

Nimbra Vision, Management System

Net Insight Academy
Course NPC0004-0001

 net insight™

© Net Insight 2010

Contents

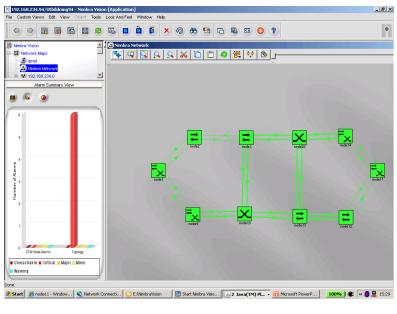
- Introduction
- The management network
 - [SNMP](#), [DLE](#), [Server redundancy](#), [Redundant networks](#)
- Server
 - [Architecture](#)
 - [Initial configuration](#)
- Client
 - [General](#)
 - [Maps](#)
 - [Network Database](#)
 - [Centralized Inventory](#)
 - [Object operations](#)
 - [Configurations](#)
 - [Fault management](#)
- Network-wide Software upgrade
- Redundant networks
- Searching and filtering
- Service provisioning
- Channel list and trace
- Performance monitoring
- Policies
- Pre-emption
- Headend protection
- Security management
- Misc
 - [Backup](#)
 - [Checklist](#)
 - [Clients](#)



Introduction Nimbra™ Vision

Key features

- Auto-discovery of Devices
- Topological Device Maps
- Fault Management
- Performance Management
- Service Provisioning
- Centralized network view
- Full FCAPS functionality
- Head-end protection and pre-emption



Nimbra Vision Essential Data

Description:
Nimbra Vision completes the multiservice Nimbra network, with management capabilities that result in a superior and cost-effective network for demanding applications.

Nimbra Vision allows the operator to provision services end-to-end across the network with full graphical support. Source and destination nodes are selected from the Nimbra Vision map. If automatic routing is chosen the actual route through the network may easily be displayed in the map using the Channel Trace function. Similarly, synchronization paths can be displayed using the Sync Trace function.

The option of predefined source routing is also available in Nimbra Vision, again using the map to quickly define the path through the network.

© Net Insight AB 2010

Web Interface

• Status Monitoring

- Alarms and Events
- Equipment inventory

• Maintenance

- Initial configurations
- Backup of configurations

• Network configuration

- Interfaces
- Addresses
- Routes

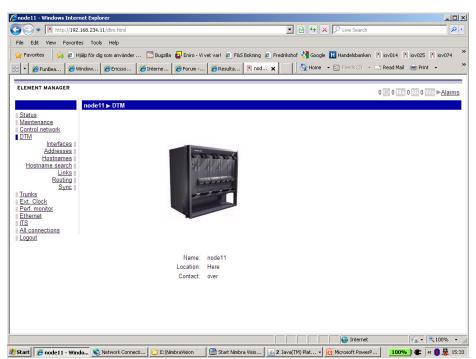
• Service Provisioning

- Set-up of services (ITS/ETS)
- Source routing
- Scheduling

• Performance Monitoring

• Built-in http server in each NE

• Complete management tool for the node



Network Management Products

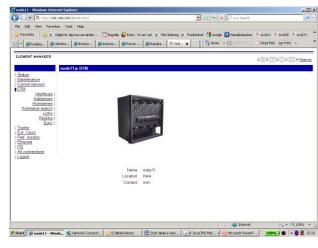
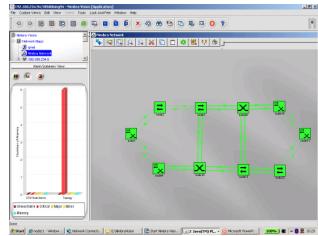


• Element Manager:

- Web access to network elements (HTTP) for access from a web browser
- Telnet access (CLI)

• Nimbra Vision Network Manager

- Managing multiple network elements in a network

© Net Insight 2010

SNMP

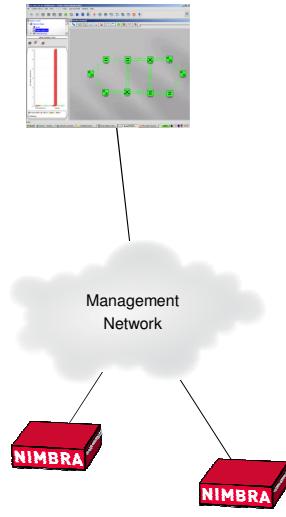


- Nodes support SNMP
- SNMPv1/v2c/v3
- get
- get-next
- get-bulk
- Set
- Notifications
- Network is e.g. UDP/IP

Supports:

- Selected parts of MIB-II
- Enterprise MIBs

Management Network



© Net Insight 2010

Managed information



- Pieces of data used for managing the unit
- Examples:
 - Integer value
 - Counters
 - Time stamp
 - Text string
- Organized as scalars or tables

Net Insight Enterprise MIBs



- | | |
|------------------------|-------------------|
| • Common | (neti-common-mib) |
| • Alarms and events | (neti-event-mib) |
| • Configurations | (neti-config-mib) |
| | |
| • Interfaces and links | (neti-dtm-mib) |
| • PM | (neti-pm-mib) |
| • Trunk | (neti-trunk-mib) |
| | |
| • ITS [Video/PDH] | (neti-its-mib) |
| • ETS [Ethernet] | (neti-eth-mib) |
| • Channels | (neti-chmgr-mib) |

MIB - Managed Information Base

```

graph TD
    iso[iso] --- org[org]
    org --- dod[dod]
    dod --- internet[internet]
    internet --- private[private]
    internet --- mgmt[mgmt]
    private --- enterprises[enterprises]
    enterprises --- netinsight[netinsight]
    enterprises --- cisco[cisco]
    mgmt --- mib2[mib-2]
    mib2 --- system[system]
    system --- sysName[sysName]
    system --- sysUpTime[sysUpTime]
    netinsight --- ellipsis1[...]
    cisco --- ellipsis2[...]
  
```

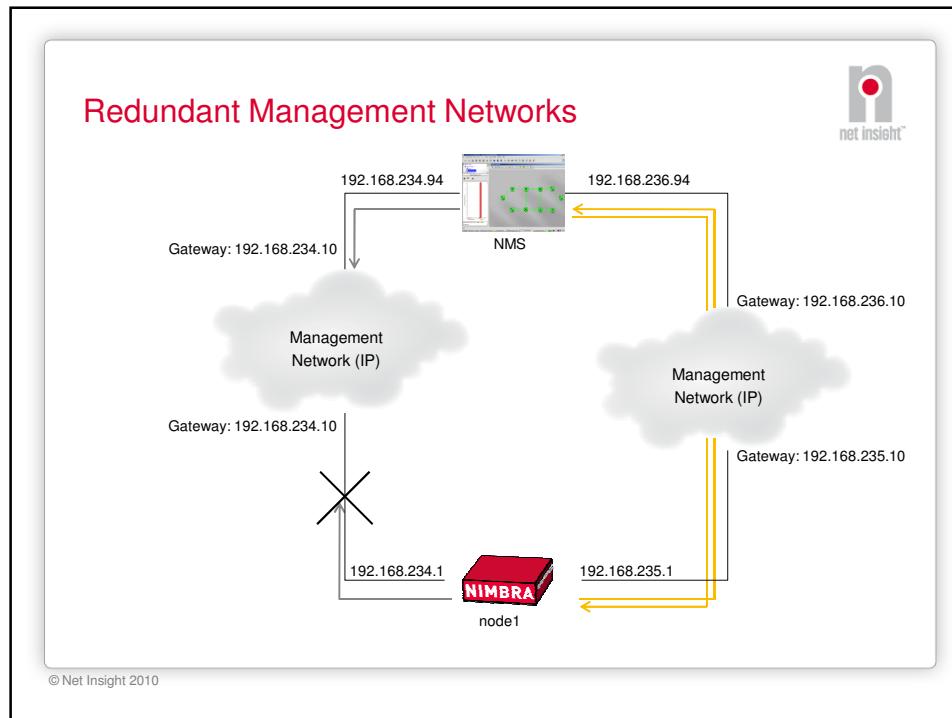
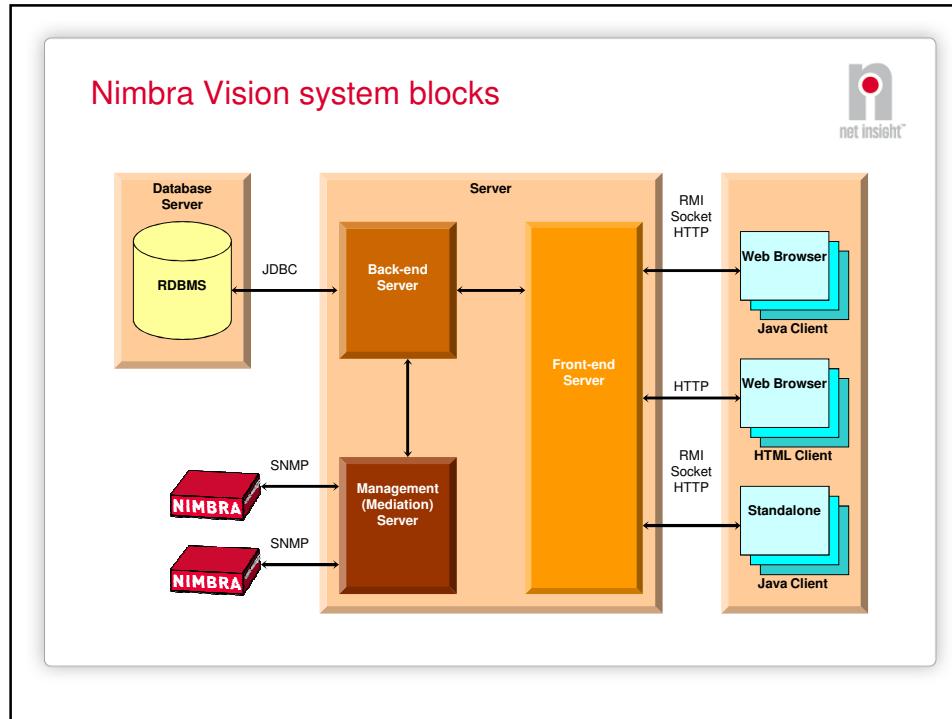
The diagram illustrates the MIB (Managed Information Base) hierarchy. At the top is the ISO organization node, which branches into 'org' and 'dod'. The 'dod' branch leads to the 'internet' node, which further branches into 'private' and 'mgmt'. The 'private' branch leads to the 'enterprises' node, which branches into 'netinsight' and 'cisco'. The 'mgmt' branch leads to the 'mib-2' node, which branches into 'system'. The 'system' node contains two leaf nodes: 'sysName' and 'sysUpTime'. Ellipses indicate additional nodes under 'netinsight' and 'cisco'.

- Global, hierarchical name space: ensures unique name
- iso.org.dod.internet.private.enterprises.neti nsight...
- 1.3.6.1.4.1.2928...
- Managed information in leafs only

Management Architecture

The diagram shows the management architecture. At the top, a yellow box labeled "Management station/local terminal" contains three components: "Terminal emulator", "Web browser", and "SNMP Manager". These components interact with a central cloud labeled "DCN (IP)". Below the cloud, a red box labeled "Network element" contains several management interfaces: "FTP", "Telnet", "Web server", and "SNMP agent". To the right of the "SNMP agent" is a red block labeled "NIMBRA". A yellow box at the bottom, labeled "Management information", contains five categories: "Alarms", "Configuration", "DTM MIB", "MIB-II", and "Etc.". Arrows point from the management station components through the DCN to the network element's management interfaces, and from there to the management information box.

© Net Insight 2010



Management



© Net Insight 2010

- In Band and Out Band

In-band Management



- Possible to access nodes without a parallel network used for:
 - Remote log in
 - Management
 - Nimbra Vision
 - 3rd party equipment
 - Redundancy
 - In-band and Out-band network
 - Multiple In-band networks

Out-band

- IP
- ISDN
- PSTN

Management station

Ethernet

In-band (DLE)

Ethernet or serial

Router/terminal server

NIMBRA

Emulation of LAN using the Nimbra network.

In Band DLE

• Lab network

In-band and DLE – What is it?

- DTM LAN Emulation
- Used only for in-band management network
- Emulates an IP sub-network using the existing DTM network (DLE segment)
- IP routing must be set-up between DLE segment and other IP sub-networks
- Totally secure from other channels transporting IP over ETS

In-band



- DLE Server
 - Responsible for the segment:
one server per segment (multiple)
 - A DLE Server can only be used for in-band management
- DLE client
 - Provides IP interface to segment in each node
- Every client has one channel to the server
- The server has one multicast channel to all clients
- Automatically sets up channel from client to client when IP data is sent
- Automatically tears down channel when not used

DLE segment

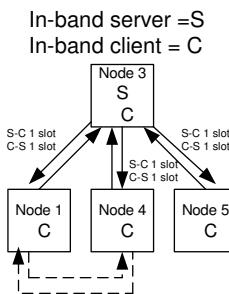


- Every DLE segment has one DLE server
 - Responsible for providing information to the DLE clients about the other nodes in the segment
 - Enables the clients to establish their connections
- Channel between DLE Server and DLE Client
 - Permanent channels between client and server, since they always must be able to communicate
 - The channels between the DLE server and DLE clients are used to distribute broadcast packets
 - The broadcast packets from a client is sent to the server, and then distributed to all the other clients on the segment, i.e. broadcast packets does not result in establishment of new channels between two clients.

In-band, Client to Client



- DLE Client asks DLE server - where is “MAC address/DTM address ”
- Server answer “MAC address/DTM address” is here
- Client to Client channel is established between the two clients



In-band, DLE Segments



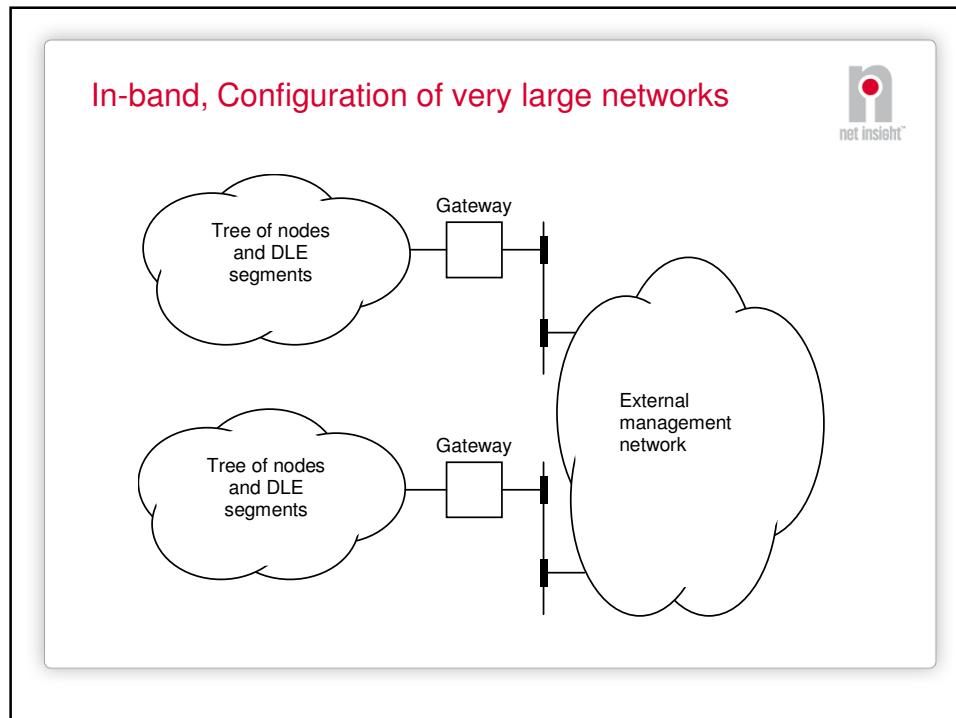
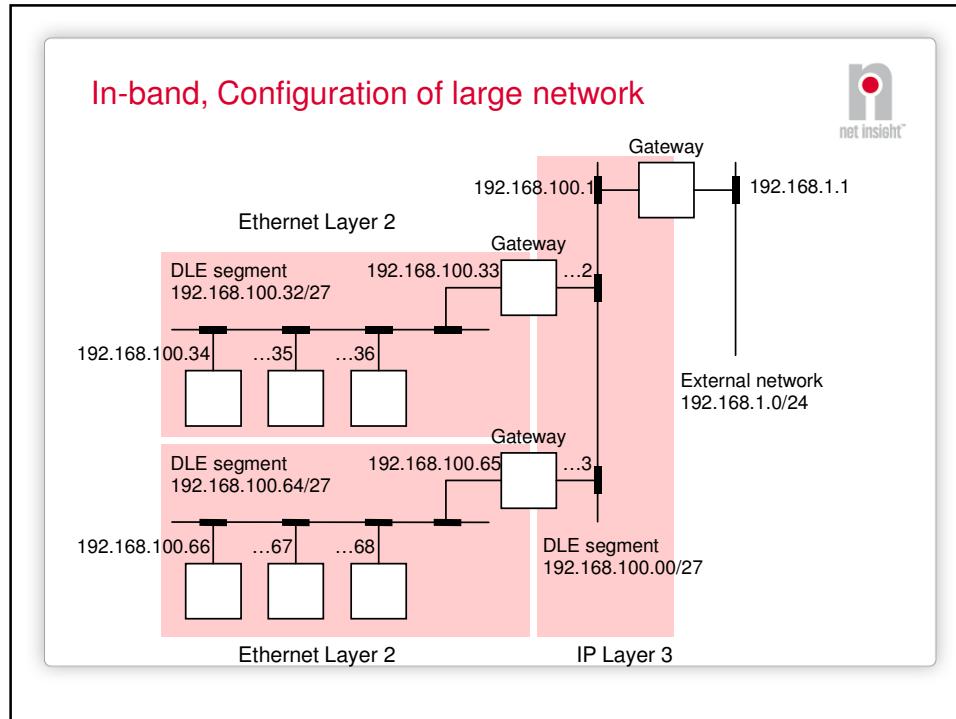
- Several DLE segments can coexist in a DTM network
 - Each DLE segment requires its own DLE Server
 - The DLE Server forwards broadcast packets to all DLE Client's within the segment
- To send data from one DLE segment to another, the packets must pass through one or several IP routers!

In-band, multiple segments

In-band server =S
In-band client = C
Gateway = GW

- DLE Client asks DLE server
- Server find the address, goes to gateway
- Routed over IP net

In-band, Configuration of a small network



In-band, Recommendations



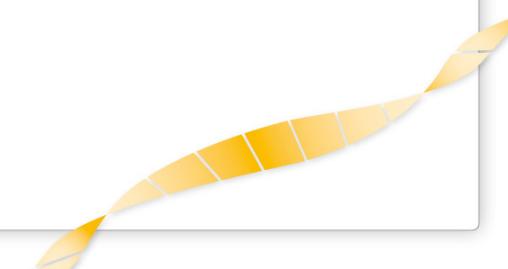
	Nimbra One	Nimbra 340	Nimbra 600
Maximum recommended number of DLE clients for one DLE server	16	16	64
When working as gateway: maximum recommended number of nodes to route traffic for	255	255	1 000
Channel capacity for DLE client-server channels	512 kbps (1 slot)	512 kbps (1 slot)	512 kbps (1 slot)
Channel capacity for DLE client-client channels	512 kbps (1 slot)	512 kbps (1 slot)	512 kbps (1 slot)
Maximum recommended number of DLE clients on a gateway	3	3	3
Time out before tearing down unused channels (flow timeout)	Configurable	Configurable	Configurable

Nimbra Vision Server



- Non-Redundant
- Redundancy
- Distributed Servers

© Net Insight 2010



Non-Redundant Configuration

net insight™

- Single server deployment (BE/FE combination)
- Optimized for simple server management
- All clients connect to a single server
- Server connects to all network elements

```

graph LR
    subgraph Network_Elements [Network Elements]
        N1[NIMBRA]
        N2[NIMBRA]
    end
    SV[Nimbra Vision Server]
    C1[Clients]
    C2[Clients]
    C3[Clients]

    N1 <--> SV
    N2 <--> SV
    SV <--> C1
    SV <--> C2
    SV <--> C3
  
```

The diagram illustrates a non-redundant configuration. It shows a central 'Nimbra Vision Server' (yellow square) connected to three clients (three computer monitors) and two network elements (red boxes labeled 'NIMBRA'). The network elements are represented by small red cubes within a cloud-like shape. Bidirectional arrows indicate communication between the server and each client and network element.

© Net Insight 2010

Redundancy

net insight™

- Redundant database servers, replicating data
- Redundant BE/FE combination (server)
- Redundant management networks
- Clients automatically reconnect to new server after fail-over

```

graph LR
    subgraph Network_Elements [Network Elements]
        N1[NIMBRA]
        N2[NIMBRA]
    end
    BEF1[BE/FE]
    DB1[DB]
    BEF2[BE/FE]
    DB2[DB]
    C1[Clients]
    C2[Clients]
    C3[Clients]

    N1 <--> BEF1
    N2 <--> BEF1
    BEF1 <--> DB1
    BEF1 <--> C1
    BEF1 <--> C2
    BEF1 <--> C3
    BEF2 <--> DB2
    DB1 <--> DB2
    DB2 <--> C1
    DB2 <--> C2
    DB2 <--> C3
  
```

The diagram illustrates a redundant configuration. It features two redundant BE/FE combinations (yellow and pink squares) connected to two redundant database servers (yellow and pink cylinders). These components are interconnected via bidirectional arrows. Each BE/FE combination is also connected to three clients (three computer monitors) and two network elements (red boxes labeled 'NIMBRA'). A dashed arrow labeled 'Replication' indicates the connection between the two database servers. The network elements are shown as red cubes within a cloud-like shape.

© Net Insight 2010

Server failover setup

© Net Insight 2010

net insight®

1. Make sure the hosts file on both servers contain the same data
2. Install NV server on primary db host
3. Install NV server on standby db host
4. Configure both NV servers to use remote db
 - i.e change from 'localhost' to 'Utbildning94' or from 'localhost' to 'Utbildning93'
5. Start mysqld on primary db host. This can be done from Explorer.
6. Start mysql client (C:/Program Files/Nimbra Vision 5.5.1/Mysql/bin/mysql –uroot –p6urk5a1l4d) in a Command Tool



Always delivering content integrity. Always simplifying complexity. Always redefining efficiency.

Server failover (cont'd)

© Net Insight 2010

net insight®

7. Give rights: >grant all on *.* to 'root'@'Utbildning94' identified by '6urk5a1l4d'
8. Give rights: >grant all on *.* to 'root'@'Utbildning93' identified by '6urk5a1l4d'
9. Enable binary logging, if not already enabled (check in conf\database_params.conf under [mysqld] that log-bin=mysql-bin)
10. Ensure ServerId = 1 on primary database (same place)
11. Give rights: >grant replication slave on *.* to 'repl'@'Utbildning94' identified by 'secret'
12. Give rights: >grant replication slave on *.* to 'repl'@'Utbildning93' identified by 'secret'



Always delivering content integrity. Always simplifying complexity. Always redefining efficiency.

Server failover (cont'd)

13. Flush all tables and lock write statements (>flush tables with read lock;)

14. DON'T CLOSE CMD TOOL

15. Read values of current binary log name and position (show master status;)

16. Write down values (file name and position)

17. Take a snapshot of the database and copy to 'Utbildning93'
➤ Copy directories (mysql\data\mysql and mysql\data\webnmsdb)

18. Reenable writing on 'Utbildning94' (unlock tables;)

19. On 'Utbildning93', set ServerId = 2 and check for binary logging.


© Net Insight 2010



Server failover (cont'd)

19. Start db (mysqld) on primary db server.

20. Start db (mysqld) on standby db server.

21. Login to db mysql client on 'Utbildning93'.

22. change master to master_host='Utbildning94',
master_user='repl', master_password='secret',
master_log_file='<recorded_file_name>',
master_log_pos=<log_pos>;

23. Start slave;

24. Show slave status;

25. Check that the setup is OK with user documentation.

26. Setup 'Utbildning94' to replicate 'Utbildning93' by repeating steps 15-17 (no lock required, no user is writing to standby db), step 22 (with 93 replacing 94) to 25.


© Net Insight 2010



Distribute Load on Multiple Hosts

net insight™

- Multiple FE servers allows more simultaneous users
 - 10 clients per FE server
- Separate front-end, back-end and database servers will improve performance in large networks

Network Elements

```
graph LR; subgraph NetworkElements [Network Elements]; NIMBRA[NIMBRA]; end; subgraph Clients [Clients]; Client1[Client 1]; Client2[Client 2]; Client3[Client 3]; end; FE1[FE] <--> Client1; FE1 <--> Client2; FE1 <--> Client3; FE2[FE] <--> Client1; FE2 <--> Client2; FE2 <--> Client3; BE[BE] <--> DB[DB];
```

© Net Insight 2010

Nimbra Vison

net insight™

- Server
- Client

© Net Insight 2010

Necessary configuration



- Before starting the server:
- On network elements
 - SNMP notification receiver
 - Event logging (size and type)
 - User for Nimbra Vision (SNMPv3)
- In Nimbra Vision
 - Hosts database
 - one entry for every IP address
- After server is started
- In Nimbra Vision
 - Network discovery parameters

Hosts database



- Maps IP addresses to hostnames (and ManagedObject names)
 - Does not rely on DNS, uses local hosts database:
C:\WINDOWS\system32\drivers\etc\hosts
(necessary when using redundant IP nets)
- For redundant management networks:
- Defines multiple IP addresses to a network element
- Order of priority is order as listed in hosts file
- Every IP address of the nodes should be in hosts file

Discovery Engine

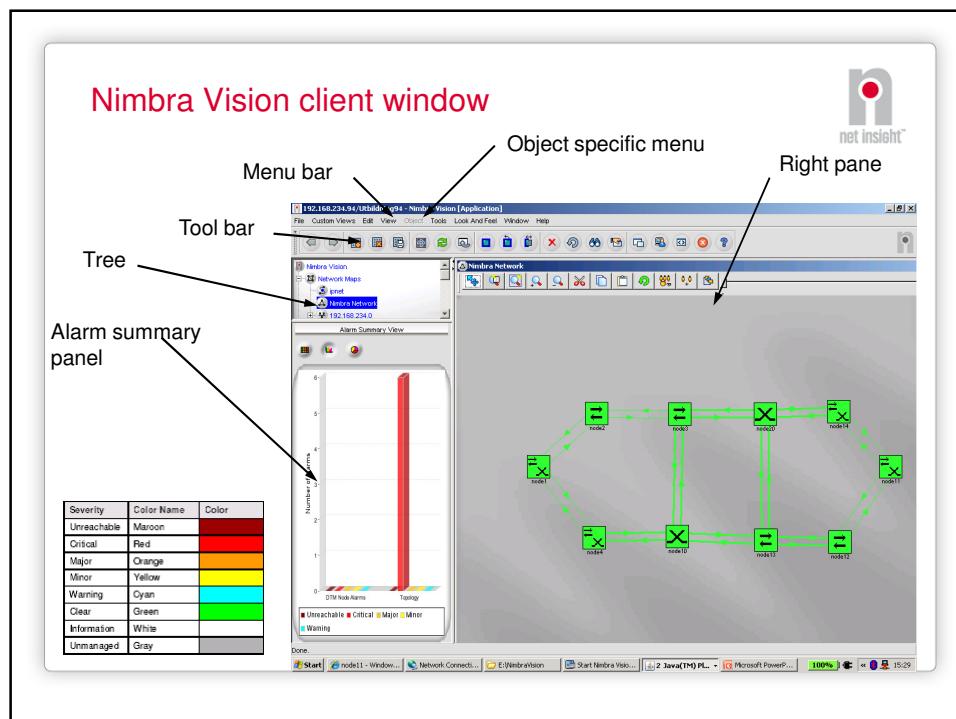
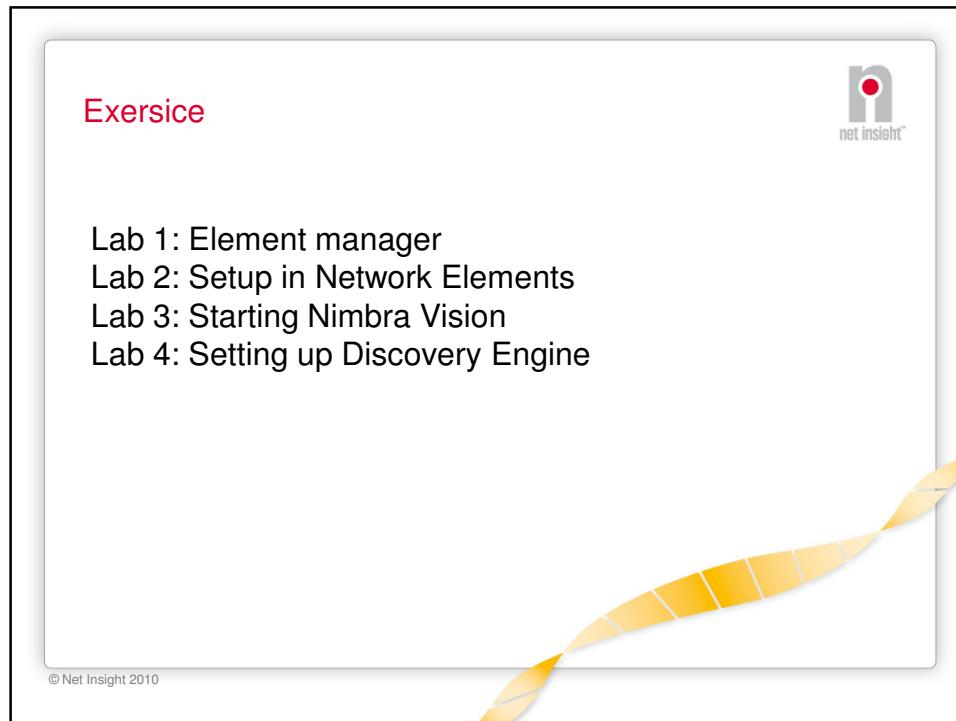


- Discovery Configurator to set-up discovery engine:
- What networks
 - IP address ranges or complete networks
- What network elements (optional)
 - individual nodes, as seed
- What type of network elements (optional)
 - filter nodes at discovery
- When to discover
- SNMPv3 access configuration

SNMPv3 access configuration



- Add user name (principal), etc., for SNMPv3 on each network, sub-network or network element
- Only Nimbra Vision (and system administrator) needs to know the user name
- Parameters to configure:
 - User Name (= principal)
 - Context Name (empty)
 - Agent Port (161)
 - Security Level (AuthNoPriv)
 - Auth Protocol (MD5)
 - Auth Password



The tree

Tree with access to different panels

Panels are shown in right pane

Panels:

- Maps
- Alarms/Events (fault management)
- Configuration (audit)
- Performance (counters and stats)
- Network Database
- Admin tools (policies)
- SNMP tools

Maps and Topology

- Map shows Nimbra network (link) topology
- Symbols represent nodes, color represent alarm status
- Link color represents status, thickness represents capacity
- Labels on symbols and links
- IP map shows management network topology
- Auto-discovery
- Access to Element Manager (Web/CLI)
- Background image possible
- Groups and hierarchical/linked maps

© Net Insight 2010

Working with maps

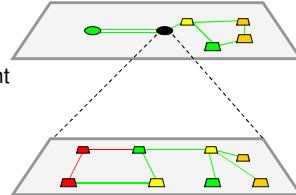


- In map
 - Select, select multiple
 - Zoom
 - Pan
 - Zoom-window
 - Cut/Copy/Paste/Move
 - Group/Ungroup
 - Undo
- With map
 - Save
 - Refresh
 - Re-layout
 - Add
 - Delete
- Map properties
 - Lock placement (anchor)
 - Background image
 - Layout (*)
 - Placement (*)
 - Renderer (*)
 - Criteria (what to show)
- (*) Default's optimized, but can be modified

Hierarchical maps



- Two ways to create:
- Group symbols in map
- Link sub-maps to symbols in parent maps
 - Create sub-maps
 - Create symbols linked to sub-maps in parent map
 - Create links



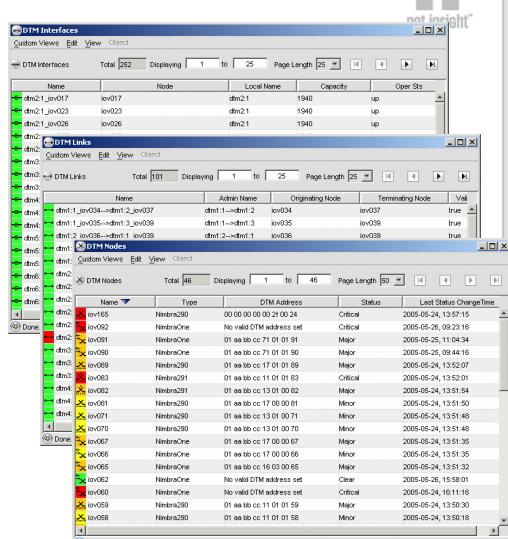
Exesice



© Net Insight 2010

Lab 5: Maps

Network database



- Network database contains all network devices (e.g. network elements, interfaces and links)
- Standard views per default

Update



- The status of an Network Element is checked and updated periodically (2 minutes), and when notification is received from Network Element.
- If a notification sent from Network Element never reached Nimbra Vision, the update function will update Nimbra Vision with the missing data.

Refresh



- Refresh: will replace all the information about a Network Element in Nimbra Vision:
 - Throws away current info
 - Reads new info from Network Element
- Refresh is invoked automatically when an object is:
 - (Re-)discovered
 - Updated, and cannot find all lost events
 - Manual invocation

Manage/UnManage



- When a managed object (MO) is managed, Nimbria Vision will monitor the corresponding Network Element (or network)
- When a managed object (MO) is UnManaged, Nimbria Vision will ignore the Network Element (or network), ignoring alarms, notifications, status update etc.
- You can change if an MO shall be Managed or UnManaged
- When an MO becomes managed, it will immediately be updated (and as a result, possibly refreshed)

Start/stop discovery



- Discovery is normally scheduled in Discovery Configurator
- Discovery is always done when discovery is started, which happens at start of the server, and when manually started
- To re-start discovery of a network, stop and then start discovery of the network

Add/Delete Managed Object



- Adding a new network or a network element
 - If you have a new network element
 - If you have a new network
 - If you don't want to wait for the Discovery Engine
 - Add is available from Network Database
- Deleting a network or network element
 - Deletes all the data associated with the MO

Exersice



- Lab 6: Network database
- Lab 7: Manage/Unmanage
- Lab 8: Delete and add nodes
- Lab 9: Start/stop discovery

© Net Insight 2010

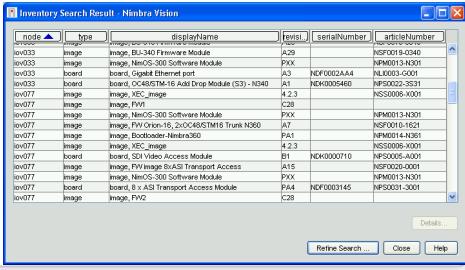
Centralized Inventory

• Inventory data (includes all Field Replaceable Units (FRU)) is automatically discovered

- Data such as hardware modules, application packages, software, etc.

• Stored in the Nimbria Vision database

• Inventory data is searchable, result presented in a table



node	type	displayname	fwinstJ	serialnumber	articleNumber
iov033	Image	Image_BLU340 Firmware Module	A29	NPF0019-N040	
iov033	Image	Image_NimOS-300 Software Module	PXX	NPM0013-N001	
iov033	board	board_Gigabit Ethernet port	A3	NDF0002AA4A	NL0003-5001
iov033	board	board_NIM-16 Add-Drop Module (S3) - N540	A1	NDF0005AB0	NFS0022-3031
iov037	Image	Image_VEC_image	4.2.3		NFS0001-3001
iov077	Image	FV2	C28		
iov077	Image	Image_NimOS-300 Software Module	PXX	NPM0013-N001	
iov077	Image	Image_NimOS-300 Software Module	A7	NPF0018-N051	
iov077	Image	Image_BlockDevice_Nimra300	P41	NPM0014-N001	
iov077	Image	Image_VEC_image	4.2.3		NFS0008-X001
iov077	board	board_SD Video Access Module	B1	NDF0000710	NFS0005-A001
iov077	Image	Image_NimOS-300 Transport Access	A15		NPM0013-N001
iov077	Image	Image_NimOS-300 Software Module	PXX	NPM0013-N001	
iov077	board	board_8x A3 Transport Access Module	P44	NDF0003145	NFS0031-3001
iov077	Image	FV2	C28		

Object operations – general

• An object is something that is known by Nimbria Vision

- Network element
- Interface
- Link
- Alarm
- Statistics report
- Etc...

• Select object in map (or list) to enable object specific menu

• Object specific menu contains operations on object

Object operations – DTM Management

net insight™

- Link and interface usage/capacity
- Link and interface status
- DTM interface configuration
- View originating/terminating connections

Operations on

- Network elements
- Interfaces
- Links

Link Utilization

net insight™

- Link utilization previously available:
- In the database (for all transmit trunk interfaces)
- As a pop-up window in the map (selectable per link)
- Highlighting of utilization for all links in the map
- Gives quick overview of current link load and possible need for capacity upgrades
- Link color green, yellow or orange depending on utilization, default is:
 - Green 0 - 50%
 - Yellow 50 - 75%
 - Orange > 75%

Object specific operations – Miscellaneous

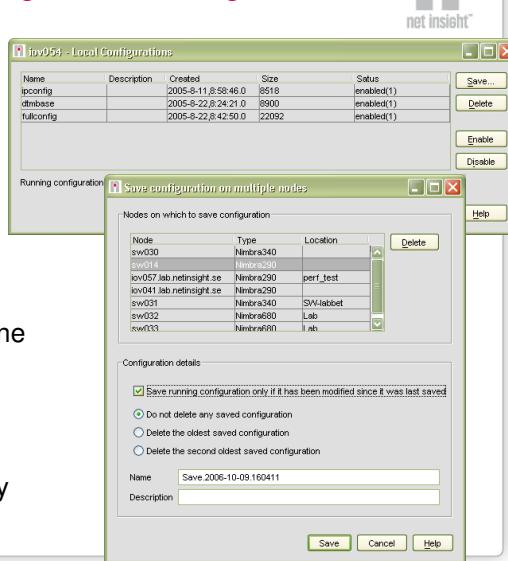


- System info (name/contact/location)
- Open element manager (web browser to network element)
- Open CLI (telnet session to network element)
- View mounted boards
- View object details
- Ping (IP)
- Trace route (IP)
- Refresh
- Manage/UnManage

Object operations – Configuration Management



- A local configuration is a persistent storage containing all the information in the node
- Manage local configurations
- Save/delete
- Enable/disable
- Save on multiple nodes in one operation
- Optionally delete old configurations prior save
- Can also save using a Policy



Name	Description	Created	Size	Status
ipconfig		2005-8-11, 8:58:46.0	8518	enabled(1)
dtmbase		2005-8-22, 8:24:21.0	8900	enabled(1)
fullconfig		2005-8-22, 8:42:50.0	22092	enabled(1)

Save configuration on multiple nodes

Nodes on which to save configuration:

Node	Type	Location
sw030	Nimbra340	Lab
lov051_lab.netinsight.se	Nimbra390	perf_test
lov041_lab.netinsight.se	Nimbra390	
sw031	Nimbra340	SW-labnet
sw032	Nimbra380	Lab
swr033	Nimbra600	Lab

Configuration details:

Save running configuration only if it has been modified since it was last saved

Do not delete any saved configuration

Delete the oldest saved configuration

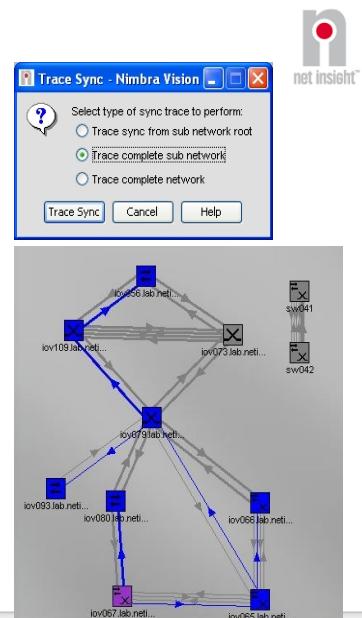
Delete the second oldest saved configuration

Name: Save 2006-10-09 160411
Description:

Save Cancel Help

Sync Trace

- Synchronization paths automatically set up by the network
 - Sync trace function in Nimbria Vision displays sync paths and master node(s)
 - In a table
 - Highlighted in the map
 - Three sync trace options
 - From root to selected node
 - Complete subnetwork
 - Complete network



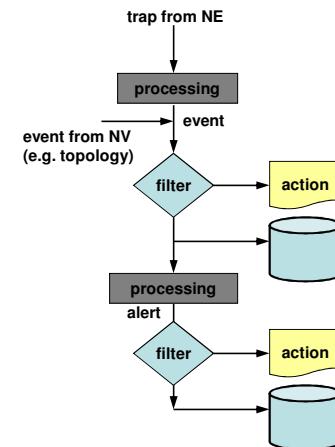
Exersice

- Lab 10: Centralized Inventory
- Lab 11: Operations on nodes
- Lab 12: Operations on links and interfaces
- Lab 13: Local configuration files

Fault management – Traps/Events/Alarms



- Notifications (traps) are processed and becomes events
- Events are stored in the database and can be viewed
- Events are processed (correlated) and becomes alerts
- Alerts are stored in the database and can be viewed
- Alerts are presented as alarms
- Filters on events and alerts can e.g. run an action
 - Send SNMPv1 trap
 - Send e-mail
 - Run command
 - Remove event/alert
 - ...



Fault management – Alarm properties



- According to X.733:
- Probable Cause
- Type
- Severity
- Message
- Alarming Object
- Time stamp
- Also
- Purpose, if alarming object has that information
- Purpose is defined in e.g. Element Manager

Fault Management

The screenshot shows the Fault Management software interface. At the top, there's a menu bar with 'Custom Views', 'Edit', 'View', and 'Actions'. Below the menu is a toolbar with icons for search, refresh, and other functions. The main area has three tabs: 'Alarms' (selected), 'Source', and 'Name'. The 'Alarms' tab displays a table of 1072 alarms, with columns for Status (Minor, Warning, Critical), Source, Name, Alarm Message, Cause, Type, and Date. The table includes rows for various network interface failures like 'Failure on underlying physical network interface' and 'Power supply failure'. Below the table is a 'Done' button. To the right of the table are three summary views: 'Alarm Summary View' (Severity and Category table), 'Alarm Summary View' (Severity and Category - Graphical view with a bar chart), and 'Alarm Summary View' (Pie chart showing the distribution of alarm types).

- Alert Browser
- Alarm escalation
- Powerful searching
- Powerful filtering
- Automatic actions on alarms & events (e.g. redundant head-end switch-over, mail, SMS, forwarding...)

Fault management – Alarm filters

This screenshot shows the 'Fault management – Alarm filters' section. It contains a large list of filter criteria:

- Alarm filtering on:
- Customer
- Probable Cause
- Severity
- Node Type
- Node Name

Fault management – Alarm details

• Pickup: Acknowledge alarm

• Annotate: information about actions etc, i.e. a log book

• Properties: additional details

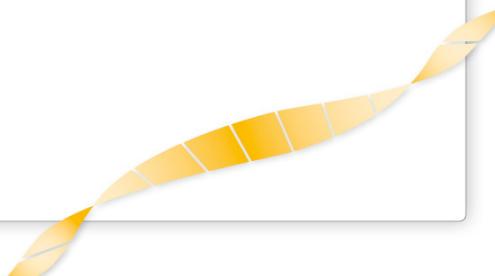
Fault management – Alarm actions

- Alarm match criteria: can set on any property
- Can pass properties to action as parameter
- Actions:
 - Suppress
 - Command
 - Trap
 - E-mail
 - Custom

Exersice

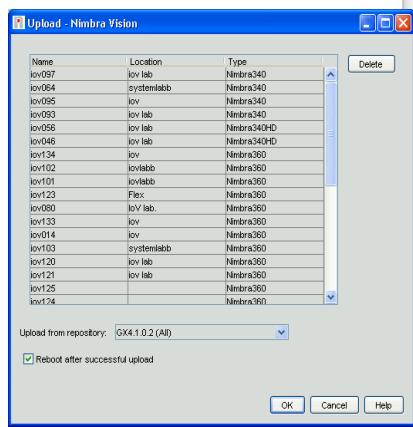
© Net Insight 2010

- Lab 14: Alarms
- Lab 15: Alarm filters and Alarm actions



Network-wide software/firmware upload

- Download of complete software and firmware package to multiple specified nodes in a single command
- Multiple software repositories may be defined for different distributions
- Rebooting of nodes either automatically after download or manually at a convenient time



Name	Location	Type
iov097	iov lab	Nimbra340
iov064	systemlab	Nimbra340
iov095	iov	Nimbra340
iov093	iov lab	Nimbra340
iov056	iov lab	Nimbra340HD
iov046	iov lab	Nimbra340HD
iov134	iov	Nimbra360
iov102	iovlab	Nimbra360
iov101	iovlab	Nimbra360
iov123	Flex	Nimbra360
iov080	iov lab	Nimbra360
iov133	iov	Nimbra360
iov014	iov	Nimbra360
iov033	systemlab	Nimbra360
iov120	iov lab	Nimbra360
iov121	iov lab	Nimbra360
iov125		Nimbra360
iov124		Nimbra360

Upload from repository: GX4.1.0.2 (All)

Reboot after successful upload

OK Cancel Help

Upload, configure

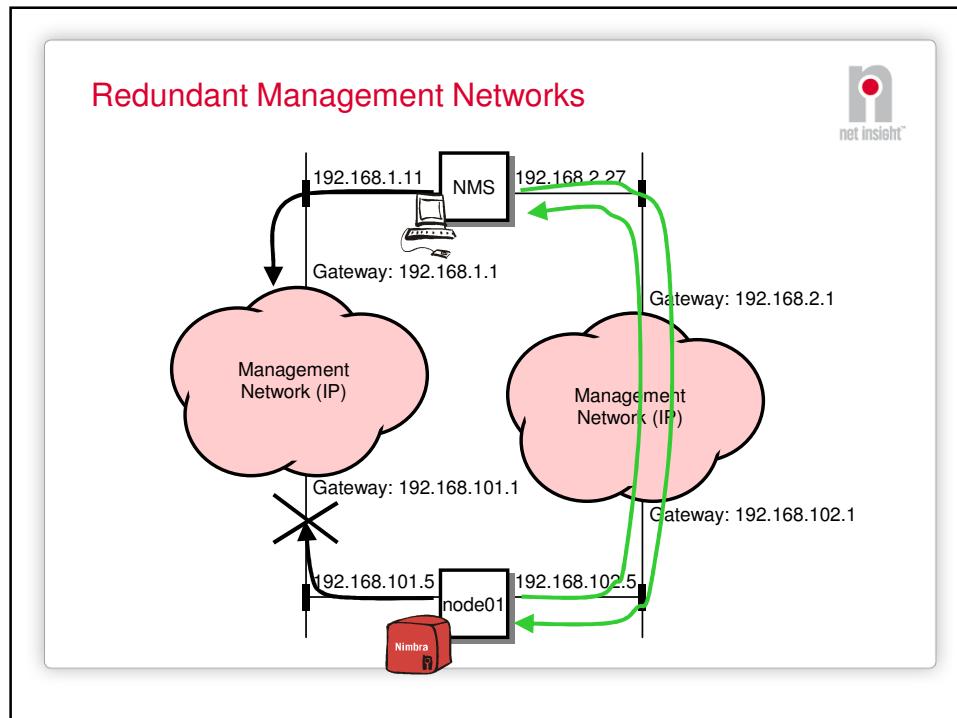
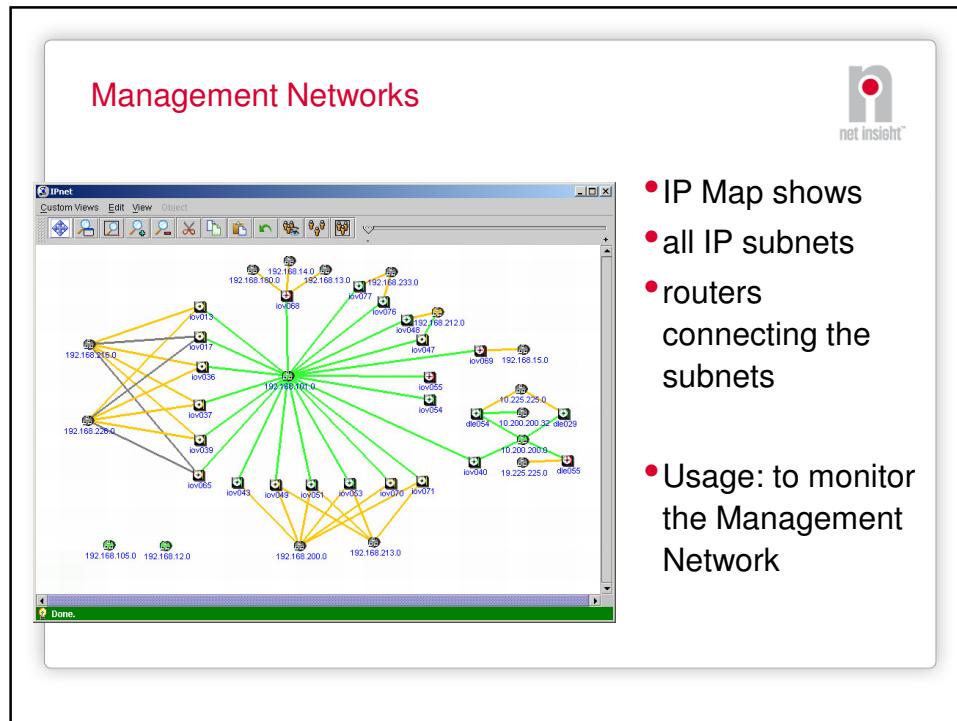


- Configure telnet login/password in Node Users
- Unpack distribution on repository server
- Define repository
- Select nodes and do Upload
 - Select Repository
 - Check Reboot if convenient

Exersice



- Lab 16: Software/firmware upload



Detecting Problems in the Management Network



- Major alarm on node's IP interface when it is unreachable
- Major alarm on IP segment if any interface within segment is unreachable
- Critical alarm on DTM node when all its IP interfaces are unreachable
- Alarms get category Topology

Properties related to Management Network

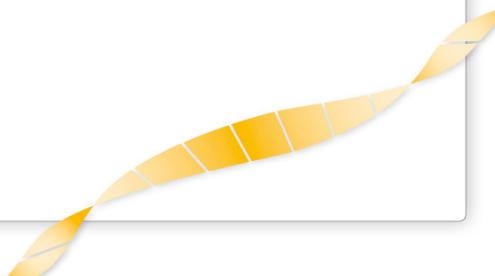


- On DTM Node properties:
- activeIpAddress: the IP address currently used to reach the node
- ipAddress: the IP address when the MO was added to the database (discovered)
- interfaceList: all IP addresses reported by node

Exesice

• Lab 17: Redundant Networks

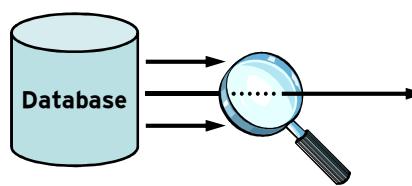
© Net Insight 2010



Custom View – is a filter

• View into the database
 • Working on a “table” in the database
 • Describes what data to present, and how

Custom View



Name	Type	DTM Address	Status	Last Task Complete
env001	Network	00:00:00:00:00:00:00	Offline	2005-05-26, 03:23:15
env002	NetrinoOne	No valid DTM address set	Critical	2005-05-26, 03:23:16
env003	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 11:04:54
env004	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env005	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env006	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env007	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env008	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env009	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env010	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env011	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env012	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env013	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env014	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env015	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env016	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env017	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env018	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env019	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env020	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env021	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env022	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env023	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env024	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env025	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env026	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env027	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env028	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env029	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env030	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env031	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env032	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env033	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env034	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env035	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env036	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env037	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env038	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env039	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env040	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env041	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env042	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env043	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env044	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env045	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env046	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env047	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env048	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env049	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env050	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env051	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env052	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env053	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env054	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env055	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env056	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env057	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16
env058	NetrinoOne	01:aa:bc:c0:71:01:01	Minor	2005-05-25, 10:44:16

Custom View

- Custom View is a view into the database
- Can be used for all type of data (maps, event, alarms, network database, ...)
- Temporary (for this session) or saved (for future sessions)
- Placed in tree
- Defines:
 - Which (which rows?)
 - View all rows that match given criteria
- What (what columns?)
- View the specified columns (properties)
- How (sorted? column order?)

Name	Type
DTM Address	Status
Last Status ChangeTime	classname
managed	isSNMP
ipAddress	netmask
pollInterval	statusUpdate
tester	uClass
isRouter	sysID
sysName	sysDescr
community	parentNet
nodeStartTime	pollFailureCo
childrenKeys	sysLocation
isNode	failureCount
eventLogLastChangedTime	updateFailure
groupNames	userName
writeCommunity	activeIpAdd
groupMembers	snmpport

Exersice

- Lab 18: Custom View
- Filter and Search

© Net Insight 2010

Service Provisioning, general

Simple process:

1. Define Trail Termination Points (TTP)
2. Associate interface with TTP
3. Define connection between TTPs

© Net Insight 2010

Service Provisioning

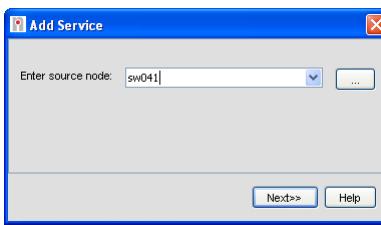
- End-to-end provisioning of services from the Nimbra Vision network manager
- Supports ITS/ETS/ETSV2, unicast/multicast, 1+1 protection and definition of source routes
- New services created either by selecting the originating and terminating nodes from the map or from the database
- Automatic generation of DSTI and TTP id's
- Creation of source routes either graphically in the map or in a table

© Net Insight 2010

Service provisioning, step 1

© Net Insight 2010

- A wizard helps the user create a new service
- Source node has typically already been chosen in the map or from the database, but may also be entered here



The screenshot shows the 'Add Service' dialog box. It has a title bar 'Add Service' with a close button. Below it is a text input field labeled 'Enter source node:' containing 'sw041'. To the right of the input field is a dropdown arrow and a browse button (...). At the bottom are 'Next>>' and 'Help' buttons.

Service provisioning, step 2

© Net. Insight 2010

- Enter type of service
 - ITS unicast, ITS multicast, ETS unicast, ETS multicast



The screenshot shows the 'Add Service' dialog box. It has a title bar 'Add Service' with a close button. Below it is a text input field labeled 'Source node:' with 'sw041' typed in. Below that is another text input field labeled 'Enter type of service:' with a dropdown menu open, showing 'ITS unicast' selected. At the bottom are '<=Previous', 'Next>>', and 'Help' buttons.

Service provisioning, step 3

© Net Insight 2010

Service provisioning, step 4 (ITS unicast)

© Net Insight 2010

Service provisioning, step 4 (ETS unicast)

The screenshot shows the Service Editor interface for a service named 'NET1' with purpose 'NET/ETH(00000360)Presemption - base'. The service is configured for bidirectional ETS unicast between nodes 'sw042' and 'sw041'. Capacity is set to 200.0 Mbps. Source routes are defined for both directions, and VLAN mappings are being configured in a separate window.

- Service Editor opened after finishing the wizard (note bidirectional service)
- Enter optional admin data for the service
- Enter node B (if not selected from the map)
- Enter capacities
- Select source routes if required
- Configure VLAN mappings in separate window

© Net Insight 2010

Channel List

The screenshot shows the Channel List window for node 'sw040'. It lists various channels, including preemption-related entries and specific links between nodes like 'eth1(0)' and 'sw041'. The table includes columns for Purpose, Type, Source, Capacity, Src DSTI, Multicast, In If, Out If, Next, and Channel Id.

Purpose	Type	Source	Capacity	Src DSTI	Multicast	In If	Out If	Next	Channel Id
:AS(00000360)Presemption - reduced 2	eth1(0)	sw041	200.0	no	dmz1	dmz1	sw042		65536
:ETH(00000360)Presemption - reduced 1	eth1(0)	sw041	207.250	no	dmz1	dmz1	sw042		65537
:ETH(00000360)Presemption - base	eth1(0)	sw041	1134.0	no	dmz1	dmz1	sw042		65538
:AS(00000362)	dmz1(0)	sw041	5.2	no	dmz1	dmz1	sw042		65539
:ETH(00000360)Presemption - base	dmz1(0)	sw042	34.0	no	dmz1	dmz1	-		65536
:ETH(00000360)Presemption - base	eth1(0)	sw042	1340.0	no	dmz1	dmz1	sw041		65537
:ETH(00000360)Presumption - reduced 1	eth1(0)	sw042	207.1	no	dmz1	dmz1	sw041		65538

© Net Insight 2010

Trace Channel - Start

© Net Insight 2010

net insight™

- Trace a channel through the network
- Unicast and multicast
- Start from either
 - Selected channel in List Channels
 - Selected node in map or Network Database
 - Selected service in Network Database

Trace Channel - Result

© Net Insight 2010

net insight™

Trace Channel - Nimbra Vision

Name:	sw041_Req-1			
Purpose:	IASI:00000359:Prescription - reduced 2			
Source:	sw041	Node	In If	Out If
Channel Id:	865536	sw040	dmx4:1	dmx5:1
Mode:	unicast	sw042	dmx5:1	> end
Type:	dh416			
Src DST:	1			

Highlight:

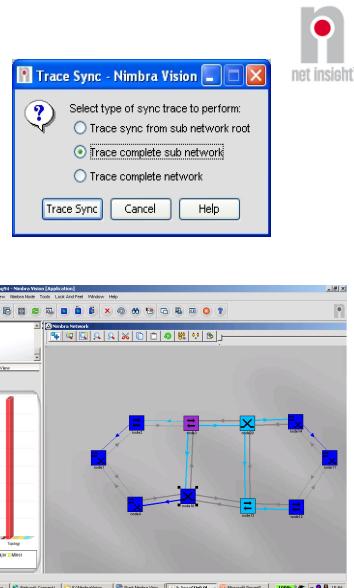
-
-
-

Result as:

- Tabular data
- Highlight in map
- Highlight all or part of trace
- Can highlight multiple channels at the same time

Trace Sync

- Synchronization paths automatically set up by the network
- Sync trace function in Nimbria Vision displays sync paths and master node(s)
 - In a table
 - Highlighted in the map
- Three sync trace options
 - From root to selected node
 - Complete sub-network
 - Complete network



© Net Insight 2010

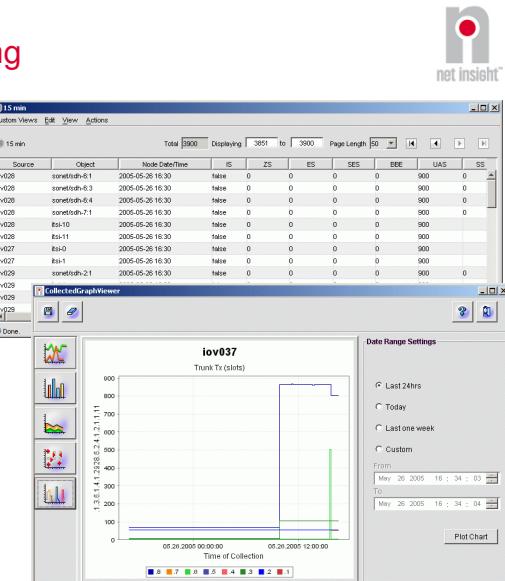
Exersice

- Lab 19:
- Service provisioning
- List channels and trace route a specific one

© Net Insight 2010

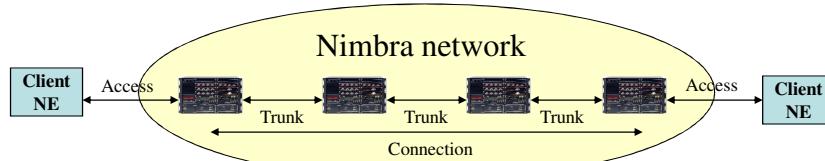
Performance Monitoring

- Present G.826 reports generated by the network elements
 - Collect interface usage data, generate reports
 - Plot statistics
 - Powerful searching
 - Powerful filtering
 - Collect statistics on any SNMP variable
 - Generate alarms on threshold crossing



© Net Insight 2010

Performance Management



- Monitoring of error statistics to ITU-T G.826 for
 - Trunk interfaces
 - Connections end-to-end (HD-SDI, SDI, ASI, AES/EBU, E1, SDH)
 - Input access interfaces (HD-SDI, SDI, ASI, AES/EBU)
 - 15 minutes and 24 hrs reports
 - Monitoring of the following parameters:
 - ES, SES, BBE, UAS, ZC
 - Ethernet packet statistics

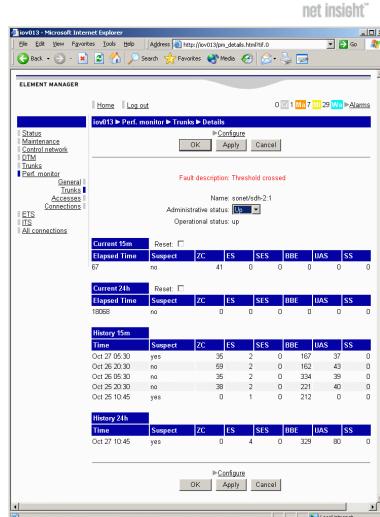
Performance Monitoring and Statistics

- Know the health of the network with performance and statistics monitoring.
- Trunks:
- G.826-like reports on trunk interfaces
- Connections:
- G.826-like reports on
 - HD-SDI connections
 - SDI connections
 - DVB/ASI connections
 - AES/EBU connections
 - SDH connections
- Services:
- Statistics counters on ETS
- Interfaces:
- Statistics on Ethernet interfaces



Performance Monitoring on Trunks

- Supports the necessary data for operator-customer Service Level Agreements (SLA).
- Performance monitoring for trunks is done in accordance with ITU-T G.826.
- Easy configuration:
 - Choose the trunk interface to monitor
 - Optional: configure alarm threshold values
- The trunk is monitored!
- Reports are generated for each 15 min and 24h period



Statistics on Connections

- Statistics on connections and Ethernet for packet-oriented transport streams.

The screenshot shows the 'ELEMENT MANAGER' interface for 'net022'. The main title is 'net022 > Connections > ECAP statistics'. Below it are two tables:

Originating traffic							
TTP name	Conn	Octets	Pkts	Used Minps	Disc'd Octets	Disc'd Pkts	Error rate
std01.V	1.V	0	0	0	0	0	0
std12.V	2.V	0	0	0.000	0	0	0
std22.V	2.V	0	0	0	0	0	0
Total		0	0	0.000	0	0	0

Terminating traffic							
TTP name	Conn	Octets	Pkts	Used Minps	Disc'd Octets	Disc'd Pkts	Error rate
std01.V	1.V	0	0	0.000	0	0	0
std12.V	2.V	0	0	0	0	0	0
Total		0	0	0.000	0	0	0

Performance Monitoring on Service

- Supports the necessary data for operator-customer Service Level Agreements (SLA).
- Performance monitoring in accordance with ITU-T G.826.
- For HD-SDI, SDI, DVB/ASI, AES/EBU, SDH
- Easy configuration:
- Choose the connection to monitor
- Optional: configure threshold values for each of the performance counters
- The service is monitored!
- Reports are generated for each 15 min and 24h period

The screenshot shows the 'ELEMENT MANAGER' interface for 'net013'. The main title is 'net013 > Perf. monitor > Connections'. Below it is a table:

Name	Current 15m			Current 24h			Oper
	ES	SES	IASS	ES	SES	IASS	
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0	0	0 up
std22.V	0	0	0	0	0	0	0 up
std01.V	0	0	0	0	0	0	0 up
std12.V	0	0	0	0	0		

Performance monitoring – G.826 like reports

Source	Object	Node/Date/Time	IS	ZS	ES	SES	BBE	UAS	SS
jav028	soneteth-6:1	2005-05-26 16:30	false	0	0	0	0	900	0
jav028	soneteth-6:3	2005-05-26 16:30	false	0	0	0	0	900	0
jav028	soneteth-6:4	2005-05-26 16:30	false	0	0	0	0	900	0
jav028	soneteth-7:1	2005-05-26 16:30	false	0	0	0	0	900	0
jav028	ttsl-10	2005-05-26 16:30	false	0	0	0	0	900	
jav028	ttsl-11	2005-05-26 16:30	false	0	0	0	0	900	
jav027	ttsl-0	2005-05-26 16:30	false	0	0	0	0	900	
jav027	ttsl-1	2005-05-26 16:30	false	0	0	0	0	900	
jav028	soneteth-2:1	2005-05-26 16:30	false	0	0	0	0	900	0
jav028	ttsl-1	2005-05-26 16:30	false	0	0	0	0	900	
jav028	ttsl-2	2005-05-26 16:30	false	0	0	0	0	900	
jav028	ttsl-12	2005-05-26 16:30	false	0	0	0	0	900	

Done.

- Present G.826 reports generated by the network elements
- IS/ZS/SES/BBE/UAS/SS
- Sent as periodic reports by the Network Element

Performance monitoring – G.826 values

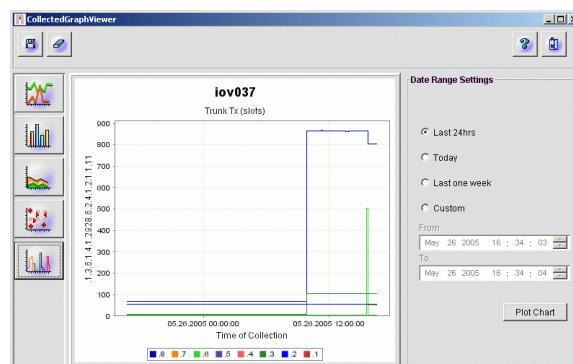
Source	Object	Node/Date/Time	IS	ZS	ES	SES	BBE	UAS	SS
jav028	soneteth-6:1	2005-05-26 16:30	false	0	0	0	0	900	0
jav028	soneteth-6:3	2005-05-26 16:30	false	0	0	0	0	900	0
jav028	soneteth-6:4	2005-05-26 16:30	false	0	0	0	0	900	0
jav028	soneteth-7:1	2005-05-26 16:30	false	0	0	0	0	900	0
jav028	ttsl-10	2005-05-26 16:30	false	0	0	0	0	900	
jav028	ttsl-11	2005-05-26 16:30	false	0	0	0	0	900	
jav027	ttsl-0	2005-05-26 16:30	false	0	0	0	0	900	
jav027	ttsl-1	2005-05-26 16:30	false	0	0	0	0	900	
jav028	soneteth-2:1	2005-05-26 16:30	false	0	0	0	0	900	0
jav028	ttsl-1	2005-05-26 16:30	false	0	0	0	0	900	
jav028	ttsl-2	2005-05-26 16:30	false	0	0	0	0	900	
jav028	ttsl-12	2005-05-26 16:30	false	0	0	0	0	900	

- 15 minutes reports
- 24 hrs reports
- Following performance parameters are monitored:
 - ES (Errored Seconds) Counts how many seconds has at least one errored block (BBE)
 - SES (Severely Errored Seconds) Counts how many seconds that has been seriously faulty
 - BBE (Background Block Errors) Counts number of errored blocks found is not part of SES
 - UAS (Unavailable Seconds) Counts how many unavailable seconds
 - ZC (Zero suppression Counter) number of error free 15min/24hr periods preceding an errored period
 - SS (Slip Seconds) Count number seconds containing slip.

Performance monitoring – Collect statistics



- Periodically collect DTM interface usage data
- Plot statistics
- Collect statistics on any SNMP variable
- Generate alarms on threshold crossing



Performance monitoring – Generate reports



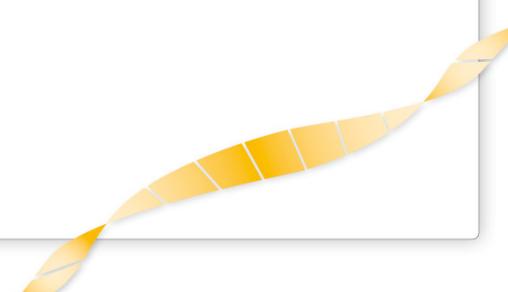
- Generate daily/weekly/monthly reports on DTM interface usage.
- Includes max/min/average
- Includes graph
- Includes table
- Reports must generated with a Policy

Exersice



- Lab 20: Performance Monitoring

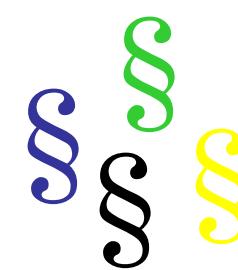
© Net Insight 2010



Policies



- Policies are specifications
- Used for controlling network activities
- Save Node's Configuration
- Host List Push
- Generate Reports
- Statistics Table Cleanup
- Events to Log File
- Database Backup
- Alert Escalation



Policy – Save DTM node Registry

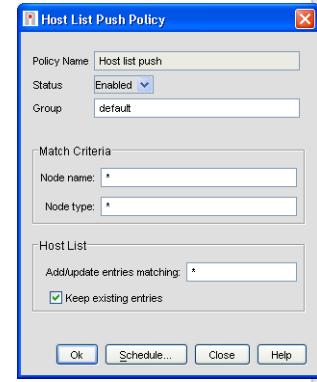



- Saves the current (running) configuration. Options:
 - Save only if not already saved
 - Delete oldest/second oldest configuration prior save
 - Store copy on Nimbria Vision server, saved in <NVHOME>\backup\nodeconfigurations
 - Store copy on Nimbria Vision server regardless if saved or not
- Set up a schedule for when to execute

Policy – Host List Push



- Push host list to configured set of nodes
 - Updates the host name to DTM address information in the nodes
 - On command and/or scheduled in calendar
 - Optionally restrict what nodes to update
 - Optionally restrict contents of pushed host list
 - Optionally remove or preserve data not included in pushed host list
- Data source is the Nimbria Vision managed object database
 - Host name is the same as the managed object name (which is the same as the hostname used in IP)
 - DTM address is retrieved from each node (at discovery)
 - Do not use dot (".") in names!



Policy – Generate Reports

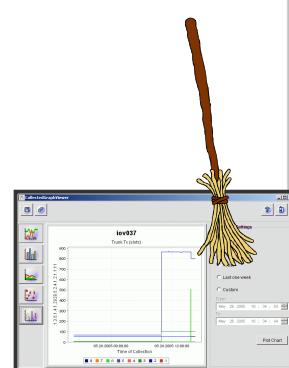


- Generate daily/weekly/monthly reports
- Operates on DTM interfaces
- Reports generated as summary and detailed reports
- Set up a schedule for when to execute

Policy – Statistics Table Cleanup



- Remove old statistics (collected data) from database
- Specify how old (in days)
- Specify what statistics (what tables)
- To prevent full database



Policy – Events to Log File



- Copies events to log file
- Specify log file folder
- Specify how often
- Events generated since last period is saved each period
- Note! Nimbra Vision enforces a maximum number of alarms. Oldest alarms are automatically deleted to enforce this maximum.

Policy – NMS Backup



- Backup Nimbra Vision database
- Set up a schedule for when to execute

Policy – Alert Escalation



- Perform action for alarms that has had the same alarm severity for a specified period
- Match on criteria for alarms
- Actions include:
 - Suppress alarm
 - Send SNMPv1 trap
 - Send e-mail
 - Set severity
 - Run command
 - Custom filter (call java class)



Exersice

- Lab 21: Policies



© Net Insight 2010

Pre-emption at Network Failure

Network in Full Operation state

The diagram illustrates the bandwidth allocation for a 'Total trunk bandwidth' across two trunks. Trunk 1 (left) contains 'Free Bandwidth' (yellow), 'Ethernet 1 (low prio)' (yellow), 'SD-SDI' (red), and 'HD-SDI' (red). Trunk 2 (right) contains 'Free Bandwidth' (white), 'Ethernet 3 (low prio)' (yellow), 'Ethernet 2 (low prio)' (yellow), and 'ASI' (pink). A legend indicates that yellow represents 'Free Bandwidth' and red represents 'Ethernet' services.

Legend:

- Free Bandwidth (Yellow)
- Ethernet 1 (low prio) (Yellow)
- SD-SDI (Red)
- HD-SDI (Red)
- Ethernet 3 (low prio) (Yellow)
- Ethernet 2 (low prio) (Yellow)
- ASI (Pink)

Total trunk bandwidth:

© Net Insight 2010

Notes:

- High priority services may preempt low priority services at network failures
- Pre-empted services are either shut down or have their bandwidths reduced (Ethernet)

A circular ring of nodes, each labeled 'NIMBRA', is shown with a lightning bolt striking one node, indicating a network failure.

Pre-emption at Network Failure

Network in Reduced Operation state

The diagram illustrates the bandwidth allocation for a 'Total trunk bandwidth' across two trunks. Trunk 1 (left) is empty. Trunk 2 (right) contains 'Ethernet 2 (reduced bandwidth)' (yellow), 'SD-SDI' (red), 'HD-SDI' (red), and 'ASI' (pink).

Legend:

- Ethernet 2 (reduced bandwidth) (Yellow)
- SD-SDI (Red)
- HD-SDI (Red)
- ASI (Pink)

Total trunk bandwidth:

Notes:

- When the network failure is fixed, the network returns to Full Operation state

A circular ring of nodes, each labeled 'NIMBRA', is shown with a red 'X' on one of the links, indicating a failed connection.

© Net Insight 2010

Nimbra Vision based Pre-emption

at Service Provisioning

- Definitions
 - Pre-emption object
 - Set of Prioritized Services
 - State
 - Full operation
 - Reduced operation
 - Function
 - Full Operation
 - Full BW available for all low prio services
 - Reduced Operation
 - Reduced BW for low prio services
 - High prio service provisioned at nominal rate
 - Trigger for state switching
 - Establishment failure of high prio services

© Net Insight 2010

Pre-emption at Service Provisioning

Network in Full Operation state

Free Bandwidth
Ethernet (low prio)
SD-SDI
HD-SDI

Total trunk bandwidth

ASI (to be provisioned)

- High priority services may pre-empt low priority services at service provisioning
- Pre-empted services are either shut down or have their bandwidths reduced (Ethernet)

© Net Insight 2010

Pre-emption at Service Provisioning

Network in Reduced Operation state

The diagram illustrates the total trunk bandwidth being shared by four services: ASI, Ethernet (reduced bandwidth), SD-SDI, and HD-SDI. A bracket on the right indicates 'Total trunk bandwidth'. Below this, a circular network loop contains six red rectangular boxes labeled 'NIMBRA'. Arrows show the flow of data between these nodes.

- If the new service is removed, the network returns to Full Operation state

© Net Insight 2010

net insight™

Pre-emption, configure

Identify and configure the pre-emption objects

- Links (interfaces)

Identify services that shall be affected by failure in pre-emption object

net insight™

Exersice

• Lab: Pre-emption

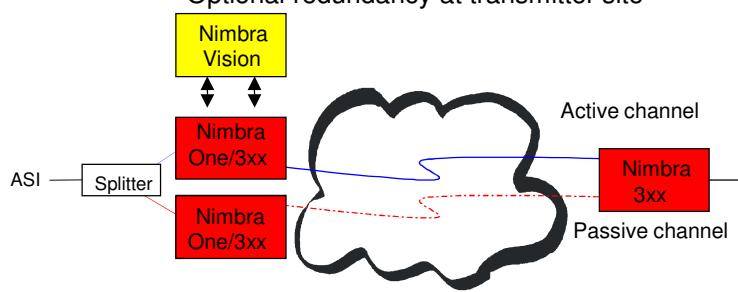
© Net Insight 2010



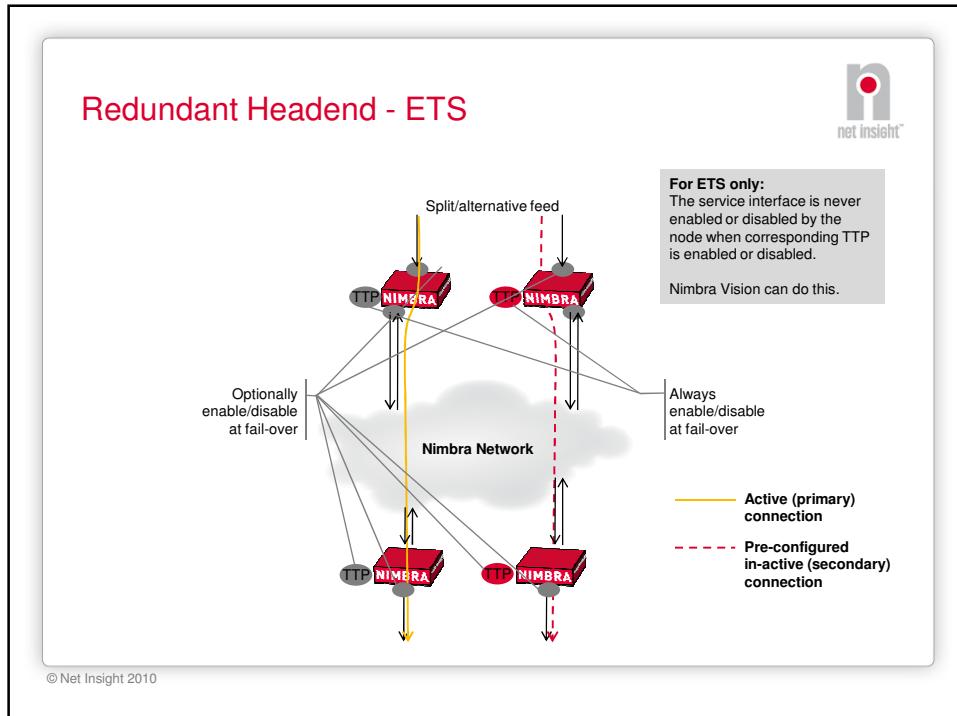
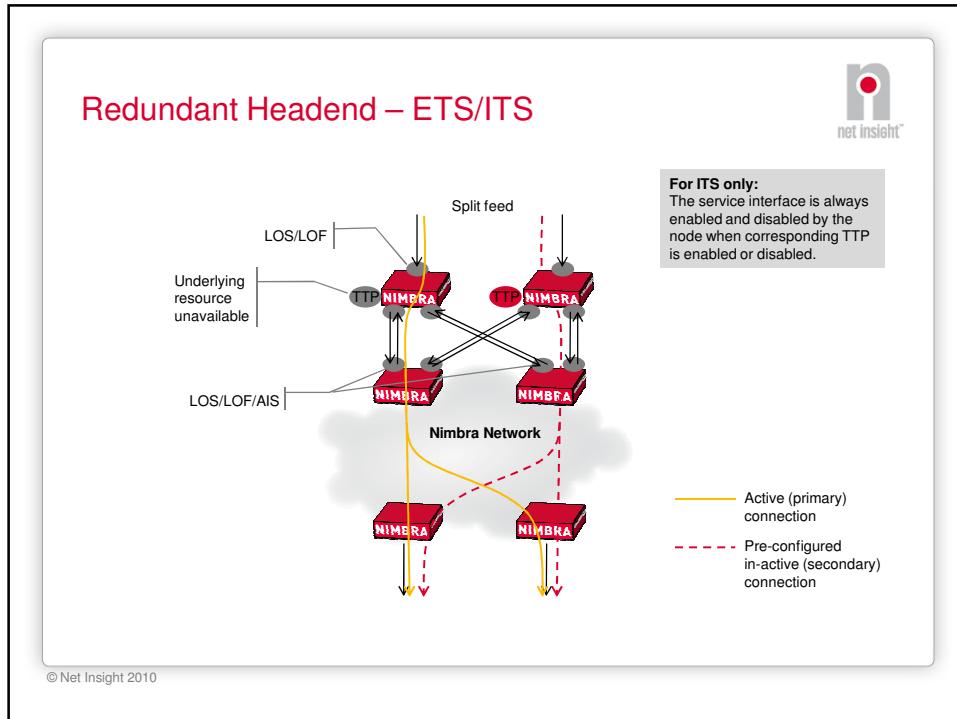
A decorative graphic at the bottom right of the slide features a stylized yellow wave or signal pattern.

Headend protection

- Full hardware redundancy at headend site
- Only one set of ASI multicast connections active at a time to minimize network bandwidth
- Nimbra Vision activates standby connections in case of signal, board or node failure
- Optional redundancy at transmitter site

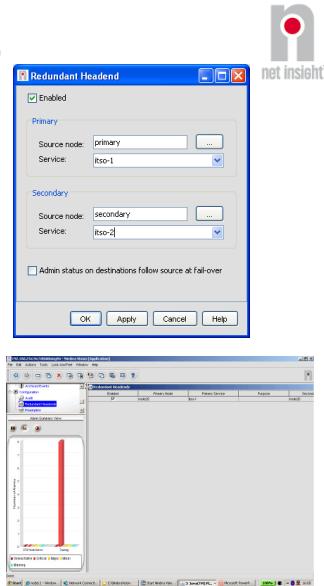


The diagram illustrates the Headend protection architecture. On the left, labeled 'Headend', an ASI signal enters a 'Splitter'. The Splitter connects to two 'Nimbra One/3xx' modules. These modules are connected to a central cloud-like symbol representing the transmission link. The connection from the Splitter to the cloud is solid blue, representing the 'Active channel'. A dashed red line from the 'Nimbra One/3xx' modules to the cloud represents the 'Passive channel'. On the right, labeled 'Transmitter site', there is a 'Nimbra 3xx' module connected to the cloud. The 'Nimbra Vision' module is shown at the top, connected to both 'Nimbra One/3xx' modules via double-headed arrows, indicating its role in managing the active connections.



Redundant Headends – Setting Up

- Configure
 - Protected node and service
 - Failover node and service
- Automatically detects
 - Service interfaces
 - DTM interfaces on neighboring nodes
 - Service type (ETS or ITS)
- For ETS, optionally configure auto-enable/disable of interfaces at switch-over:
 - Toggles all Ethernet interfaces (source and destinations) at switchover.

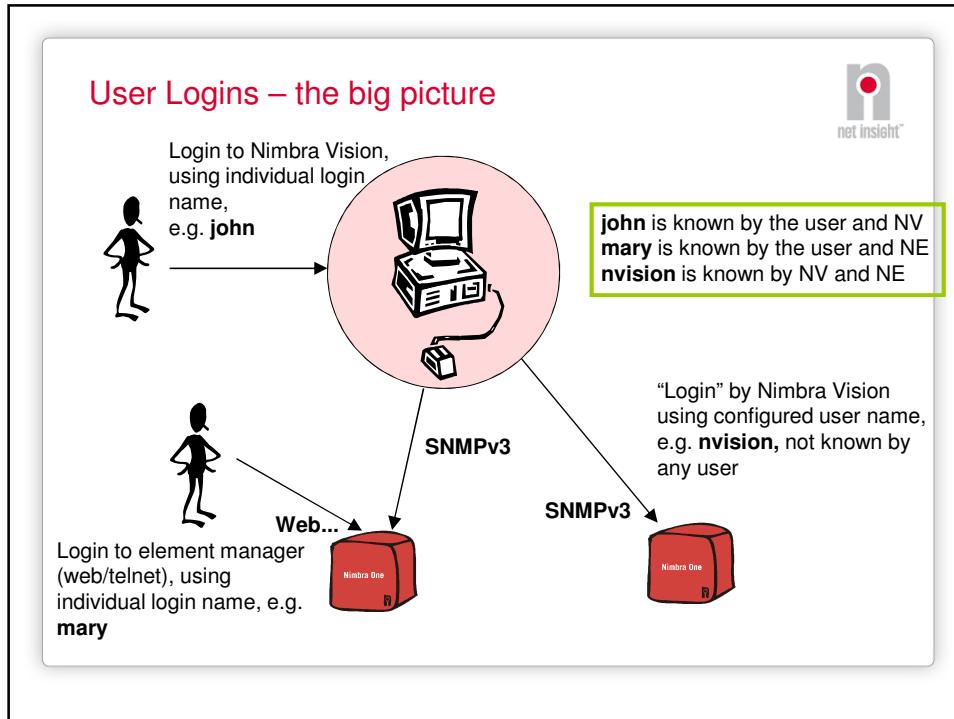


© Net Insight 2010

Exercise

- Lab 23: Redundant Headends

© Net Insight 2010



Security management

The screenshot shows the **Security Administration** interface with several windows open:

- Permissions For User [sic]**: A table showing permissions assigned to a user profile. Operations listed include: Get Node Configuration, Service Programming, Get Node Tree, Get Alert Filters, Network Map Tree Node, Get System Information, Get Node Tree Node, Network Database Tree Node, List Change, Polling Units, Trace Route Remote Node, Get Node Status, and Get Event Processors. All permissions are marked as "Included".
- Assign Permissions**: A dialog box showing the **Permissions tree hierarchy** for "root". It lists various operations under categories like **Administrative Operations**, **Services**, **Network Administration**, **Security Administration**, **Events**, and **System Administration**.
- Audit Details**: A table showing audit log entries. The table has columns for **User Name**, **Operation Name**, **Time**, and **Status**. Examples of entries include:

User Name	Operation Name	Time	Status
root	Authentication	2005-05-24 13:24:49.02	SUCCESS
root	Authentication	2005-05-24 13:24:49.12	SUCCESS
root	Runtime Administration	2005-05-24 13:24:39.197	SUCCESS
root	Runtime Administration	2005-05-24 13:24:46.424	SUCCESS
root	Add Node	2005-05-24 13:24:19.54	SUCCESS
root	Delete Object	2005-05-24 14:52:21.921	SUCCESS
root	Delete Object	2005-05-24 14:52:44.864	SUCCESS
root	Delete Object	2005-05-24 14:57:26.251	SUCCESS

• Individual user logins

- Groups, Users and Operations

• Assign permitted operations to users and/or groups

- Restrict what a user can do

• Assign permitted objects to users and/or groups

- Restrict which object the user can access

• Audit log

• Note!
User logins in Nimbra Vision are not the same as the user logins in the Network Elements

Security management – Users and Groups



- A group is representing a group of users
 - You can set permissions for a group
 - You can Assign Authorized Scopes for groups
- A user is representing a person
 - You can set permissions for a user
 - A user is a member of one or many groups
- A user has the permissions for:
 - Each member group
 - Its own settings
- View the audit for all or individual users

Security management – Operations



Assign Permissions

Permissions tree hierarchy

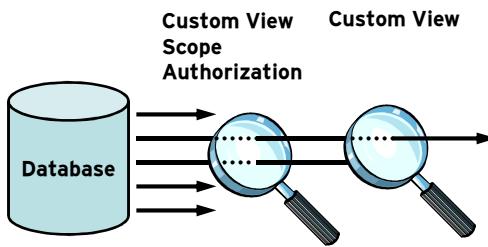
Allow / Disallow

- Operation Tree Root
- Administrative Operation
 - Services
 - Clear Discovery
 - Start Backup
 - Resume NMS
 - Shutdown Web NMS Server
 - Configure Log Levels
 - Runtime Administration
 - Security Administration
 - Group Operations
 - Add Group
 - Remove Group
 - Set Group Permission
 - Operation Settings
 - Add Operation
 - Remove Operation
 - Scope Settings
 - Create Scope For Group
 - Modify Group Scope Relation
 - System Administration
- Events
 - Event Filters And Parsers
 - Get Event Parsers
 - Set Event Parsers
 - Get Event Filters

Reset Done Cancel

- An operation represents something that can be done
- Permissions for user or group
- For a user/group, an operation can be
 - Allowed (checked)
 - Disallowed (crossed)
 - Not specified (empty)
- If contradictory (from e.g. different groups), then the operation is allowed

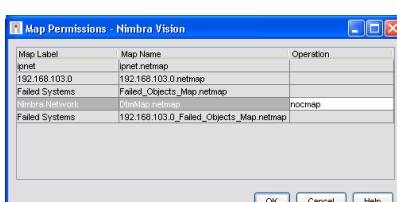
Security management – Custom View Scope



• Which rows group is allowed to view
 • Match criteria much like Custom View
 • Each scope has its own criteria
 • Maps/NetDB/Alarms/Events/Stat/...

Mode	Type	DTM Address	Status	Last Status ChangeTime
onv16	Nimbra209	01 web cc 10 00 00 24	Other	2005-05-24, 13:57:15
onv17	Nimbra209	No valid DTM address set	Other	2005-05-24, 13:57:15
onv18	Nimbra209	01 web cc 71 01 01 91	Minor	2005-05-25, 11:04:34
onv19	Nimbra209	01 web cc 71 01 01 90	Minor	2005-05-25, 10:44:16
onv20	Nimbra209	01 web cc 17 00 01 89	Minor	2005-05-24, 13:52:07
onv21	Nimbra209	01 web cc 17 00 00 88	Minor	2005-05-24, 13:52:07
onv22	Nimbra209	01 web cc 17 00 00 82	Minor	2005-05-24, 13:51:54
onv23	Nimbra209	01 web cc 17 00 00 81	Minor	2005-05-24, 13:51:50
onv24	Nimbra209	01 web cc 17 00 00 71	Minor	2005-05-24, 13:51:48
onv25	Nimbra209	01 web cc 17 00 00 70	Minor	2005-05-24, 13:51:48
onv26	Nimbra209	01 web cc 17 00 00 67	Minor	2005-05-24, 13:51:35
onv27	Nimbra209	01 web cc 17 00 00 66	Minor	2005-05-24, 13:51:35
onv28	Nimbra209	01 web cc 16 00 00 62	Minor	2005-05-24, 13:51:32
onv29	Nimbra209	No valid DTM address set	Other	2005-05-24, 13:51:30
onv30	Nimbra209	01 web cc 11 01 01 99	Minor	2005-05-24, 13:50:30
onv31	Nimbra209	01 web cc 11 01 01 99	Minor	2005-05-24, 13:50:18

Security management – Private maps



- Generally, maps are shared among all users.
- Disable access to map by assigning an Operation to the map
- Enable access to users by granting the same Operation to users
- Menu: Custom Views > Edit Map Permissions

Security management – Audit trail

The screenshot shows the 'Audit' interface with a list of audit tasks. The tasks are:

Task Name	Device Name	Start Time	Finish Time	Severity
RegistryTable_task	datac042.lab.netinsight.se	okt 02,2003 04:48:05 PM	okt 02,2003 04:48:09 PM	Success
RegistryTable_task	datac042.lab.netinsight.se	okt 02,2003 04:47:58 PM	okt 02,2003 04:48:02 PM	Success
SystemName_task	datac041.lab.netinsight.se	okt 02,2003 04:46:16 PM	okt 02,2003 04:46:18 PM	Success
SystemName_task	datac041.lab.netinsight.se	okt 02,2003 04:41:58 PM	okt 02,2003 04:42:02 PM	Success
DtmInterface_task	datac041.lab.netinsight.se	okt 02,2003 03:48:36 PM	okt 02,2003 03:48:38 PM	Success
DtmInterface_task	datac041.lab.netinsight.se	okt 02,2003 03:45:18 PM	okt 02,2003 03:45:21 PM	Success

A modal window titled 'Audit Details' is open, showing a list of audit operations:

User Name	Operation Name	Time	Status
root	Authentication	2005-05-24 13:26:49.002	SUCCESS
root	Shutdown Web NMS Server	2005-05-24 13:26:49.122	SUCCESS
root	Authentication : 192.168.1... 2005-05-24 13:34:39.197		SUCCESS
root	Runtime Administration	2005-05-24 13:35:46.424	SUCCESS
root	Runtime Administration	2005-05-24 13:43:16.581	SUCCESS
root	Add Node	2005-05-24 13:58:00.052	SUCCESS
root	Add Node	2005-05-24 13:58:19.54	SUCCESS
root	Delete Object	2005-05-24 14:55:21.921	SUCCESS
root	Delete Object	2005-05-24 14:55:44.886	SUCCESS
root	Delete Object	2005-05-24 16:01:26.281	SUCCESS

• Logs all operations
• Details per task execution in tree

Configuration:Audit

Done.

Exersice

• Lab 24: Security Management

© Net Insight 2010

Backup/Restore



- Backup/Restore the database
- Offline (when server is taken down)
 - Run:
 - <NVHOME>\bin\backup\backupDB.bat
 - <NVHOME>\bin\backup\restoreDB.bat file
 - Files saved in folder <NVHOME>\backup
- Online (when server is running)
 - Run as a policy (scheduled)

Reinitialize Nimbra Vision database

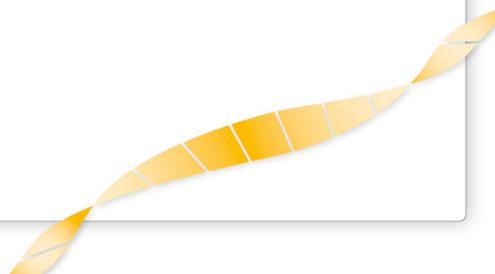


- To reinitialize the Nimbra Vision database
- Will empty the database, but not affect any other configurations
 - Run:
<NVHOME>\bin\reinitialize_nms.bat

Exersice

Lab 25: Backup, reinitialize and restore the database

© Net Insight 2010



The net insight logo, featuring a stylized 'n' icon above the word 'net insight'.

Exercises

- Lab 26: User clients
- Lab 27: License key



The net insight logo, featuring a stylized 'n' icon above the word 'net insight'.

Initial Checklist



- Defining individual user accounts with permissions depending on roles
- Generate daily, weekly and/or monthly reports
- Backing up the NMS database
- Backing up the nodes' configurations
- Saving old events to files.
- Clean old statistical data from the database
- Clean old alarms from the database
- Clean old reports from the file system
- Clean saved events from the file system
- Clean old NMS database backups from the file system
- Clean old node configuration backups from the file system



Summary



- Advanced system functionality enables simple network management:
 - Automatic neighbor discovery
 - Automatic topology discovery
 - Automatic routing (DRP)
 - End-to-End provisioning
 - Non-hierarchical architecture
 - Optimized capacity usage – no need for over provisioning

© Net Insight 2010