



# **Net Insight Training Web interface**

## **Level 2**

November 2010

**Workbook  
NID3655  
A1**

This page is intentionally blank.

# Contents

<b>Introduction to Workbook .....</b>	<b>5</b>
Revision handling.....	5
<b>Lab. 1 Initial Parameters.....</b>	<b>6</b>
Settings for Tera Term (VT100 emulator).....	6
Serial Device Server – MOXAN Port 5610 .....	6
IP settings for Nimbra One/Nimbura 300 series .....	7
IP settings for Nimbra 600 series .....	8
<b>Lab. 2 DTM Address Configuration .....</b>	<b>10</b>
Initial network configuration.....	11
<b>Lab. 3 Configuration Handling.....</b>	<b>13</b>
Back up files .....	13
<b>Lab. 4 Hostnames .....</b>	<b>14</b>
<b>Lab. 5 Dynamic Routing .....</b>	<b>15</b>
Redundancy in DTM networks.....	16
Dynamic routing .....	17
<b>Lab. 6 Management with DLE .....</b>	<b>20</b>
In band Management (DLE).....	21
<b>Lab. 7 Internal versus external sync .....</b>	<b>25</b>
<b>Lab. 8 Time Transfer .....</b>	<b>27</b>
<b>Lab. 9 Source routes .....</b>	<b>29</b>
Source Routes .....	29
<b>Lab. 10 Streaming Services .....</b>	<b>31</b>
Asynchronous Serial Interface (ASI).....	31
Serial digital interface (SDI) .....	32
ASI Unicast .....	34
ASI Multicast.....	38
<b>Lab. 11 Ethernet Transport Service (ETS) .....</b>	<b>40</b>

ETS Customer mode (VLAN switching) .....	45
Lab. 12 Performance Monitoring .....	48
Performance Monitoring Set-up .....	48
Lab. 13 Scheduling of connections .....	50
Scheduling set-up .....	50
Appendix A - Start of PC .....	52

# Introduction to Workbook

In this workbook, it is described how two different lab groups work together with a problem oriented approach to configure certain nodes in the Net Insight Academy facility, located in Stockholm, Sweden.

This workbook is intended to be used together with Element Manager for Nimbra Networks. Element manager should be distributed together with this document, as a .pdf file.

## Revision handling – NID3655

Version	Date	Responsible	Comment
PA1	2010-11-16	Marco Basile/ Gunnar Larsson	First version

# Lab. 1 Initial Parameters

All Nimbra switches are delivered with boot monitor and operating system. When powered, the nodes start with pre-installed software. Parameters, which need to be entered at the initial start-up and their configuration, are described in this text. When Nimbra nodes are started for the first time, a serial connection is used for the initial communication with the node and node configuration. The IP network parameters are entered enabling subsequent remote communication via the Ethernet port/web interface.

## Goal

In this exercise you set the initial parameters of various Nimbra nodes.

All nodes should have assigned IP addresses, netmasks and gateways (if relevant). If more information is needed, use Element Manager.

To test if all settings have been made correctly, connect all Nimbra nodes to the Ethernet switch, as well as the configuring computers. From the computers, 'ping' to the nodes or connect to the http server residing on them by typing the IP address in the URL window of the web browser.

## Settings for Tera Term (VT100 emulator)

From a VT100 terminal emulator (e.g. Tera Term, Hyper terminal), log in via the serial interface port. 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. If there is no DSUB-9 connector on the PC, the serial port of the PC has to be adapted to the serial port of the Nimbra by other means. In this case, please contact Net Insight. The other end of the adapter has a female RJ-45 port and should be directly connected to the serial port of the Nimbra node with a regular, straight Ethernet cable.

The communication settings are:

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

## Serial Device Server – MOXAN Port 5610

All nodes in the Net Insight Academy facility, located in Stockholm, are also connected to a MOXA NPort® 5610-16 rackmount device server that can conveniently and transparently connect the node's serial interface to an Ethernet, allowing you to network the serial devices using "Reverse Telnet Mode".

That means that, via the Serial Device Server (IP 192.168.234.222), you can transparently connect to the serial port of a Nimbra node with a Telnet

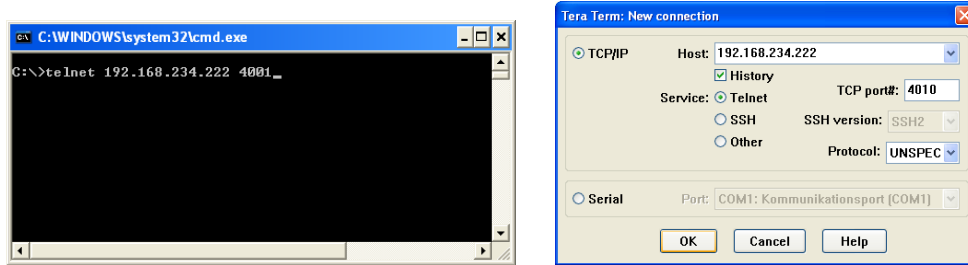
session using a port number specific for the node you want to reach (4001 for node1, 4002 for node2, 4010 for node10, etc).

### Serial port of a Nimbra node via Serial Device Server

Connect to the serial port of a Nimbra node by issuing the command

```
telnet 192.168.234.222 40[nodeId]
```

e.g. for node1 and node10



### **IP settings for Nimbra One/Nimbra 300 series**



Connect a straight Ethernet cable to the serial port of the Nimbra node. Connect the other end of the cable to an RJ45-RS232 adapter, NPA0006-0001, which is already connected to a regular DSUB-9

serial port (like COM1) on your working computer.

Open a VT100 terminal emulator, with settings given above on the PC, and hit the **Enter** key

Alternatively you can log on to serial port of the Nimbra node using the Serial Device Server with Reverse Telnet Mode according the instruction given above.

The default user name/password combination is `root/neti`.

#### List IP registry

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.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:11:49:7f"
.ipconf.if.0.mtu              1500
```

This is true for nodes with system release software version GX4.7.0.0 and later. Earlier versions do not have a set IP address.

### Set the IP address and subnet mask

If it is not already present (prior to GX4.7.0.0), create the address structure `ipconf.if.0.address` with the following command:

```
resedit create -n ipconf.if.0.address
```

Subsequently set the IP address and subnet mask with the following commands

```
resedit set -n ipconf.if.0.address.0.inet -v xxx.xxx.xxx.xxx  
resedit set -n ipconf.if.0.address.0.netmask -v yyy.yyy.yyy.yyy
```

`xxx.xxx.xxx.xxx` is the IP address

`yyy.yyy.yyy.yyy` is the subnet mask.

## 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.

Alternatively you can log on to serial port of the Nimbra node using the Serial Device Server with Reverse Telnet Mode according the instruction above.

The default user name/password combination is `root/neti`.

### List IP registry

List current IP registry with (the reply from the node is an example)



```

resedit get -r -n ipconf

.ipconf
.ipconf.if
.ipconf.if.0
.ipconf.if.0.name      "eth-aux"
.ipconf.if.0.address
.ipconf.if.0.media
.ipconf.if.0.media.current      "autoselect"
.ipconf.if.0.media.active      "link down"
.ipconf.if.0.mac      "00:10:5b:20:2b:42"
.ipconf.if.0.mtu      1500
.ipconf.if.1
.ipconf.if.1.name      "eth-front"
.ipconf.if.1.address
.ipconf.if.1.address.0
.ipconf.if.1.address.0.inet      "192.168.125.125"
.ipconf.if.1.address.0.netmask  "255.255.255.0"
.ipconf.if.1.media
.ipconf.if.1.media.current      "autoselect"
.ipconf.if.1.media.active      ""
.ipconf.if.1.mac      "00:30:d6:02:b1:a8"
.ipconf.if.1.mtu      1500
.ipconf.routes

```

This is true for nodes with system release software version GX4.7.0.0 and later. Earlier versions do not have a set IP address.

#### Set IP address and subnet mask

If it is not already present (prior to GX4.7.0.0), create the address structure `ipconf.if.1.address` with the following command:

```
resedit create -n ipconf.if.1.address
```

Subsequently set the IP address and subnet mask with the following commands:

```

resedit set -n ipconf.if.1.address.0.inet -v xxx.xxx.xxx.xxx
resedit set -n ipconf.if.1.address.0.netmask -v yyy.yyy.yyy.yyy

```

`xxx.xxx.xxx.xxx` is the IP address

`yyy.yyy.yyy.yyy` is the subnet mask.

# Lab. 2 DTM Address Configuration

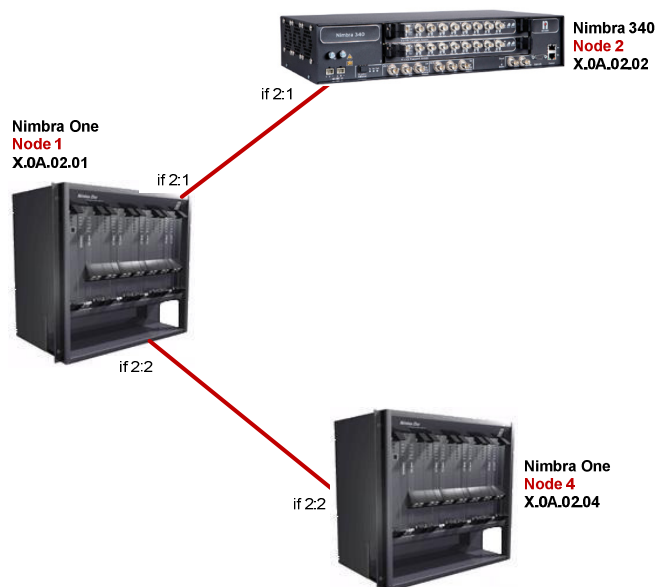
## Goal

In this exercise, you set DTM addresses of Nimbra nodes in a Point-to-Point network, according to the illustration below.

### Lab. 2 DTM Address Configuration

Group A

X=00.00.00.00.05



Group B

X=00.00.00.00.05

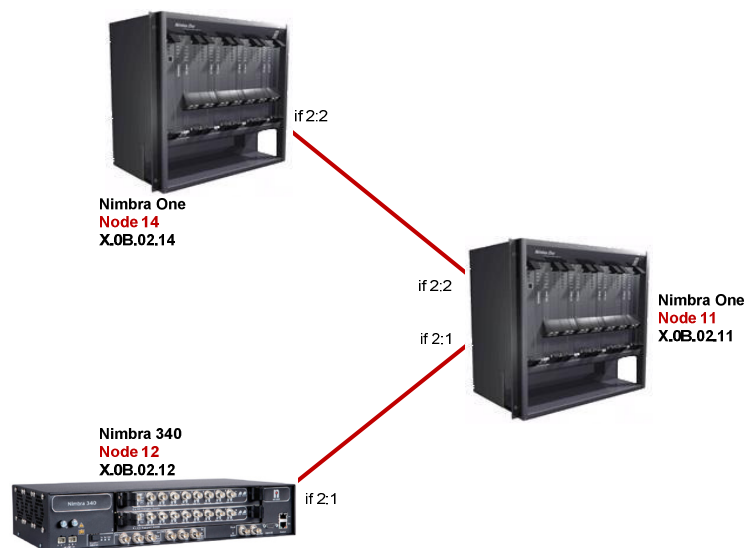


Figure 1. Network configurations for the two lab groups (A) and (B).

## Initial network configuration

Configure the network according to the topology shown above

### Connect Cables

Connect fiber cables according to the network illustration for lab 2.

### Set the DTM Address

Follow the DTM → Addresses link. Click on the Add address... link. Enter the DTM address of the node.

Set Primary address to 'Yes'. This causes the defined DTM address to be the primary DTM address of the node. Let the predefined loopback DTM address 00.00.00.00.00.00.01 remain. Click on the 'OK' button.

### Save configuration

Navigate to the Maintenance menu and from there click on the Configurations link.

Click on the 'Save configuration...' button. Enter a name in the Name field and a suitable description in the Description field. Make sure the valid tick box is selected.

Click on the 'OK' button to save the configuration. If needed, delete a saved configuration before saving the configuration. There can only be nine simultaneous configurations saved on a given node, numbered from 0 to 8.

### Reboot

Navigate to the Maintenance menu and click on the System link. Click on the Restart link. Click on the 'Restart node' button. Confirm the restart, if prompted by the operating system to do so.

### Check DTM connectivity

Open a command tool or similar, and telnet to the node. Log in to the node with the user/password combination root/neti (default) or other user-defined combination.

Use CLI command

```
dcp ping -bw 10 [DTM address]
```

or

```
while true; do dcp ping -bw 10 [DTM address]; sleep 1; done
```

e.g.

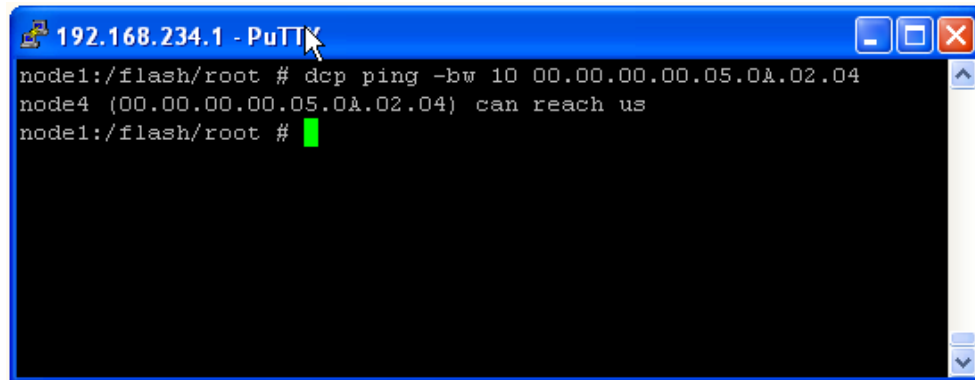
```
while true; do dcp ping -bw 10 00.00.00.00.05.0A.02.04;  
    sleep 1; done
```

or

```
while true; do dcp ping -bw 10 node4; sleep 1; done
```

In this example, 10 slots for the dcp ping are used (or rather the used channel has 10 slots).

Test connectivity between all nodes with this command. The expected reply from the far end node should be as below.



```
192.168.234.1 - PuTTY
node1:/flash/root # dcp ping -bw 10 00.00.00.00.05.0A.02.04
node4 (00.00.00.00.05.0A.02.04) can reach us
node1:/flash/root #
```

## Lab. 3 Configuration Handling

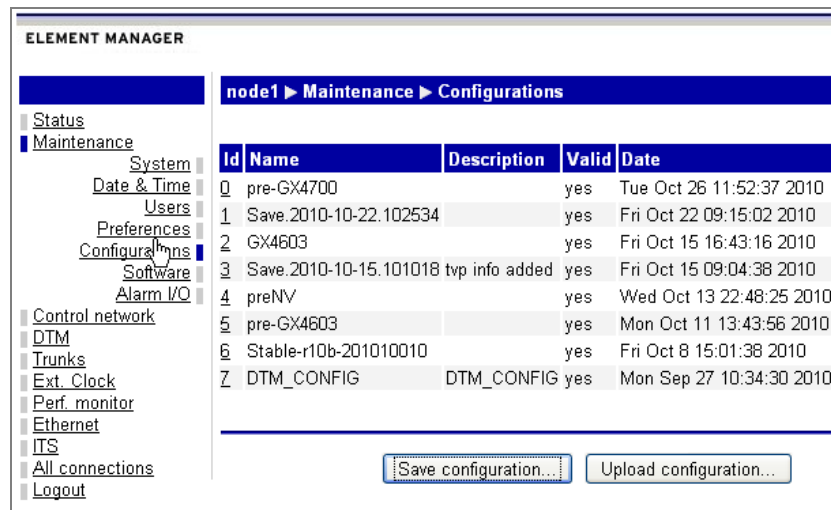
Changes made to the configuration become immediately active, but they are stored in volatile RAM memory. When the node reboots, it reverts to the latest backed-up configuration.

For this reason, it is recommended to back up the configuration as soon as changes has been made and verified.

### Goal

In this exercise you practice downloading a configuration file to the PC (to use as a back-up file) and then uploading it back to the node. Finally, the uploaded configuration is made active.

### Back up files



Navigate to the link Configurations in the Maintenance menu. Click on the link Id of the file that should be downloaded to the desktop. Click on the button 'Download file' and click on the 'Save' button in the pop-up window that appears. Save the configuration on the desktop. Enter a meaningful name and click on the 'Save' button.

Navigate to the link Configurations in the Maintenance menu. Click on the 'Upload configuration ...' button. Select your configuration as 'Local filename' and click on the buttons 'Open' and 'OK'.

The uploaded configuration is chosen as current, even though it does not reside in RAM memory. At reboot/start-up as the lowest numbered configuration with flag valid set to "Yes", it becomes active.

The previous configurations are retained in the node until they are deleted. To make any previous configuration in the list active, set the valid flag to "No" for all configurations with lower number than the selected configuration and reboot the node.

## Lab. 4 Hostnames

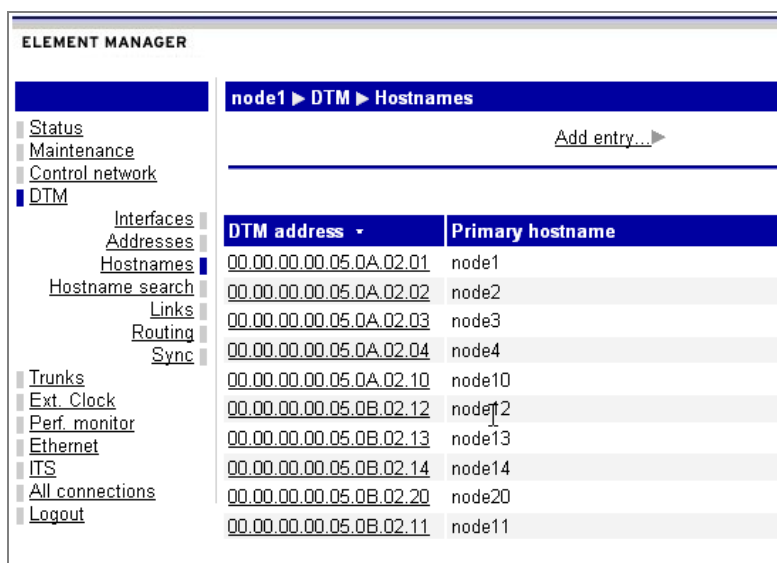
Nodes in a DTM network can be assigned names using the hostnames function. Host names are configured locally in each node and used as alias for DTM addresses.

The Hostnames table shows the DTM hosts, as follows:

**DTM address:** The DTM address of the node.

**Primary hostname:** The primary name for the host.

Remember to include the list of the host names in every node; all nodes in the network must know all hostnames!



The screenshot shows the 'ELEMENT MANAGER' interface. On the left is a navigation tree with categories like Status, Maintenance, Control network, DTM, Interfaces, Addresses, Hostnames, Hostname search, Links, Routing, Sync, Trunks, Ext. Clock, Perf. monitor, Ethernet, ITS, All connections, and Logout. The 'Hostnames' link under the 'DTM' category is selected. The main panel displays 'node1 ► DTM ► Hostnames' with an 'Add entry...' button. Below this is a table with two columns: 'DTM address' and 'Primary hostname'. The table contains 11 entries, each with a unique DTM address and a corresponding node name.

DTM address	Primary hostname
00.00.00.00.05.0A.02.01	node1
00.00.00.00.05.0A.02.02	node2
00.00.00.00.05.0A.02.03	node3
00.00.00.00.05.0A.02.04	node4
00.00.00.00.05.0A.02.10	node10
00.00.00.00.05.0B.02.12	node12
00.00.00.00.05.0B.02.13	node13
00.00.00.00.05.0B.02.14	node14
00.00.00.00.05.0B.02.20	node20
00.00.00.00.05.0B.02.11	node11

The list of all Hostnames could be pushed (Policy “Push Host list”) to every node from Nimbra Vision, the management system.

### Goal

In this exercise you assign hostnames (aliases) to the nodes.

#### Hostnames

In the DTM menu, navigate to the Hostnames link. Click on the ‘Add Entry ...’ link. The Add page is shown. Enter the DTM address and the Hostname(s) for that address. Click on the ‘OK’ button. The hostnames list reappears with a new entry.

It is possible, but not recommended, to specify several names per address, by entering different names on separate lines. Only the name on the first line will be shown on the hostname page. To get all listings of multiple hostnames, use several entries with the same DTM address.

# Lab. 5 Dynamic Routing

## Goal

In this exercise you configure a redundant network, verify the redundancy and check the connectivity. You'll also disturb the network by pulling fiber and examine the impact on connectivity.

### Lab. 5 Network – Dynamic Routing

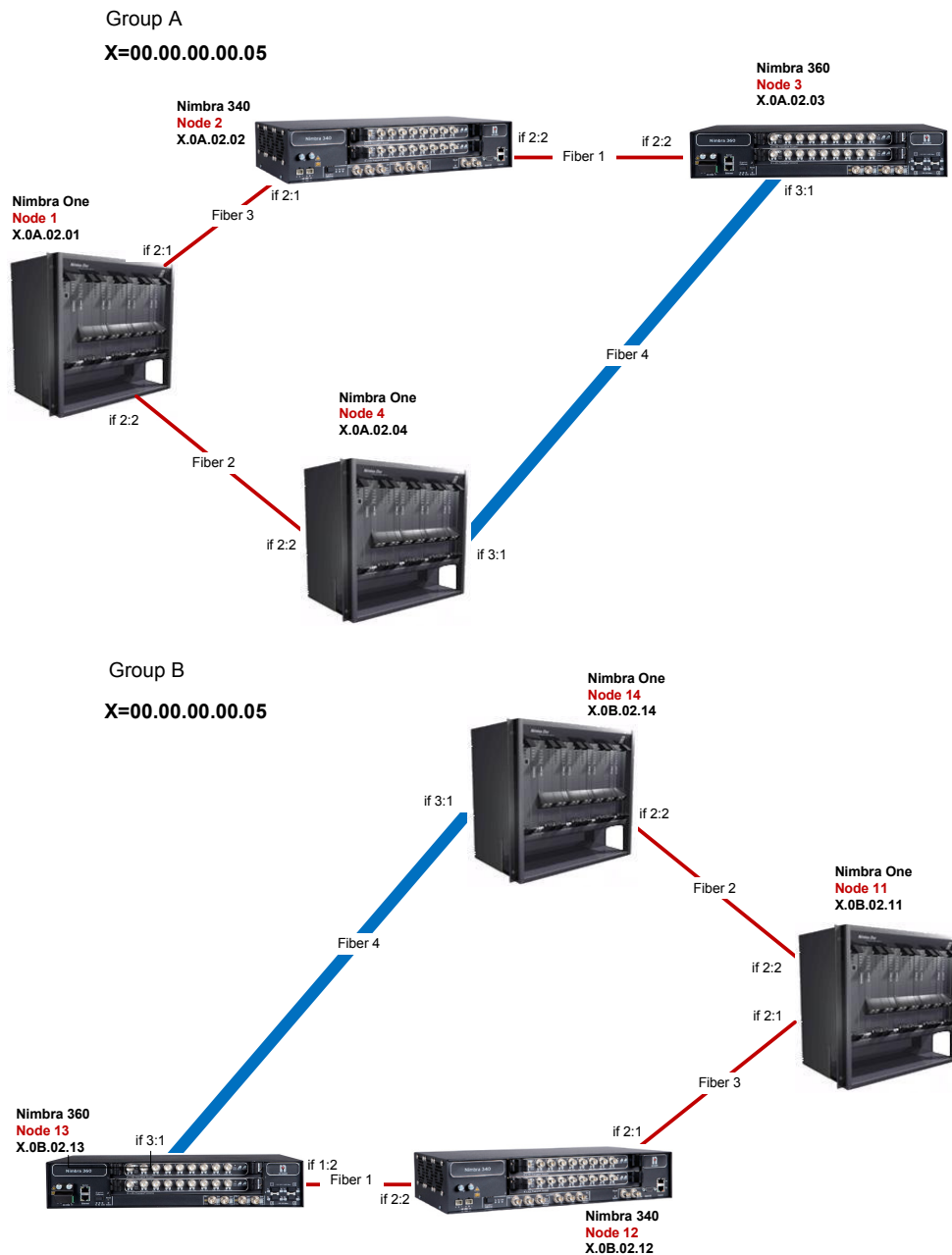


Figure 2. Network redundancy for Group A and Group B.

## Redundancy in DTM networks

Configure the network according to the illustration shown above.

### Connect Cables and check connectivity

Connect the fiber cables according to network topology. Check connectivity with DCP ping described in lab 2. Test DCP connectivity between all nodes, pairwise.

Start a DCP ping session in a CLI window between end nodes.

Pull one fiber connecting the nodes. Is connectivity lost? If so, for how long is it lost? If not, put back the fiber and pull the alternative route fiber between the nodes. Reply to the questions again.

### Check routing

Open a command tool or similar and telnet to the node. Log in to the node with user/password combination root/neti (default) or other user-defined combination.

To check routing, use CLI command

**drp rt**

The routing table for the node is presented, with all possible routes and their respective costs listed. DRP is setting up routes on a low-cost basis, i.e. channels are established along the low cost route at the time of establishment.

Example:

```
node1:/flash/root # drp rt
Routing Table, Number of Entries = 3:
  Destination/Mask = 00.00.00.00.05.0A.02.02/64
    Next Hop List, Number of Entries = 4:
      Cost      1, next hop 00:10:5B:10:FB:41, type dlsp
      Cost      1, next hop 00:10:5B:10:FB:41, type adj.
      Cost      1, next hop 00:10:5B:10:FB:41, type drp
      Cost      3, next hop 00:10:5B:10:DE:50, type drp
  Destination/Mask = 00.00.00.00.05.0A.02.03/64
    Next Hop List, Number of Entries = 2:
      Cost      2, next hop 00:10:5B:10:FB:41, type drp
      Cost      2, next hop 00:10:5B:10:DE:50, type drp
  Destination/Mask = 00.00.00.00.05.0A.02.04/64
    Next Hop List, Number of Entries = 4:
      Cost      1, next hop 00:10:5B:10:DE:50, type dlsp
      Cost      1, next hop 00:10:5B:10:DE:50, type adj.
      Cost      1, next hop 00:10:5B:10:DE:50, type drp
      Cost      3, next hop 00:10:5B:10:FB:41, type drp
node1:/flash/root #
```

The Destination/Mask shows the DTM address of the destination node.

Each entry in the respective destination's hop list shows:

- the cost to reach that specific destination
- the next hop's Node MAC address (also called System MAC address).



The web page “DTM → Links” shows the adjacent nodes (with their Node MAC addr) and what DTM interface is used for that link.

node1 ► DTM ► Links					
Id	I/f MAC addr	Node MAC addr	Node addr	Oper	Last changed
dtm2:1/rx	00:10:5B:20:1F:79	00:10:5B:10:FB:41	node2	Up	09:29:20
dtm2:1/tx	00:10:5B:20:1F:79	00:10:5B:10:FB:41	node2	Up	09:29:20
dtm2:2/rx	00:10:5B:20:25:1A	00:10:5B:10:DE:50	node4	Up	09:28:52
dtm2:2/tx	00:10:5B:20:25:1A	00:10:5B:10:DE:50	node4	Up	09:28:52

Note that each DTM interface has a unique MAC address referred as “i/f MAC addr”, which is different from the “System MAC address”.

Note also that to the next-node neighbors, there are three entries created: dlsp, adj and drp. These entries are all equivalent.

## Dynamic routing

Make sure the (DTM) node metric is one and that the (DTM) interface metric is one for all interfaces. These are the ‘costs’ associated with passing through the node and the particular interface. The total cost for a connection is the transit cost for all nodes and interfaces. Observe that the interface cost is only applied to outgoing interfaces.

### Connectivity and restoration

Between each fiber removal, each group should use the command **dcp ping** described previously, to test connectivity between the nodes.

Check also the routing table with the command **dcp rt**.

Follow the Links link in the DTM menu and check the link table to see all different links, both terminating and originating links in the node and check how the table is updated between the different steps.

How are the routing and link tables changing between steps 1 and 2?  
Between step 2 and 3?

1. Remove fiber 1.
2. Reconnect fiber 1, Remove fiber 2.
3. Reconnect fiber 2, Remove fiber 3.

### Disable DRP in one of the nodes

Change the setting for DRP by following the Routing link from the DTM menu. Click on the Dynamic routing config link. Disable all DTM Interface metric parameters on one of the nodes by unticking the enable boxes.

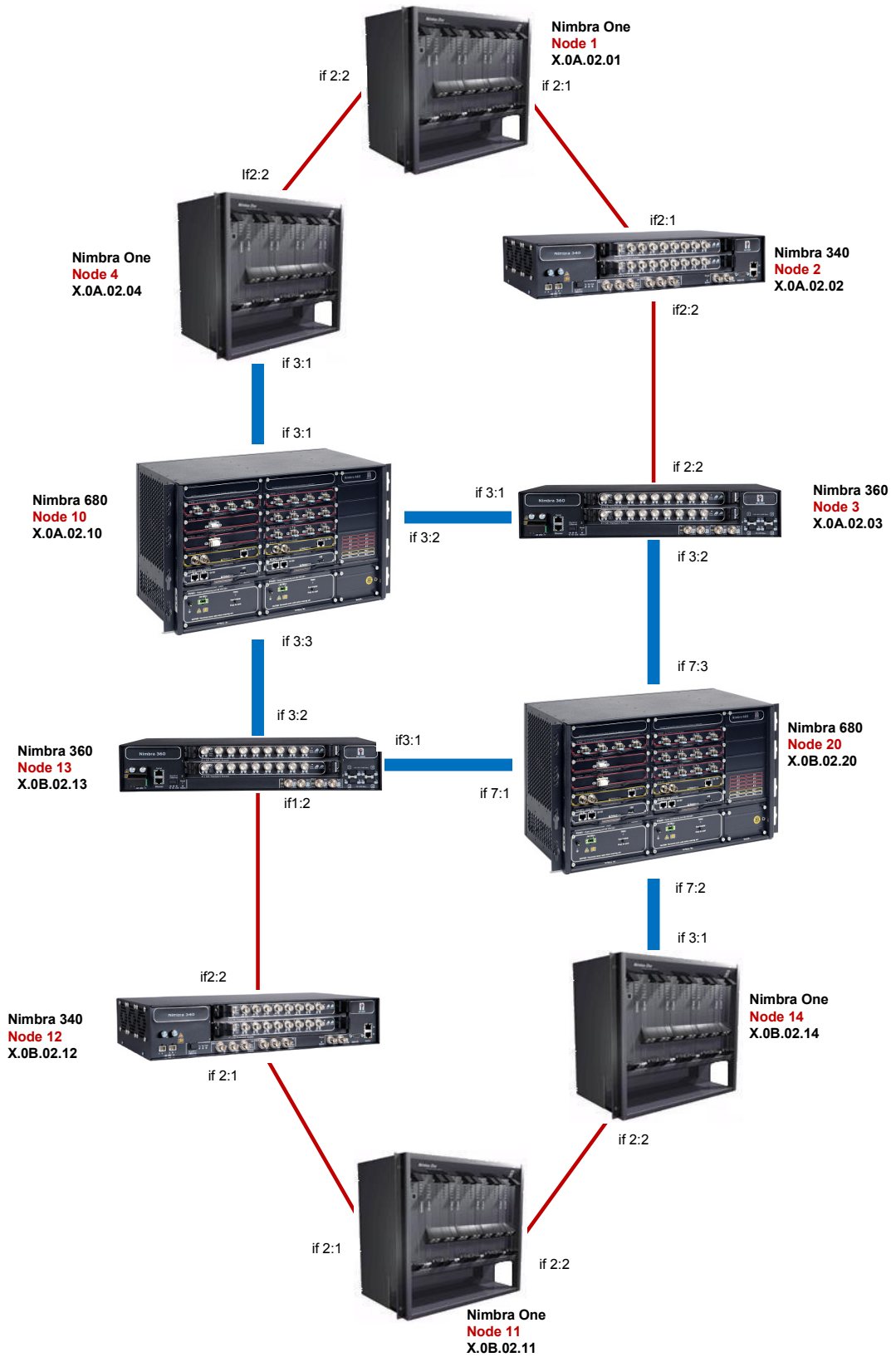
Each group should now use the command **dcp ping** to test connectivity between the nodes; how is the connectivity affected by the fiber removals and how it is affected by the disabling of the DTM Interface metric.

Check connectivity to all other nodes and finally save the configuration.

Save configuration

Finish the exercise with saving the configuration.

# Net Insight Academy Network



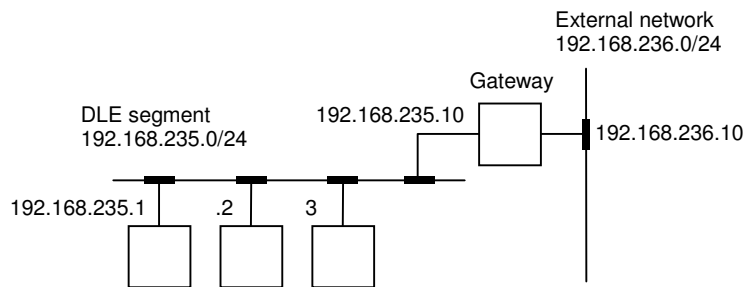
**Figure 3. Net Insight Academy Network.**

## Lab. 6 Management with DLE

DLE (DTM LAN Emulation) emulates a LAN (Local Area Network) as an Ethernet segment on top of DTM. It is using channels through the DTM network. Seen from DLE, each node in the segment has direct connectivity to all other nodes, as on any 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.

Running IP over DLE enables a management workstation connected to one DTM node to reach other DTM nodes over the DTM network. This is also called in-band Management.

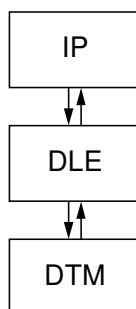
Communication is done with network management stations, either from a network management system such as Nimbra Vision, or from a web browser or telnet session. Direct communication between nodes is limited. Typically, few nodes in the DTM network are simultaneously reached from a management station.



**Figure 4.** A network with one DLE segment and one external network. Note that the DLE segment is a logical segment and that the nodes are not necessarily physically connected.

### Goal

In this exercise you configure DLE for In-band Management and verify the installation. You also set up SNMP notification receivers.



**Figure 5.** DLE stacked on top of DTM.

## In band Management (DLE)

Configure the network according to the topology illustration below. The management network setup for the exercise is shown below.

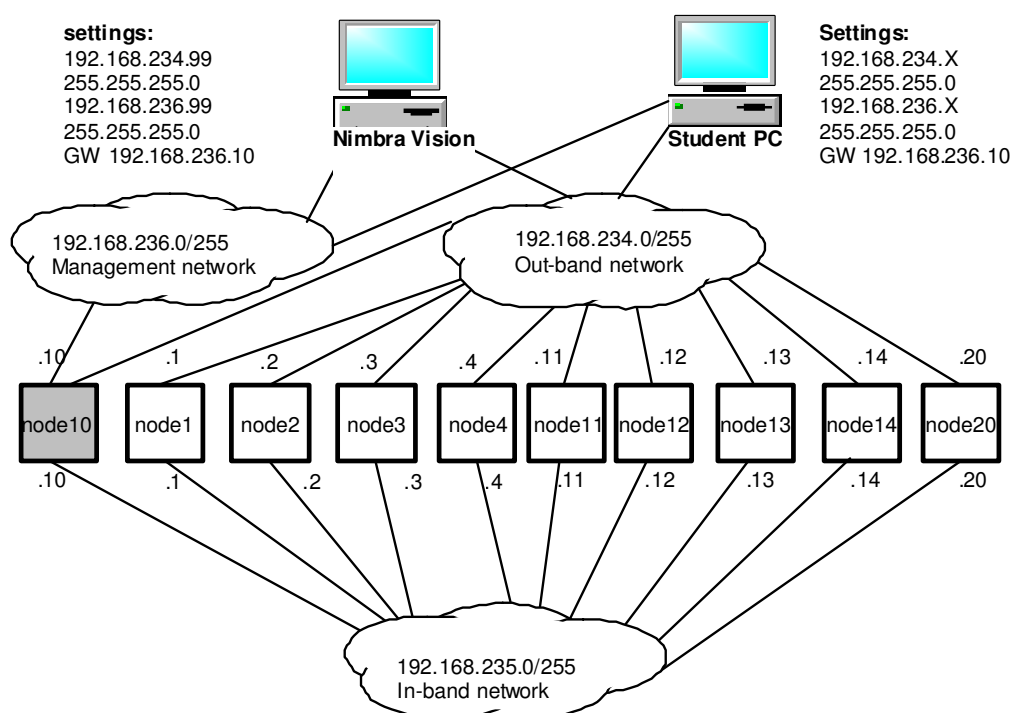


Figure 6. Redundant management networks, where node10 is gateway and DLE server

Set routes so that all nodes have an IP-route to the network 192.168.235/24 and the Management station can reach all DTM-nodes. Use node10 as the in-band server for the in-band management network.

### Configuration of the In-band server

Navigate to the Control network menu and click on the In-band servers link. Click on the 'Add' button. Set the **Administrative status** to 'Up' in the drop-down menu. Configure the other parameters as:

**Purpose:** An arbitrary text string, which can be used to identify the server

**DSTI:** (channel identifier) The first In-band server DSTI is by default 32769. Keep this value.

**Server-to-client connection capacity:** By default, this parameter is set to 0.485 Mbps. In almost all cases, this bandwidth should be enough.

**Server-to-server connection capacity:** By default, this parameter is set to 0.485 Mbps. In almost all cases, this bandwidth should be enough.

There is no need to change the settings under the Advanced or Destinations links. Destinations are used for server-to-server connections in case there is a backup server.

In order to finalize the settings, click on the 'Apply' or 'OK' button.

### Configuration of the in-band client

An in-band client must be configured on every node in the in-band segment, including the node with the in-band server. To define and configure the in-band client, proceed as follows:

Navigate to the Control network menu and click on the In-band clients link. Click on the 'Add' button. Set the **Administrative status** to 'Up' in the drop-down menu. Configure the other parameters as:

**Purpose:** An arbitrary text string, which can be used to identify the client

**DSTI:** The In-band client DSTI is an identification number, unique for the node and service type (ETS or ITS).

**Client-to-client connection capacity:** By default, this parameter is set to 0.485 Mbps. In almost all cases, this bandwidth should be enough.

**Tear down unused channels after:** Channels are torn down when they are no longer used. This parameter controls the time in seconds before the channel is torn down. The default setting is 600 s, which should be used in this lab. A setting of 0 s disables the functions, i.e. channels are never torn down.

**Server DTM node** is the hostname or DTM address of the In-band server node.

**Server DSTI** is the Server DTM Service Type Instance. Normally, the default 32769 is kept.

**Alternative server DTM node:** DTM address or hostname of backup DTM server. For this exercise, this field is left blank, as no backup DLE server is used.

**Alternative server DSTI** is the DSTI of the backup server. For this exercise, this field is left blank. Otherwise, the default 32769 is normally kept.

**Client to server connection capacity** is recommended to keep at the default 0.485 Mbps.

There is no need to change the settings under the Advanced link.

In order to finalize the settings, click on the 'Apply' or 'OK' button.

After definition of both In-band server and client, verify that the client is active by looking at the operational status of the created dlecXX, which should be 'Up'.

### IP settings

In order to finish the configuration of the In-band client, its IP address must be set. This is made from the [IP interfaces](#) link. The link takes the user to a page of defined IP addresses. In order to configure the client, the relevant [dlecXX](#) link should be selected. Proceed with the 'Add address ...' button. This button takes you to a menu with fields for IP address and IP netmask.

Note that an IP address must be configured on every node in the DLE segment. The client configuration is not finished until the IP settings have been made.

### Configuration of IP routing

In order to transfer IP traffic to IP addresses not on the DLE segment, IP routes must be defined for all In-band clients, except the client that is hosting the In-band server. The configuration tells the node how to handle IP traffic to a node outside the DLE segment.

Click on the link [IP Routing Conf](#) under the Control Network menu. Click on the [Add route ...](#) link and fill in the parameters:

**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 the lab, these settings should be 0.0.0.0 for Destination; 0.0.0.0 for Netmask and 192.168.235.10 for Gateway. Note that the setting 0.0.0.0 for destination is listed as default on the web interface.

### Verification of the in-band management network

Verify the in-band management network by disconnecting all the Ethernet cables except for the one to the in-band server node (node 10) and then try to access the nodes with in-band management IP addresses. IP Ping each node from the PC with the node's in-band management IP. If needed, routes must be set in the operating system of the PC.

IP address or open a web browser and type the in-band IP address in the URL field.. Troubleshoot as needed.

Test connectivity to all nodes.

### Setting up notification receiver

A notification receiver is the management station that processes notifications (SNMP traps) sent from all network elements. Typically, this is the IP address of the Nimbra Vision server. You may send notifications to multiple management stations, in case you use multiple Nimbra Vision servers. You may also send notifications to multiple IP addresses from the same management station.

Navigate to the SNMP link in the Control network menu. Click the 'Add SNMP notification receiver...' button to create a new receiver of notifications. For all receivers, add

**IP address** The IP address of the management station, i.e. Nimbra Vision server.

**UDP Port number** The used UDP port is normally 162 (standard).



## Lab. 7 Internal versus external sync

Synchronization is timekeeping, which requires the coordination of events to operate a system in unison. Systems operating with all their parts in synchrony are said to be synchronous or in sync. The lessons of timekeeping are part of engineering technology. In electrical engineering terms, for digital logic and data transfer, a synchronous object requires a clock signal. TEST123 Timekeeping technologies such as the GPS (Global Positioning System) satellites and Network time protocol (NTP) provide real-time access to a close approximation to the UTC time, and are used for many synchronization applications.

Today, synchronization can occur on a global basis due to GPS-enabled timekeeping system. An atomic clock is a type of clock that uses an atomic resonance frequency standard as its timekeeping element. They are the most accurate time and frequency standards known, and are used as primary standards for international time distribution services, and to control the frequency of television broadcasts and GPS satellite signals.

The network can use internal sync (the sync is retrieved from one of the Nimbra nodes in the network) or external sync (one of the Nimbra nodes retrieves the sync from a GPS or atomic clock).

### Goal

In this exercise you will see the difference between internal and external sync.

#### Internal sync

Set administrative status to 'Down' for all external synchronization sources.

**ELEMENT MANAGER**

node3 ► DTM ► Sync

Sync oper. state: up  
External clock priority: 5  
External clock admin. status: Down

Apply

Type	Id	Current source	Backup source	TR Prio
internal clock	N/A	no	yes	15
dtm interface	dtm3:1	yes	yes	15
dtm interface	dtm3:2	no	yes	15
external clock	N/A	no	no	5
dtm interface	dtm2:2	no	no	15

Which node in the network is the sync master and how is the sync spread?

Pull the fiber where the sync is transported; how is the sync affected? Which node is now sync master?

## External Sync

Configure the network according to the illustration below.

### Lab. 7 Internal sync versus External sync

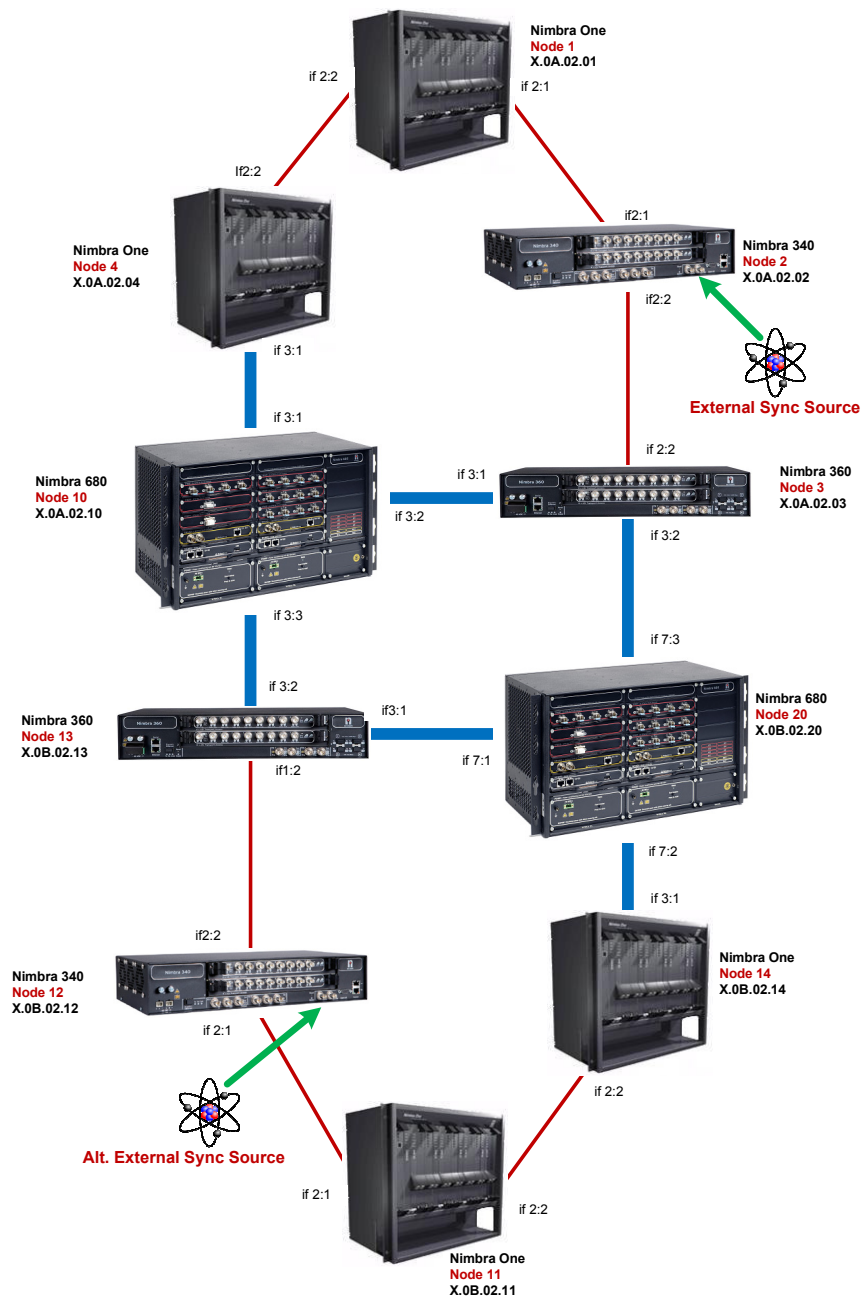


Figure 7. Network with attached external sync source.

In this lab, we attach an external sync source to one of the nodes in the network. Make sure the external sync source has administrative status 'Up', i.e. that it is active.

How is the sync spread in this case? How can I trace the sync?

## Lab. 8 Time Transfer

Time transfer describes methods for transferring reference clock synchronization from one point to another, often over long distances. Radio-based navigation systems are frequently used as time transfer systems.

In some cases, multiple measurements are made over a period of time, and exact time synchronization only determined retrospectively.

### Goal

In this exercise you use Net Insight Time Transfer feature.

### Time Transfer

Configure the network according to the below.

Lab. 8 Time transfer

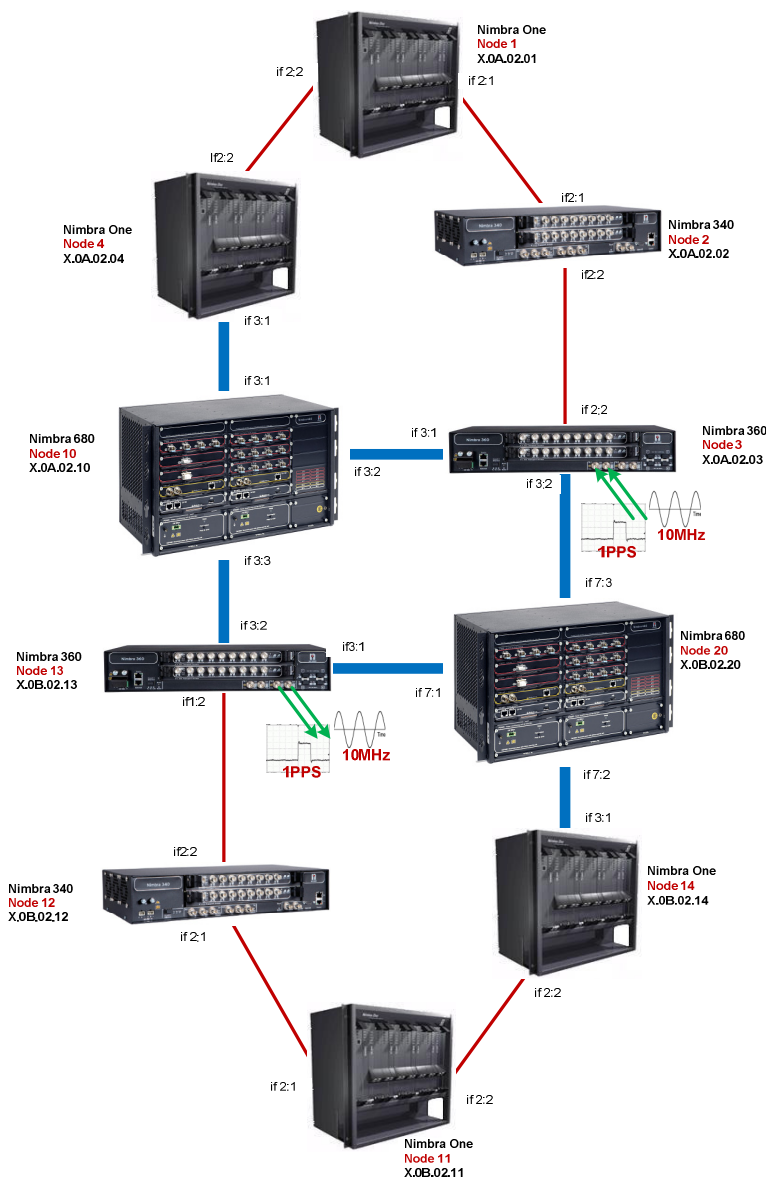


Figure 8. Net Insight time transfer configuration.

Navigate to the **DTM** menu and go to Time Transfer link to enable the functionality for the interfaces.

Attach the 1 PPS and 10 MHz according to the topology. Take out the Time Transfer signal in node 13 and verify the outgoing signal.

Check the sync tree, how is it spread? The available clocks on a specific node are seen by following the links DTM → Sync.

Configure all nodes involved in time transfer, i.e. nodes 3, 13, 10 and 20. Observe that Nimbra 680 nodes must be configured in order for the time transfer signal to pass through them (to the other Nimbra 360 node), even though they are only receiving the time transfer signal through a DTM link.

Pull the fiber between the sync master and the second hop; how is the sync affected by this action? Reinsert the fiber and study how this affects how the sync is distributed.

# Lab. 9 Source routes

## Source Routes

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 (i.e. the shortest and most efficient route in terms of 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 making up the connection take different paths from the source to the destination. This means that if a link or a node in the network fails for any reason, only one of the channels is affected.

There are other situations when it may be of interest to specify explicit paths, e.g. to avoid a link or node scheduled for maintenance. Using source routing, it is possible to specify the exact path for a channel through the network. Pinpointing all nodes that a channel traverses from source to destination specifies the path. Also, the outgoing interface can be specified. A source-route is always specified in the source node of the connection.

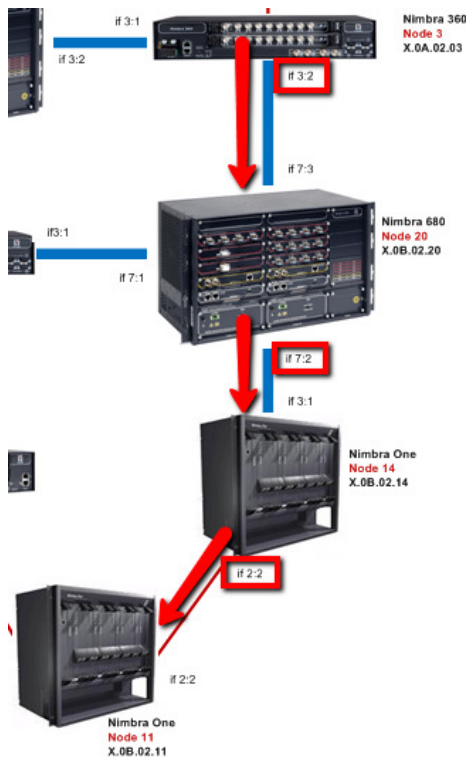
***It is possible to configure three different source-routes for a single channel. If no source-route is configured, then the channel is established along the optimal path from source to destination, using DRP.***

This is the most robust mode of operation, since the network is allowed to find another path for the channel if the shortest path is not available. By specifying a source-route for a channel, an operator tells the network that the channel must be established along this path. If the particular path is not available, then the channel cannot be established.

### Loose and strict source-routes

A source-route can be strict or loose. For a strict source route, every node from source to destination must be specified. For a loose source route, only nodes required to be traversed, are specified. The path between the specified nodes is found via hop-by-hop routing (partial DRP).

## Source-routes



We want to establish a 1+1-protected tunnel from node3 to node11.

The primary channel shall pass through nodes node20 and node14 (see illustration on the left).

The secondary channel shall pass through node10, node 13 and node12.

To create a source route, go to the All Connections Menu and click on the Source Routes link. Click on the 'Create' button. Parameters needed are **name**, **type of routing** (strict/loose), **used outgoing interface** and **nodes** traversed. For strict source-routes, all intermediary nodes must be specified; for loose source-routes at least one intermediary node must be specified.

When there are several trunks available between two nodes, it is possible to specify which interface to use 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. If no interface is specified, then the node is free to choose any of the available interfaces. Each node is written on a separate line and can be represented either by its host name or by its DTM address

The following illustration shows how to configure the Source-route for the primary channel. Note that, in this case, specifying the outgoing interfaces is not needed to define the source-route correctly.

node3 ► All connections ► Source routes ► Edit	
►Used by	
Source route id:	0
Name:	SR_to_node11_via_node20_node14
Routing:	Strict ▼
Outgoing interface:	3:2
Nodes (one per line):	node20 7:2 node14 2:2

How would you configure the secondary channel through node10, node 13 and node12?

## Save configuration

Finish with saving the configuration.

## Lab. 10 Streaming Services

The Video service provides a transparent Video connection through a network by creating a Video transport channel. Management of video transport includes configuration and supervision of the Video access functions.

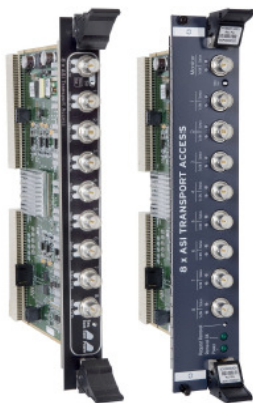
The Access Modules adapt specific service data for transport over the network.

### Asynchronous Serial Interface (ASI)

Asynchronous Serial Interface, or ASI, is a streaming data format which often carries an MPEG Transport Stream (MPEG-TS).

ASI Transport Access Module enables digital multimedia transports with guaranteed quality of service in various networks. With a unique configurable bandwidth feature, the ASI Transport Access Module keeps overhead to a minimum and makes optimal use of network resources.

#### Nimbra One/300 series



The 8 x ASI Transport Access Module for the Nimbra One/300 series is ideal for use in video production, post-production and broadcast environments.

It allows MPEG transport streams ranging from 2 to 212 Mbps with built-in network redundancy and support for sub 50 ms 1+1 protection.

Each port can individually be configured as ASI In or Out. One monitor port can monitor any in or out port.

#### Nimbra 600 series



The 8-port Video access board for the Nimbra 600 series multiservice switches enables transport of MPEG encoded video, with guaranteed quality of service in studio, distribution and contribution networks.

Each port may be individually configured as In or Out DVB-ASI signals. With built-in network restoration and support for external sub-50ms 1+1 protection, the 8 x Video Access Module together with the Nimbra 600 Series switch offers a flexible protection switching solution in which the level of protection is free of choice.

Any port can be used to monitor any other port.

## Serial digital interface (SDI)

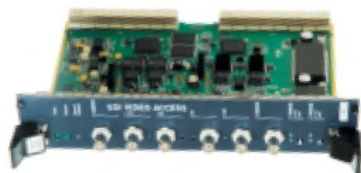
Serial digital interface (SDI) is a serial link standardized by ITU-R BT.656 and the Society of Motion Picture and Television Engineers (SMPTE ) that transmits uncompressed digital video over 75-ohm coaxial cable within studios and is seen on most professional video infrastructure equipment.

(SD) SDI	SMPTE 259M	Analog video (NTSC/PAL)	143/270/360 Mbps
HD SDI	SMPTE 292M	1080i and 720p	1.485 Gbps European HD TV 1.485/1.001 Gbps, NTSC
3-Gbps(3G)-SDI	SMPTE 424M	1080p	2.97 Gbps

The SDI Video Access Module offers 270 Mbps SDI interfaces to the nodes, allowing full-uncompressed SDI signals to be transported over the network based on the ITU-R BT.601/656 (SMPTE 259M-C) video standards. The SDI Video Access module uses 563 slots per SDI channel.

The module supports the Serial Data Transport Interface (SDTI), according to SMPTE 305M-C for carrying data within the 270 Mbps signal.

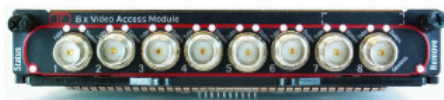
### Nimbra One/300 series



The SDI Video Access Module provides a versatile SDI digital video transport for the professional media industry. The module offers a 270 Mbps SDI interface based on the ITU-R BT.601/656 digital video standard

It includes two Transmit and two Receive SDI ports. A Receive port takes an SDI or SDTI signal and maps it into a fixed size network channel that is transported across the backplane of the Nimbra node, across the network and to one or several Destination SDI ports in other nodes. The system also allows for setting up a channel to Transmit ports in the same Nimbra One or even to the same Module.

### Nimbra 600 series



The 8-port Video access board for the Nimbra 600 series multiservice switches enables transport of high or standard definition uncompressed digital video, with guaranteed quality of service in studio, distribution and contribution networks.

Each port may be individually configured as In or Out. There are some limitations on the module. If the module has 10 Gbps capacity towards the



backplane, up to 6 in + 2 out or 2 in + 6 out HD-SDI signals can be simultaneously connected to the module.

With built-in network restoration and support for external sub-50ms 1+1 protection, the 8 x Video Access Module together with the Nimbra 600 Series switch offers a flexible protection switching solution.

Any port can be used to monitor any other port.

## Goal

Since the configuration settings on the webinterface are almost identical for ASI and (HD) SDI services, the following examples will focus on ASI services only.

The images below illustrate the small differences between ASI and (HD) SDI signals. The only differences, Local interface (type) and Requested capacity, are highlighted.

The figure displays two side-by-side screenshots of a web interface for configuring Trail Termination Points (TTPs). Both screenshots show the 'Edit originating' page for a TTP. The left screenshot is for an 'HD SDI Service' (Trail termination point name: itso-0) and the right screenshot is for an 'ASI Service' (Trail termination point name: itso-1). Both services have an administrative status of 'Down' and an operational status of 'down'. The 'Local interface' field is highlighted with a red box in both: 'sdi-2:1' for HD SDI and 'asi-2:4' for ASI. The 'Requested capacity' field is also highlighted with a red box: '1.485 Gbps' for HD SDI and '120,000 kbps (uses 5 slots)' for ASI. Other fields like 'Destination DTM node', 'Destination DSTI', 'Connection protection', and 'First channel source routes' are also visible but not highlighted.

**Figure 9. Configuration of HD/SD-SDI (left) and ASI in the originating Trail Termination point (TTP).**

The web interface for ITS service allows an operator to define ASI/(HD)SDI channels. In this exercise, you learn how to set up an ASI channel (both uni- and multicast) by using the dynamic routing protocol, source-routes. In addition, 1+1 protection is configurable.

## ASI Unicast

In this lab, we are setting up an ASI (Asynchronous Serial Interface) channel from one port to another (ASI unicast).

Configure the DTM-network and Video Input/Output according to illustration below.

### Lab. 10 ASI, Unicast

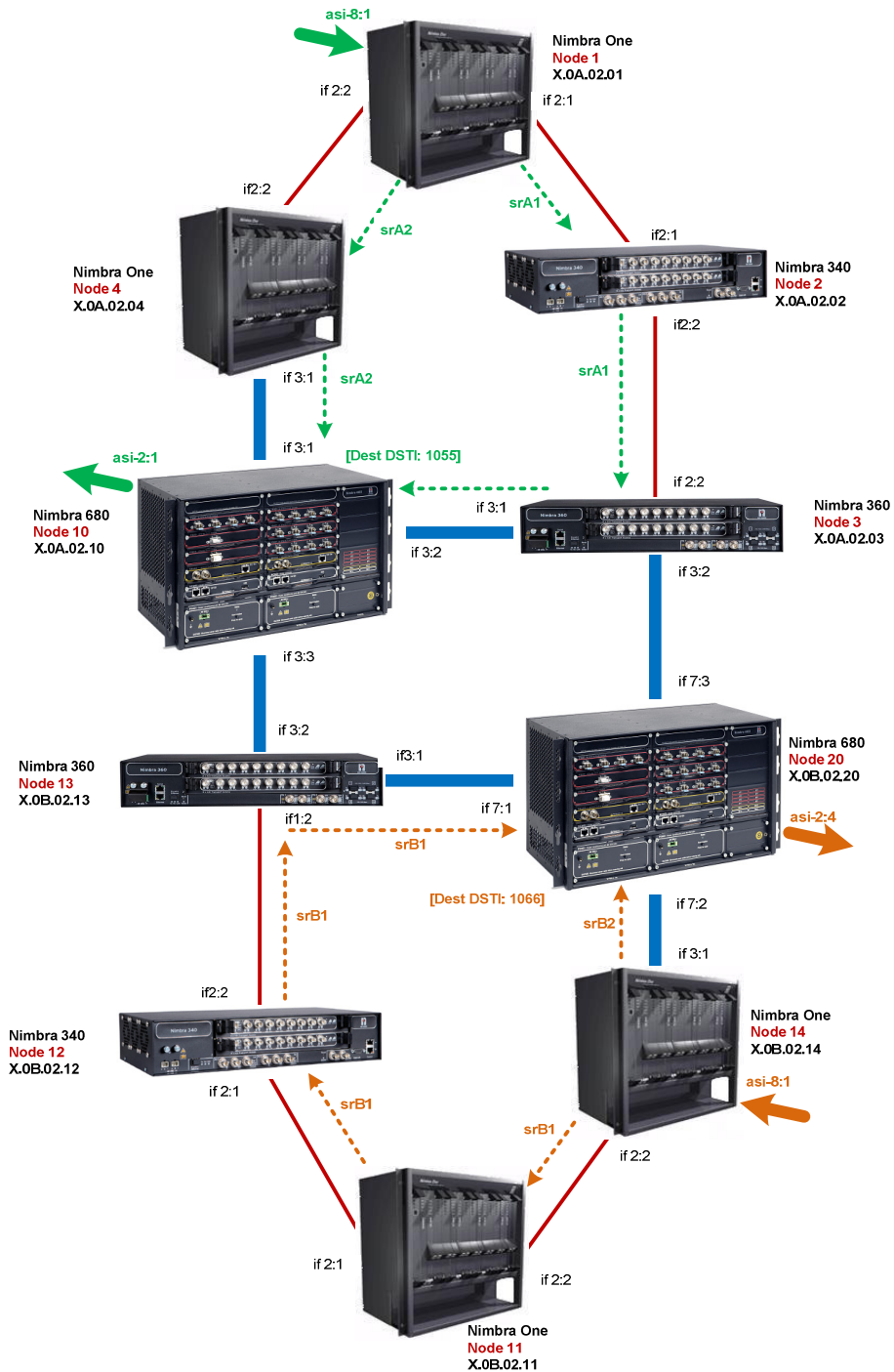


Figure 10. Configuration of ASI Unicast. Group A sets up the connection from node1 and Group B from node14.

#### Add TTPs at the source

Navigate to the ITS menu and click on the TTPs link. Click on the 'Add TTPs ...' link and choose "Type: **Originating**".

Configure the node as follows:

**Mode:** Unicast

**Local interface:** The port selected for the specific (originating) channel.

Click on the 'Add' button. Additional configurations are needed. Enter the parameters of the video tunnel

**Customer ID:** 555

**Purpose:** Test connection

**Local interface,** asi-8:1 or other suitable interface

**DSTI:** 55

**Destination DTM node:** node10

**Destination DSTI:** 1055

**Requested capacity:** For this connection, 20 Mbps

Set the **Administrative status** to 'Up'. Click on the 'OK' or 'Apply' button.

#### Add TTPs for the destination

Navigate to the ITS menu and click on the TTPs link. Click on the 'Add TTPs ...' link and choose "Type: **Terminating**".

Configure the node as follows:

**Customer ID:** 555

**Purpose:** Test connection

**Local interface,** asi-2:1 or other suitable interface

**DSTI:** 1055

Set the **Administrative status** to 'Up'. Click on the 'OK' or 'Apply' button.

### Source-routes and 1+1 protection

Create the source-routes according the illustration above and test:

- The connection re- established using source-routes instead of the dynamic routing.

► Advanced ► Scheduler

Destination DTM node:	node10
Destination DSTI:	1055
Requested capacity:	20.000 Mbps (uses 5 slots)
Connection protection:	Off
First channel source routes, 1st:	srA1
2nd:	srA2
3rd:	( none )
Second channel source routes, 1st:	( none )
2nd:	( none )
3rd:	( none )

- The 1+1 connection protection using source-routes

Destination DTM node:	node10
Destination DSTI:	1055
Requested capacity:	20.000 Mbps (uses 5 slots)
Connection protection:	On
First channel source routes, 1st:	srA1
2nd:	( none )
3rd:	( none )
Second channel source routes, 1st:	srA2
2nd:	( none )
3rd:	( none )

### Open ended 1+1 protection

Note that there are two terminating connections connected to one single TTP. This is because of the open ended 1+1 protection feature. This feature does not change the web interface in any way, but what is new is that two different connections originating from different nodes can be terminated on a single TTP. At the receiving side only one of the streams is used. In this way we get head end protection and network protection.

Follow the illustration below and create two unicast ASI that terminates to the same DSTI the receiving side.

Note that the Originating TTPs don't need to have the Connection Protection parameter set to On, whereas the Terminating TTPs must have Connection Protection enabled.

## Lab. 11 ASI, Open ended 1+1 Protection

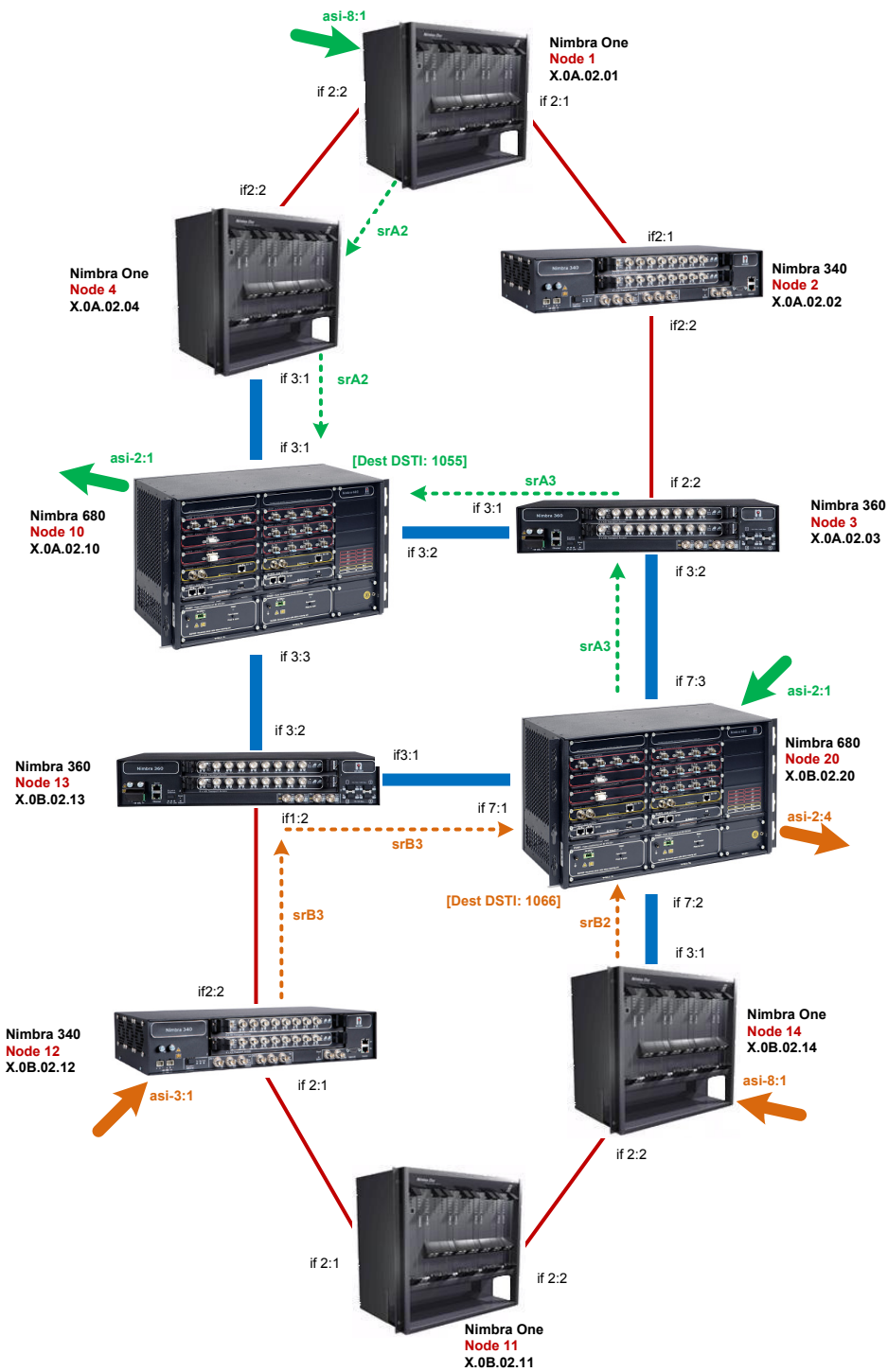


Figure 11. Open ended 1+1 Protection

## ASI Multicast

Multicast is a way to transport data from one single source to many destinations without a need to duplicate data on multiple channels. Each individual destination can either be network (DRP) or source routed. They can furthermore be dynamically added and deleted while a connection is still administratively up.

### Lab. 11 ASI, Open ended 1+1 Protection

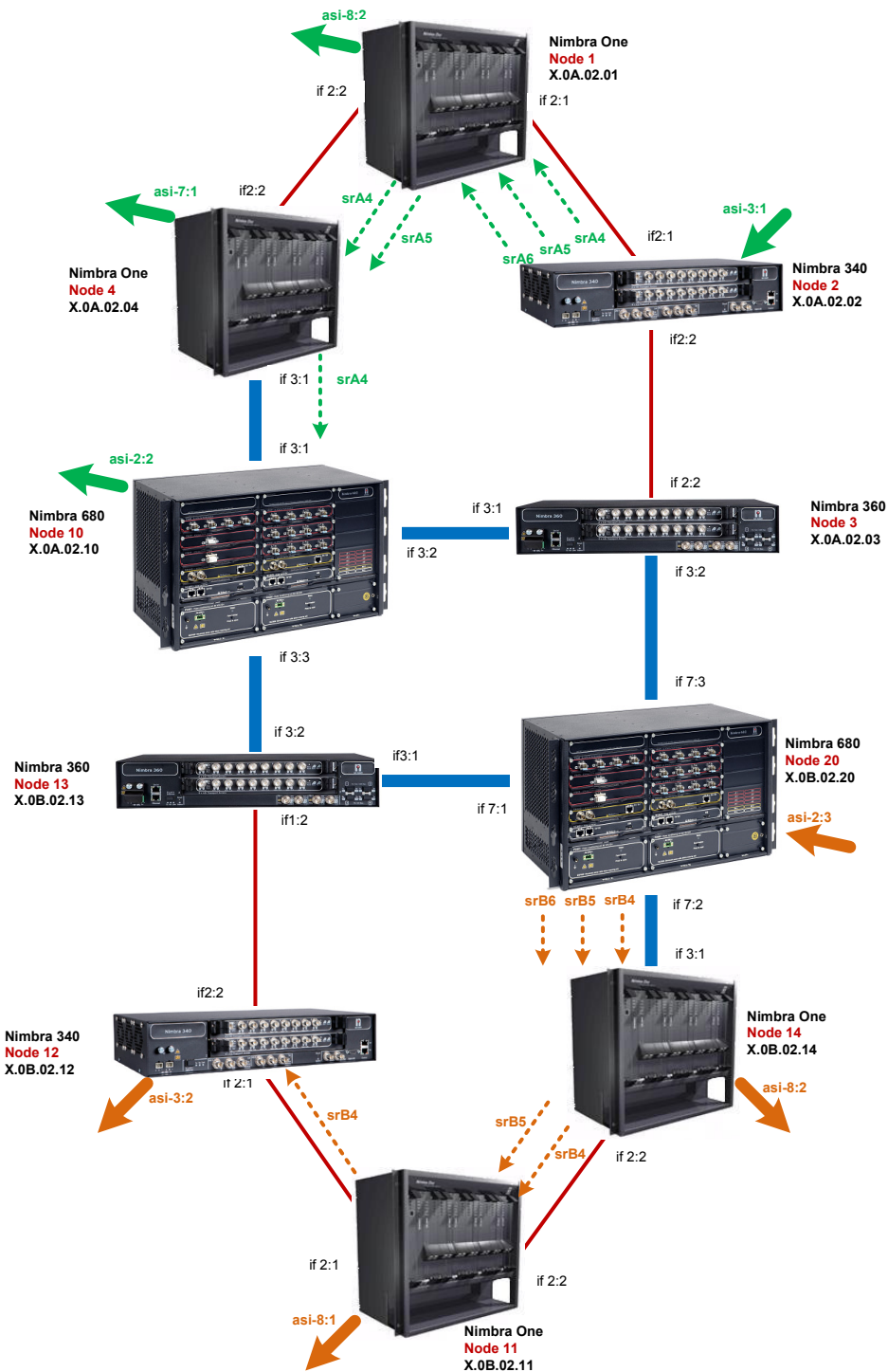


Figure 12.ASI Multicast configuration. Group A sets up the connection from node2 and Group B from node 20.

The ports on the ASI Transport Access Module can be the source and destination of such multicast channels for ASI traffic.

In this lab, we are going to set up ASI (Asynchronous Serial Interface) tunnels from one source to multiple destinations.

Multicast is a way to transport data from one single source to many destinations without a need to duplicate data on multiple channels. Each individual destination can either be network (DRP) or source routed. They can furthermore be dynamically added and deleted while a connection is still administratively up.

#### Add TTPs at the source

Navigate to the ITS menu and click on the TTPs link. Click on the 'Add TTPs ...' link.

Configure the node as follows:

**Type:** Originating

**Mode:** Multicast

**Local interface:** The port selected for the specific (originating) channel.

Click on the 'Add' button.

Enter the parameters of the connection

**Customer ID:**

**Purpose:**

**Local interface,**

**DSTI:**

**Requested capacity:** For the connection

Click on Destinations link and then on the Add destination ... link.

Configure

**Administrative status** to 'Up'

**Destination DTM node** according to the topology illustration

**Destination DSTI** according to the topology illustration

Click **OK**.

Repeat the configuration for all the destination nodes.

#### Add TTPs at the destinations

Navigate to the ITS menu and click on the TTPs link. Click on the 'Add TTPs ...' link.

Configure the node as follows:

**Type:** Terminating

**Mode:** Should be grayed out, as it is not relevant.

**Local interface:** The port selected for the specific (terminating) channel.

Click on the 'OK' or 'Apply' button. Repeat for all destination nodes.

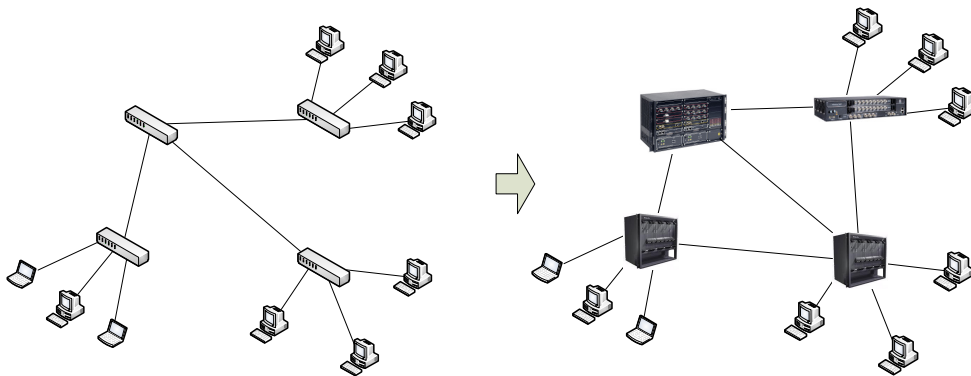
## Lab. 11 Ethernet Transport Service (ETS)



Net Insight's Ethernet Transport Service offers a transparent transport service for Ethernet traffic fully compliant with IEEE 802.3.

ETS is available as ETS unicast or ETS multicast. ETS unicast is a bidirectional, point-to-point service between two access points of the network. ETS multicast is a unidirectional, point-to-multipoint service connecting one ingress point and several egress points.

Ethernet Transport Service is an end-to-end service, or rather edge-to-edge service. It creates point-to-point or point-to-multipoint connections over the network spanned by Net Insight's network equipment (the DTM network).



The Ethernet Transport Service supports use of IEEE 802.1Q VLAN. Ethernet traffic received at separate physical or virtual (VLAN) ports is forwarded to the same or separate ETS connections based upon VLAN information that is either contained in the packets when received at the Ethernet port or added, in the form of a configurable default VLAN for respective port, to the Ethernet packets at the Ethernet port.

All layer 2 traffic forwarding decisions are based on such VLAN identification and are made at the edges of the DTM network, i.e. at the edge point of the ETS connection. This edge point will be a Fast or Gigabit Ethernet card of the network equipment that forms the interface between the connected Ethernet network/equipment and the DTM network. In the following, the term access switch refers to a device that defines such an edge point, as compared to a core switch, which performs switching of channels within the DTM network.

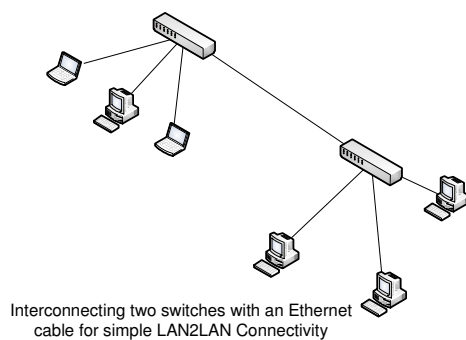
The network offers any-to-any connection, meaning that an ETS connection can be established between any Ethernet ports of the DTM network, independently of link structures or other services.



## Forwarding Function (FF)

Within internetworking, the practice of connecting network elements, one of the simplest ways to connect two or more Ethernet segments is by means of a straight cable between Ethernet switches (see illustration below).

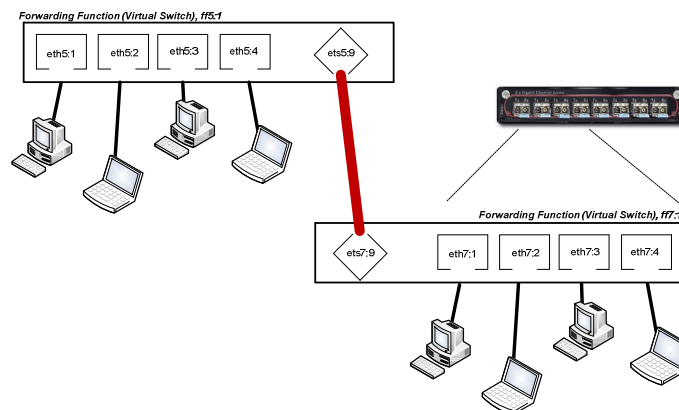
ETS allows the Nimbra network to be used as a connection within different Ethernet segments, providing transparent point-to-point Layer 2 connectivity, basically replacing the Ethernet cable in the picture below with the Nimbra Network, allowing a secure and very distant Ethernet connectivity with 100% QoS between segments.



The cornerstone of the Ethernet configuration model, the Forwarding Function (FF), is a virtual Ethernet switch defined on a module.

Each Forwarding Function is associated with a number of interfaces: anything that serves as an end-point of an Ethernet connection is called interface.

An interface may be a physical Ethernet port (ETH) or a virtual port of an Ethernet Transport Service (ETS) through the Nimbra Network. ETS endpoints of a DTM channel are connected to different forwarding functions (see picture below).



Note how similar the two pictures above look like: just replace the “real switches” with Forwarding Functions (FF) (virtual Ethernet switches) and the cable interconnecting the two switches with an ETS channel (DTM channel) through the Nimbra network.

While a Nimbra One/300 can be configured with only one Forwarding Function, for the Nimbra 680’s “8 x Gigabit Ethernet Access Module”, it is possible to have 8 separate Ethernet switches (FFs) on one board, configured with up to 255 ports, 8 physical (on the front) and 247 “logical” that is the ETS channel end points.

The FF is created and deleted by the user. The first time an 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.

node10 ► Ethernet ► Forward. Functions ► ff7:1 Basic Settings

Name: ff7:1  
Device: eth7

Basic Settings Diffserv Spanning Tree Statistics

Customer ID: 0  
Purpose:   
VLAN Mode: transparent  
Mac Mode: transparent (nac)  
Mac Aging Time: 300 seconds  
Spanning tree: auto  
Jumbo frames: on

OK Apply Delete Cancel

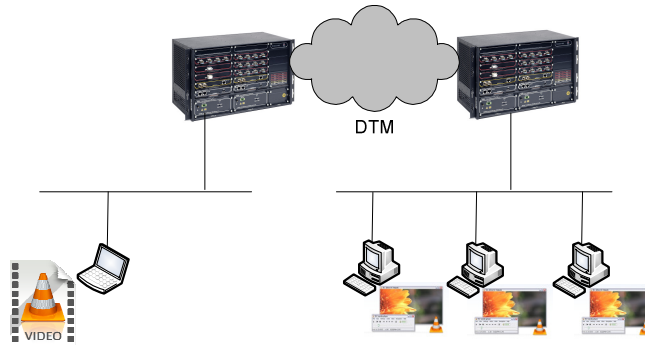
A Forwarding Function can currently be set in two different VLAN modes:

- **VLAN mode transparent:** the frames are forwarded unchanged. In this way it is possible to configure the DTM network to act as a completely transparent Ethernet transport vehicle, to work as a very long Ethernet extension cable.
- **VLAN mode customer:** 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. Pre-GX4.5, the configuration model used this model. For all Nimbra One/300 nodes, VLAN mode is preconfigured to Customer. This is also the only available alternative.

## Transparent Ethernet switching

### Goal

The goal of this lab is to configure a transparent Ethernet service through an existing DTM-network and to verify the connectivity of the service distributing a multicast UDP video from one Ethernet segment to another.

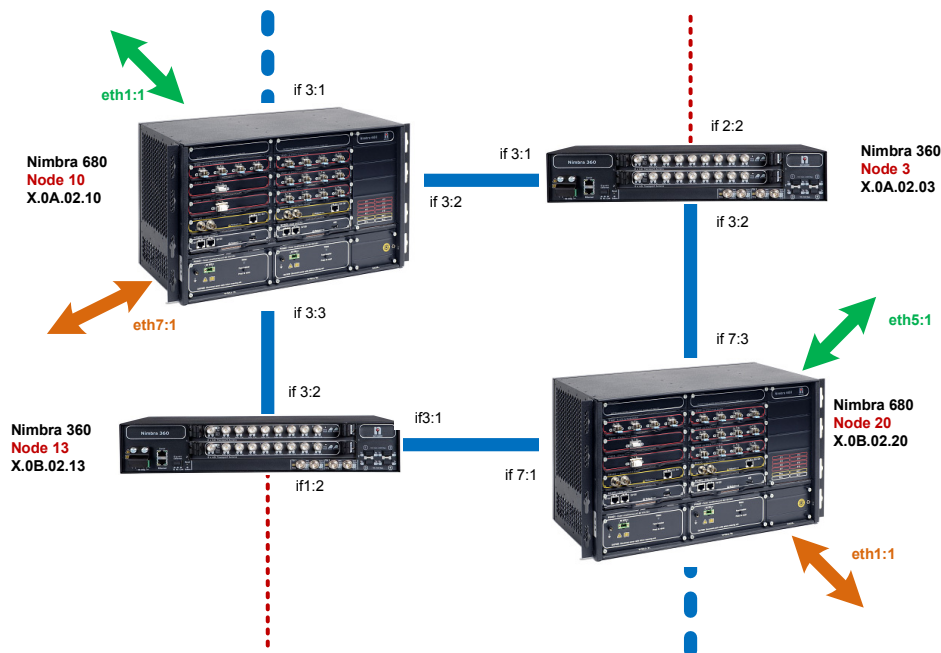


Set up Transparent ETS connections between node 10 and 20

Group A will choose one port of the “8 x Gigabit Ethernet Access Module” in slot 1 on node10 and one port of the “8 x Gigabit Ethernet Access Module” in slot 5 in node20.

Group B will choose one port of the “8 x Gigabit Ethernet Access Module” in slot 1 on node20 and one port of the “8 x Gigabit Ethernet Access Module” in slot 7 in node10 (see illustration below).

### Lab. 10 ETS, Transparent



For Group A, the Forwarding Functions ff1:1 and ff5:1 must be configured the same way. In order to create and configure the forwarding functions, follow the [Ethernet](#) link. Use the following settings:

node10 ► Ethernet ► Forward Functions ► ff1:1 Basic Settings

Name: ff1:1  
Device: eth1

Basic Settings Diffserv Spanning Tree Statistics

Customer ID: 0  
Purpose:   
VLAN Mode: transparent  
Mac Mode: auto (nomac)  
Mac Aging Time: 300 seconds  
Spanning tree: auto  
Jumbo frames: on

OK Apply Delete Cancel

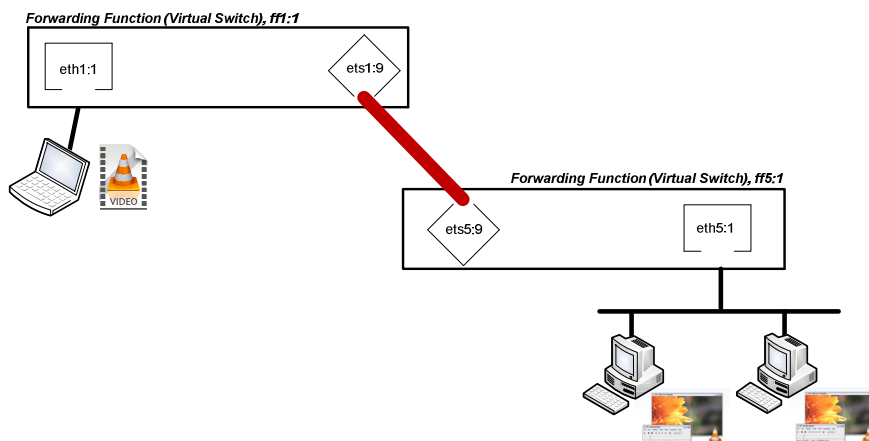
Interfaces

Name	DSTI	Mode	Adm	Oper	FF	Destination	Speed in	Speed out	Purpose
eth1:1			up	up	ff1:1		100 Mbps	100 Mbps	
ets1:9	0	uc	up	up	ff1:1	node20	20 Mbps	20 Mbps	

With these settings, VLAN tags are ignored. All packets are forwarded to the interface they didn't arrive on. The Ethernet interfaces (eth1:1 and 5:1) must be tied to their respective Forwarding Function (ff1:1 and ff5:1).

In order to create an Ethernet unicast connection between ets1:9 and ets5:9, an Ethernet service must be set-up on two different web pages. The local DSTI number must match the destination DSTI configured on the other configuration page.

The following picture shows how Ethernet ports, ETS interfaces and Forwarding Functions are related to each other, in the case of Transparent VLAN mode and unicast ETS interface.



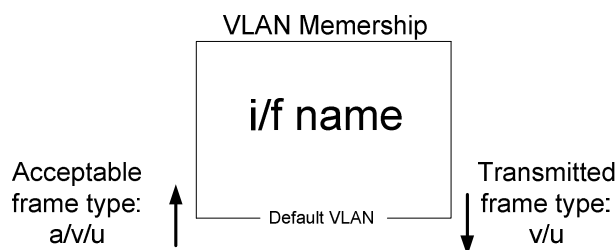
## ETS Customer mode (VLAN switching)

Forwarding is based on VLAN ID only so that incoming packets are forwarded/switched to the interfaces belonging to the same FF and (customer) VLAN (see VLAN Membership).

This is the only mode supported in Nimbra One/300 products.

When Switching is based on VLANs then 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 (Default VLAN in picture below) in case no VLAN tag is included in the incoming frame (i.e. in all untagged, received frames).

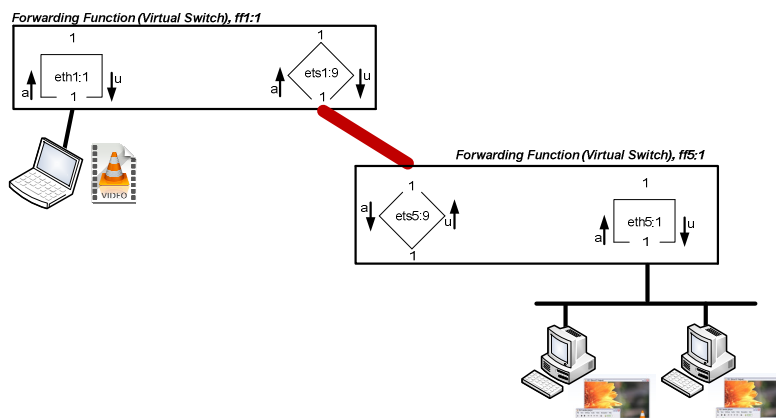
Each interface, both Ethernet and ETS, need to be configured with the parameters that are illustrated below. See Element Manager User Guide for more information.



Since forwarding/switching is based on VLAN tags, we have to rethink the configuration model taking into account the parameters above.

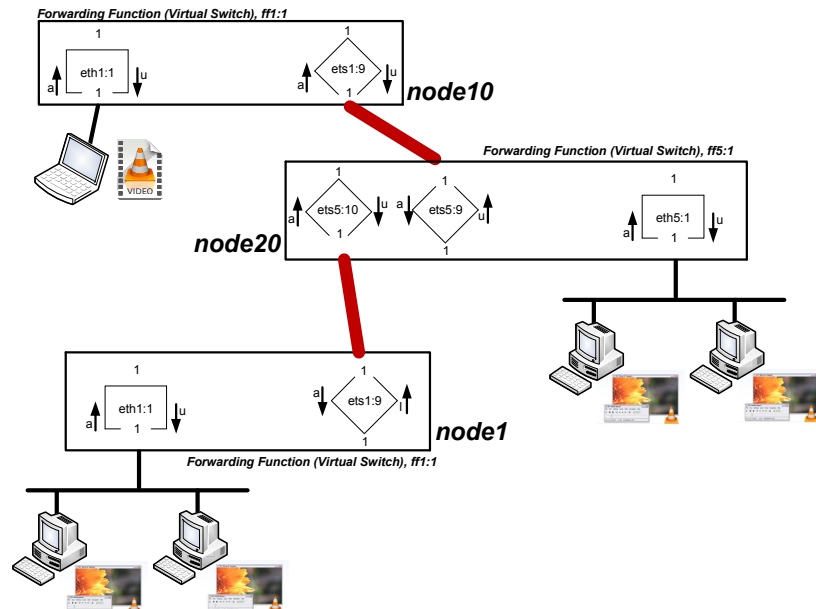
You can modify the FFs and interface settings of the previous exercise (ETS transparent) and convert all to Customer mode.

The picture below will help to see how the different VLAN settings should be used. In this case we'll use VLAN tag 1, but any VLAN value can of course be used – as long as you do it consistently.



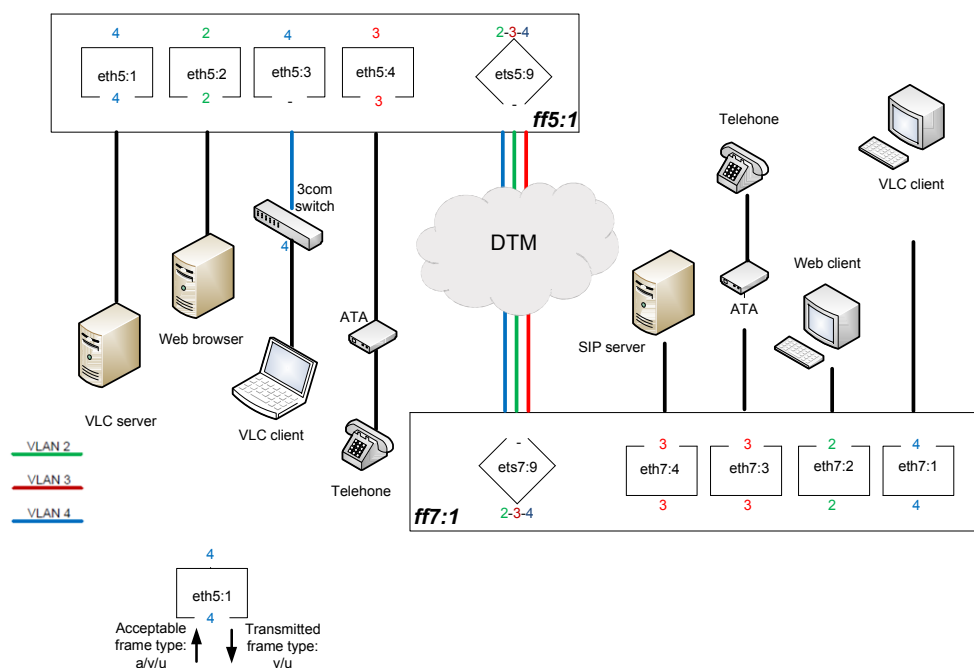
If you want to add an Ethernet segment from another Nimbra node, for instance node1, then you configure as below: adding a new ETS interface, belonging to the same VLAN, that connects to node1.

Forwarding functions are tied to the module on which they are active. On Nimbra One/300, there can be only one FF per interface module (or Gigabit Ethernet Access Port). On Nimbra 600 nodes, there can be up to eight FFs per module.



The following picture illustrates a more general example where different VLANs are used to separate services (Video, VoIP, Data) entering the Ethernet Access Module. All of them are carried by a single DTM channel that acts as VLAN trunk.

On the other side, the services are split to different ports on the destination Ethernet Access Module.



## ETS Multicast

As mentioned before, it is also possible to configure an ETS multicast, which is a unidirectional, point-to-multipoint service connecting one ingress point and several egress points.

To establish an ETS multicast choose “Create Multicast ETS i/f” when you are creating an ETS interface and then click the link “Destinations”.

The screenshot shows the configuration window for 'ets7:9 Basic Settings'. The 'Destinations' tab is selected, indicated by a red arrow. The window displays the following settings:

- Interface name: ets7:9
- Forwarding function: ff7:2
- Device name: eth7
- Administrative status: Up (dropdown)
- Operational status: up
- Last changed: 23:33:55
- Customer ID: 0
- Purpose: (empty text field)
- Forwarding function: ff7:2 (dropdown)
- Interface type: ETS
- Local DSTI: 3
- Active speed in: 0.000 Mbps
- Active speed out: 0.000 Mbps
- Acceptable frame type: all (dropdown)
- Default VLAN: 1
- Transmitted frame type: vlantagged (dropdown)
- Requested capacity: 20,000 Mbps (uses 0 slots)
- Suppress primary source-route alarm: ☒

At the bottom, there are buttons for OK, Apply, Delete, and Cancel.

In the same way like you configured a ITS multicast, here you select all the nodes and DSTI where this originating ETS is going to terminate.

## Lab. 12 Performance Monitoring

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.

If an end user has a problem with the signal in the end-equipment, the PM function can be used to isolate the problem as either internal to the DTM network or external to it.

### Goal

In this exercise you practice configuration of performance monitoring from the web interface.

### Performance Monitoring Set-up

In order to configure all performance monitoring parameters, proceed as follows:

Navigate to the 'Perf. Monitor' menu and click on the link General to set-up the maximum number of entries in the small and in the large history log.

Small history: Consist of 15 entries of 15 minute and 1 entry of 24 hrs

Large history: Consist of 96 entries of 15 minute and 30 entry of 24 hrs

Click on the Trunks or Accesses link, in order to configure a trunk or an access interface. Click on the particular trunk or access interface to start performance measurement. Set the **Administrative Status** to 'Up' in the drop-down menu.

Click on the Configure link at the top of the page. Set the **Administrative Status** to 'Up' by selecting it from the drop-down menu. Edit the Performance Monitoring parameters for the connection and click on the 'OK' or 'Apply' button to set the changes.

Performance Monitoring counters are accumulated in intervals of 15 minutes (15m) and 24 hours (24h). The counters are described below.



Counter	Description
<b>Suspect</b>	If the parameter is 'yes', then the counters could be less accurate than 100%. This is often set to 'yes' during the first (incomplete) period.
<b>Zero sessions (ZS)</b>	Number of faultless sessions (i.e. periods) before (and not including) the current period.
<b>Errored Second (ES)</b>	One second of available time containing one or more Errored Blocks (EB) or at least one defect.
<b>Severely Error Second (SES)</b>	One second of available time containing $\geq 30\%$ Errored Blocks or at least one defect. Ten consecutive SES starts UAT (UnAvailable Time) while ten consecutive non-SES stops UAT. SES is a subset of ES.
<b>Background Block Error (BBE)</b>	Number of EB during one second of available time not part of SES.
<b>Unavailable Second (UAS)</b>	One second of UAT. During UAT, calculations of BBE, ES and SES are inhibited and no data collection of them is performed.
<b>Slip Second (SS)</b>	One second with a slip, i.e. a loss of one or more sequential frames. The cause is buffer under- or overflow.

**Figure 13. Description of performance monitoring parameters**

## Lab. 13 Scheduling of connections

Although the mechanisms for provisioning and reconfiguration of connections for ITS and ETS services are easy and fast to use, they typically 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 or change of a certain connection in future. It also allows the operator to schedule events to occur on a 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 the establishment of an SDI channel 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.

An important aspect to note is that a scheduled connection is denied if there is a lack of capacity in the network at the actual time when the operation is scheduled. Thus, reliable scheduling requires good planning and control of resources and utilization in the network.

### Goal

In this exercise, you learn to schedule actions from the web interface.

### Scheduling set-up

The scheduler function can be reached in the following ways:

#### ITS→Scheduler

Allows creation of new ITS schedules and lists all schedules for ITS connections.

#### 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 of and ITS service.

### Example

Navigate to the ITS menu and click on the Scheduler link. Select for which ITS the scheduled connection is going to be defined. In the drop-down menu, the scheduling is created.

Click on **Daily** and fill in **Start** and **Stop** time. Enter the **Requested capacity** and select **Established**. Finally, Set the **Admin Status** to 'Up' and click **OK**.

The administrative status in the scheduling entry must be set to 'up' in order to activate the scheduling mechanism. If the administrative status is 'down', the entry is visible in the scheduler list, but no scheduling takes place.

The operator must also choose whether the connection from the TTP shall be "Established" or "Unestablished" during the active scheduling interval. For variable bit-rate services (Ethernet and ASI transport), choosing "established" also implies choosing the capacity for the connection during the established period. Choosing the value of the TTP as "Established" is the recommended practice.

# Appendix A - Start of PC

## Start of PC

Log in to the PC.

Username: Administrator (utbildning)

Password: 4neti

## Define IP settings of Nimbra nodes

The required IP settings are made in Lab. 1. Follow this description and set IP addresses, unless they already have been set.

All Nimbra nodes have IP addresses on 192.168.234.0/24 subnet.

Node 1 has the IP address 192.168.234.1

Node 2 has the IP address 192.168.234.2 etc.

## Start the web browser

Log in to the unit with a web browser (Mozilla 2.0.0.14/Internet Explorer 7 or higher).

Enter the name or the IP-address of the unit in the address field. Entering the name requires proper DNS settings and that the association between IP addresses and unit names have been defined in the C:\WINDOWS\System32\drivers\etc\hosts file.

## Log in to the node

Login: root

Password: neti