Introduzione ad HP-OV NNM

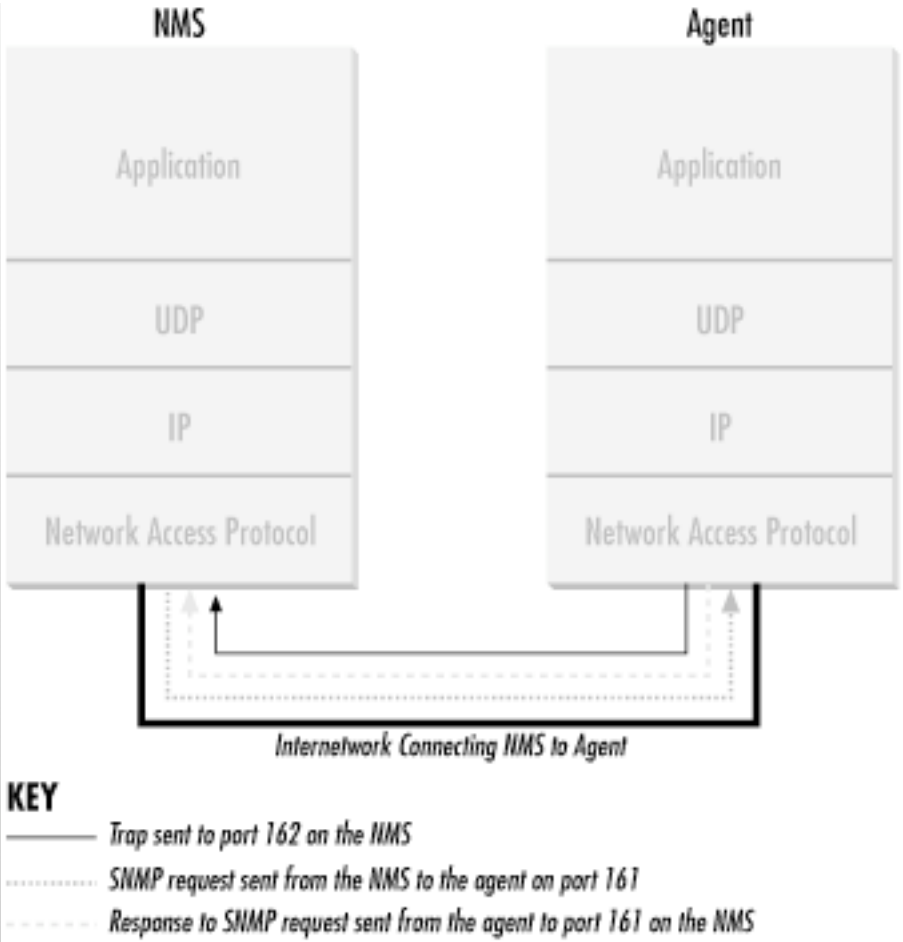
Luca Deri <deri@ntop.org>

Marzo 2003

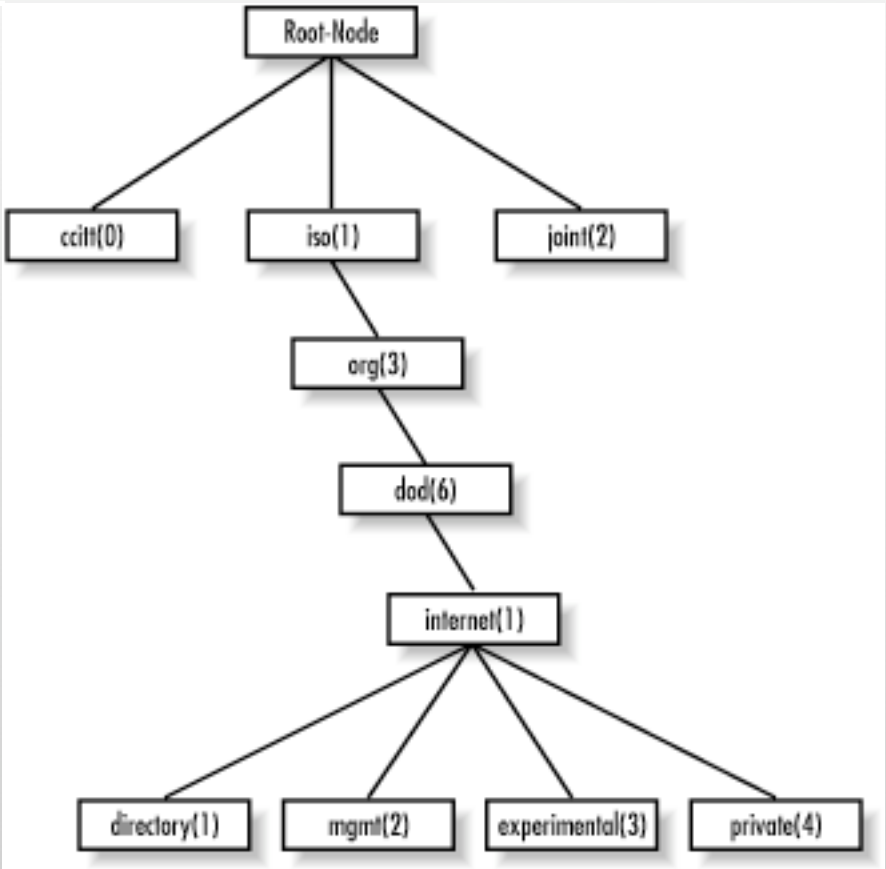
Agenda del Corso

-
- Introduzione al System Management e SNMP
-
- Caratteristiche Principali di HP-OV NNM
-
- Configurazione ed utilizzo di HP-OV NNM

Architettura di un NMS



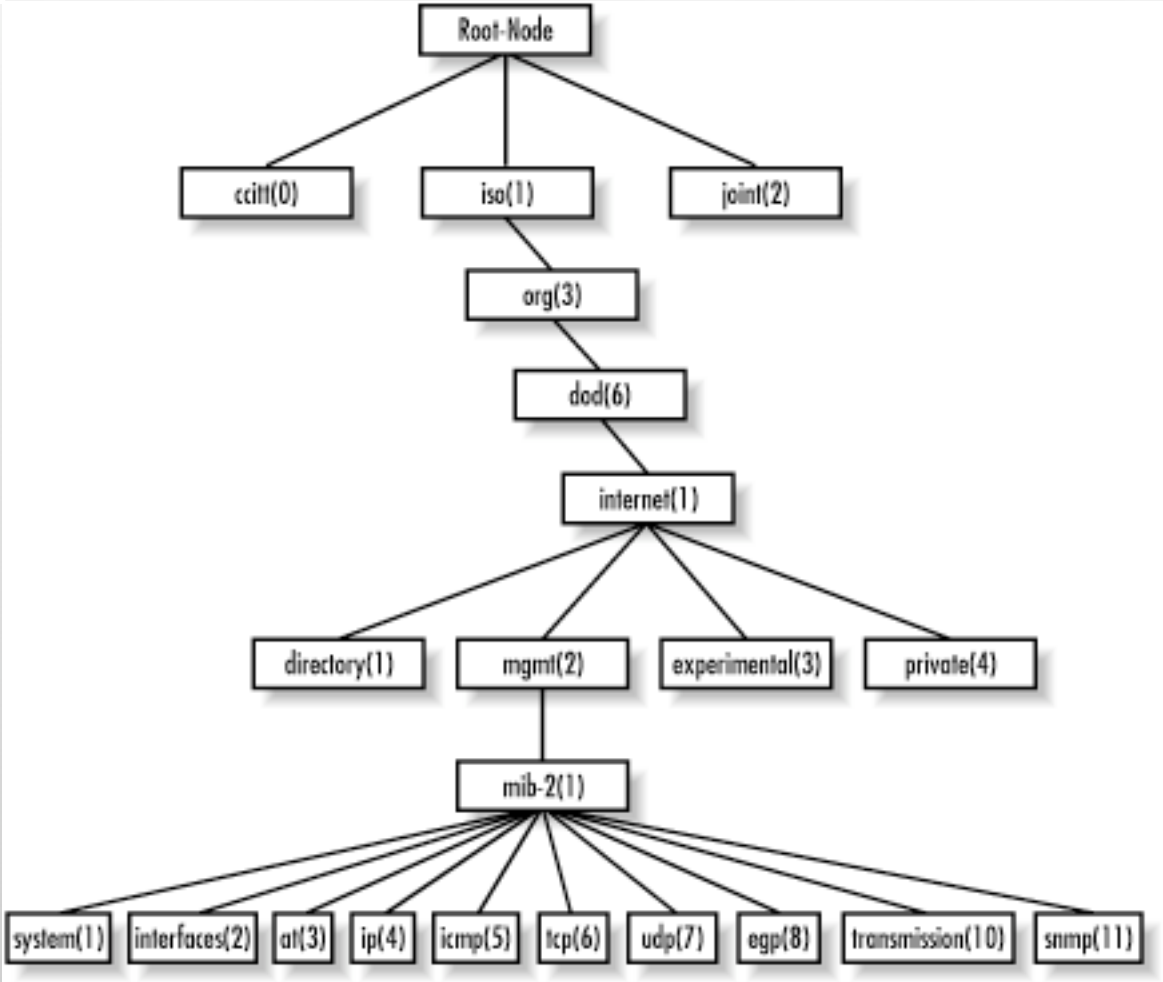
ISO Registration Tree



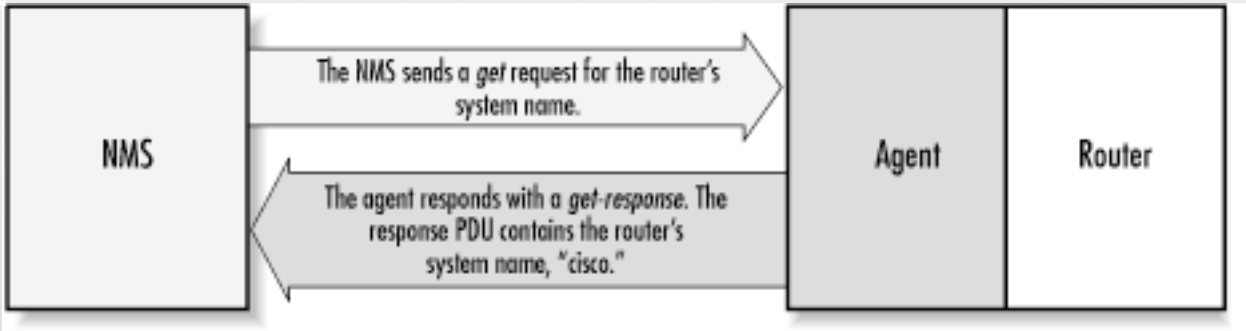
Le Primitive di SNMP

- SNMP Get
- SNMP Get-Next
- SNMP Get-Reply
- SNMP Set
- SNMP Get-Bulk (v2c/v3)
- SNMP Trap
- SNMP Inform (v2c/v3)

SNMP MIB-II

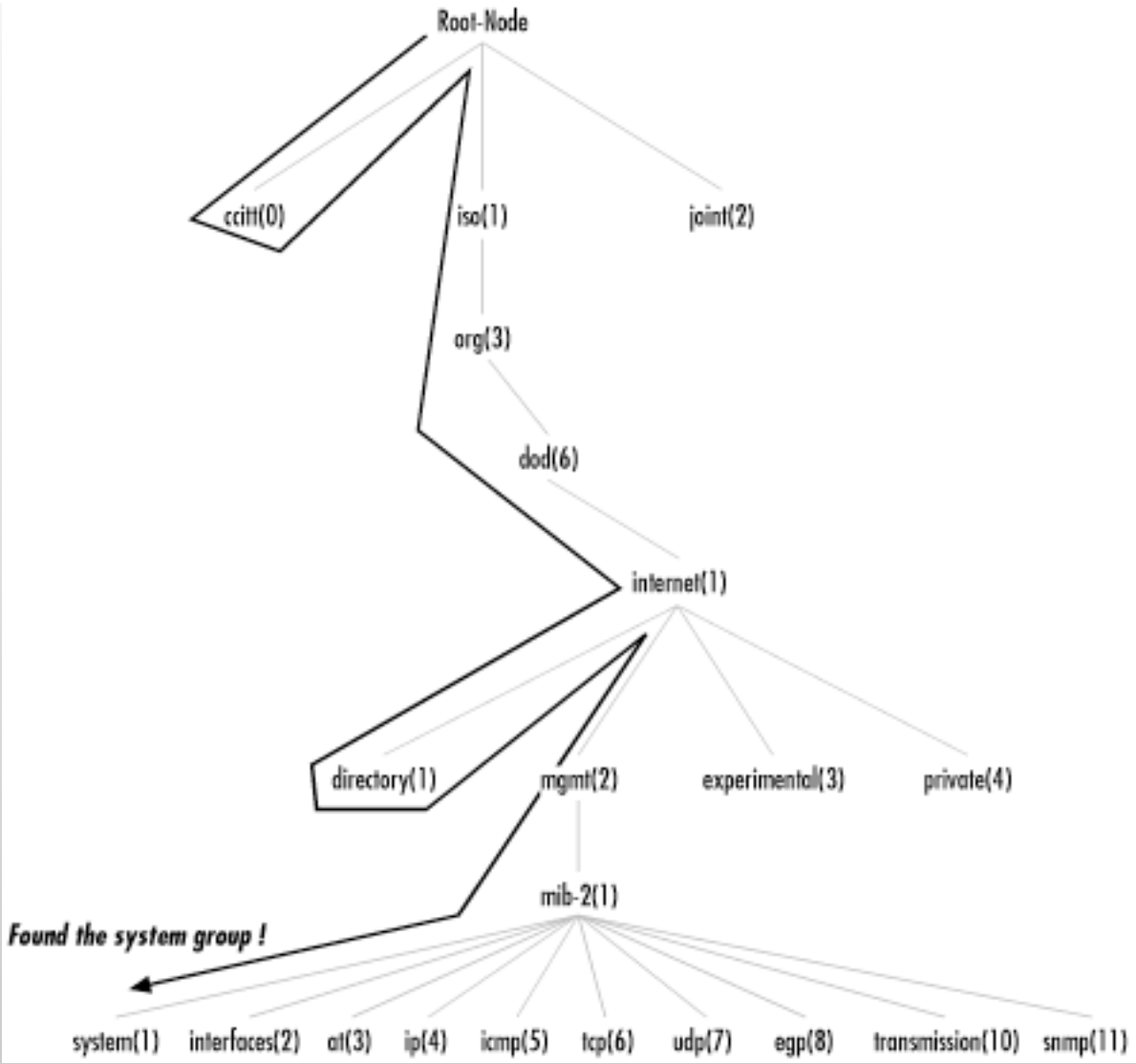

Root-Node
ccitt(0)
iso(1)
joint(2)
org(3)
dod(6)
internet(1)
directory(1)
mgmt(2)
experimental(3)
private(4)
mib-2(1)
system(1)
interfaces(2)
at(3)
ip(4)
icmp(5)
tcp(6)
udp(7)
egp(8)
transmission(10)
snmp(11)

SNMP Get




```
$ snmpget cisco.ora.com public .1.3.6.1.2.1.1.6.0
system.sysLocation.0 = "Pisa"
```

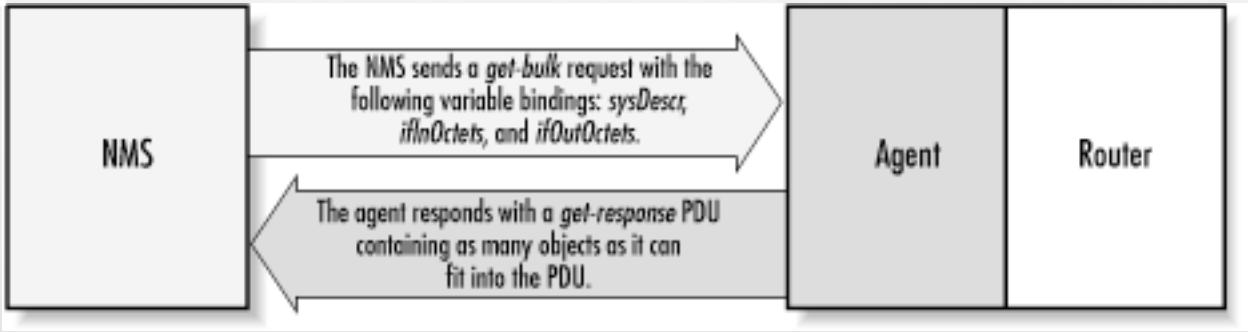
SNMP Get-Next [1/2]



SNMP Get-Next [2/2]

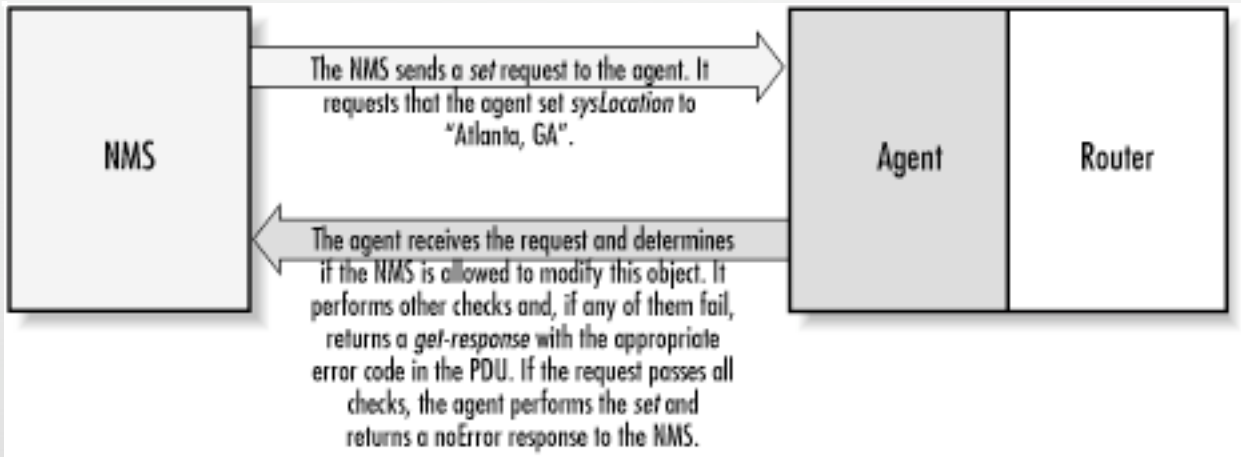
```
$ snmpwalk cisco.ora.com public system
system.sysDescr.0 = "Cisco Internetwork Operating System Software
..IOS (tm) 2500 Software (C2500-I-L), Version 11.2(5), RELEASE
SOFTWARE (fc1)..Copyright (c) 1986-1997 by cisco Systems, Inc...
Compiled Mon 31-Mar-97 19:53 by ckralik"
system.sysObjectID.0 = OID: enterprises.9.1.19
system.sysUpTime.0 = Timeticks: (27210723) 3 days, 3:35:07.23
system.sysContact.0 = ""
system.sysName.0 = "cisco.ora.com"
system.sysLocation.0 = ""
system.sysServices.0 = 6
```

SNMP Get-Bulk



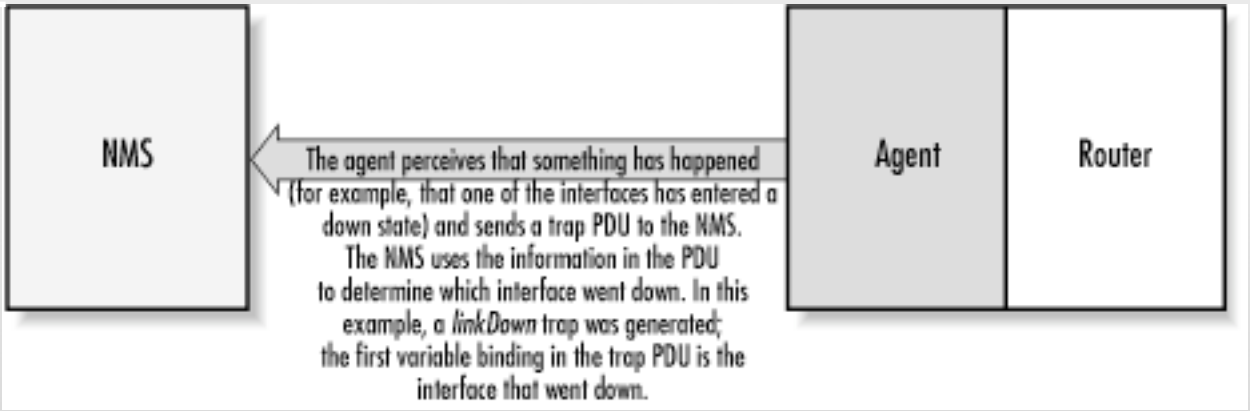

```
$ snmpbulkget -v2c -B 1 3 linux.ora.com public sysDescr ifInOctets ifOutOctets
system.sysDescr.0 = "Linux linux 2.2.5-15 #3 Thu May 27 19:33:18 EDT 1999 i686"
interfaces.ifTable.ifEntry.ifInOctets.1 = 70840
interfaces.ifTable.ifEntry.ifOutOctets.1 = 70840
interfaces.ifTable.ifEntry.ifInOctets.2 = 143548020
interfaces.ifTable.ifEntry.ifOutOctets.2 = 111725152
interfaces.ifTable.ifEntry.ifInOctets.3 = 0
interfaces.ifTable.ifEntry.ifOutOctets.3 = 0
```

SNMP Set




```
$ snmpget cisco.ora.com public system.sysLocation.0
system.sysLocation.0 = ""
$ snmpset cisco.ora.com private system.sysLocation.0 s "Atlanta, GA"
system.sysLocation.0 = "Atlanta, GA"
$ snmpget cisco.ora.com public system.sysLocation.0
system.sysLocation.0 = "Atlanta, GA"
```

SNMP Trap [1/2]


NMS
The agent perceives that something has happened (for example, that one of the interfaces has entered a down state) and sends a trap PDU to the NMS. The NMS uses the information in the PDU to determine which interface went down. In this example, a *linkDown* trap was generated; the first variable binding in the trap PDU is the interface that went down.
Agent
Router

SNMP Trap [2/2]

Trap MIB-II

```
coldStart(0)
warmStart(1)
linkDown(2)
linkUp(3)
authenticationFailure(4)
egrNeighborLoss(5)
enterpriseSpecific(6)
```

Trap Specifica

```
rdbmsOutOfSpace TRAP-TYPE
    ENTERPRISE  rdbmsTraps
    VARIABLES   { rdbmsSrvInfoDiskOutOfSpaces }
    DESCRIPTION
        "An rdbmsOutOfSpace trap signifies that one of the database
         servers managed by this agent has been unable to allocate
         space for one of the databases managed by this agent. Care
         should be taken to avoid flooding the network with these traps."
    ::= 2
```

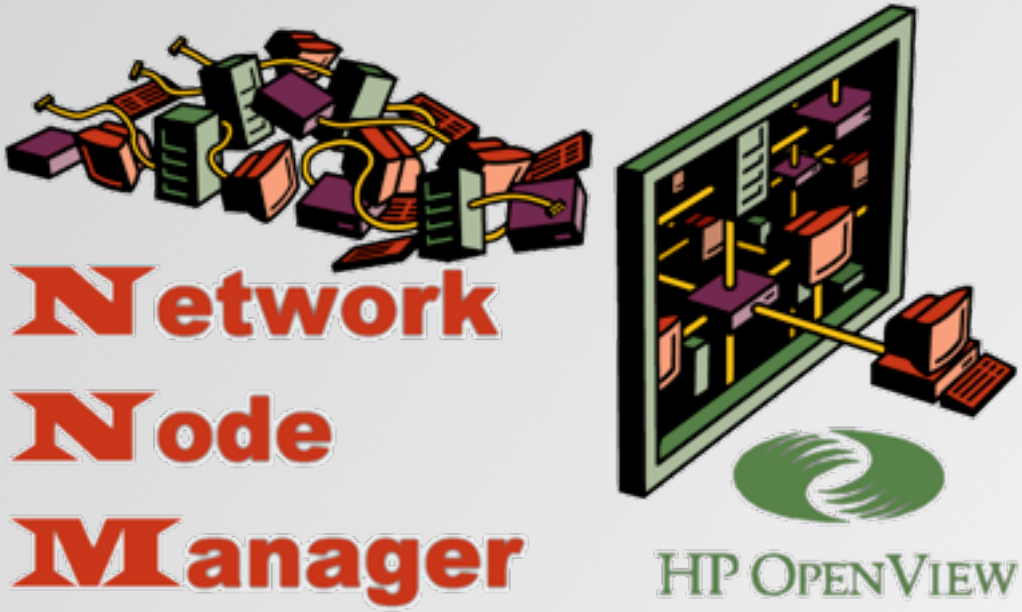
Errori SNMPv1

Error(0)	There was no problem performing the request.
tooBig(1)	The response to your request was too big to fit into one response.
noSuchName(2)	An agent was asked to get or set an OID that it can't find; i.e., the OID doesn't exist.
badValue(3)	A read-write or write-only object was set to an inconsistent value.
readOnly(4)	This error is generally not used. The noSuchName error is equivalent to this one.
genErr(5)	This is a catch-all error. If an error occurs for which none of the previous messages is appropriate, a genError is issued.

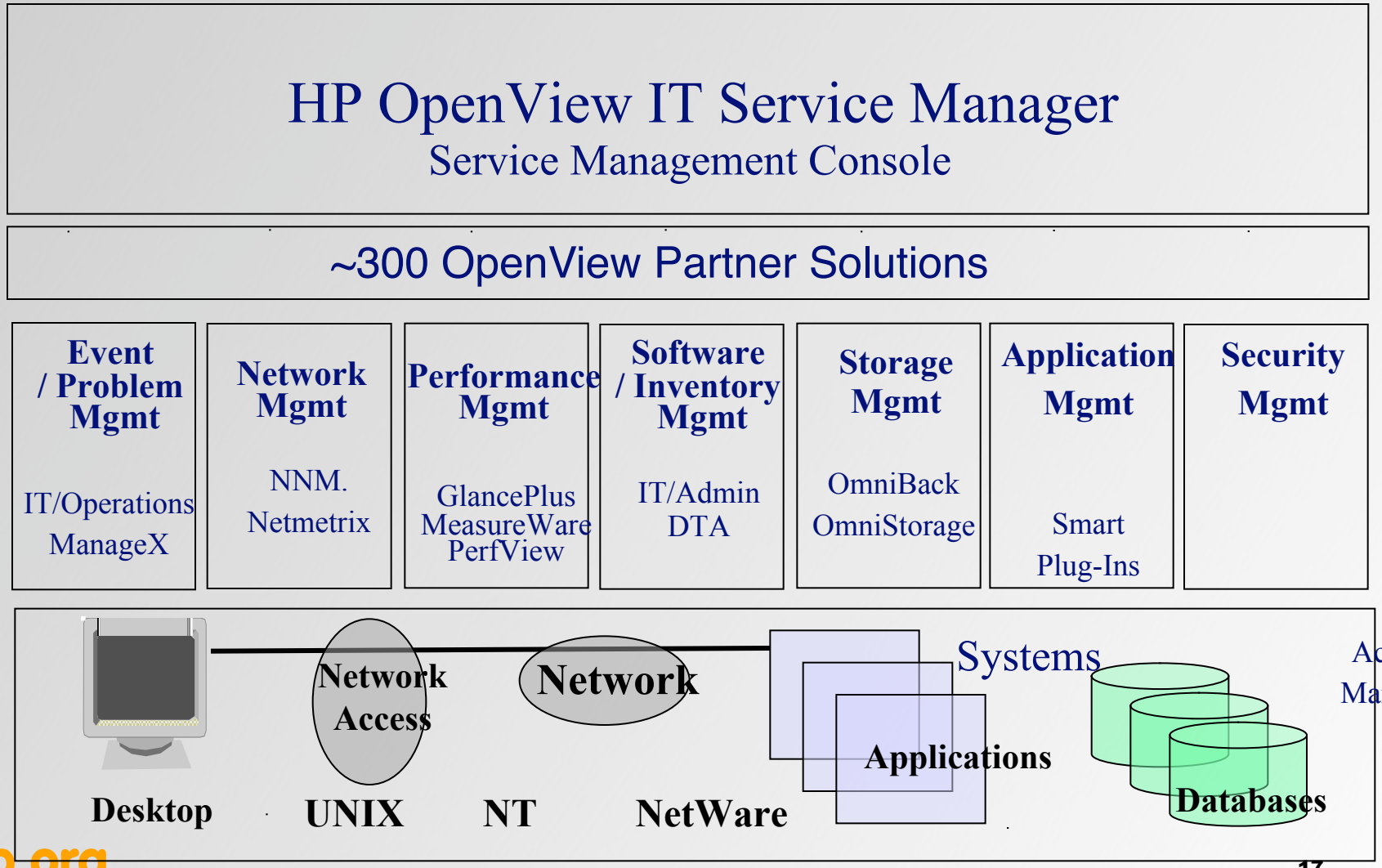
Eccezioni SNMPv2c/3

noAccess(6)
wrongType(7)
wrongLength(8)
wrongEncoding(9)
wrongValue(10)
noCreation(11)
resourceUnavailable(13)
commitFailed(14)
undoFailed(15)
authorizationError(16)
notWritable(17)
inconsistentName(18)

Panoramica di HP-OpenView Network Node Manager



HP-OpenView: Architettura a blocchi



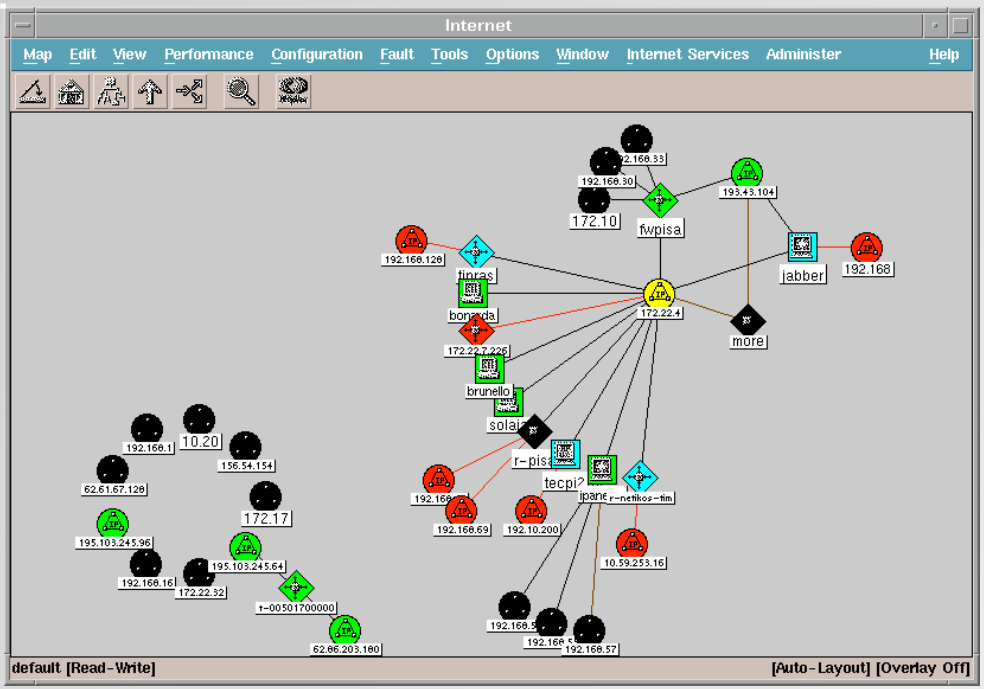
Network Node Manager: Quick feature Overview

- Autodiscovery
- Network Map
- Filtering
- Pan & Zoom
- Drag & Drop
- User-Defined Maps
-

- Status Polling
- Alarms Browser
- Event Correlation
- Alarms Sorting & Filtering
- Color-coded Alarms
- Automated Actions
-
-

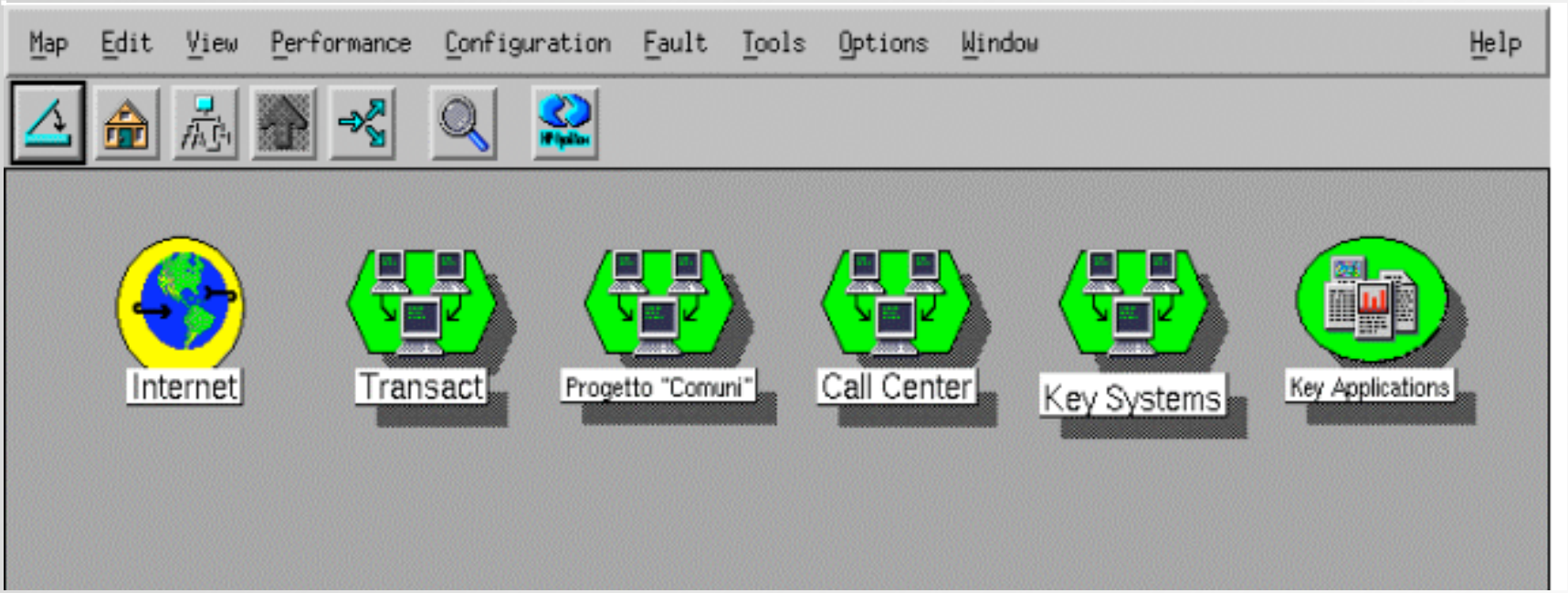
- Data Warehouse
- MIB Data Collection
- User-defined thresholds
- User-defined alarms
- MIB Application Builder
- SNMP Support

Network Node Manager: Rappresentazione reale della rete

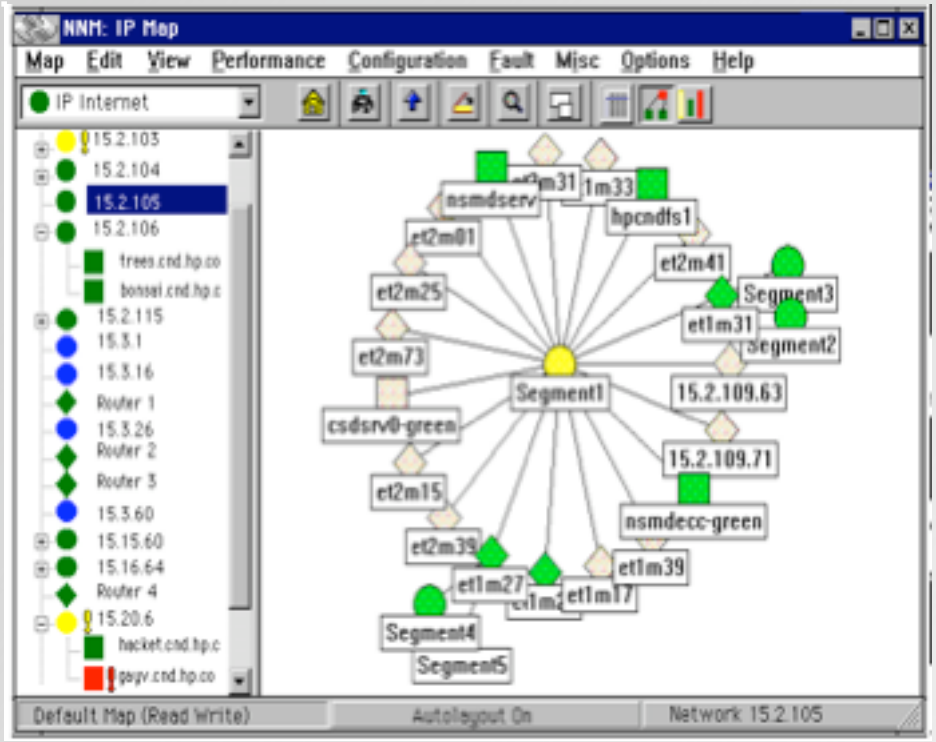


- Discovery & Mapping della rete in modo automatico
- Filtri sul discovery e sulla topologia della mappa
- Pan & Zoom
- Drag & Drop
- Mappe personalizzate
- Monitoring continuo della rete

Network Node Manager: Personalizzazione della mappa



Network Node Manager: Accesso Remoto via Web



- ✓ OpenView Launcher
- ✓ Network Presenter
- ✓ Alarms Browser
- ✓ SNMP MIB Browser
- ✓ Help system
- ✓ Windows UI-style compliant
- ✓ Same look-and-feel as native UI's
- ✓

Configurazione ed Utilizzo di HP-OV NNM

Variabili d'Ambiente

- Le variabili di ambiente necessarie per utilizzate NNM sono impostate dal comando /opt/OV/bin/ov.envvars.csh (utilizzare ov.envvars.pl o ov.envvars.sh a secondo della shell)

- I files di configurazione sono in /etc/opt/OV/share/conf ($OV_CONF)

- I programmi binari in /opt/OV/bin ($OV_BIN)

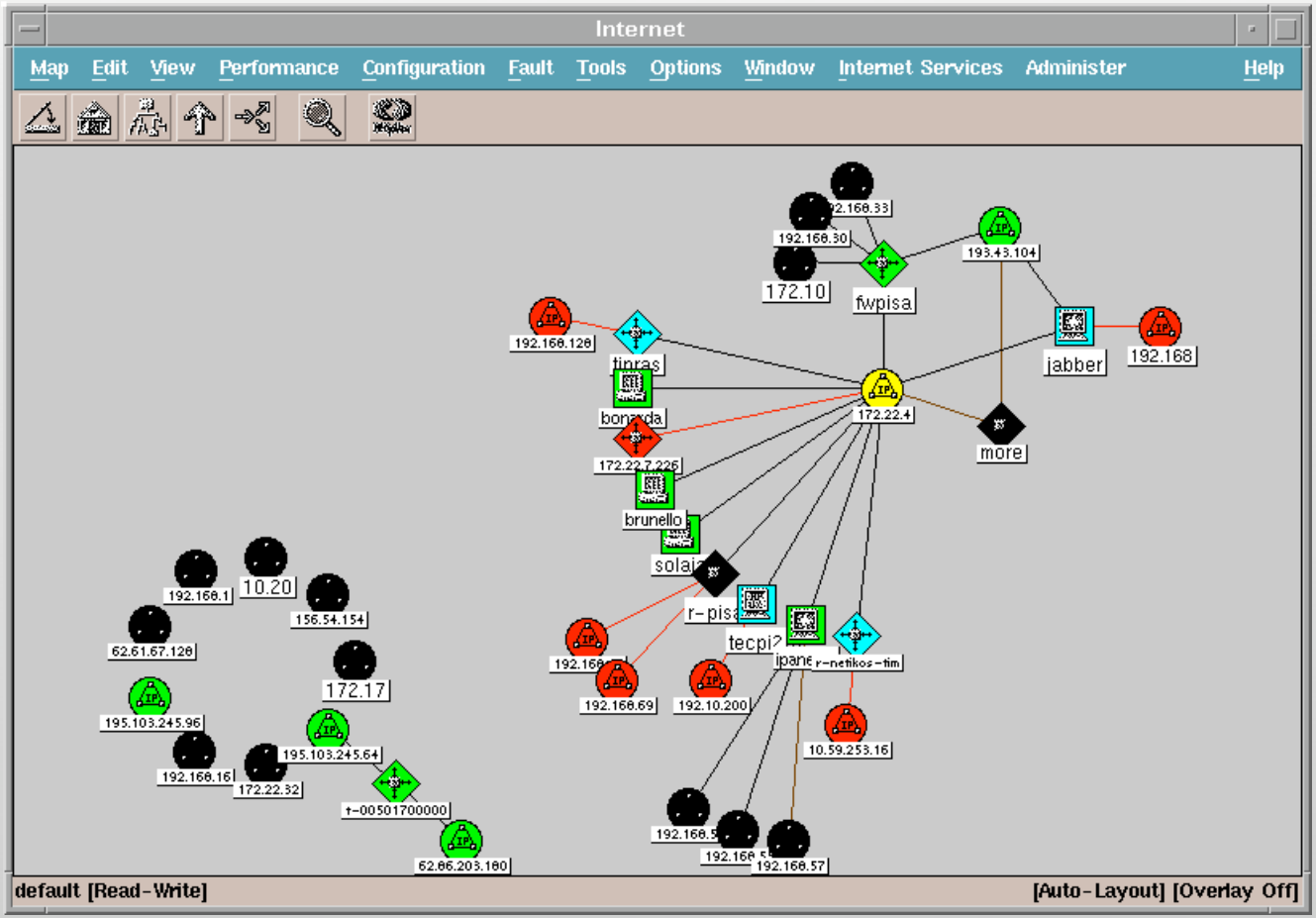
Avvio di NNM

- Startup Interfaccia Grafica: $OV_BIN/ovw
- Avvio/terminazione di NNM:
- $OV_BIN/ovstart
- $OV_BIN/ovstop
- $OV_BIN/ovstatus -c

Una Tipica Mappa di NNM

Menu Bar

Oggetti Conosciuti



netmon: Discovery delle Risorse di Rete

- netmon e' un demone che parte al boot
- Tutti gli oggetti di rete sono scoperti tramite netmon
- Per impostare i parametri di configurazione occorre selezionare Options -> Network Polling Configuration
- netmon periodicamente cerca nuovi nodi effettuando un polling intelligente (auto adjust polling frequency): la frequenza di discovery e' direttamente proporzionale al numero di nuovi nodi scoperti ad ogni scan.

Network Polling Configuration for seabone.netikos.com

Configuration Area: General

General Discovery Options

- [x] Use Discovery Filter Everything
- [ ] Discover Beyond License Limit

- [x] Perform Topology Checks On Connector Devices

Topology Polling Interval 4h

- [x] Perform Configuration Checks

Configuration Polling Interval 1d

OK | Apply | Defaults | Cancel | Help

ntop.org

Network Polling Configuration for seabone.netikos.com

Configuration Area: IP Discovery

Auto Adjust: La velocita' del discovery e' proporzionale al numero di nuove devices scoperte ad ogni scan

☑ Discover New IP Nodes

Discovery Polling Interval

○ Use Auto Adjust Discovery Interval

○ Use Fixed Discovery Interval Of 15m

☐ Discover Level-2 Objects (see the level2conf white paper)

Esempio: unmanaged hubs, AppleTalk devices

OK | Apply | Defaults | Cancel | Help

Network Polling Configuration for seabone.netikos.com

Configuration Area: Status Polling

- [x] Perform Status Polling
  - [x] Delete Nodes If Down For 1w
  - [x] DHCP Polling Options
    - [x] Identify DHCP IP Addresses Using Filter DHCPRange
    - [x] Delete Identified DHCP IP Addresses If Down For 8h

Configure Node Status Polling Intervals...

Specifica un range di indirizzi gestiti dal DHCP

OK | Apply | Defaults | Cancel | Help

Network Polling Configuration for seabone.netikos.com

Configuration Area: Secondary Failures

☑ Secondary Failure Polling Options

Status Polling Reduction Multiplier 2

☐ Identify Important Nodes Using Filter

Failure Status For Important Nodes Down

Failure Status For All Other Nodes Unknown

☑ Suppress Alarms For Secondary Failures

Secondary failure: come reagire quando un nodo aldila' di una device down diventa irraggiungibile

OK Apply Defaults Cancel Help

Il Processo di Discovery

- Al boot, netmon scopre solo i nodi locali (apparenenti alla sottorete)
- Successivamente scopre via SNMP (no SNMP no discovery) i router (devices con 2 o piu' NIC e IP forwarding abilitato) e i segmenti adiacenti. Tali nodi sono impostati ad "unmanaged" (Edit -> Manage Objects)
- $OV_bin/loadhosts permette di caricare nuovi nodi oltre a quelli gia' scoperti.

Configurazione di SNMP (Options -> SNMP Configuration)

SNMP Configuration for sealone

Specific Nodes

Node	Get Community	Set Community	Proxy	Timeout	Retry	Port	Polling
margot	-	-	<none>	-	-	30065	-
qeti	-	-	<none>	60.0	-	2161	-
solaia	-	-	<none>	60.0	-	2161	-
webcc	-	-	<none>	60.0	-	2161	-

IP Address Wildcards

IP Wildcard	Get Community	Set Community	Proxy	Timeout	Retry	Port	Polling

Default

Default	Get Community	Set Community	Proxy	Timeout	Retry	Port	Polling
Global Default	public	-	<none>	0.8	2	-	5m

SNMP Parameters

Use Proxy to Access Target

Proxy

Target

Get Community

Set Community

Timeout

Retry Count

Remote Port

Status Polling

Add

Reset

Replace

Delete

Reorder

OK

Apply

Close

Help

SNMP Filters [1/2]

- NNM permette di selezionare un insieme di risorse di rete che non sono gestibili (es. utenti non appartenenti al local management domain, dialup users, DHCP nodes)
- Il filtro di default e' specificato in $OV_CONF/C/filters
- I filtri sono divisi in tre sezioni: Sets, Filters e FilterExpressions

SNMP Filters [2/2]

```
// Sets are a simple way to list string values to test
// against in a filter.
Sets {
        myServers "Set of Servers" { "sv1", "sv2", "sv3" }
        myGateways "Backbone gateways " { "gw1", "gw2", "gw3" }
}

// Filters and FilterExpressions are used as Topology, Discovery,
// Map or Persistence filters.
Filters {
        Networks "Any network" { isNetwork }
        EngrLan "The 15.2.112 subnet used by engineering"
                { ("IP Address" ~ 15.2.112-119.* ) || isSegment }
        Routers "Any Router" { isRouter }
        IPRouters "Any IP Router" { isIPRouter }
        Bridges "Any bridge" { isBridge }
        SNMPNode "Any node supporting SNMP" { isNode && isSNMPSupported }
}

// FilterExpressions are simply combinations of filters defined in the
// same filter file
FiltersExpressions  {
    NetInfrastructure "Any network connecting device and what they connect"
                { Routers || Bridges || Hubs || myServers }
        NetBackbone "Networks and gateways/routers"
                { Routers || Networks }
}
```

Accesso a Variabili di SNMP

- **Command Line:**

  ```
  $OV_BIN/snmpget -c mypc 1.3.6.1.2.1.1.4.9
  system.sysContact.0 : DISPLAY STRING- (ascii): Luca's PC
  ```

-
- **Grafico con xnmbrowser:**

  Misc -> SNMP MIB Browser

  ```
  $OV_BIN/xnmbrowser
  ```

-

Browse MIB

File View Help

Name or IP Address: jabber

Community Name:

MIB Object ID: .iso.org.dod.internet.mgmt.mib-2

- system
- interfaces
- at
- ip
- icmp
- tcp
- udp
- egp
- transmission

Up Tree | Down Tree | Describe | Start Query | Stop Query | Graph

MIB Instance | SNMP Set Value | Set

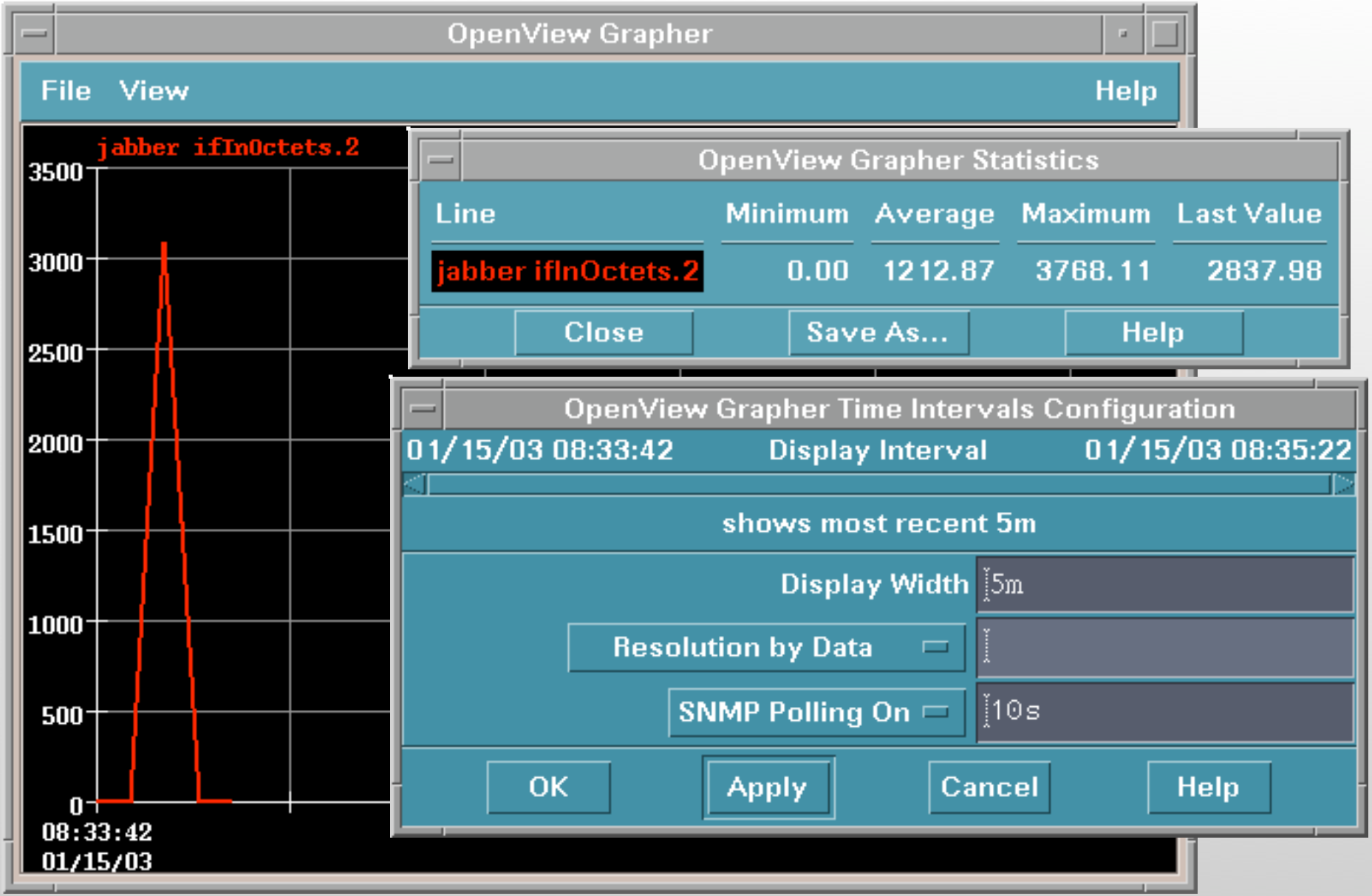
MIB Values

```
sysDescr.0 : Sun SNMP Agent,
sysObjectID.0 : .iso.org.dod.internet.private.enterprises.42.2.1.1
sysUpTime.0 : (983866822) 113 days, 20:57:48.22
sysContact.0 : System administrator
sysName.0 : jabber
sysLocation.0 : System administrators office
sysServices.0 : 76
```

ntop.org

Data Display: xnmbrowser e xnmgraph

- xnmgraph si puo' attivare in due modi:
- Tramite linea di comando digitando $OV_BIN/ xnmgraph
- Selezionando Graph da xnmbrowser


OpenView Grapher
File
View
Help
jabber ifInOctets.2
3500
3000
2500
2000
1500
1000
500
0
08:33:42
01/15/03
OpenView Grapher Statistics
Line
Minimum
Average
Maximum
Last Value
jabber ifInOctets.2
0.00
1212.87
3768.11
2837.98
Close
Save As...
Help
OpenView Grapher Time Intervals Configuration
01/15/03 08:33:42
Display Interval
01/15/03 08:35:22
shows most recent 5m
Display Width
5m
Resolution by Data
SNMP Polling On
10s
OK
Apply
Cancel
Help

Esempio di utilizzo di xnmgraph

```
> cat graphOctets
#!/bin/sh
# filename: /opt/OV/local/scripts/graphOctets
# syntax: graphOctets <hostname>
/opt/OV/bin/xnmgraph -c public -mib \
".iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInOctets::::::::,\
.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutOctets::::::::" \
$1

>./graphOctets myRouter.mycompany.com
```

Sintassi:
object:label:match:expression:instance-label:truncator:multiplier:nodes

Data Collection

-
- Per collezionare dati in maniera continua occorre fare polling periodico.
- In base ai valori collezionati e' anche possibile associare allarmi o emettere eventi (es. trap SNMP)
- Il collezionamento automatico dei dati e' importante per rilevare malfunzionamenti anche in mancanza di un operatore umano.

Data Collection: xnmcollect

Data Collection & Thresholds: SNMP for seabone

File Edit Actions Help

MIB Objects Configured For Collection

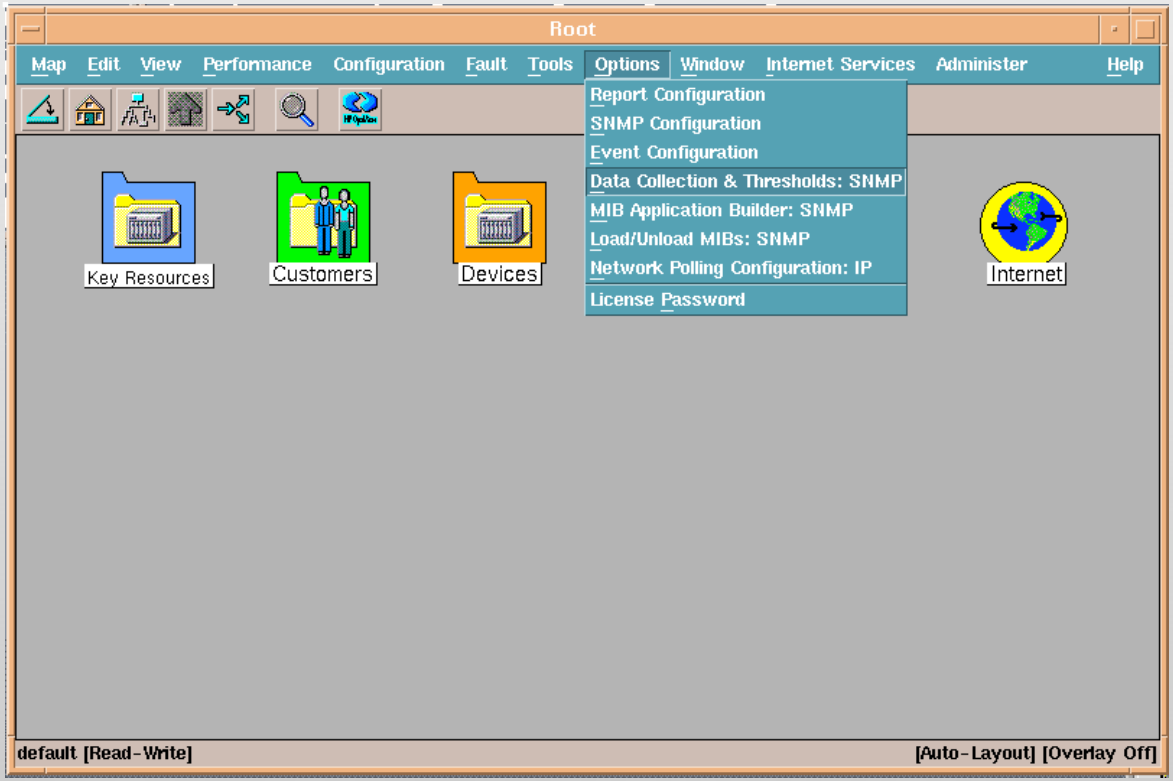
Origin	Status	Label	MIB Object ID
DataCollect	Suspended	ifInOctets	.1.3.6.1.2.1.2.2.1.10
DataCollect	Suspended	ifOutOctets	.1.3.6.1.2.1.2.2.1.16
DataCollect	Suspended	ifInErrors	.1.3.6.1.2.1.2.2.1.14
DataCollect	Suspended	ifOutErrors	.1.3.6.1.2.1.2.2.1.20
DataCollect	Collecting	ISNinLoadAvg	.1.3.6.1.4.1.11.2.3.1.1.5
DataCollect	Collecting	snmpInPkts	.1.3.6.1.2.1.11.1
DataCollect	Suspended	If%util	If%util
DataCollect	Suspended	Disk%util	Disk%util

MIB Object Collection Summary

Interval	Store	Threshold	Instances	Source
1h	Yes	>10.00 <=5.00%	ALL	0.0.0.0

Data Collection: xnmcollect [1/3]

- Per aggiungere un nuovo collezionamento: Options -> “Data Collection & Thresholds: SNMP” -> Edit -> Add MIB Object



Data Collection: xnmcollect [2/3]

Add udpInErrors Collection for seabone.netikos.com

Set Collection Mode: Don't Store, Check Thresholds

List Of Collection Sources

Add From Map

Delete

Delete All

Source

Add

Instances: All

Only Collect On Sources With sysObjectIDs:

Create Event When SNMP Request Fails: 58720266

Polling Interval 1h

Threshold > 0 For 1 Consecutive Samples

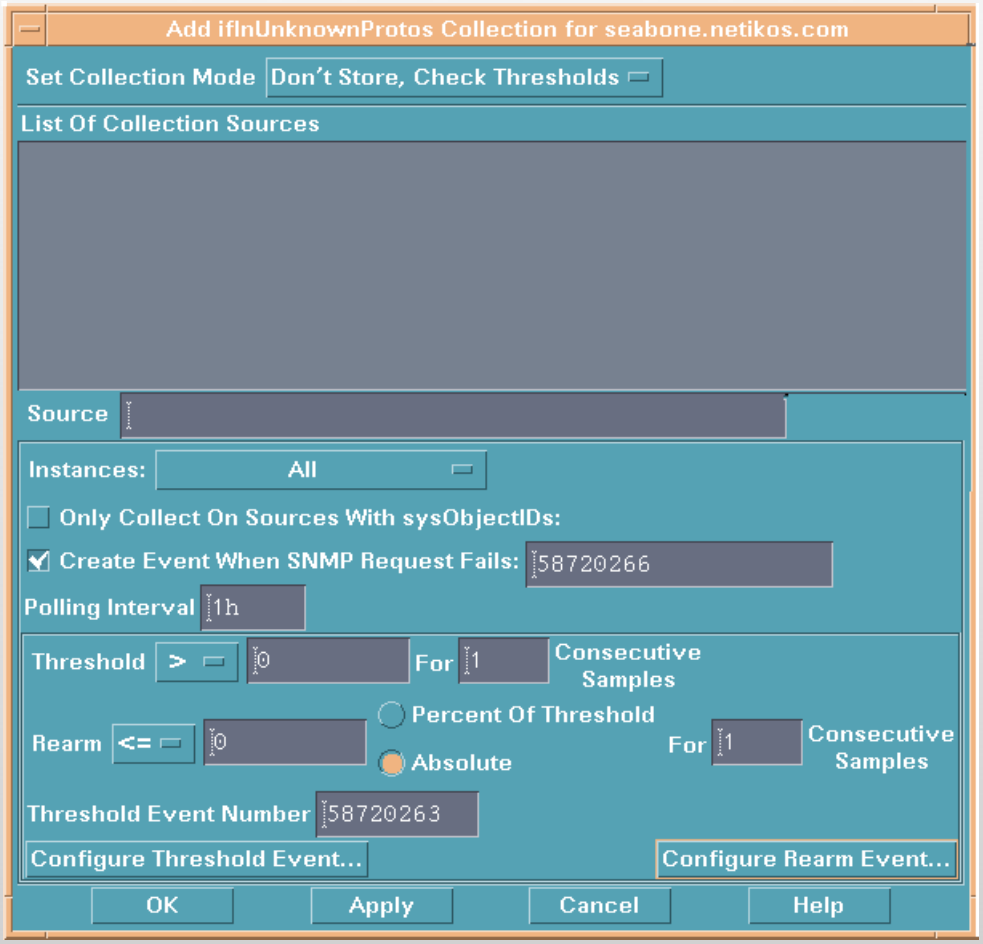
Rearm <= 0 Percent Of Threshold / Absolute For 1 Consecutive Samples

Threshold Event Number 58720263

Configure Threshold Event... Configure Rearm Event...

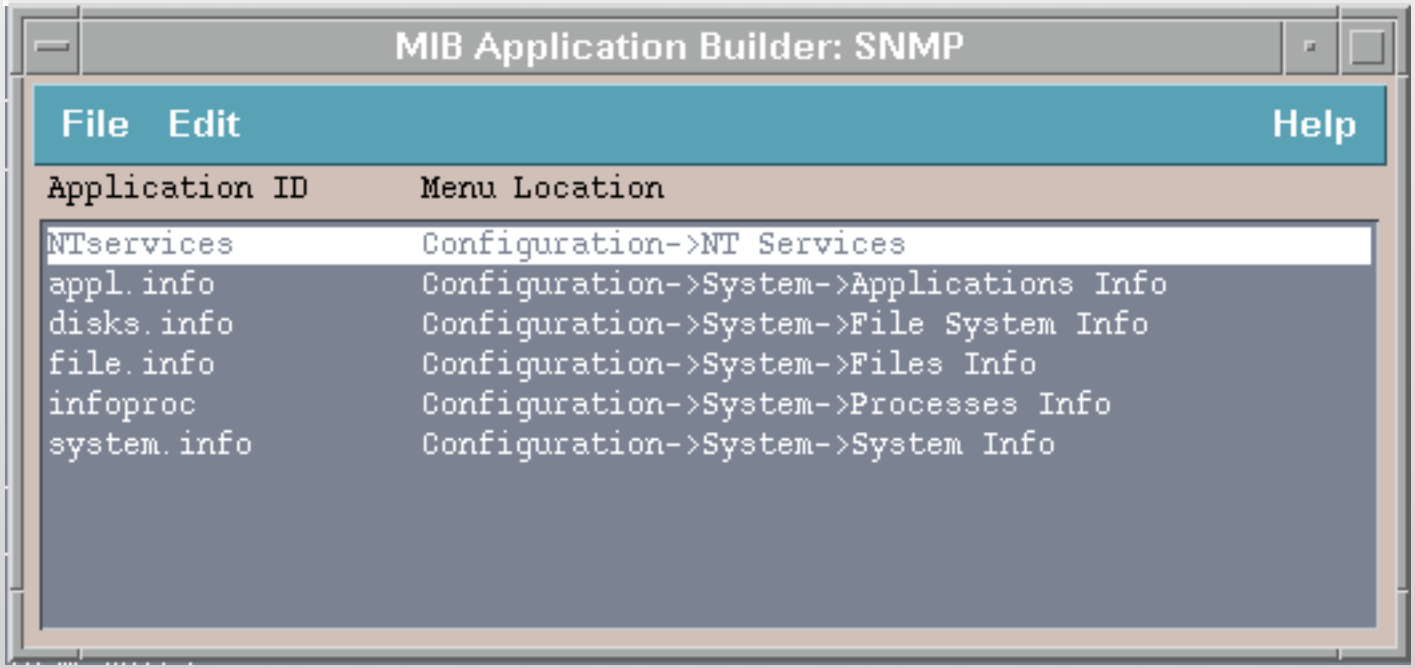
OK Apply Cancel Help

Data Collection: xnmcollect [3/3]

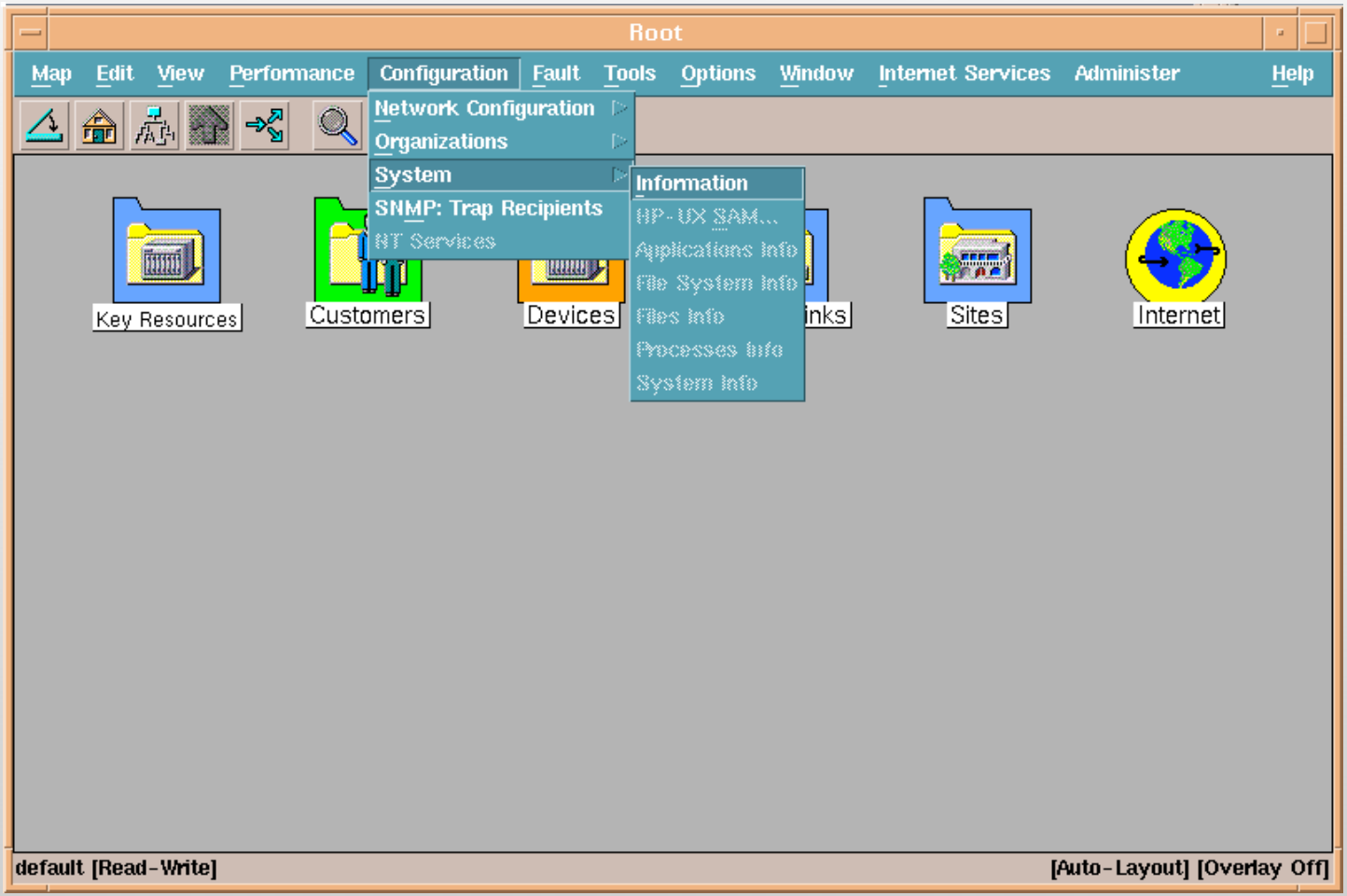


Modifica ed Estensione di NNM [1/3]

- **Options -> MIB Application Builder SNMP**



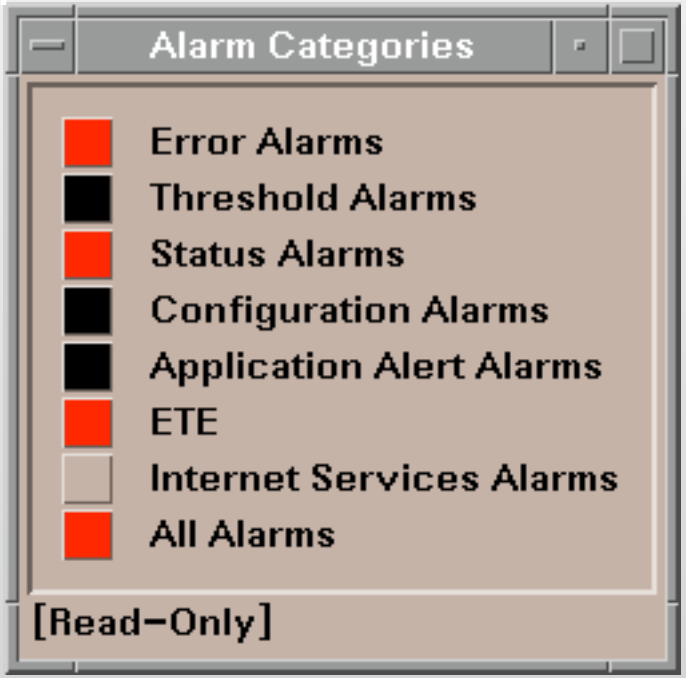
Modifica ed Estensione di NNM [2/3]



Modifica ed Estensione di NNM [3/3]

ntop.org

Visualizzazione Eventi [1/2]



Visualizzazione Eventi: Alarm Browser [2/2]

Status Alarms Browser

File Actions View Help

Ack	Cor	Severity	Date/Time	Source	Message
	*	Warning	Mon Dec 23 14:43:51	172.22.7.233	Node down
	*	Warning	Mon Dec 23 14:55:44	172.22.7.224	Node down
		[redacted]	**Mon Dec 23 14:56:54**	**172.22.4.Segment374**	**Segment critical**
		Warning	Mon Dec 23 15:18:19	stefaniagamba.netikos.com	Node status - warning
	*	Warning	Mon Dec 23 15:36:09	172.22.7.224	Node down
	*	Warning	Mon Dec 23 15:39:22	172.22.7.233	Node down
	*	Warning	Mon Dec 23 16:15:42	172.22.7.238	Node down
	*	Warning	Mon Dec 23 16:35:11	172.22.7.229	Node down
		[redacted]	**Mon Dec 23 16:55:41**	**172.22.4.Segment348**	**Segment critical**
	*	Warning	Mon Dec 23 17:16:39	172.22.7.224	Node down
		[redacted]	**Mon Dec 23 18:03:37**	**172.22.4.Segment326**	**Segment critical**
		Warning	Mon Dec 23 18:08:26	stefaniagamba.netikos.com	Node down
		[redacted]	**Mon Dec 23 18:10:44**	**172.22.4.Segment345**	**Segment critical**
		Warning	Mon Dec 23 18:15:45	chesi.netikos.com	Node down
		[redacted]	**Mon Dec 23 18:16:39**	**172.22.4.Segment361**	**Segment critical**
	*	Warning	Mon Dec 23 20:28:13	172.22.7.224	Node down
	*	Warning	Mon Dec 23 21:43:47	172.22.7.224	Node down
	*	Warning	Mon Dec 23 23:44:09	172.22.7.244	Node down

1464 Alarms - Critical:41 Major:560 Minor:42 Warning:518 Normal:303 (92 acknowledged

Configurazione di Nuovi Eventi

- Definisce come reagire in particolari situazioni
- La gestione di queste situazioni viene fatta da xnmtrap
- xnmtrap vieve avviato da linea di comanddo o da menu (Options -> Event Configurations)

Event Configuration for seabone

File Edit View Help

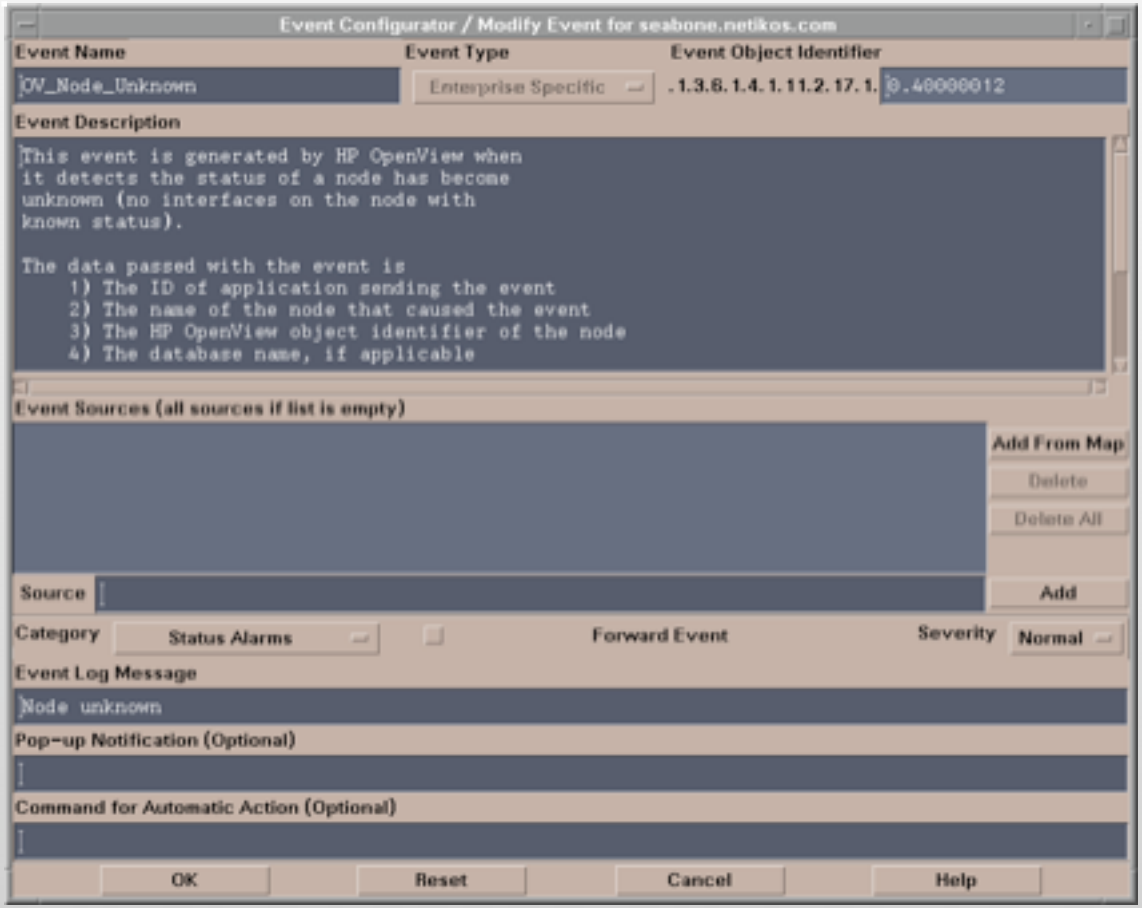
Enterprise Identification

Enterprise Name	Enterprise ID
rmon	.1.3.6.1.2.1.16
rdbmsMIB	.1.3.6.1.2.1.39
ENTERPRISES	.1.3.6.1.4.1
OpenView	.1.3.6.1.4.1.11.2.17.1
svrMgt	.1.3.6.1.4.1.36.2.18.22.2
svrClu	.1.3.6.1.4.1.36.2.18.22.4.1
oraListenerTraps	.1.3.6.1.4.1.111.5.2
oraAgentTraps	.1.3.6.1.4.1.111.12.2
dmiIndications	.1.3.6.1.4.1.412.1.2

Event Identification

Event Name	Event Identif
OV_Default	.1.3.6.1.4
OV_IF_Marginal	.1.3.6.1.4
OV_IF_IP_Addr_Chg	.1.3.6.1.4
OV_Network_SubMskChg	.1.3.6.1.4
OV_Connection_Up	.1.3.6.1.4
OV_Connection_Down	.1.3.6.1.4
OV_Connection_Marg	.1.3.6.1.4
OV_DataCollect_Check	.1.3.6.1.4
OV_IF_Disconnected_Segs	.1.3.6.1.4
OV_Map_Change	.1.3.6.1.4
OV_Network_IPAddrChg	.1.3.6.1.4
OV_Network_Name_Chg	.1.3.6.1.4
OV_IF_Unknown	.1.3.6.1.4
OV_Node_Unknown	.1.3.6.1.4
OV_Segment_Unknown	.1.3.6.1.4
OV_Network_Unknown	.1.3.6.1.4

Configurazione Eventi



Menu Options -> Event Configurator

Configurazione Eventi

- Il file di configurazione per le trap utilizzato anche dall'Event Configurator e' $OV_CONF/C/trapd.conf
- Il file definisce l'azione da eseguire a fronte della ricezione di una trap da parte di NNM
- Possibili azioni sono esecuzione di comandi (es. shell script), invio di altre trap, invio di eventi (es. colorazione di oggetti sulla mappa) di HP-OV

Sintassi di trapd.conf

- $1..$n Parametri 1..n della trap
- $A Host che ha inviato la trap
- $S Codice della trap (trapId)

```
EVENT SL_USR_NUM .1.3.6.1.4.1.512.0.113 "Status Alarms" Normal
FORMAT Trap N.$S ------- Informaz.di sistema--> Il numero di utenti connessi ($1) sul sistema $A e' sotto la soglia configurata.
EXEC /etc/opt/OV/share/conf/C/armtrap $A $S
SDESC
Solo per Unix
EDESC
```

Eventi HP-OV: Colorazione Oggetti Mappe

```
OVEVENT="/opt/OV/bin/ovevent"
TRCOLOR=".1.3.6.1.4.1.11.2.17.1.0.58916871 .1.3.6.1.4.1.11.2.17.2.1.0 Integer 14 .1.3.6.1.4.1.11.2.17.2.2.0 OctetString"
TRERROR=".1.3.6.1.4.1.11.2.17.1.0.58851329 .1.3.6.1.4.1.11.2.17.2.1.0 Integer 14 .1.3.6.1.4.1.11.2.17.2.2.0 OctetString"
TRNORMAL=".1.3.6.1.4.1.11.2.17.1.0.58916872 .1.3.6.1.4.1.11.2.17.2.1.0 Integer 14 .1.3.6.1.4.1.11.2.17.2.2.0 OctetString"
OCTSTR=".1.3.6.1.4.1.11.2.17.2.4.0 OctetString"


$OVEVENT -s Normal "" $TRCOLOR $HOST $OCTSTR " "
$OVEVENT -s Critical "" $TRCOLOR $HOST $OCTSTR " "
$OVEVENT -s Minor "" $TRCOLOR $HOST $OCTSTR " "
```