8/26/2007

Network Monitor Analysis

Preformed for Home National Bank

Paul F Bergetz

Network Monitor Analysis

Preformed for Home National Bank

Scope of Project: Determine proper Network Monitor System (NMS) for a 25+ branch bank located across several States connected by Cisco routing equipment.

Product Selection: Initial search for products begin in trade journals like "The Processor" and Google. I eliminated all but two vendors. I have been using NMS products since 1996 and have a good background on features required to make a good product. Most off the products that were eliminated had one or all of the following faults.

1-Freeware or Open Source : These are a poor choice for most clients because of security and lack of consistent product or support. Example - www.nagios.org we use this on our Linux mail/web servers

2-Feature set to marginal: Designed for a small network or only one polling frequency. Example – www.NumaraSoftware.com NMS from Numara. I have used the original version of this product since 1997 and still use it today. It has changed owners four times in six years (not a good sign).

3-Poor initial contact response: The sales person had little or no interest in helping me. Several firms had no interest in pre-sales questions and told me to use the website.

4-Price: HP Openview this is a very flexible system however, the price starts at $ 100K plus a full time operator.

Many of the products are management tools not just monitors. I eliminated these because of the additional complexity and the fact that any network manager will have access to a web browser , telnet and various remote clients needed for their operation. All agent based systems were also eliminated because of reliability concerns.

My choice for the review was one software based tool and one hardware. Solarwinds was chosen because of their longevity in the market and the fact that they are the primary competition for Netmon as well as my experience with their network diagnostic tools.

Software Based Network Monitor: Solarwinds Orion is a windows server based solution with numerous options allowing complete configuration to suite any SMB. Cost as configured $ 13975 without hardware software support and updates included for 1 year.

Hardware based Network Monitor: Netmon Enterprise Edition is Linux based system on a dual cpu raid hardware solution. It has no options and is designed for any SMB. Cost as configured $ 21995 including hardware, software, support and updates for 1 year.

Note: Both of these products have deployments in financial institutions. (names available on request)

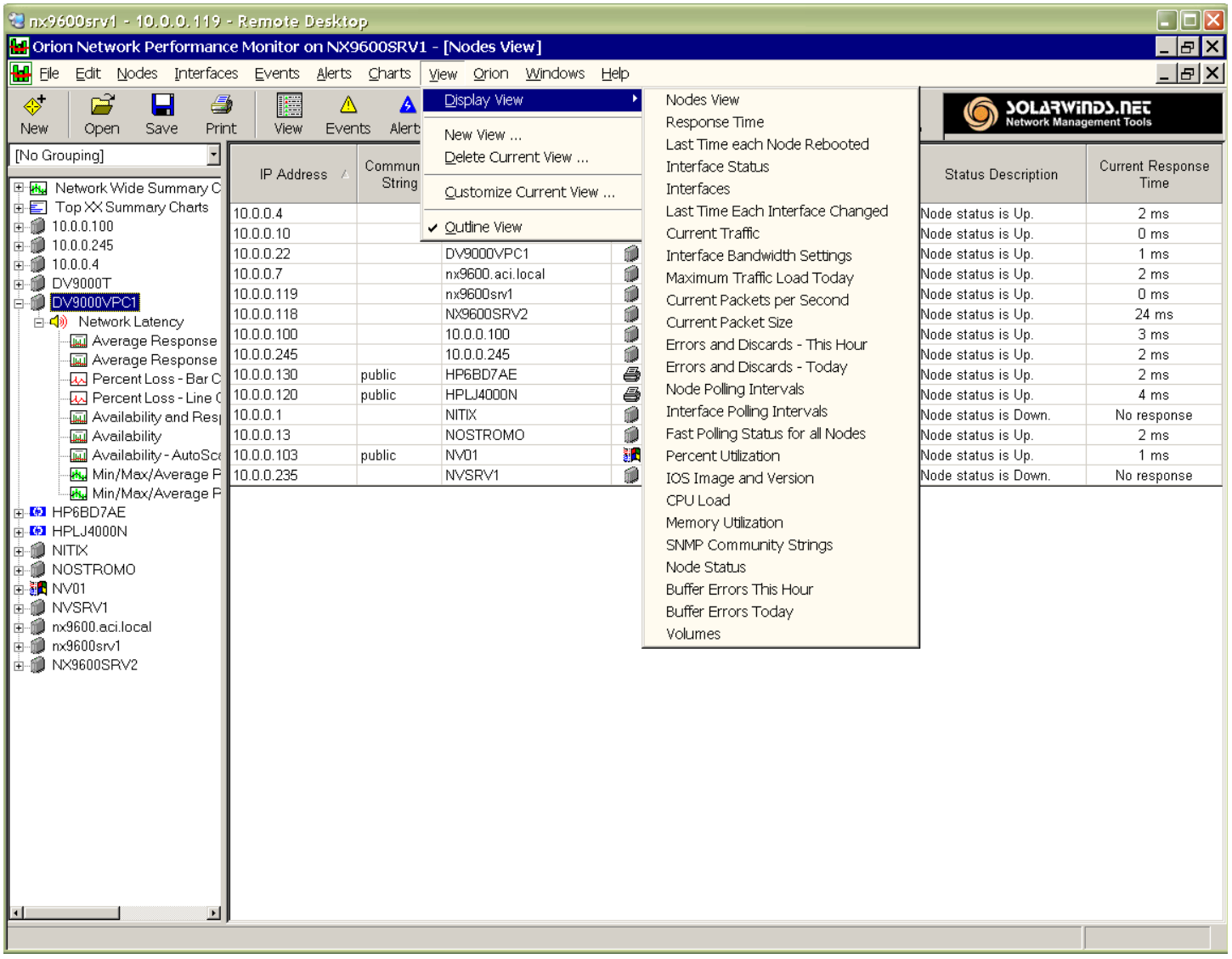
Test Configurations: Each product was setup in a virtual machine on a separate hardware server. The Solarwinds Orion product was setup on a virtual image of Windows 2003 on a host server running Windows 2003 R2 with the latest virtual server. The Netmon product was setup on Vmware Virtual Server 1.03 in a host server running Windows 2003 R2 server. The Netmon Linux image was run on the Virtual Server 1.03. No other applications were running on the host servers. SQL access for the Orion product was from a third real server on the test network. The test network was composed of several managed switches, 10 physical hardware servers / workstations and 6 virtual systems as well as wireless components all routed to internet via Comcast cable.

Installation: The Solarwind Orion product did not install properly because problems with the Microsoft SNMP service. This was isolated to problem with the fact that the original CD did not copy correctly to the network distribution point. Once this was corrected the install went as it was supposed to. The support at Solarwinds was not helpful in resolving the SNMP issue I was left for week without help however, I was able to correct during that time (Solarwinds support did call to see if I had their product installed)

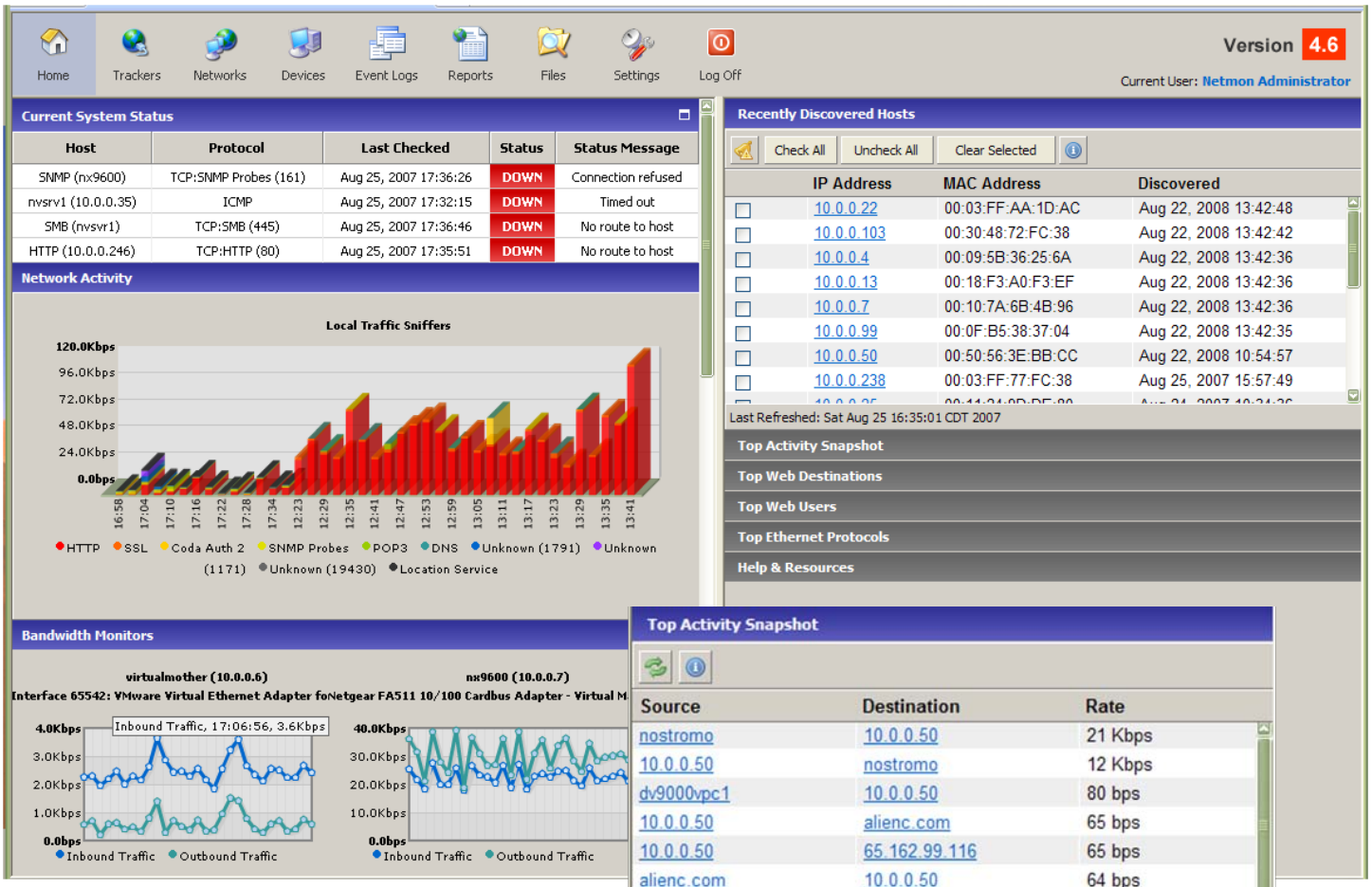
Netmon was simple to install. I installed the Vmware host server and then pointed the Vmware console to the Netmon image and the rest was automatic. The whole process took less than an hour. I immediately had help as needed from their staff.

Test categories: Included Interface, Discovery/SNMP, Alerts, Web and Reporting. The side by side tests took place over a 25 day 24x7 period. They are detailed in the following pages.

Interface: Both products use entirely different interface schemes. Orion is locked into the Windows API which as good an idea it is it begins creating problems as programs become more complicated and additions are made over time. Below is a screen of the Orion manager with “Nodes View” display. The only active information that can be accessed is on the left hand pane.

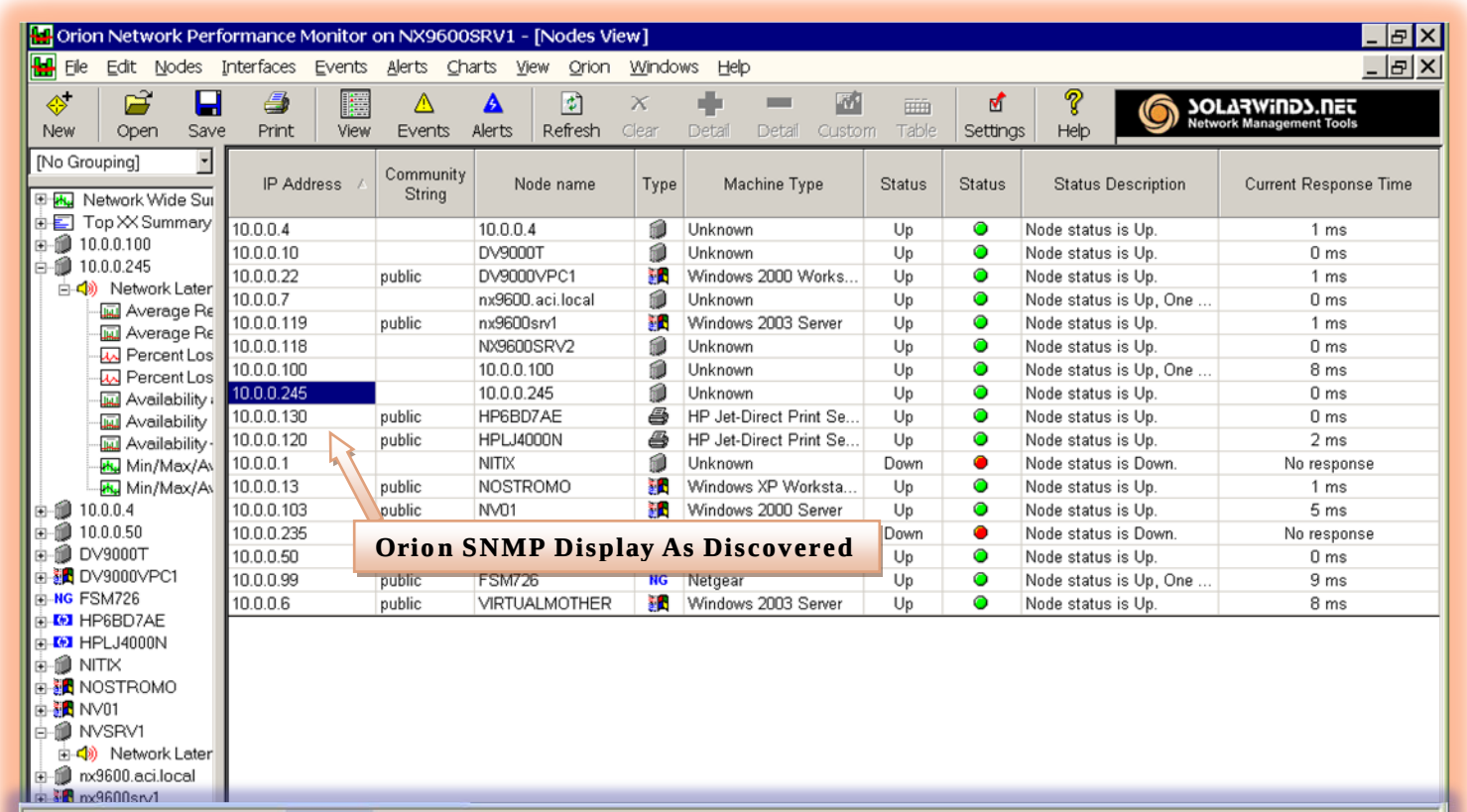


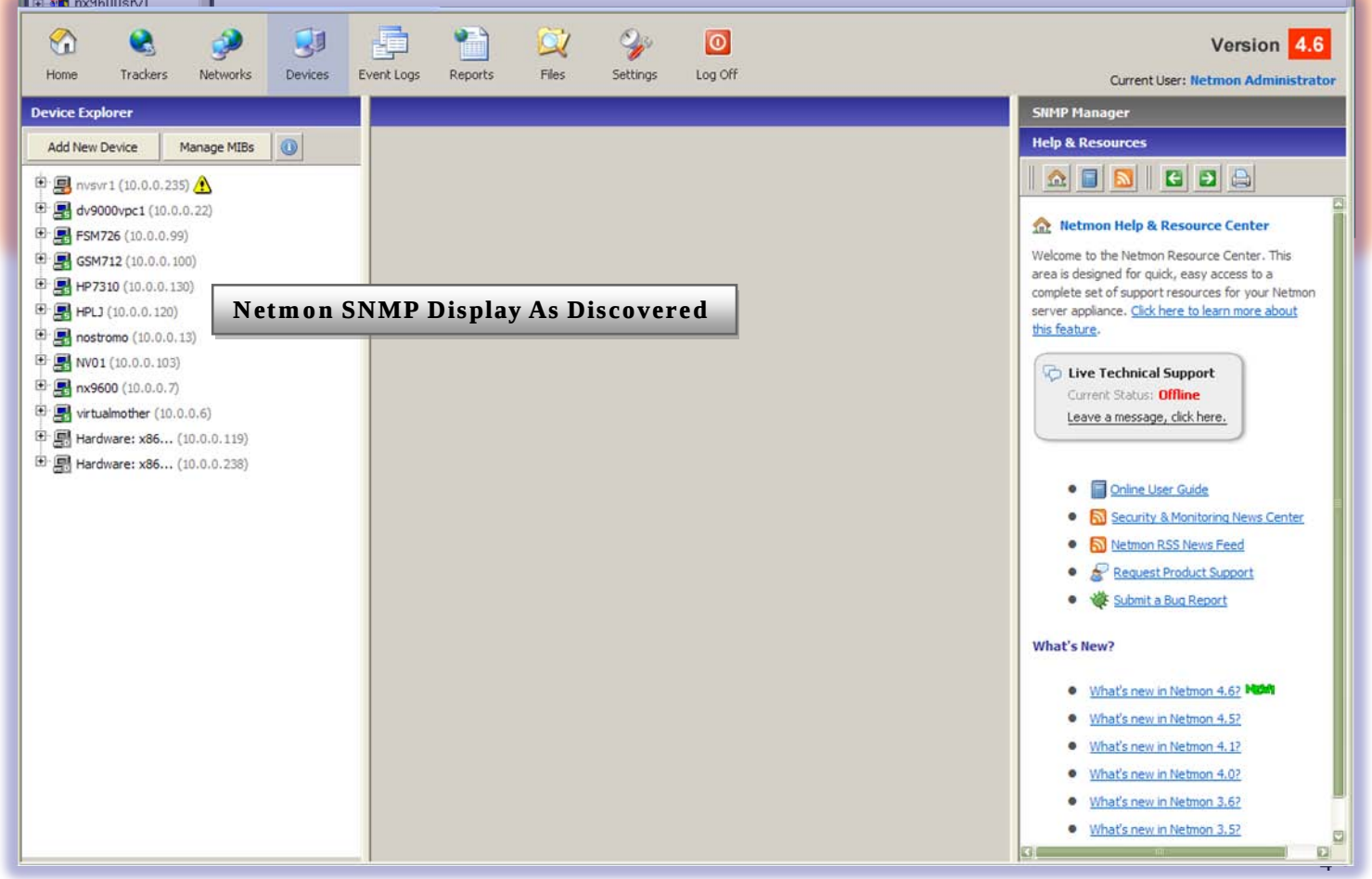
Interface (cont): Netmon has the advantage of being designed from the ground up for a specific task. The challenge with this type of freedom is to make what is presented intuative. Below is the home page from the Netmon server. They present all information that is of most importance at this level. The information that is found in the icon bar at the screen top takes the operator to a page that is used to setup what is displayed on the home screen (except for event logs, reports and files) .

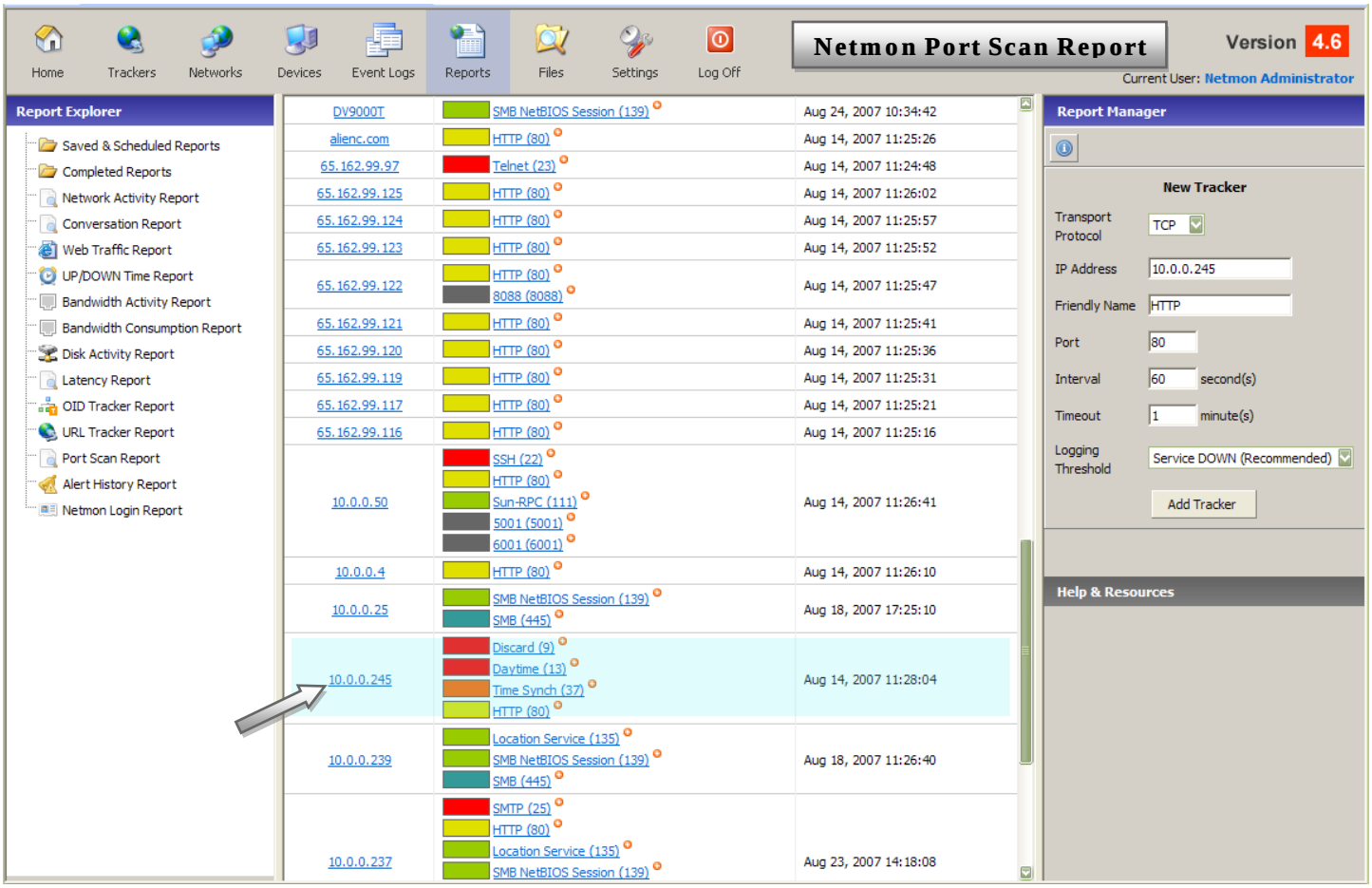


In this chart (inset) we can see a quick snapshot of what is going on at a moment in time with the Top Activity Snapshot.

Discovery/SNMP: Both Orion and Netmon can auto discover items on the network however, the information that is brought back is quite different. Orion brings back both SNMP and non SNMP information and displays it in the main screen on the left hand pane as in the following screen . Non SNMP information like a ping response has very limited usefulness unless it has more relevant data to help the manager diagnose what is going on (ref 10.0.0.245 below). The Netmon display only shows SNMP data so 10.0.0.245 is not there however, If you look at the Port Scan Report on page 5 10.0.0.245 shows up and contains a lot more information than the ping logged with Orion. This is one of the most powerful features of Netmon. Automatic port scans are run on a 2 hour interval on every network as soon as the networks are defined. This data is used with the SNMP data to create in depth history of each address on the network.


Orion Network Performance Monitor on NX9600SRV1 - [Nodes View]
File Edit Nodes Interfaces Events Alerts Charts View Orion Windows Help
New Open Save Print View Events Alerts Refresh Clear Detail Detail Custom Table Settings Help
SOLARWINDS.NET Network Management Tools
[No Grouping]
IP Address | Community String | Node name | Type | Machine Type | Status | Status | Status Description | Current Response Time
10.0.0.4 | | 10.0.0.4 | Unknown | Up | Node status is Up. | 1 ms
10.0.0.10 | | DV9000T | Unknown | Up | Node status is Up. | 0 ms
10.0.0.22 | public | DV9000VPC1 | Windows 2000 Works... | Up | Node status is Up. | 1 ms
10.0.0.7 | | nx9600.aci.local | Unknown | Up | Node status is Up, One ... | 0 ms
10.0.0.119 | public | nx9600srv1 | Windows 2003 Server | Up | Node status is Up. | 1 ms
10.0.0.118 | | NX9600SRV2 | Unknown | Up | Node status is Up. | 0 ms
10.0.0.100 | | 10.0.0.100 | Unknown | Up | Node status is Up, One ... | 8 ms
10.0.0.245 | | 10.0.0.245 | Unknown | Up | Node status is Up. | 0 ms
10.0.0.130 | public | HP6BD7AE | HP Jet-Direct Print Se... | Up | Node status is Up. | 0 ms
10.0.0.120 | public | HPLJ4000N | HP Jet-Direct Print Se... | Up | Node status is Up. | 2 ms
10.0.0.1 | | NITIX | Unknown | Down | Node status is Down. | No response
10.0.0.13 | public | NOSTROMO | Windows XP Worksta... | Up | Node status is Up. | 1 ms
10.0.0.103 | public | NV01 | Windows 2000 Server | Up | Node status is Up. | 5 ms
10.0.0.235 | | | | Down | Node status is Down. | No response
10.0.0.50 | | | | Up | Node status is Up. | 0 ms
10.0.0.99 | public | FSM726 | Netgear | Up | Node status is Up, One ... | 9 ms
10.0.0.6 | public | VIRTUALMOTHER | Windows 2003 Server | Up | Node status is Up. | 8 ms
Orion SNMP Display As Discovered

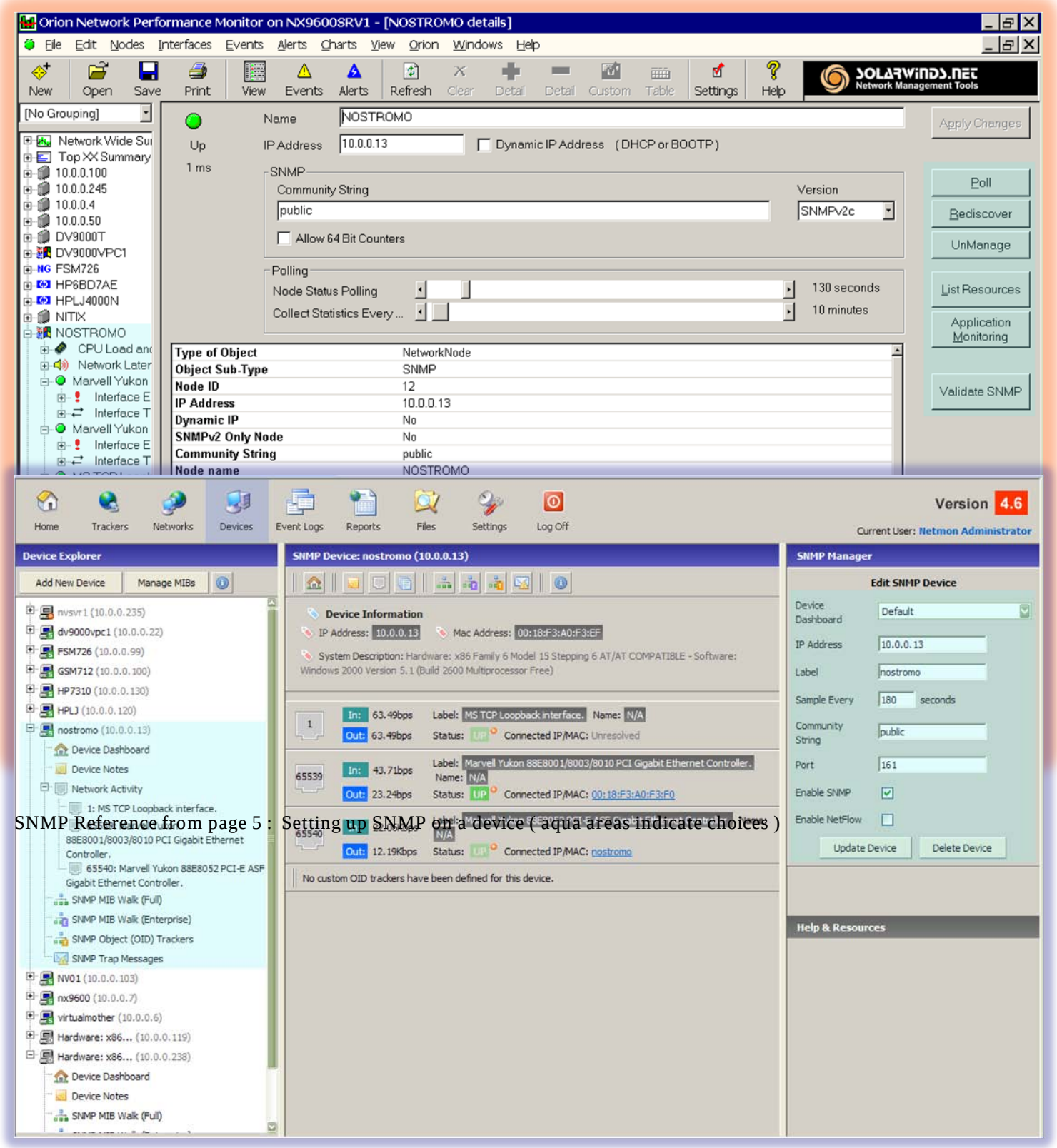

Home Trackers Networks Devices Event Logs Reports Files Settings Log Off
Version 4.6
Current User: Netmon Administrator
Device Explorer
Add New Device Manage MIBs
nvsvr1 (10.0.0.235)
dv9000vpc1 (10.0.0.22)
FSM726 (10.0.0.99)
GSM712 (10.0.0.100)
HP7310 (10.0.0.130)
HPLJ (10.0.0.120)
nostromo (10.0.0.13)
NV01 (10.0.0.103)
nx9600 (10.0.0.7)
virtualmother (10.0.0.6)
Hardware: x86... (10.0.0.119)
Hardware: x86... (10.0.0.238)
Netmon SNMP Display As Discovered
SNMP Manager
Help & Resources
Netmon Help & Resource Center
Welcome to the Netmon Resource Center. This area is designed for quick, easy access to a complete set of support resources for your Netmon server appliance. Click here to learn more about this feature.
Live Technical Support
Current Status: Offline
Leave a message, click here.
Online User Guide
Security & Monitoring News Center
Netmon RSS News Feed
Request Product Support
Submit a Bug Report
What's New?
What's new in Netmon 4.6?
What's new in Netmon 4.5?
What's new in Netmon 4.1?
What's new in Netmon 4.0?
What's new in Netmon 3.6?
What's new in Netmon 3.5?



Discovery/SNMP (cont): Since SNMP is the only way to collect information on these systems. It is imperative that SNMP Community names, trap information and all security related SNMP information be properly setup on all devices on any network that will be monitored. This can take more time than any of the other settings on either Orion or Netmon. The next series of screens take you through what is required to get SNMP interface information displayed on both systems and setup a network interface.

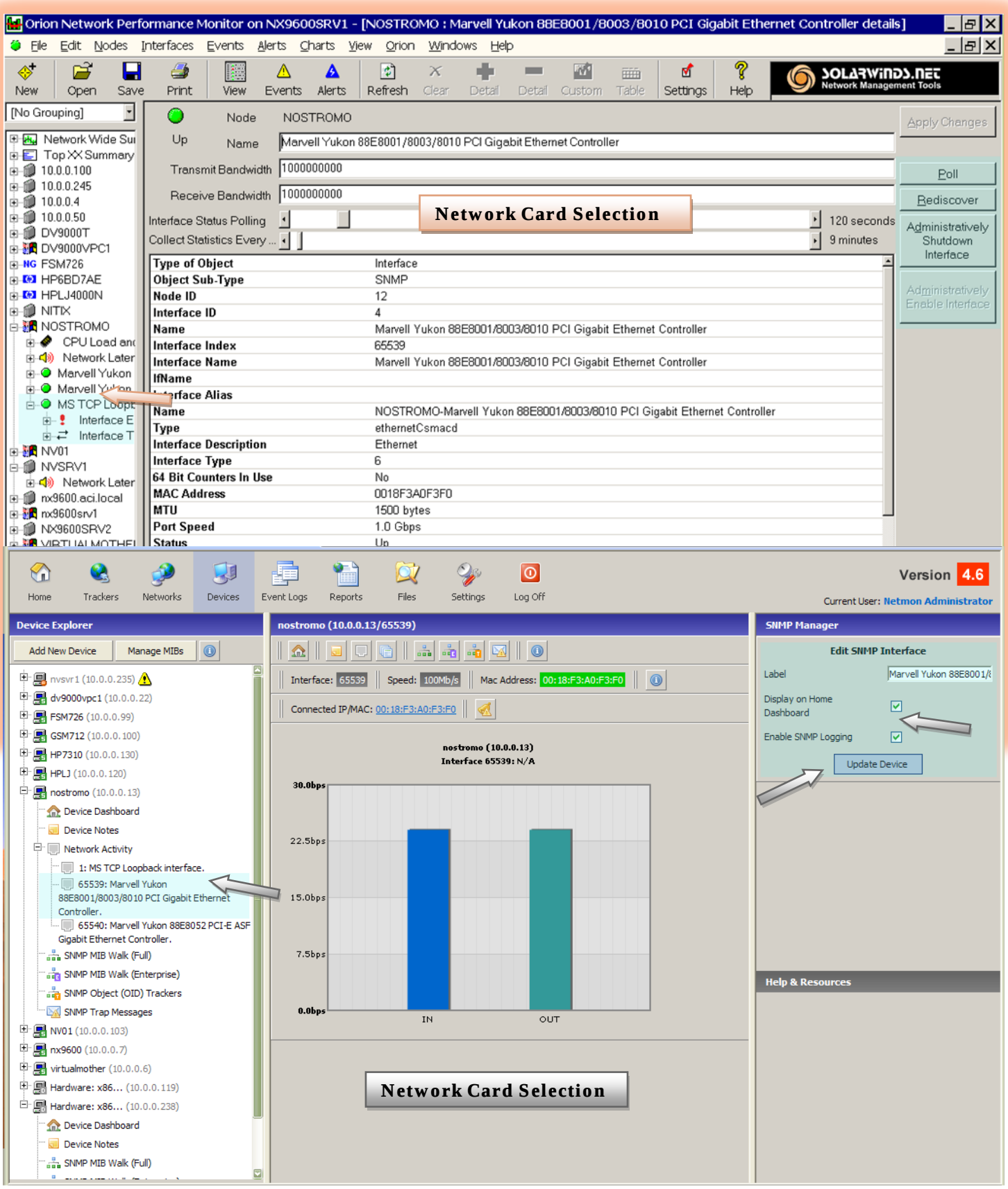
Orion uses a drill down display in the right center area which has several active controls as you go deeper (see pages 6-8). You have to select the information wanted on the right which may cause confusion if you are already viewing other data on the same SNMP device. You need to go back to the right to tune your selection. This type of arrangement gives the user limitless choices at the cost of a more complex interface.

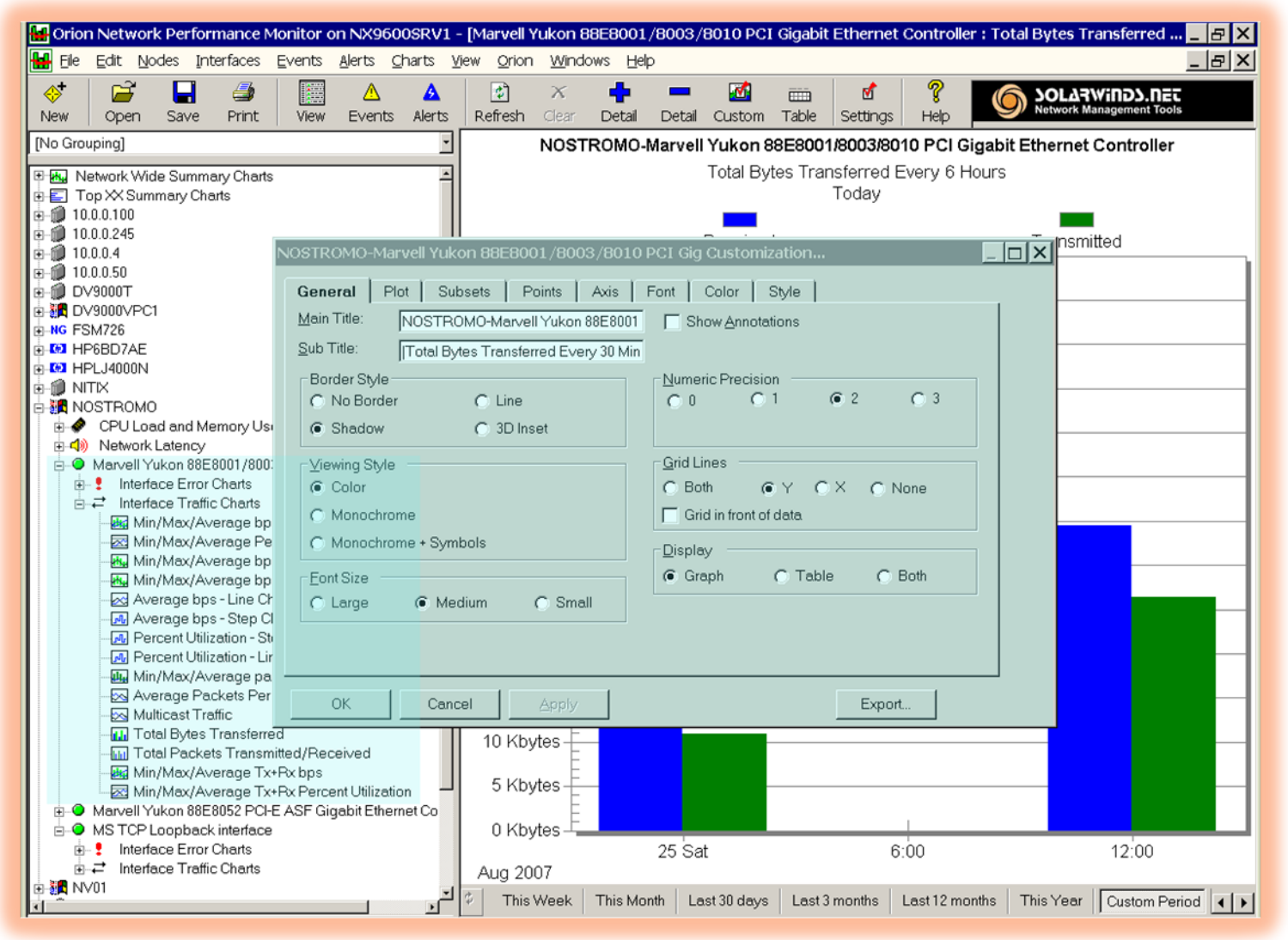
Netmon keeps everything in one view for simplicity you are never required to move back and forth between screens. A selection on the left gives you choices in the center which again when selected give you choices on the right. This type of interface provides faster setup at the cost of extra features. (see pages 6-8)



SNMP Reference from page 5 : Setting up SNMP on a device (aqua areas indicate choices)

SNMP Reference from page 5: Selection of an interface for monitoring





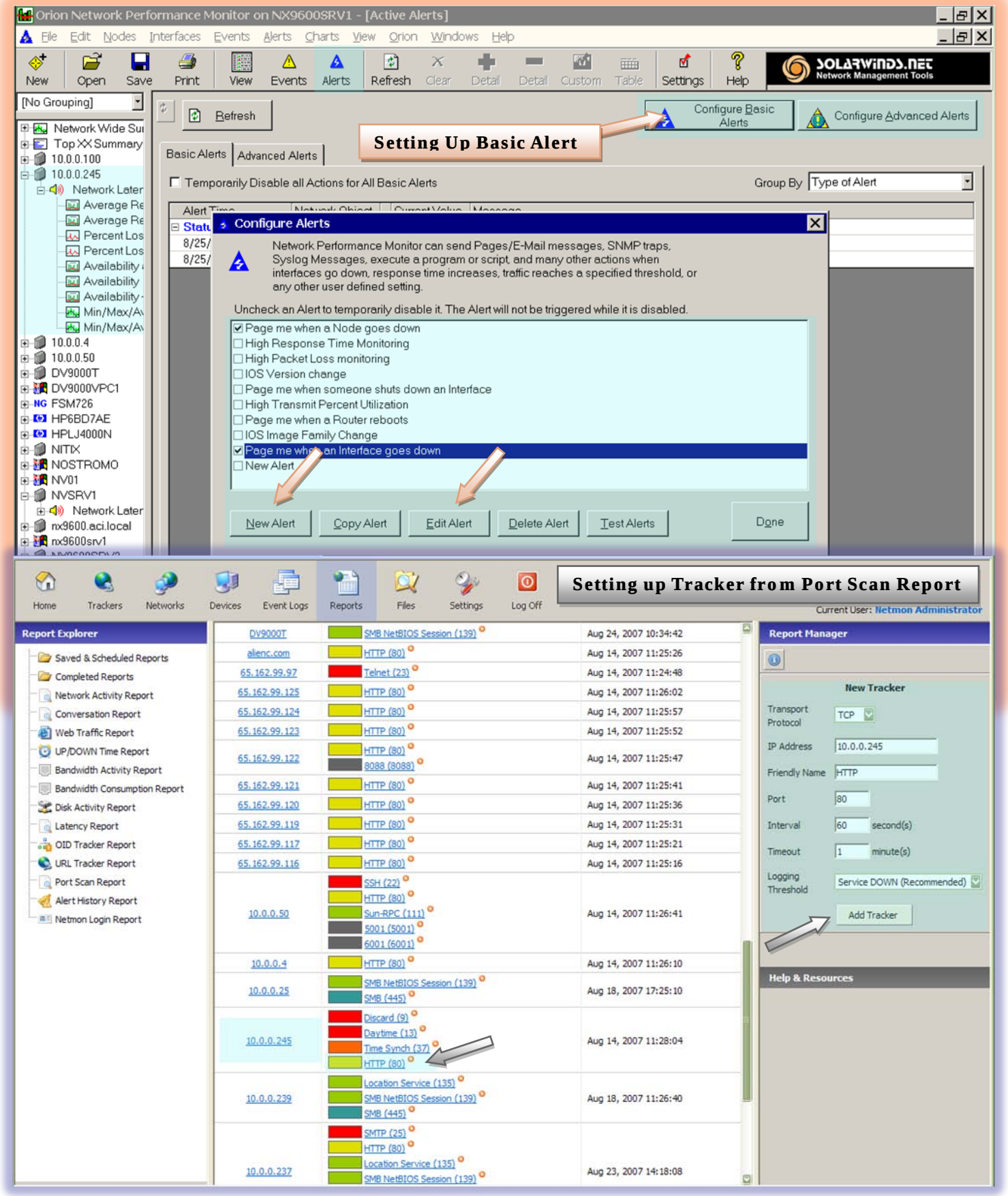
SNMP Reference from page 5 (end): There are many more selections available with Orion

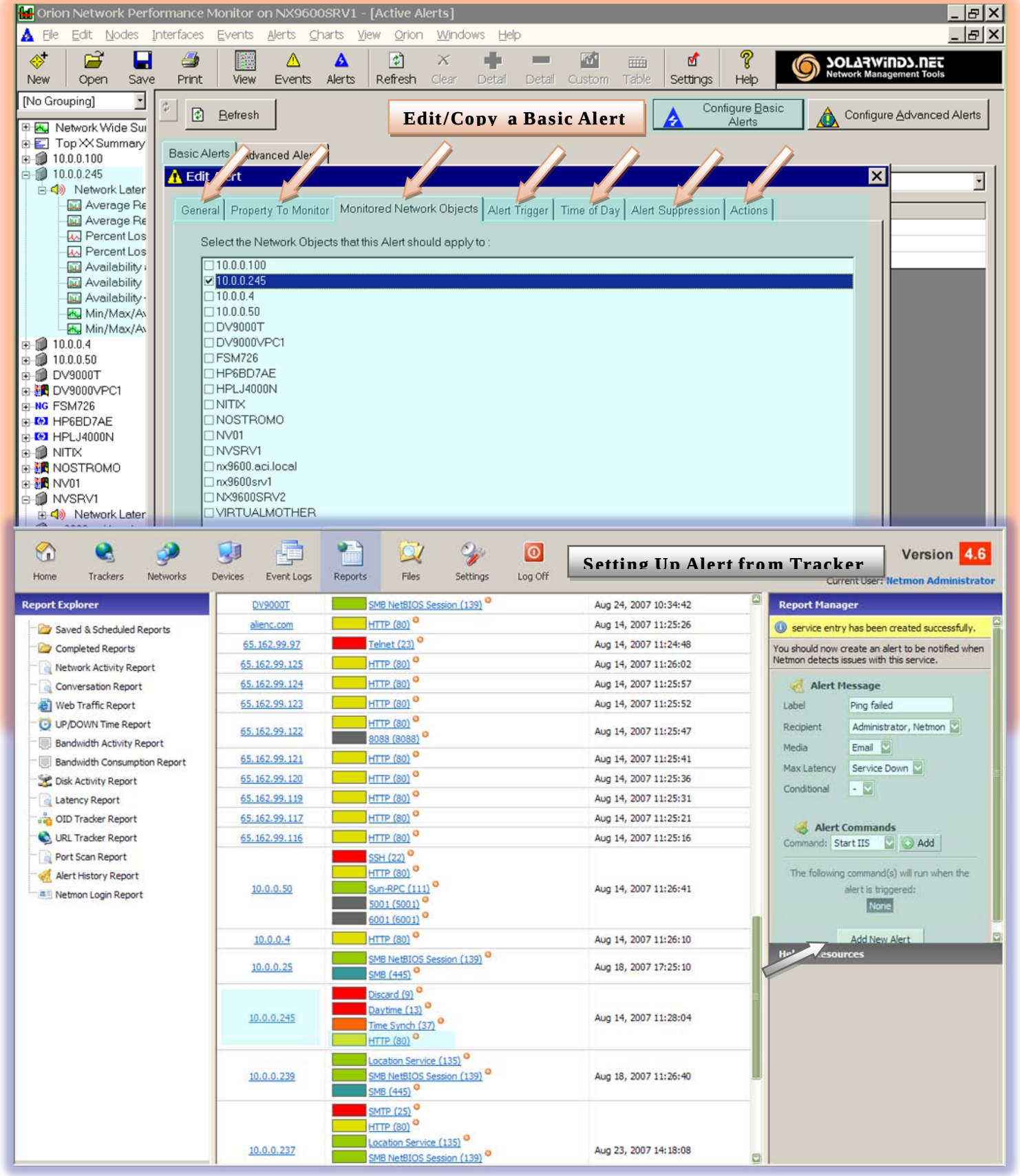
Alerts: Next to SNMP control alerting is one the most important features in a monitoring system. Both programs use totally different methods of setting up alerts.

Orion alerts are set by selecting “Alert” from the upper menu area. You can choice basic or advanced. Basic is more than complex for most situati[illegible]ven tabs each with around 50 choices, this type of arrangement gives the us[illegible] more complex interface. (see pages 9-10)

More Network Card Selections

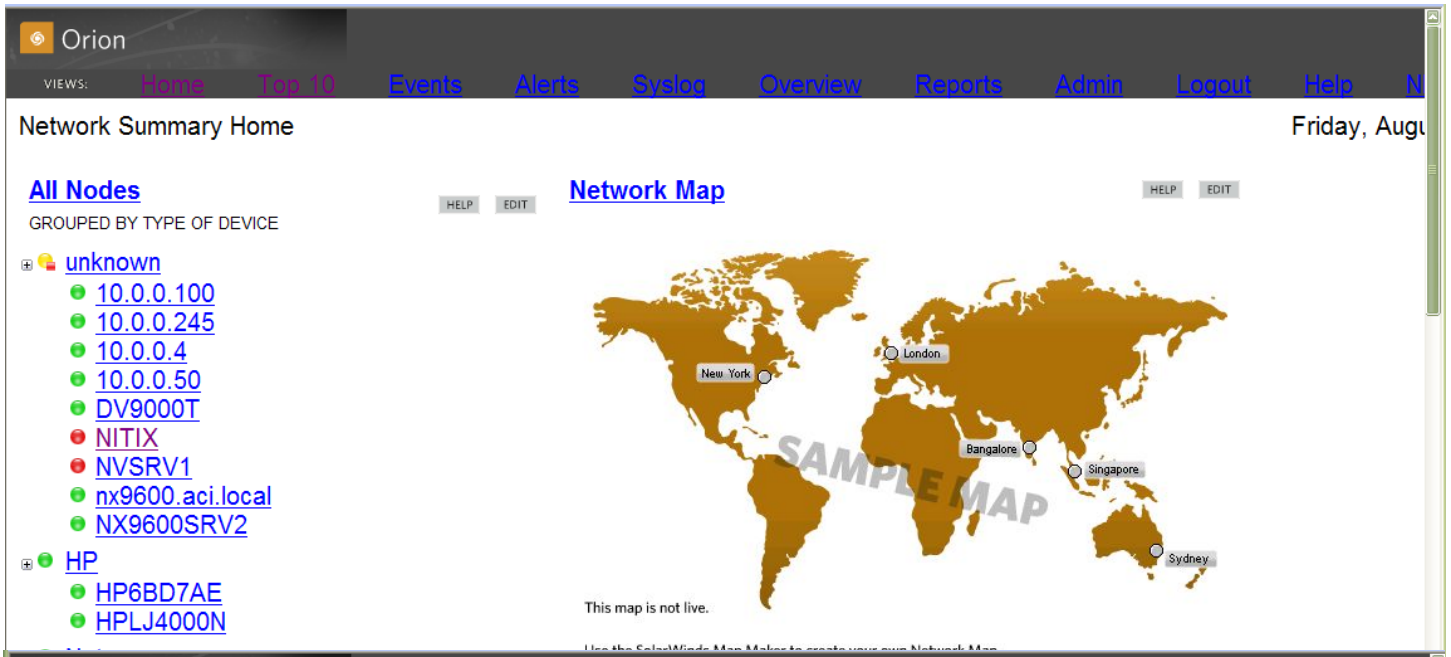
Netmon alerts can be set in several areas however; the simplest method is to use the port scan report. In several steps you can define the device to be tracked and then set the alert all from one screen. This time savings can be very beneficial in large networks. (see pages 9-10)

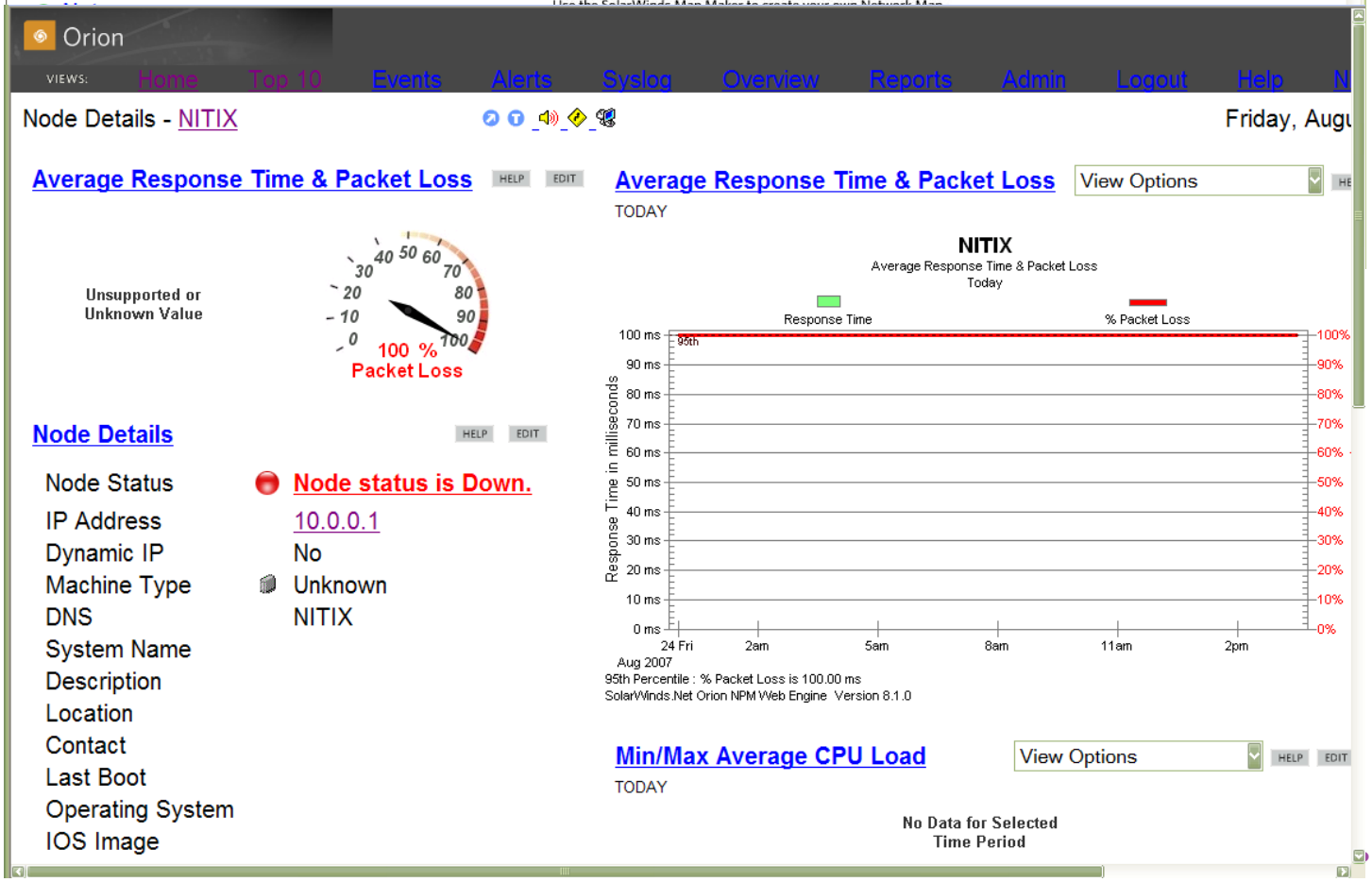



Orion Network Performance Monitor on NX9600SRV1 - [Active Alerts]
Edit/Copy a Basic Alert
Configure Basic Alerts
Configure Advanced Alerts
General
Property To Monitor
Monitored Network Objects
Alert Trigger
Time of Day
Alert Suppression
Actions
Select the Network Objects that this Alert should apply to :
Setting Up Alert from Tracker
Version 4.6
Report Explorer
Report Manager
service entry has been created successfully.
You should now create an alert to be notified when Netmon detects issues with this service.
Alert Message
Alert Commands
Add New Alert

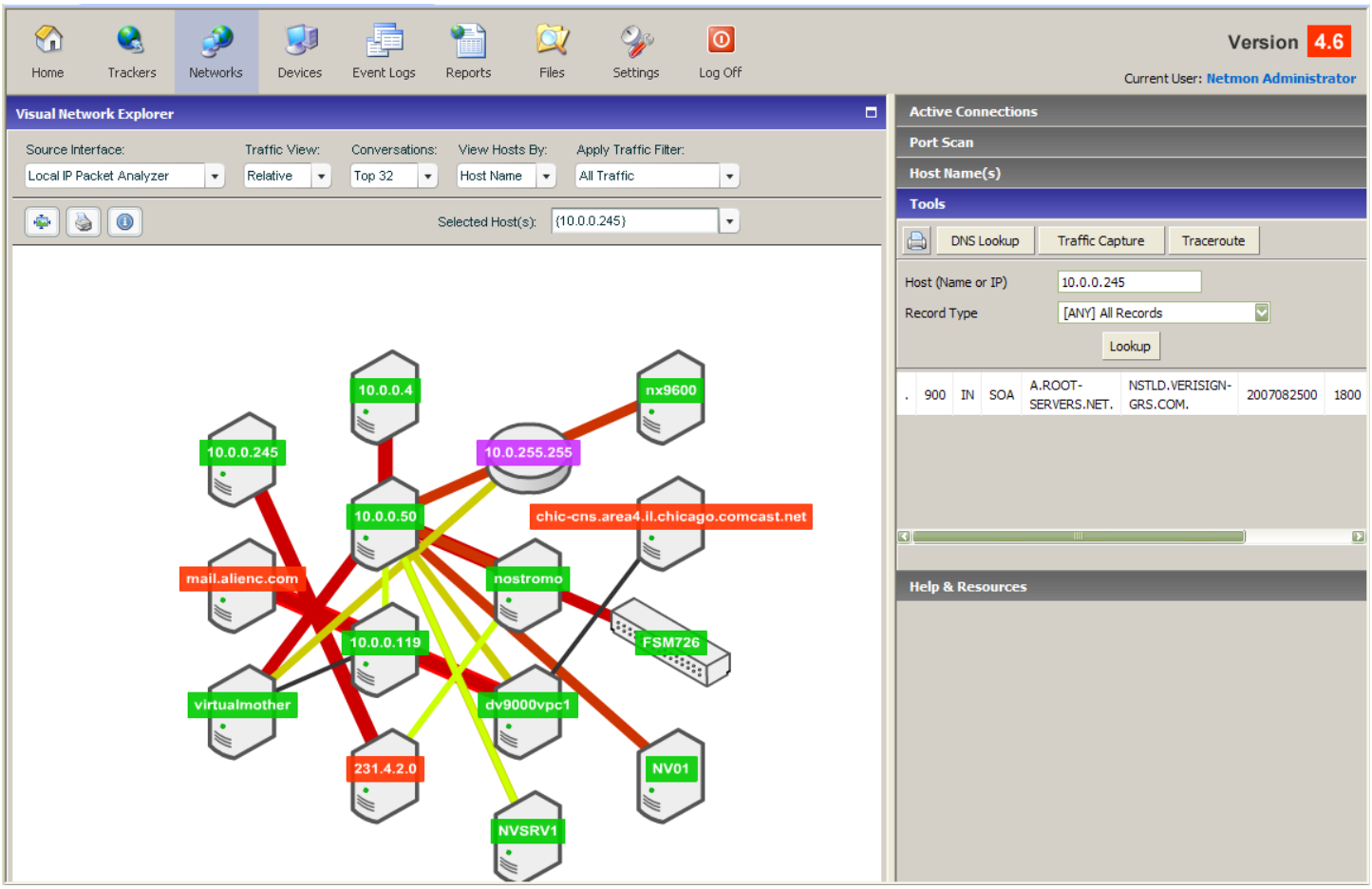
Web Interface/Mapping: This test category is only relevant with the Orion product since Netmon is a web based application and can only be accessed and displayed in a web browser.

The Orion web interface and default mapping is very poorly laid out. I find it barely useable in its current state.



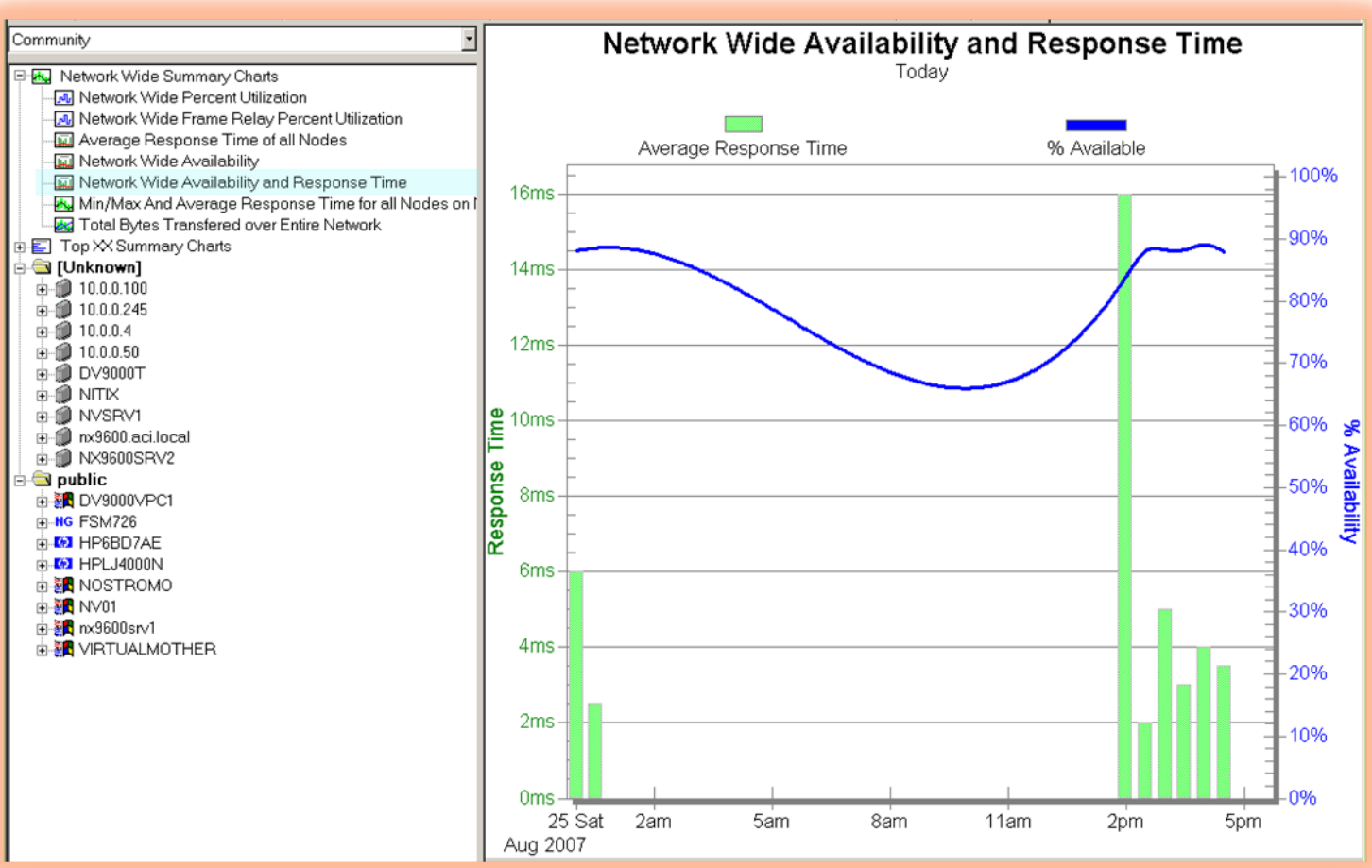


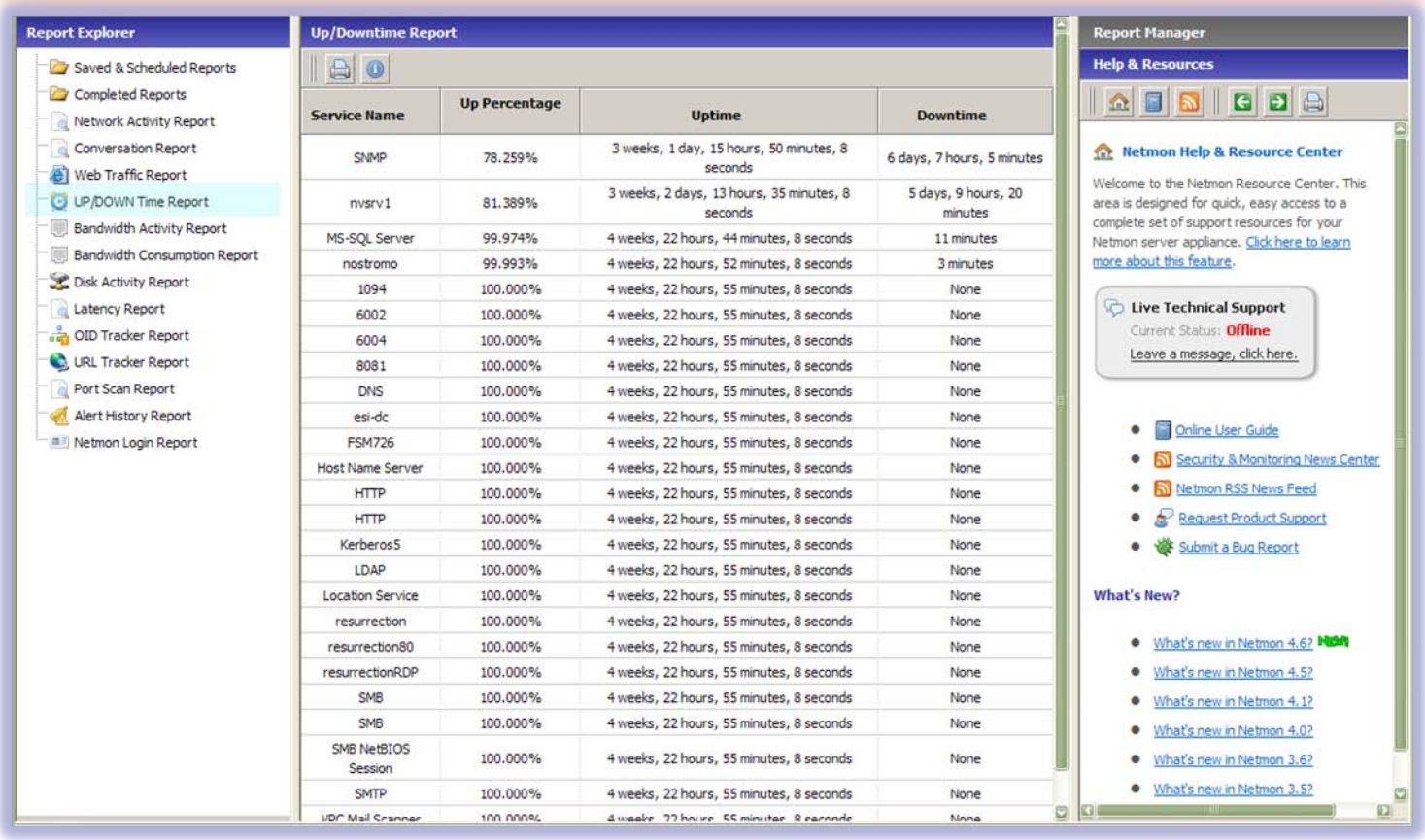
VNE (Virtual Network Explorer): Netmon VNE is software at its best. This is a dynamic network map that can bring back a wealth of information from just one view. The user can tune the data rate by top conversations, protocol filter and more in a dynamic interface. You can select an object in the map and look at connections, port scan info and capture packets to your analyzer quickly and with little help.



Reporting: The report capabilities of Orion are totally configurable while Netmon reports are fixed. This may seem like a problem however, Netmon can write its data to SQL if you want to query and print in a reporting program such as Crystal Reports. Netmon's fixed reports are very useful and easier to read then the default Orion reports. Orion reports tend to be graphical while Netmon uses more statistical listings. Each has their place in data display.

Two sample reports are included on page 13. The Orion report "Network Wide Availability and Response Time" is a good sample of a report that cannot be easily represented statistically. The Netmon Up/Downtime report on page 13 gives the reader very clear information in a statistical format.


Community
Network Wide Summary Charts
Network Wide Percent Utilization
Network Wide Frame Relay Percent Utilization
Average Response Time of all Nodes
Network Wide Availability
Network Wide Availability and Response Time
Min/Max And Average Response Time for all Nodes on
Total Bytes Transfered over Entire Network
Top XX Summary Charts
[Unknown]
10.0.0.100
10.0.0.245
10.0.0.4
10.0.0.50
DV9000T
NITIX
NVSRV1
nx9600.aci.local
NX9600SRV2
public
DV9000VPC1
FSM726
HP6BD7AE
HPLJ4000N
NOSTROMO
NV01
nx9600srv1
VIRTUALMOTHER
Network Wide Availability and Response Time
Today
Average Response Time
% Available
Response Time
% Availability
16ms
14ms
12ms
10ms
8ms
6ms
4ms
2ms
0ms
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
25 Sat
Aug 2007
2am
5am
8am
11am
2pm
5pm


Report Explorer
Saved & Scheduled Reports
Completed Reports
Network Activity Report
Conversation Report
Web Traffic Report
UP/DOWN Time Report
Bandwidth Activity Report
Bandwidth Consumption Report
Disk Activity Report
Latency Report
OID Tracker Report
URL Tracker Report
Port Scan Report
Alert History Report
Netmon Login Report
Up/Downtime Report
Service Name
Up Percentage
Uptime
Downtime
SNMP
78.259%
3 weeks, 1 day, 15 hours, 50 minutes, 8 seconds
6 days, 7 hours, 5 minutes
nvsrv1
81.389%
3 weeks, 2 days, 13 hours, 35 minutes, 8 seconds
5 days, 9 hours, 20 minutes
MS-SQL Server
99.974%
4 weeks, 22 hours, 44 minutes, 8 seconds
11 minutes
nostromo
99.993%
4 weeks, 22 hours, 52 minutes, 8 seconds
3 minutes
1094
6002
6004
8081
DNS
esi-dc
FSM726
Host Name Server
HTTP
HTTP
Kerberos5
LDAP
Location Service
resurrection
resurrection80
resurrectionRDP
SMB
SMB
SMB NetBIOS Session
SMTP
100.000%
4 weeks, 22 hours, 55 minutes, 8 seconds
None
Report Manager
Help & Resources
Netmon Help & Resource Center
Welcome to the Netmon Resource Center. This area is designed for quick, easy access to a complete set of support resources for your Netmon server appliance. Click here to learn more about this feature.
Live Technical Support
Current Status: Offline
Leave a message, click here.
Online User Guide
Security & Monitoring News Center
Netmon RSS News Feed
Request Product Support
Submit a Bug Report
What's New?
What's new in Netmon 4.6?
What's new in Netmon 4.5?
What's new in Netmon 4.1?
What's new in Netmon 4.0?
What's new in Netmon 3.6?
What's new in Netmon 3.5?

Summary: There are several areas that have not been covered for various technical reasons.

1-Syslog capabilities were not setup on either test system being that we had no external Cisco routers or Unix systems. Both systems appear to have complete facilities for syslog managing, viewing and alerting.

2-Cisco Netflow traffic analyzers were not setup on both systems since the test network did not have internal or external access to Cisco routing equipment.

3-VoIP phones can be monitored with either system like any IP/SNMP device without the addition of special software programs. Solarwinds does have a new VoIP monitor for Orion which can extend the QoS metrics beyond the normal functionality of both systems. Monitoring IP phones with the same system that monitors all your critical infrastructure devices does not seem like a wise use of these resources. Possibly a second Cisco specific application could handle this.

Making a choice on a network monitor should be by one metric first – Reliability - with all others features taken as secondary. If your monitor system is not up 100% of the time it cannot be trusted. If it cannot be trusted it is not a true monitor. In 25 days of use the Orion system crashed several times with serious “run-time” errors as I worked in the menus and one time the SQL database went offline , corrupted and could not be connected to at all even after a recovery. The error message it sent was not coded correctly because it actually passed my administrator’s password through in clear text in the the error dialog. In the same time period Netmon never crashed once. I pulled the plug several times and Netmon always came back up.

Several Netmon specific problems were also found: 1- Non Admin users could create trackers and alerts from the “Port Scan Report”, 2- You could not put multiple email address in an alert, I like to send important alerts to my email screen and my cell phone (this could be handled my copying the alert) and 3-Orion allows you to stop traffic to individual interfaces this cannot be done in Netmon.

Support from Solarwinds was not very good if it related to host OS. Support for everything on Netmon was excellent.

The final choice should be made by requiring the selected vendor to submit several references in the financial industries that have the product in use for more than 6 months. I would also like to see a 90 day clause in the purchase contract stating that if the product could not handle the capacity requirements it could be returned for a small fee. I would also like to see second system of minimal configuration on a different network completely that would function as a failsafe on critical devices and help diagnose problems from outside the client network.

If you’re looking for a large array of customizable features and add on modules with the possibility of more failures and you have the support staff to maintain it choose Orion. If you want rock solid reliability with limited customizable features requiring little support choose Netmon.

Regards

Paul F Bergetz

President alienconcepts incorporated