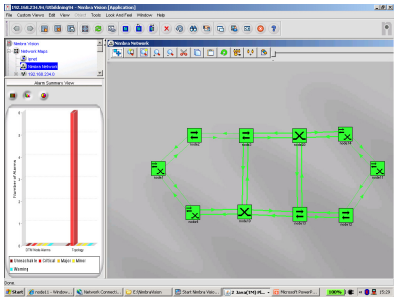
Nimbra Vision, Management System

Net Insight Academy
Course NPC0004-0001

Contents

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.

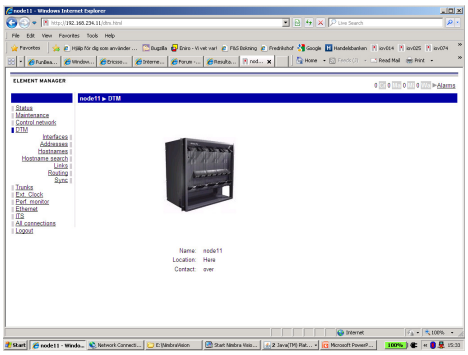
Nimbra Vision allows the operator to provision services end-to-end across the network with full graphical support. Source and destination nodes are selected from the Nimbra Vision map. If automatic routing is chosen the actual route through the network may easily be displayed in the map using the Channel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

Web Interface

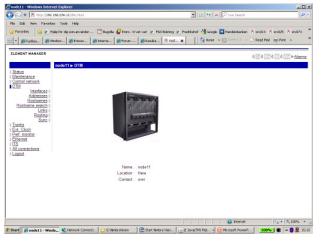
- **Status Monitoring**
  - Alarms and Events
  - Equipment inventory
- **Maintenance**
  - Initial configurations
  - Backup of configurations
- **Network configuration**
  - Interfaces
  - Addresses
  - Routes
- **Service Provisioning**
  - Set-up of services (ITS/ETS)
  - Source routing
  - Scheduling
- **Performance Monitoring**

- **Built-in http server in each NE**
- **Complete management tool for the node**

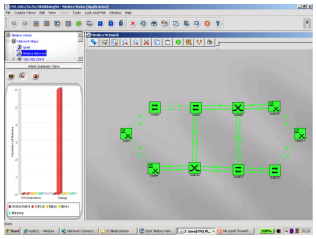


Network Management Products

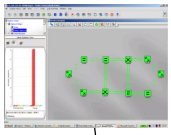
- Element Manager:
  - Web access to network elements (HTTP) for access from a web browser
  - Telnet access (CLI)



- Nimbra Vision Network Manager
  - Managing multiple network elements in a network



SNMP

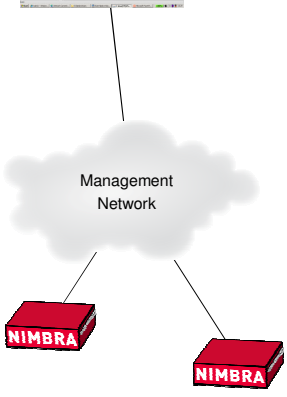


- Nodes support SNMP
- SNMPv1/v2c/v3

- get
- get-next
- get-bulk
- Set
- Notifications

- Network is e.g. UDP/IP

Supports:
- Selected parts of MIB-II
- Enterprise MIBs



Managed information

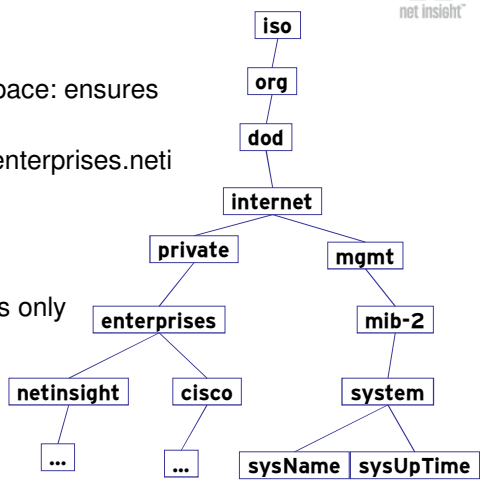
- Pieces of data used for managing the unit
- Examples:
  - Integer value
  - Counters
  - Time stamp
  - Text string
- Organized as scalars or tables

Net Insight Enterprise MIBs

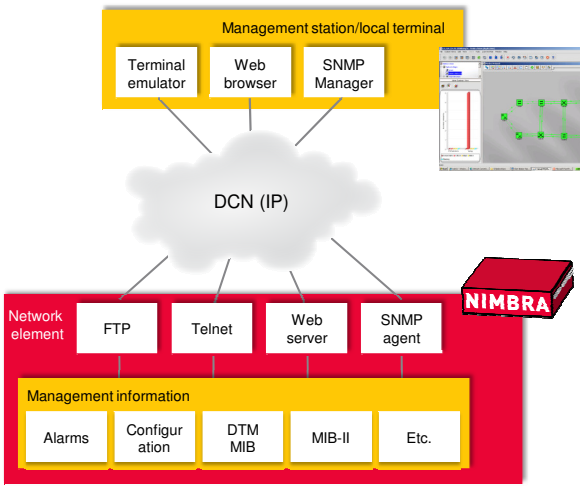
• Common	(neti-common-mib)
• Alarms and events	(neti-event-mib)
• Configurations	(neti-config-mib)
• Interfaces and links	(neti-dtm-mib)
• PM	(neti-pm-mib)
• Trunk	(neti-trunk-mib)
• ITS [Video/PDH]	(neti-its-mib)
• ETS [Ethernet]	(neti-eth-mib)
• Channels	(neti-chmgr-mib)

MIB - Managed Information Base

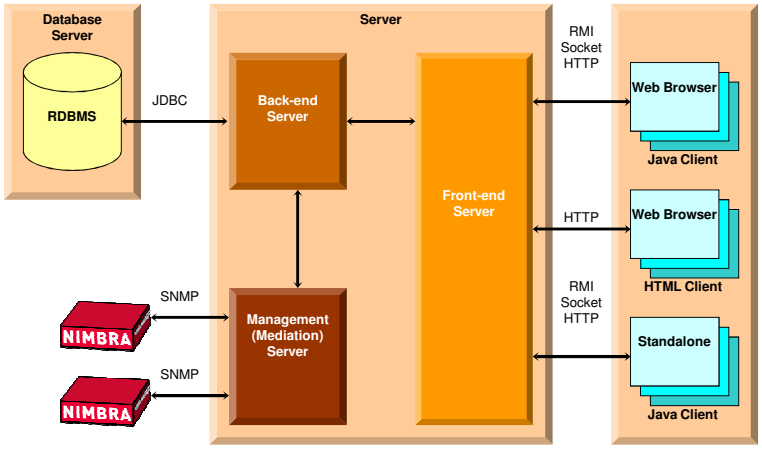
- Global, hierarchical name space: ensures unique name
- iso.org.dod.internet.private.enterprises.netinsight…
- 1.3.6.1.4.1.2928…
- Managed information in leafs only



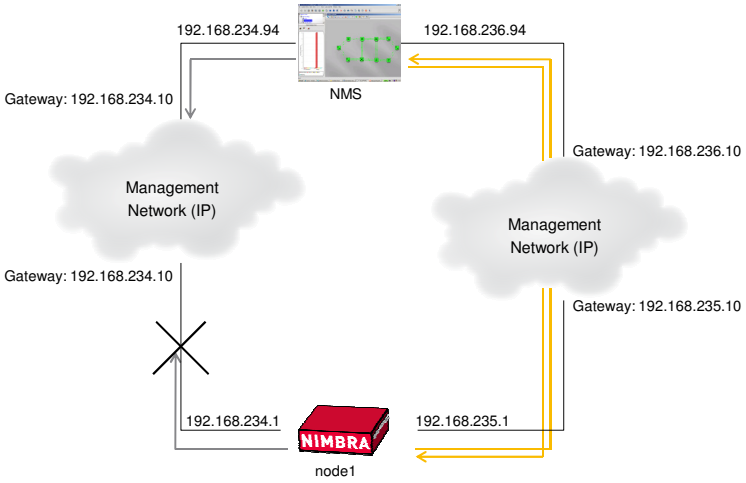
Management Architecture



Nimbra Vision system blocks



Redundant Management Networks

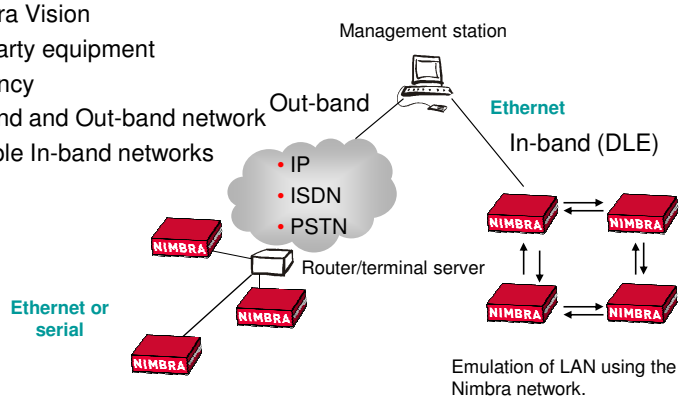


Management

- In Band and Out Band

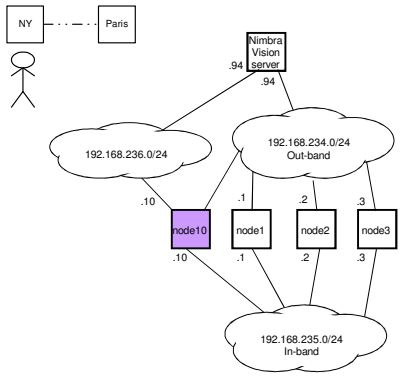
In-band Management

- 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



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

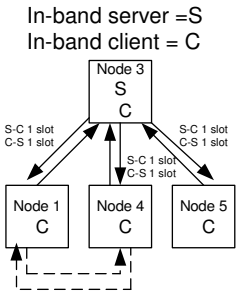
DLE segment

- 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

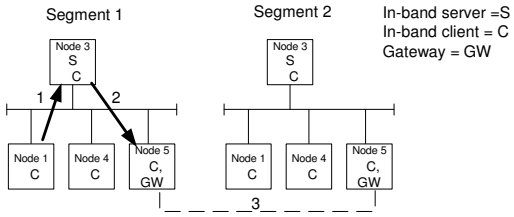
- DLE Client asks DLE server - where is “MAC address/DTM address ”
- Server answer “MAC address/DTM address” is here
- Client to Client channel is established between the two clients



In-band, DLE Segments

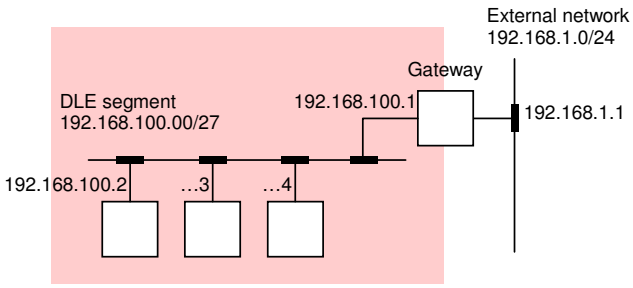
- Several DLE segments can coexist in a DTM network
  - Each DLE segment requires it’s own DLE Server
  - The DLE Server forwards broadcast packets to all DLE Client’s within the segment
- To send data from one DLE segment to another, the packets must pass through one or several IP routers!

In-band, multiple segments

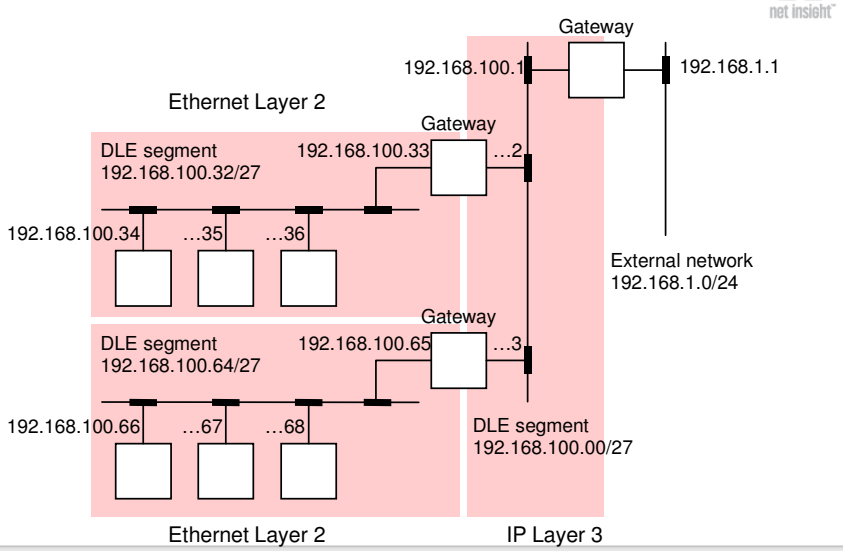


- DLE Client asks DLE server
- Server find the address, goes to gateway
- Routed over IP net

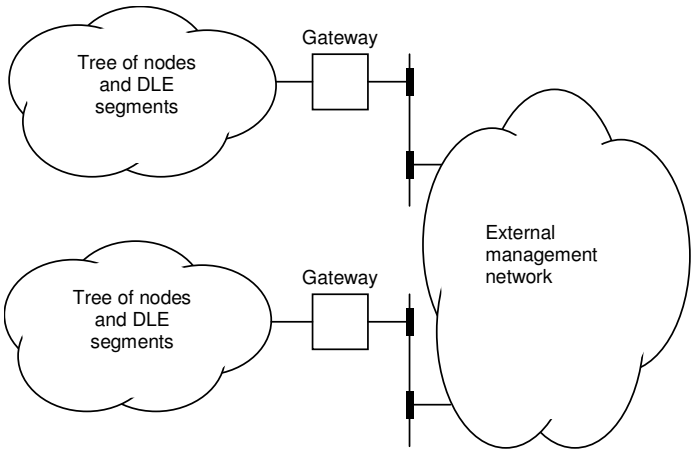
In-band, Configuration of a small network



In-band, Configuration of large network



In-band, Configuration of very large networks



In-band, Recommendations

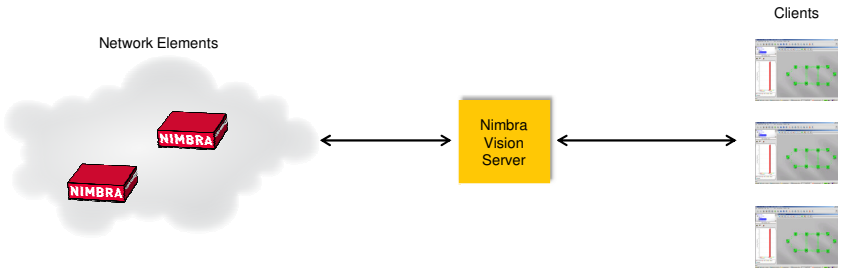
	Nimbra One	Nimbra 340	Nimbra 600
Maximum recommended number of DLE clients for one DLE server	16	16	64
When working as gateway: maximum recommended number of nodes to route traffic for	255	255	1 000
Channel capacity for DLE client-server channels	512 kbps (1 slot)	512 kbps (1 slot)	512 kbps (1 slot)
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

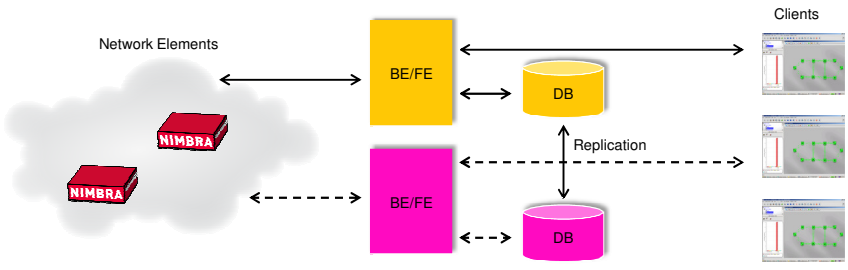
Non-Redundant Configuration

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



Redundancy

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



Server failover setup

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

Server failover (cont'd)

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'

Server failover (cont'd)

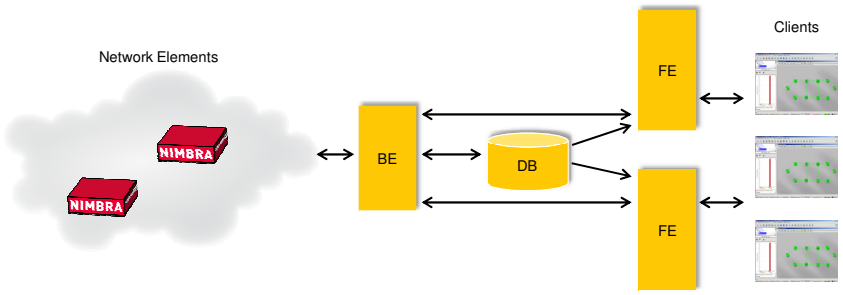
13. Flush all tables and lock write statements (>flush tables with read lock;)
14. DON'T CLOSE CMD TOOL
15. Read values of current binary log name and position (show master status;)
16. Write down values (file name and position)
17. Take a snapshot of the database and copy to 'Utbildning93'
    - Copy 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.

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.

Distribute Load on Multiple Hosts

- 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



Nimbra Vison

- Server
- Client

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

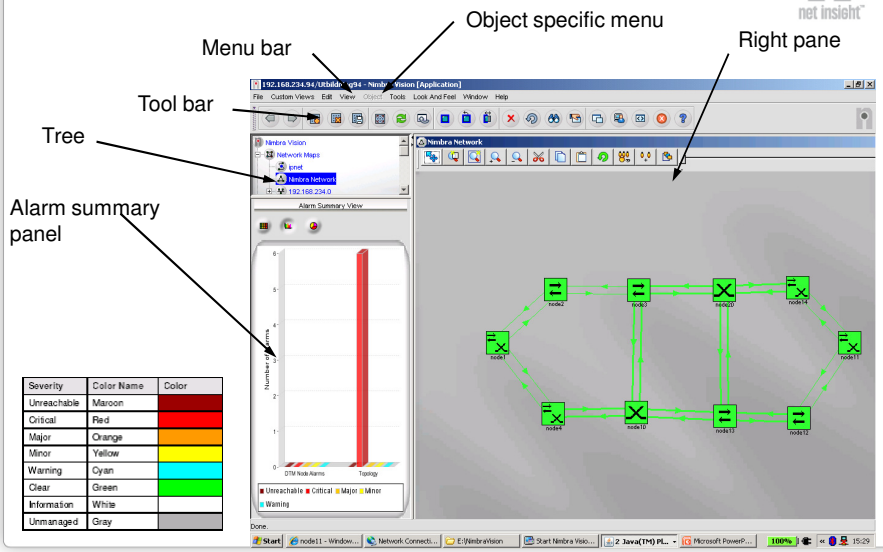
- Add user name (principal), etc., for SNMPv3 on each network, sub-network or network element
- Only Nimbra Vision (and system administrator) needs to know the user name

- Parameters to configure:
  - User Name (= principal)
  - Context Name (empty)
  - Agent Port (161)
  - Security Level (AuthNoPriv)
  - Auth Protocol (MD5)
  - Auth Password

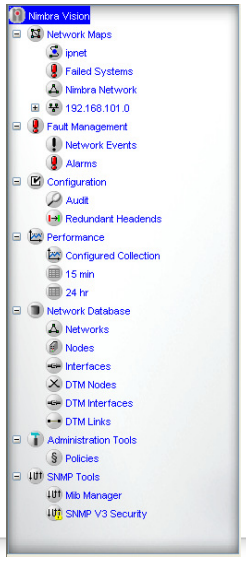
Exersice

Lab 1: Element manager
Lab 2: Setup in Network Elements
Lab 3: Starting Nimbra Vision
Lab 4: Setting up Discovery Engine

Nimbra Vision client window



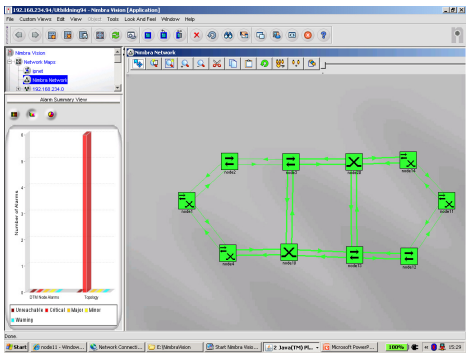
The tree



- 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 Manger (Web/CLI)
- Background image possible
- Groups and hierarchical/linked maps



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

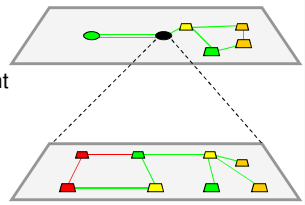
- Map properties
  - Lock placement (anchor)
  - Background image
  - Layout (*)
  - Placement (*)
  - Renderer (*)
  - Criteria (what to show)

- (*) 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

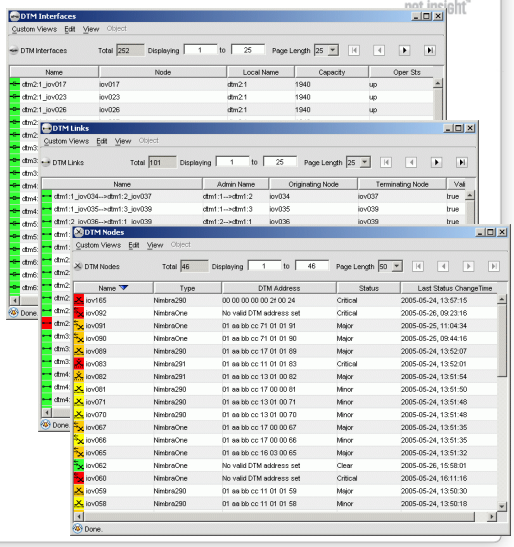


Exersice

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, Nimbra Vision will monitor the corresponding Network Element (or network)
- When a managed object (MO) is UnManaged, Nimbra Vision will ignore the Network Element (or network), ignoring alarms, notifications, status update etc.
- You can change if an MO shall be Manged 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

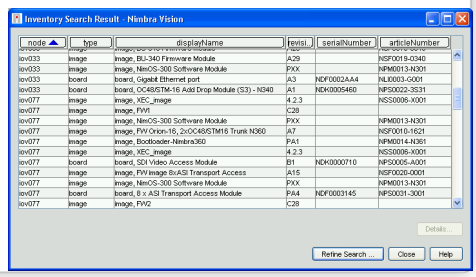
- Adding a new network or a network element
  - If you have a new network element
  - If you have a new network
  - If you don't want to wait for the Discovery Engine
  - Add is available from Network Database
- Deleting a network or network element
  - Deletes all the data associated with the MO

Exersice

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

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 Nimbra Vision database
- Inventory data is searchable, result presented in a table



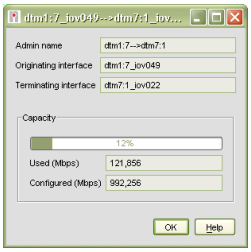
Object operations – general

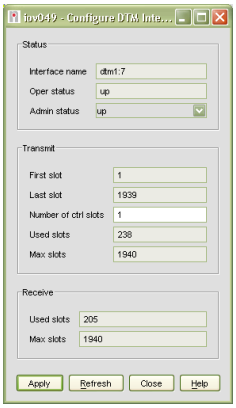
- An object is something that is known by Nimbra Vision
  - Network element
  - Interface
  - Link
  - Alarm
  - Statistics report
  - Etc…
- Select object in map (or list) to enable object specific menu
- Object specific menu contains operations on object

Object operations – DTM Management

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

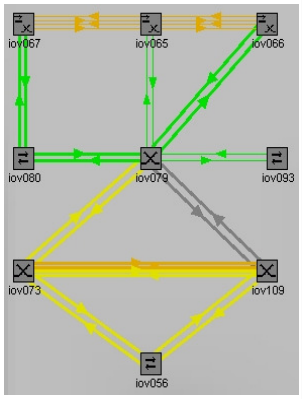
- Operations on
  - Network elements
  - Interfaces
  - Links





Link Utilization

- 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%

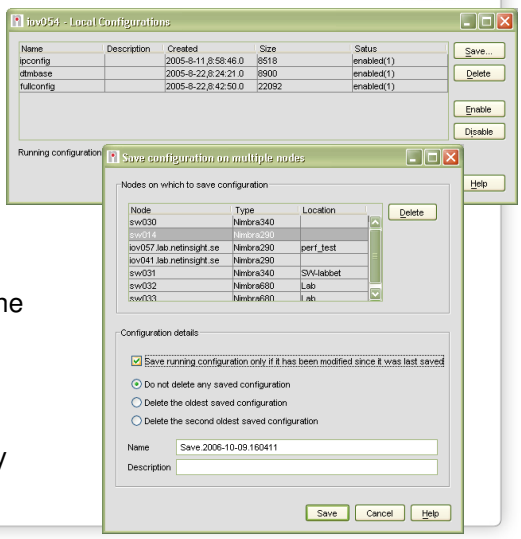


Object specific operations – Miscellaneous

- 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

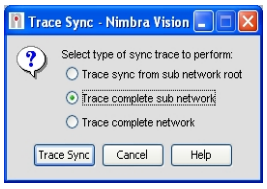
Object operations – Configuration Management

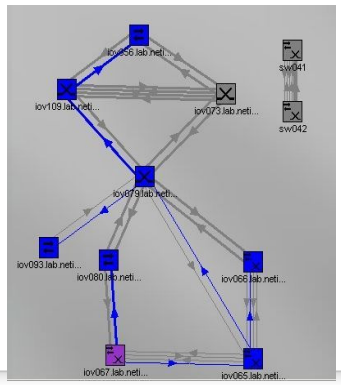
- A local configuration is a persistent storage containing all the information in the node
- Manage local configurations
- Save/delete
- Enable/disable
- Save on multiple nodes in one operation
- Optionally delete old configurations prior save
- Can also save using a Policy



Sync Trace

- Synchronization paths automatically set up by the network
- Sync trace function in Nimbra 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





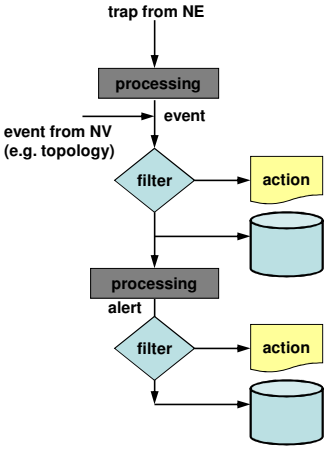
Exersice

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
  - ...

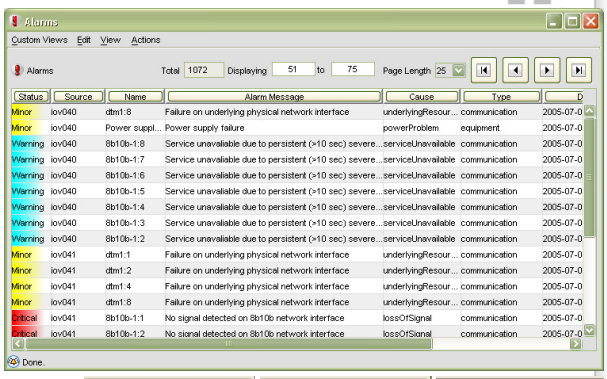


Fault management – Alarm properties

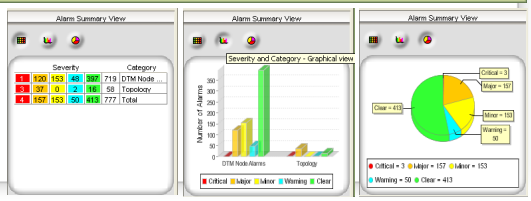
- According to X.733:
- Probable Cause
- Type
- Severity
- Message
- Alarming Object
- Time stamp

- Also
- Purpose, if alarming object has that information
- Purpose is defined in e.g. Element Manager

Fault Management



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

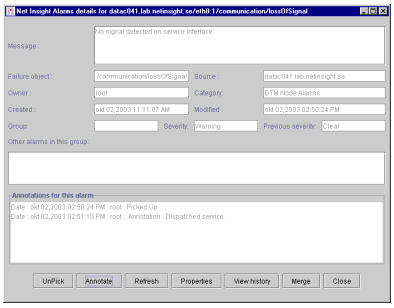


Fault management – Alarm filters

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

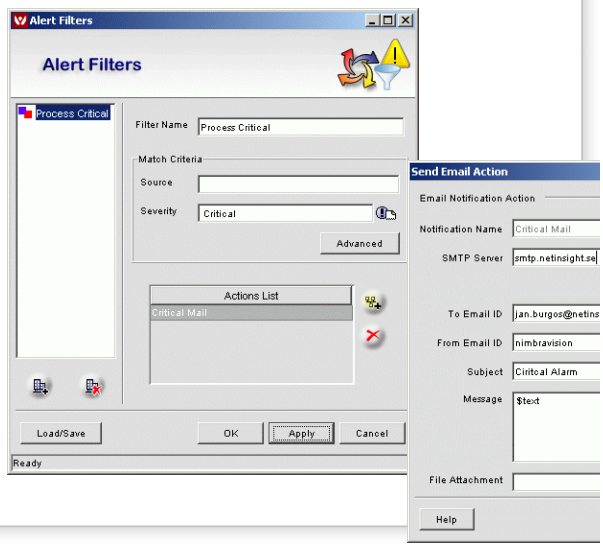
Fault management – Alarm details

- 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

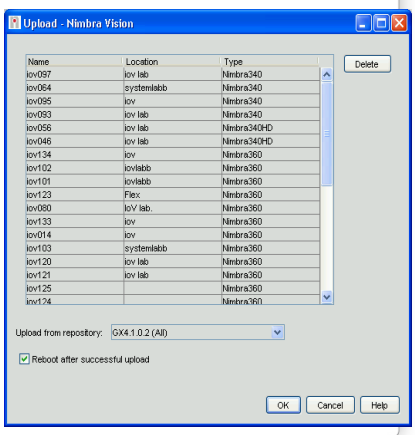


Exersice

- 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



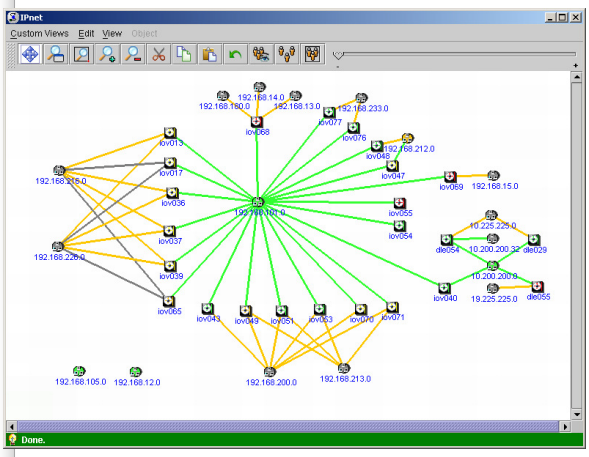
Upload, configure

- 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

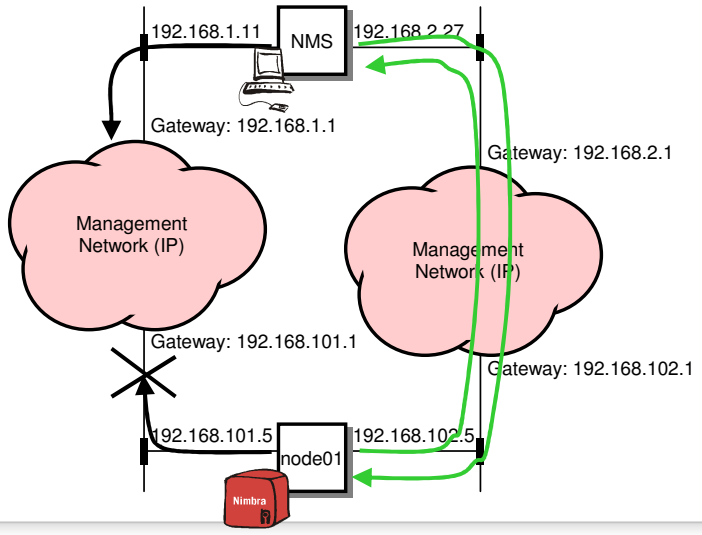
Management Networks



- IP Map shows
- all IP subnets
- routers connecting the subnets

- Usage: to monitor the Management Network

Redundant Management Networks



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

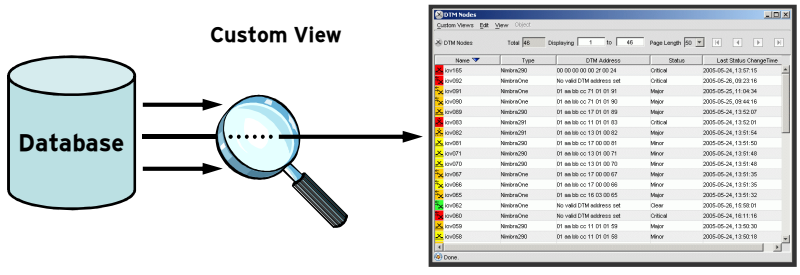
- On DTM Node properties:
- activeIpAddress: the IP address currently used to reach the node
- ipAddress: the IP address when the MO was added to the database (discovered)
- interfaceList: all IP addresses reported by node

Exersice

- Lab 17: Redundant Networks

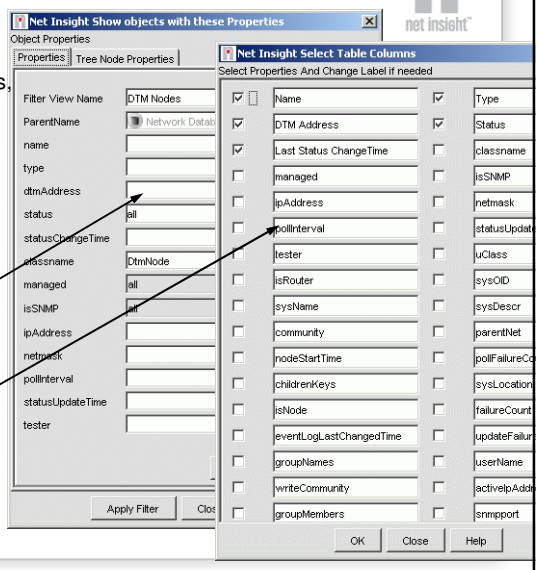
Custom View – is a filter

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



Custom View

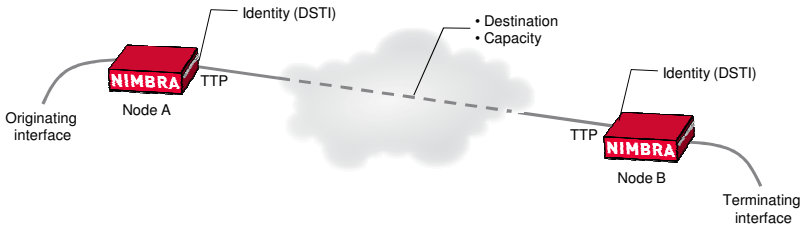
- Custom View is a view into the database
- Can be used for all type of data (maps, event, alarms, network database, …)
- Temporary (for this session) or saved (for future sessions)
- Placed in tree
- Defines:
- Which (which rows?)
  - View all rows that match given criteria
- What (what colums?)
  -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



Exersice

- Lab 18: Custom View
- Filter and Search

Service Provisioning, general



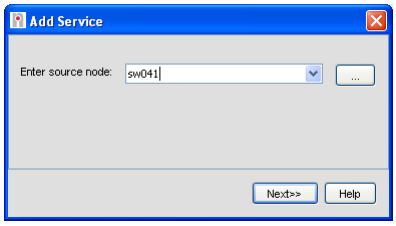
Simple process:
1. Define Trail Termination Points (TTP)
2. Associate interface with TTP
3. Define connection between TTPs

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

Service provisioning, step 1

- 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

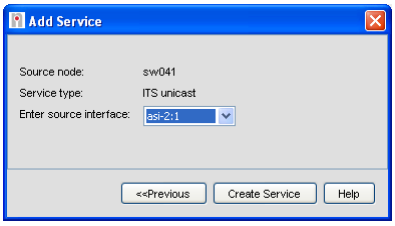


Service provisioning, step 2

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

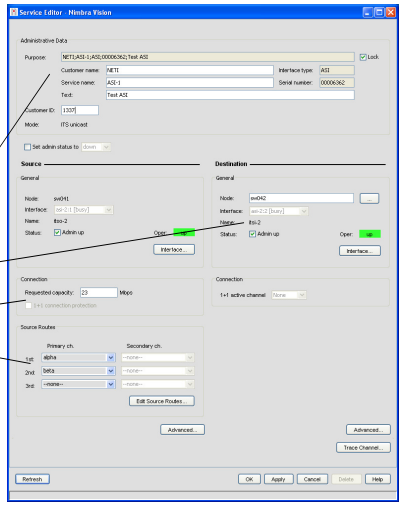
Service provisioning, step 3

- Enter source interface (ITS only)



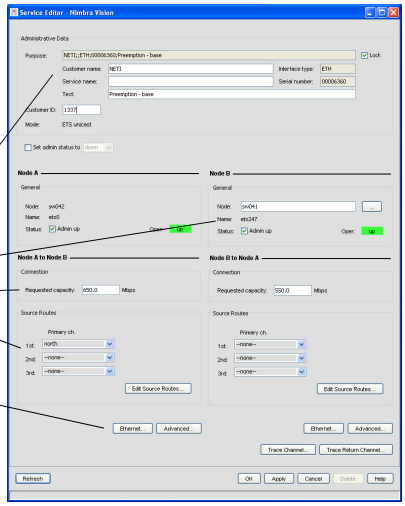
Service provisioning, step 4 (ITS unicast)

- Service Editor opened after finishing the wizard
- Enter optional admin data for the service
- Enter destination node and interface
- Enter capacity (ASI only)
- Select source routes if required



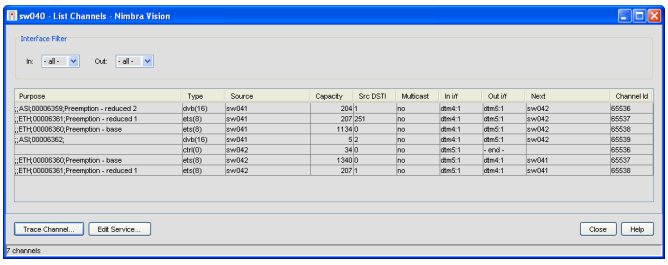
Service provisioning, step 4 (ETS unicast)

- 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



Channel List

- Lists all channels originating/transiting/terminating in a node, link or interface
- Start from map or Network Database, from selected node, link or interface
- Lists data about each channel
- Run multiple channel list simultaneously
- Start Channel Trace on selected channel
- Data displayed in tabular format

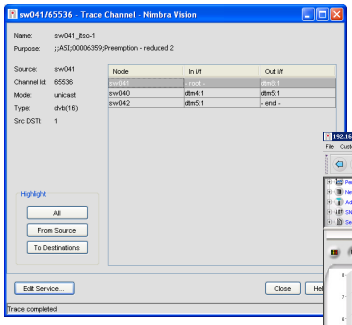


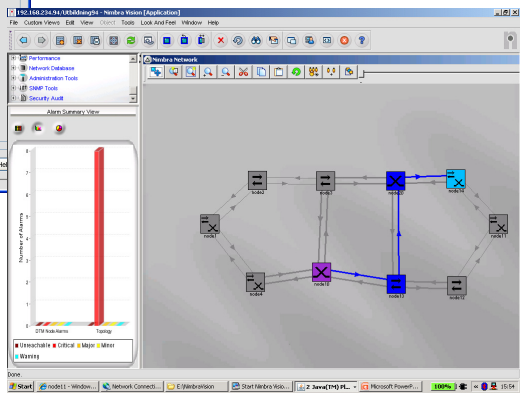
Trace Channel - Start

- 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



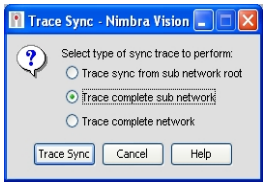


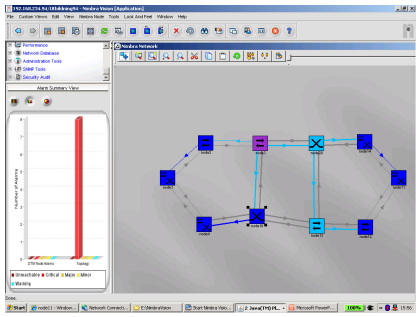
Result as:

- 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 Nimbra 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





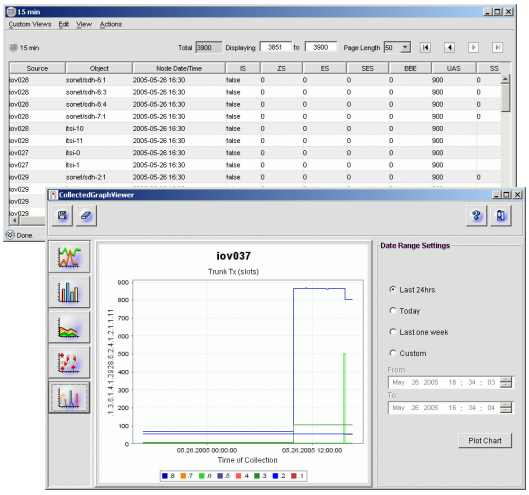
Exersice

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

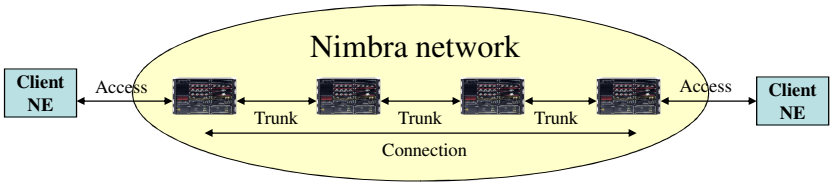
Performance Monitoring

- 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



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

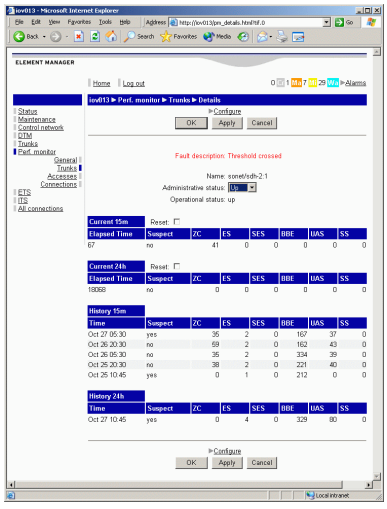
Performance Monitoring and Statistics

- 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

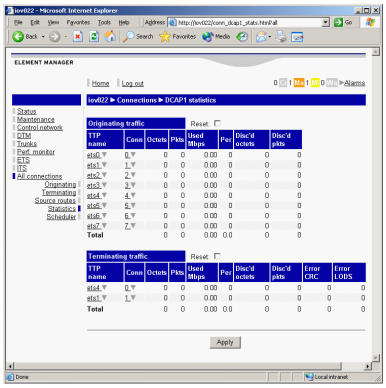
Performance Monitoring on Trunks

- 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



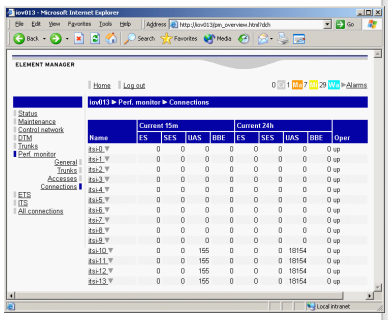
Statisitcs on Connections

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

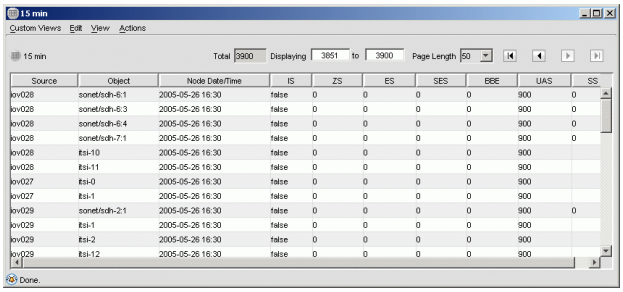


Performance Monitoring on Service

- 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



Performance monitoring – G.826 like reports



- 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

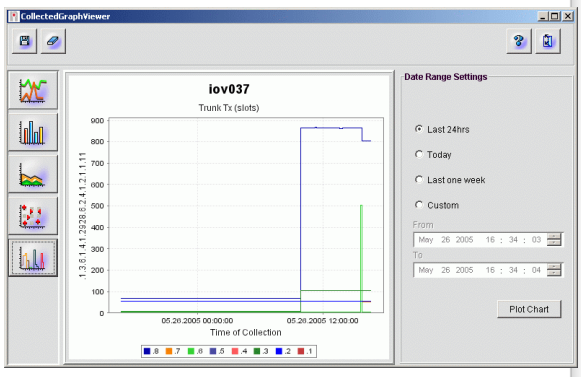
- 15 minutes reports
- 24 hrs reports

- Following performance parameters are monitored:
  - ES (Errored Seconds) Counts how many seconds has at least one errored block (BBE)
  - SES (Severly 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

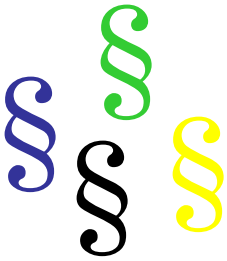
Exersice

- Lab 20: Performance Monitoring

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

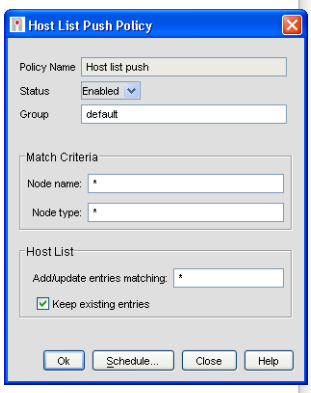


Policy – Save DTM node Registry

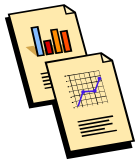
- Saves the current (running) configuration. Options:
  - Save only if not already saved
  - Delete oldest/second oldest configuration prior save
  - Store copy on Nimbra Vision server, saved in <NVHOME>\backup\nodeconfigurations
  - Store copy on Nimbra Vision server regardless if saved or not
- Set 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 Nimbra 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!



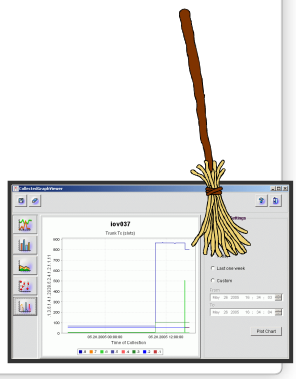
Policy – Generate Reports



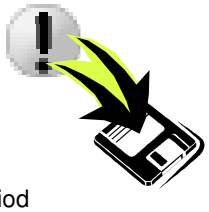
- Generate daily/weekly/monthly reports
- Operates on DTM interfaces
- Reports generated as summary and detailed reports
- Set up a schedule for when to execute

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

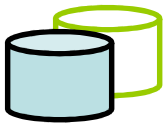


- Copies events to log file
- Specify log file folder
- Specify how often
- Events generated since last period is saved each period

- Note! Nimbra Vision enforces a maximum number of alarms. Oldest alarms are automatically deleted to enforce this maximum.

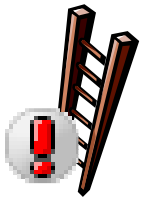
Policy – NMS Backup

- 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)

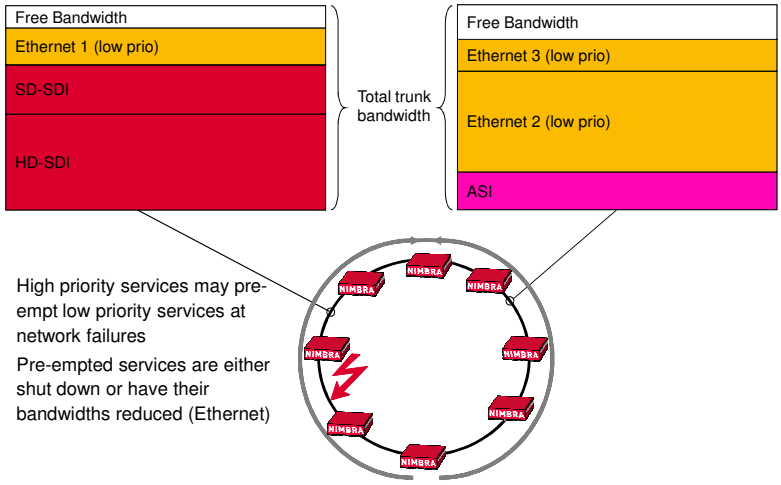


Exersice

- Lab 21: Policies

Pre-emption at Network Failure

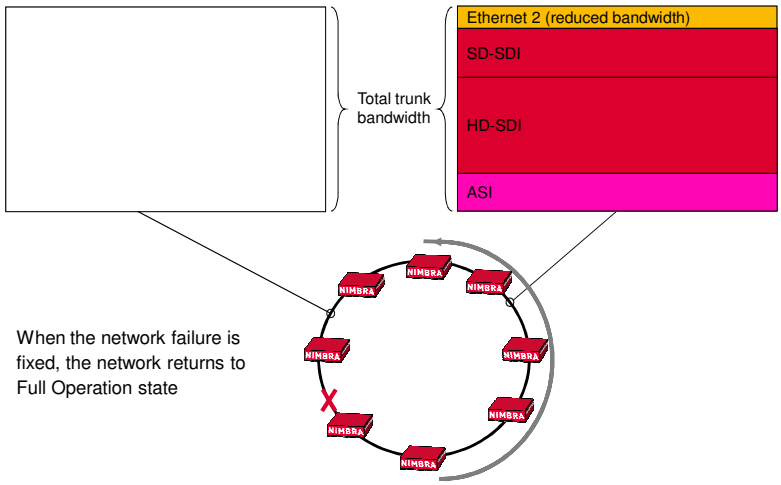
Network in Full Operation state



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

Pre-emption at Network Failure

Network in Reduced Operation state

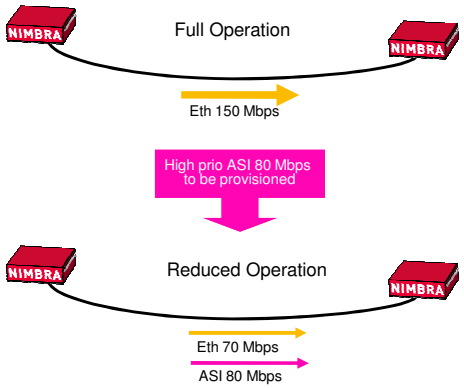


- When the network failure is fixed, the network returns to Full Operation state

Nimbra Vision based Pre-emption

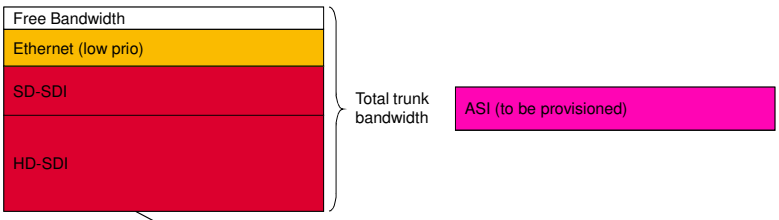
at Service Provisioning

- 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

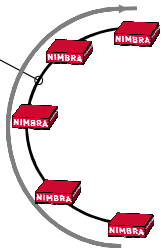


Pre-emption at Service Provisioning

Network in Full Operation state

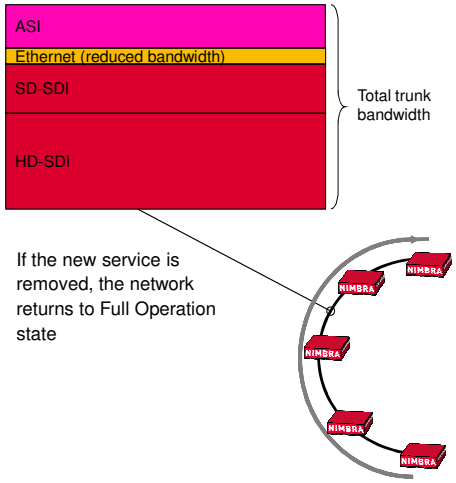


- High priority services may pre-empt low priority services at service provisioning
- Pre-empted services are either shut down or have their bandwidths reduced (Ethernet)



Pre-emption at Service Provisioning

Network in Reduced Operation state



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

Pre-emption, configure

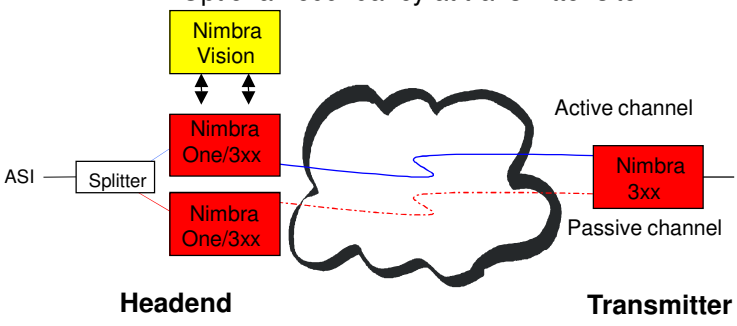
- Identify and configure the pre-emption objects
  - Links (interfaces)
- Identify services that shall be affected by failure in pre-emption object

Exersice

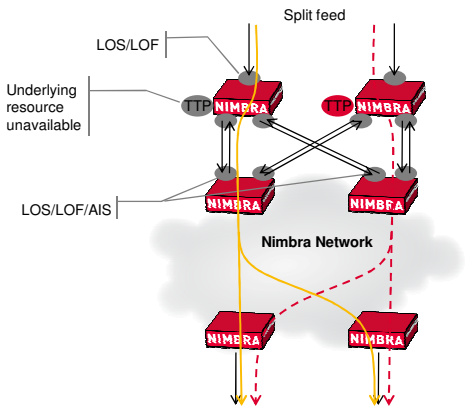
- Lab: Pre-emption

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



Redundant Headend – ETS/ITS

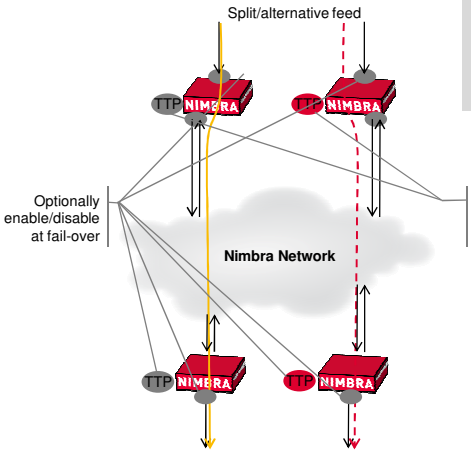


For ITS only:
The service interface is always enabled and disabled by the node when corresponding TTP is enabled or disabled.

Active (primary) connection

Pre-configured in-active (secondary) connection

Redundant Headend - ETS



For ETS only:
The service interface is never enabled or disabled by the node when corresponding TTP is enabled or disabled.

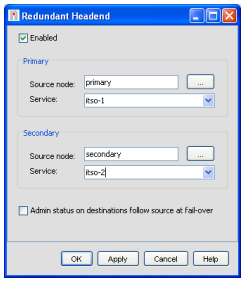
Nimbra Vision can do this.

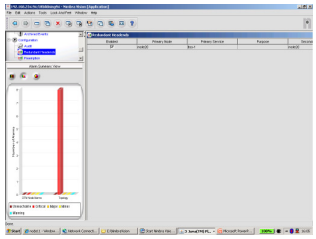
Active (primary) connection

Pre-configured in-active (secondary) connection

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.

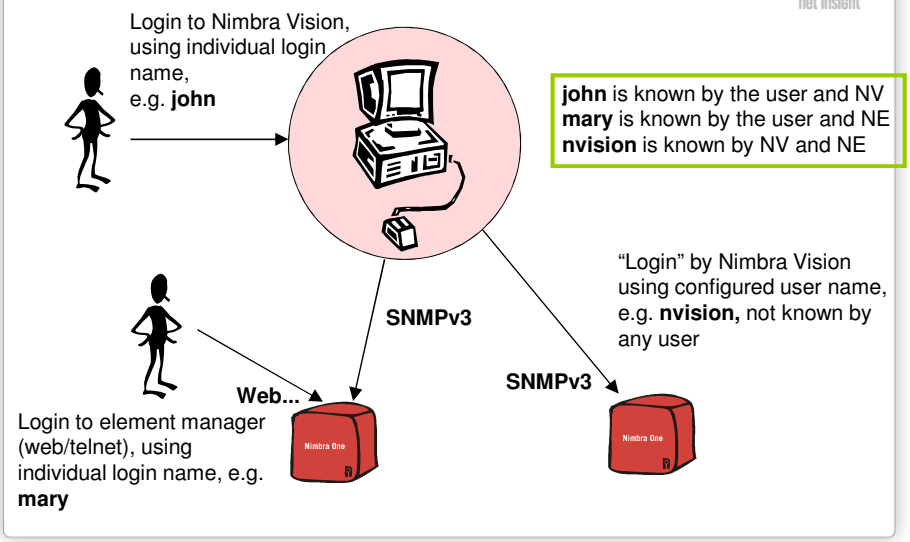




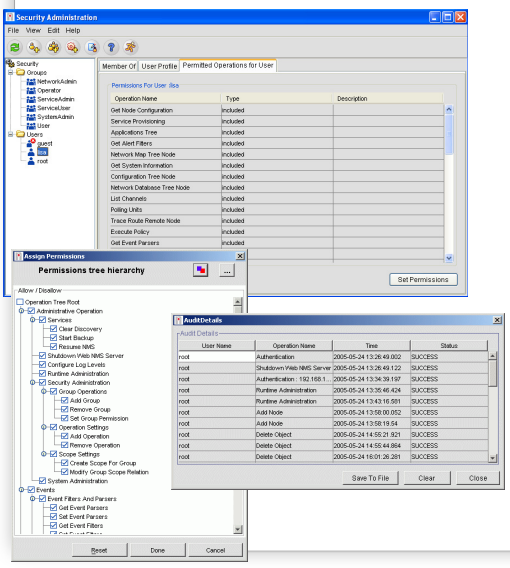
Exersice

- Lab 23: Redundant Headends

User Logins – the big picture



Security management

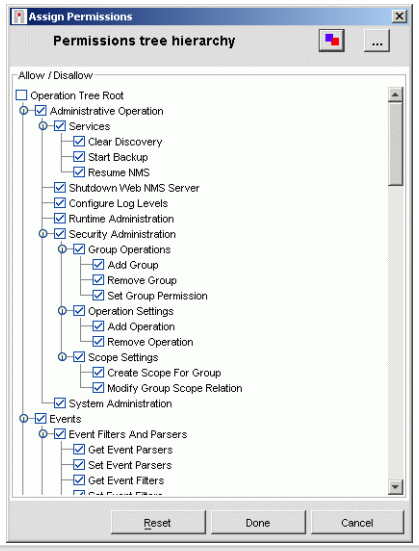


- Individual user logins
  - Groups, Users and Operations
- Assign permitted operations to users and/or groups
  - Restrict what a user can do
- Assign permitted objects to users and/or groups
  - Restrict which object the user can access
- Audit log
- Note!
  User logins in Nimbra Vision are not the 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

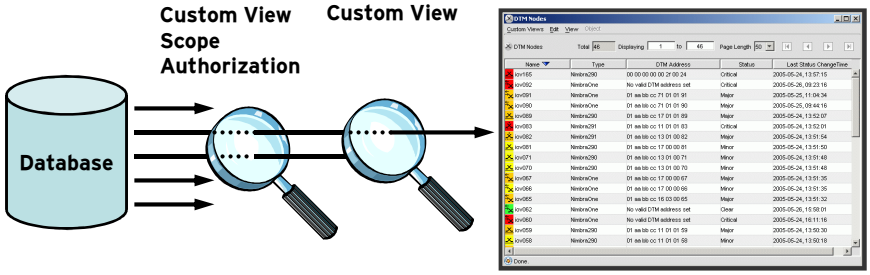
Security management – Operations



- 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

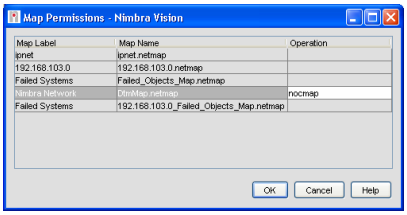
Security management – Custom View Scope

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

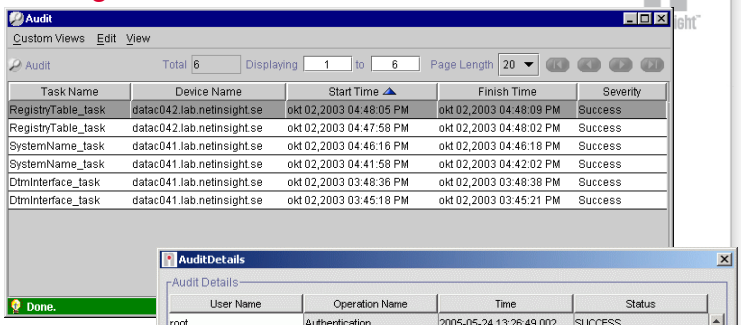


Security management – Private maps

- 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



- Logs all operations
- Details per task execution in tree Configuration:Audit

Exersice

- Lab 24: Security Management

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

Exercises

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

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