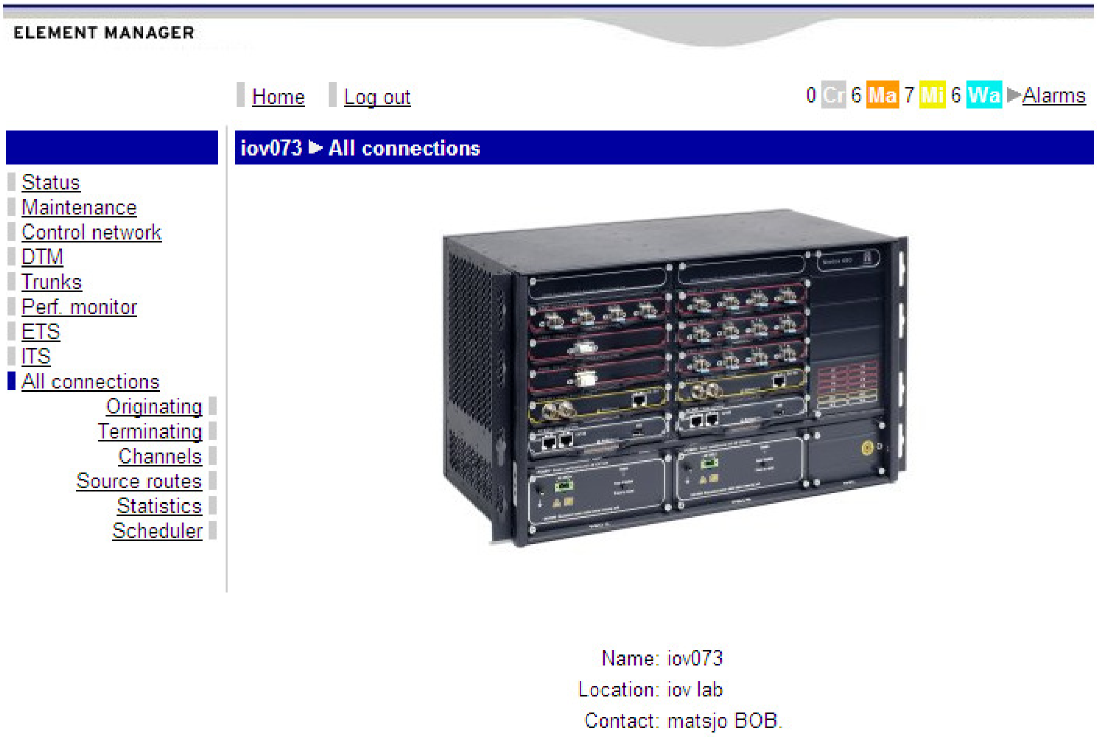
Terminating node

To configure the terminating side of an ITS connection, log in on the terminating node, click on the ITS link and then on the TTPs link. From here, follow the Add TTPs … link. Select type as terminating and fill in the local interface from the drop-down menu. Click on the ‘Add’ button to define the TTP. A new web page comes up, with additional settings.

Administrative status: Can be ‘up’ or ‘down’, but is as default set to ‘down’. It must be set to ‘up’ for the connection to be active.
Customer ID: A unique customer number, like 3
Purpose: String entered by the user, like ASI
Local Interface: Type of interface and port used. It is selected from a roll-down menu, e.g. sdi-5:1
DSTI: 3 (DTM Service Type Instance, a number chosen by you.)
Suppress alarms: Selected from a drop-down menu. Can have three values, ‘None’ = no alarm suppression, ‘Warning’ = alarms with severity warning are suppressed, ‘All’ = all alarms are suppressed.

Click on the ‘OK’ button when the settings are made.

All connections menu

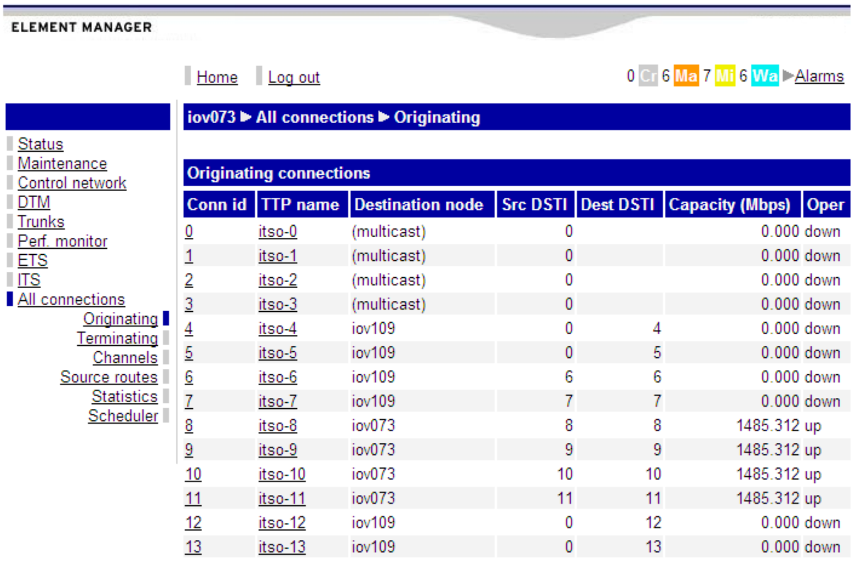


Name: iov073
Location: iov lab
Contact: matsjo BOB.

Figure 13. All connections menu in the web browser.

Under this heading, a number of various links appear. Most of them handle connections in one form or another, but source-routes and scheduling is configured from here as well. In addition, total data amount and current bandwidth can be found for all connections.

The Originating link displays a list of all connections originating in the node. By clicking on the name of the TTP, the configuration can be modified.



Originating connections

Conn id	TTP name	Destination node	Src DSTI	Dest DSTI	Capacity (Mbps)	Oper
0	itso-0	(multicast)	0		0.000	down
1	itso-1	(multicast)	0		0.000	down
2	itso-2	(multicast)	0		0.000	down
3	itso-3	(multicast)	0		0.000	down
4	itso-4	iov109	0	4	0.000	down
5	itso-5	iov109	0	5	0.000	down
6	itso-6	iov109	6	6	0.000	down
7	itso-7	iov109	7	7	0.000	down
8	itso-8	iov073	8	8	1485.312	up
9	itso-9	iov073	9	9	1485.312	up
10	itso-10	iov073	10	10	1485.312	up
11	itso-11	iov073	11	11	1485.312	up
12	itso-12	iov109	0	12	0.000	down
13	itso-13	iov109	0	13	0.000	down

Figure 14. All connections, originating listing.

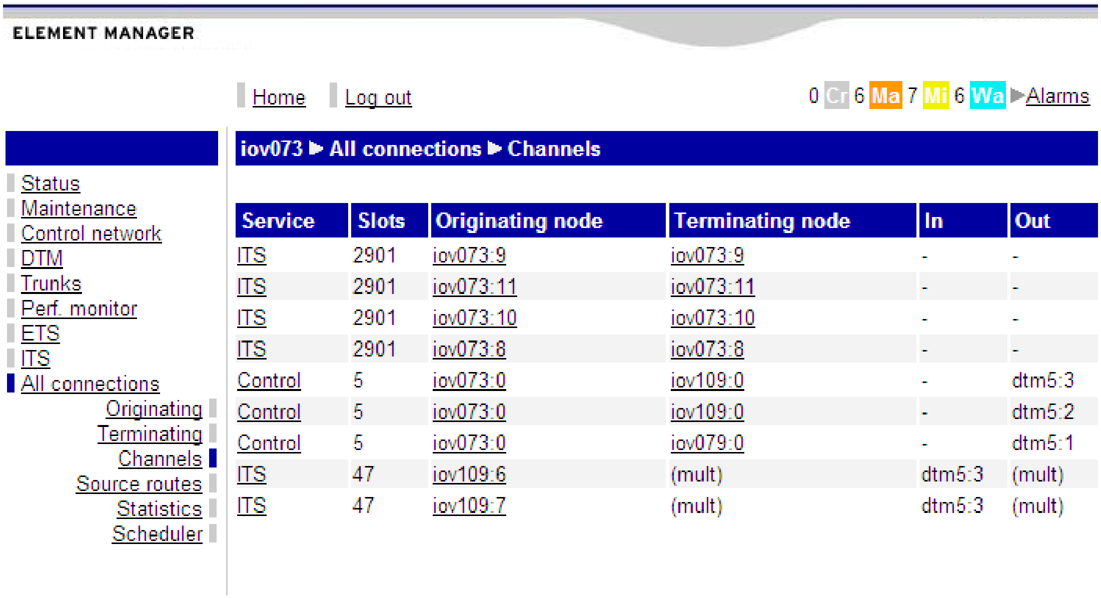
The headers are:

Header	Explanation
Conn id	Connection ID, a connection identifier
TTP name	Trail Termination Point (name), provided by the user at creation of the connection
Destination Node	Remote node
Src DSTI Source node.	DSTI (DTM Service Type Instance) at the source node
Dest DSTI	DSTI (DTM Service Type Instance) at destination
Capacity (Mbps)	Bandwidth reserved by the user
Oper	Operational status of the connection. Can be set to up, down or dormant (lacking physical interface)

Table 1. Common headers in all connections, originating and terminating web menus.

Following the Terminating link, a list of all connections terminating in the node is displayed. The headers follow the example of the Originating link described earlier.

Clicking on the Channels link, the user is presented with a listing of all channels originating at the node, passing through the node and terminating at the node.



Service	Slots	Originating node	Terminating node	In	Out
ITS	2901	iov073:9	iov073:9	-	-
ITS	2901	iov073:11	iov073:11	-	-
ITS	2901	iov073:10	iov073:10	-	-
ITS	2901	iov073:8	iov073:8	-	-
Control	5	iov073:0	iov109:0	-	dtm5:3
Control	5	iov073:0	iov109:0	-	dtm5:2
Control	5	iov073:0	iov079:0	-	dtm5:1
ITS	47	iov109:6	(mult)	dtm5:3	(mult)
ITS	47	iov109:7	(mult)	dtm5:3	(mult)

Figure 15. All connections, channels web page.

Header	Explanation
Service	Type of service, ITS, ETS or Control channel
Slots	Reserved bandwidth, expressed as slots (1 slot = 512 kbit/s)
Originating node	Source node for the channel
Terminating node.	Drain node for the channel
In	Originating interface, in originating node
Out	Terminating interface, in terminating node

Table 2. All connections web page, headers.

From the Source routes link, it is possible to create source routes, i.e. static routes not using DRP (DTM Routing Protocol). Click on Create and fill in the entries.

Name: A name decided by you.
Routing: Strict (all nodes are specified in the route) or loose (only some nodes are specified in the route).

Outgoing interfaces: Selected interface for the routing.
Nodes: Node(s) that the source route must pass.

The maximum number of source routes that can be used by any connection is three.

The link Statistics informs the user on all originating and terminating connections in the node. What is presented is

TTP name: Trail Terminating Point name
Conn id: An identifier of the connection
Octets: Number of octets (bytes) passed through the connection
Packets: Number of DTM packets passed through the connection
Used Mbps: Used bandwidth by the connection
Used %: Percentage of available bandwidth used.

Clicking on the Error statistics link at the top of the page, gives the user access to additional statistical numbers.

The Scheduler link takes the user to a scheduler menu, where a TTP can be scheduled to go active on a daily or weekly basis or booked for a particular one-time event in future. Enter the required parameters and click on the ‘Apply’ or ‘OK’ button.