

8/26/2007



Network Monitor Analysis

Performed for Home National Bank



Paul F Bergetz

Network Monitor Analysis

Performed 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)

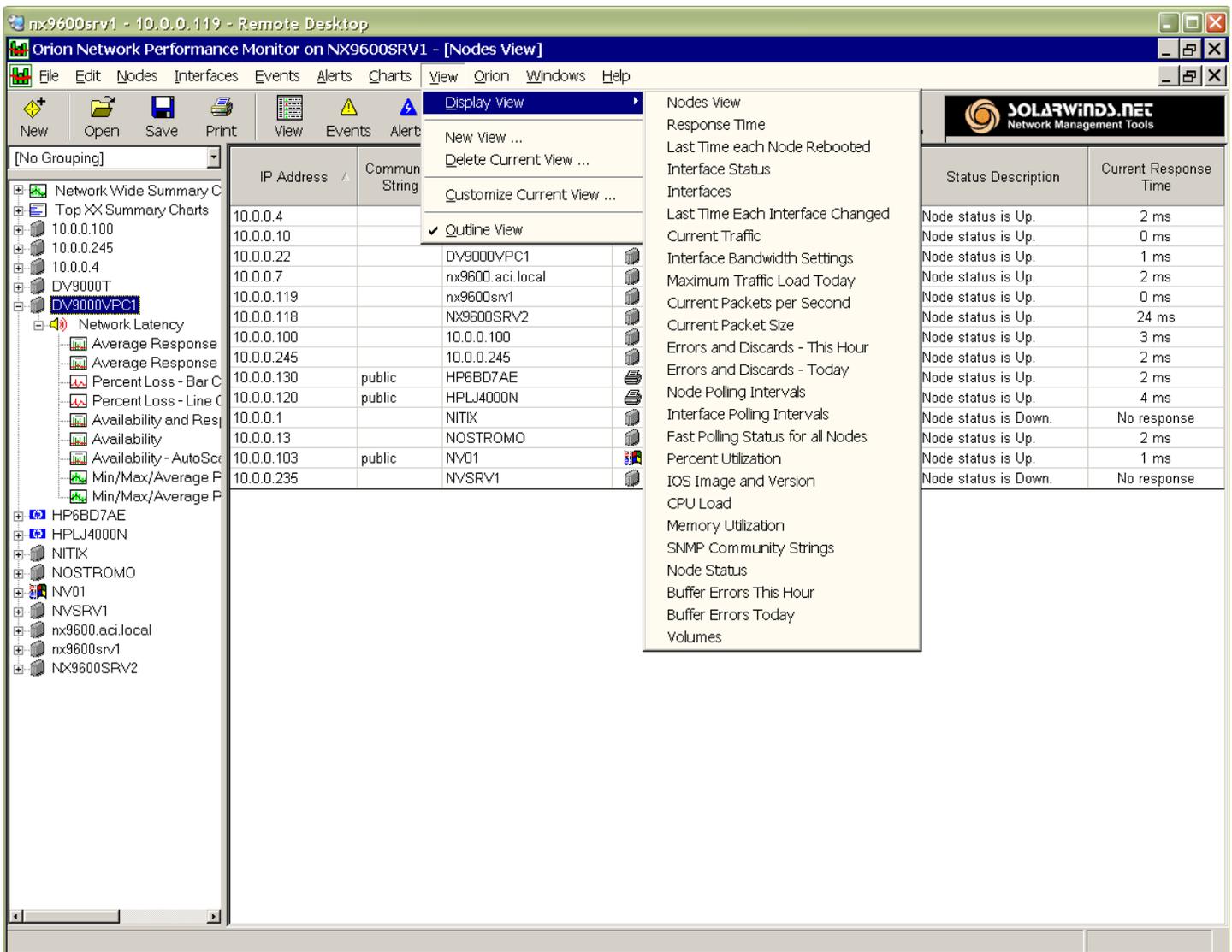
Test Configurations: Each product was setup in a virtual machine on a separate hardware server. The Solarwinds Orion product was setup on a virtual image of Windows 2003 on a host server running Windows 2003 R2 with the latest virtual server. The Netmon product was setup on Vmware Virtual Server 1.03 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 intuitive. 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) .

The screenshot displays the Netmon 4.6 interface. At the top, there is a navigation bar with icons for Home, Trackers, Networks, Devices, Event Logs, Reports, Files, Settings, and Log Off. The version number 4.6 and the current user, Netmon Administrator, are shown in the top right corner.

The main content area is divided into several sections:

- Current System Status:** A table showing the status of various services.

Host	Protocol	Last Checked	Status	Status Message
SNMP (nx9600)	TCP:SNMP Probes (161)	Aug 25, 2007 17:36:26	DOWN	Connection refused
nvsrv1 (10.0.0.35)	ICMP	Aug 25, 2007 17:32:15	DOWN	Timed out
SMB (nvsrv1)	TCP:SMB (445)	Aug 25, 2007 17:36:46	DOWN	No route to host
HTTP (10.0.0.246)	TCP:HTTP (80)	Aug 25, 2007 17:35:51	DOWN	No route to host
- Network Activity:** A bar chart titled "Local Traffic Sniffers" showing traffic volume over time. The y-axis ranges from 0.0Kbps to 120.0Kbps. The x-axis shows time intervals from 16:58 to 13:41. The legend includes HTTP, SSL, Coda Auth 2, SNMP Probes, POP3, DNS, Unknown (1791), and Unknown (1171).
- Bandwidth Monitors:** Two line graphs showing in-bound and out-bound traffic for specific interfaces. The left graph is for "virtualmother (10.0.0.6)" and the right is for "nx9600 (10.0.0.7)".
- Recently Discovered Hosts:** A table listing discovered hosts with their IP addresses, MAC addresses, and discovery dates.

IP Address	MAC Address	Discovered
10.0.0.22	00:03:FF:AA:1D:AC	Aug 22, 2008 13:42:48
10.0.0.103	00:30:48:72:FC:38	Aug 22, 2008 13:42:42
10.0.0.4	00:09:5B:36:25:6A	Aug 22, 2008 13:42:36
10.0.0.13	00:18:F3:A0:F3:EF	Aug 22, 2008 13:42:36
10.0.0.7	00:10:7A:6B:4B:96	Aug 22, 2008 13:42:36
10.0.0.99	00:0F:B5:38:37:04	Aug 22, 2008 13:42:35
10.0.0.50	00:50:56:3E:BB:CC	Aug 22, 2008 10:54:57
10.0.0.238	00:03:FF:77:FC:38	Aug 25, 2007 15:57:49
10.0.0.25	00:14:04:0D:DE:00	Aug 24, 2007 10:24:30
- Top Activity Snapshot:** A table showing the top activity snapshot with source and destination IP addresses and their respective rates.

Source	Destination	Rate
nostromo	10.0.0.50	21 Kbps
10.0.0.50	nostromo	12 Kbps
dv9000vpc1	10.0.0.50	80 bps
10.0.0.50	alienc.com	65 bps
10.0.0.50	65.162.99.116	65 bps
alienc.com	10.0.0.50	64 bps
65.162.99.116	10.0.0.50	64 bps
10.0.0.50	nx9600	48 bps
nx9600	10.0.0.50	20 bps

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	NG	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

- nsvr1 (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? **Netmon**
- 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?

Netmon Port Scan Report Version 4.6
Current User: Netmon Administrator

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

IP Address	Service	Timestamp
DV9000T	SMB NetBIOS Session (139)	Aug 24, 2007 10:34:42
allenc.com	HTTP (80)	Aug 14, 2007 11:25:26
65.162.99.97	Telnet (23)	Aug 14, 2007 11:24:48
65.162.99.125	HTTP (80)	Aug 14, 2007 11:26:02
65.162.99.124	HTTP (80)	Aug 14, 2007 11:25:57
65.162.99.123	HTTP (80)	Aug 14, 2007 11:25:52
65.162.99.122	HTTP (80)	Aug 14, 2007 11:25:47
65.162.99.121	HTTP (80)	Aug 14, 2007 11:25:41
65.162.99.120	HTTP (80)	Aug 14, 2007 11:25:36
65.162.99.119	HTTP (80)	Aug 14, 2007 11:25:31
65.162.99.117	HTTP (80)	Aug 14, 2007 11:25:21
65.162.99.116	HTTP (80)	Aug 14, 2007 11:25:16
10.0.0.50	SSH (22)	Aug 14, 2007 11:26:41
10.0.0.4	HTTP (80)	Aug 14, 2007 11:26:10
10.0.0.25	SMB NetBIOS Session (139)	Aug 18, 2007 17:25:10
10.0.0.245	Discard (9) Daytime (13) Time Synch (37) HTTP (80)	Aug 14, 2007 11:28:04
10.0.0.239	Location Service (135) SMB NetBIOS Session (139) SMB (445)	Aug 18, 2007 11:26:40
10.0.0.237	SMTP (25) HTTP (80) Location Service (135) SMB NetBIOS Session (139)	Aug 23, 2007 14:18:08

Report Manager

New Tracker

Transport Protocol: TCP

IP Address: 10.0.0.245

Friendly Name: HTTP

Port: 80

Interval: 60 second(s)

Timeout: 1 minute(s)

Logging Threshold: Service DOWN (Recommended)

Add Tracker

Help & Resources

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)

Orion Network Performance Monitor on NX9600SRV1 - [NOSTROMO details]

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]

Up 1 ms

Name: NOSTROMO

IP Address: 10.0.0.13 Dynamic IP Address (DHCP or BOOTP)

SNMP

Community String: public Version: SNMPv2c

Allow 64 Bit Counters

Polling

Node Status Polling: 130 seconds

Collect Statistics Every: 10 minutes

Apply Changes

Poll

Rediscover

UnManage

List Resources

Application Monitoring

Validate SNMP

Type of Object: NetworkNode

Object Sub-Type: SNMP

Node ID: 12

IP Address: 10.0.0.13

Dynamic IP: No

SNMPv2 Only Node: No

Community String: public

Node name: NOSTROMO

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)

Device Dashboard

Device Notes

Network Activity

1: MS TCP Loopback interface.

88E8001/8003/8010 PCI Gigabit Ethernet Controller.

65540: Marvell Yukon 88E8052 PCI-E ASF Gigabit Ethernet Controller.

SNMP MIB Walk (Full)

SNMP MIB Walk (Enterprise)

SNMP Object (OID) Trackers

SNMP Trap Messages

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)

Device Dashboard

Device Notes

SNMP MIB Walk (Full)

SNMP Device: nostromo (10.0.0.13)

Device Information

IP Address: 10.0.0.13 Mac Address: 00:18:F3:A0:F3:EF

System Description: Hardware: x86 Family 6 Model 15 Stepping 6 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.1 (Build 2600 Multiprocessor Free)

1	In: 63.49bps	Label: MS TCP Loopback interface. Name: N/A	Status: UP	Connected IP/MAC: Unresolved
65539	In: 43.71bps	Label: Marvell Yukon 88E8001/8003/8010 PCI Gigabit Ethernet Controller. Name: N/A	Status: UP	Connected IP/MAC: 00:18:F3:A0:F3:F0
65540	Out: 23.24bps	Label: N/A	Status: UP	Connected IP/MAC: nostromo
65540	Out: 12.19Kbps	Label: N/A	Status: UP	Connected IP/MAC: nostromo

No custom OID trackers have been defined for this device.

SNMP Manager

Edit SNMP Device

Device Dashboard: Default

IP Address: 10.0.0.13

Label: nostromo

Sample Every: 180 seconds

Community String: public

Port: 161

Enable SNMP:

Enable NetFlow:

Update Device Delete Device

Help & Resources

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

The screenshot displays the Orion Network Performance Monitor interface. The top window shows the details for the 'Marvell Yukon 88E8001/8003/8010 PCI Gigabit Ethernet Controller' on node 'NOSTROMO'. A callout box labeled 'Network Card Selection' points to the controller name in the 'Name' field.

The 'Properties' table for the selected interface is as follows:

Type of Object	Interface
Object Sub-Type	SNMP
Node ID	12
Interface ID	4
Name	Marvell Yukon 88E8001/8003/8010 PCI Gigabit Ethernet Controller
Interface Index	65539
Interface Name	Marvell Yukon 88E8001/8003/8010 PCI Gigabit Ethernet Controller
ifName	
Interface Alias	
Name	NOSTROMO-Marvell Yukon 88E8001/8003/8010 PCI Gigabit Ethernet Controller
Type	ethernetCsmacd
Interface Description	Ethernet
Interface Type	6
64 Bit Counters In Use	No
MAC Address	0018F3A0F3F0
MTU	1500 bytes
Port Speed	1.0 Gbps
Status	Up

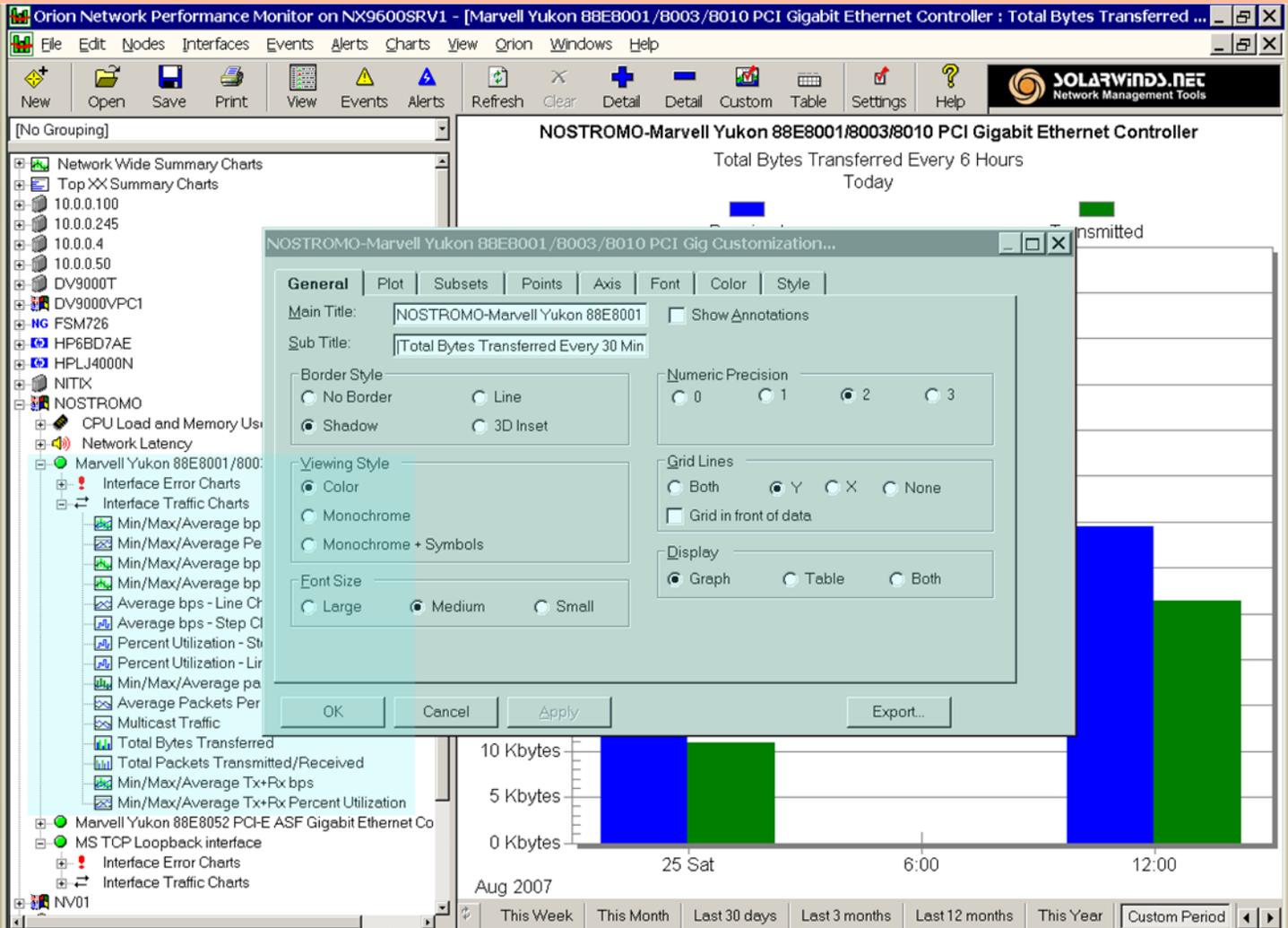
Below this, the 'Device Explorer' shows a tree view of devices. An arrow points to the selected interface '65539: Marvell Yukon 88E8001/8003/8010 PCI Gigabit Ethernet Controller'.

The 'SNMP Manager' panel shows the 'Edit SNMP Interface' configuration. The 'Label' is 'Marvell Yukon 88E8001/8003/8010 PCI Gigabit Ethernet Controller'. The 'Display on Home Dashboard' and 'Enable SNMP Logging' checkboxes are checked. An arrow points to the 'Update Device' button.

The 'nostromo (10.0.0.13) Interface 65539: N/A' section shows a bar chart of network activity:

Direction	Speed (bps)
IN	~23.5
OUT	~23.5

A callout box labeled 'Network Card Selection' points to the interface name in the chart title.



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 situations. Advanced has more tabs each with around 50 choices, this type of arrangement gives the user a 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)

Setting Up Basic Alert

Configure Alerts

Network Performance Monitor can send Pages/E-Mail messages, SNMP traps, Syslog Messages, execute a program or script, and many other actions when interfaces go down, response time increases, traffic reaches a specified threshold, or any other user defined setting.

Uncheck an Alert to temporarily disable it. The Alert will not be triggered while it is disabled.

- Page me when a Node goes down
- High Response Time Monitoring
- High Packet Loss monitoring
- IOS Version change
- Page me when someone shuts down an Interface
- High Transmit Percent Utilization
- Page me when a Router reboots
- IOS Image Family Change
- Page me when an interface goes down
- New Alert

New Alert Copy Alert Edit Alert Delete Alert Test Alerts Done

Setting up Tracker from Port Scan Report

Current User: Netmon Administrator

Device	Protocol	Time
DV9000T	SMB NetBIOS Session (139)	Aug 24, 2007 10:34:42
alienc.com	HTTP (80)	Aug 14, 2007 11:25:26
65.162.99.97	Telnet (23)	Aug 14, 2007 11:24:48
65.162.99.125	HTTP (80)	Aug 14, 2007 11:26:02
65.162.99.124	HTTP (80)	Aug 14, 2007 11:25:57
65.162.99.123	HTTP (80)	Aug 14, 2007 11:25:52
65.162.99.122	HTTP (80)	Aug 14, 2007 11:25:47
65.162.99.121	HTTP (80)	Aug 14, 2007 11:25:41
65.162.99.120	HTTP (80)	Aug 14, 2007 11:25:36
65.162.99.119	HTTP (80)	Aug 14, 2007 11:25:31
65.162.99.117	HTTP (80)	Aug 14, 2007 11:25:21
65.162.99.116	HTTP (80)	Aug 14, 2007 11:25:16
10.0.0.50	Sun-RPC (111)	Aug 14, 2007 11:26:41
10.0.0.4	HTTP (80)	Aug 14, 2007 11:26:10
10.0.0.25	SMB NetBIOS Session (139)	Aug 18, 2007 17:25:10
10.0.0.245	Discard (9)	Aug 14, 2007 11:28:04
	Daytime (13)	
	Time Synch (37)	
	HTTP (80)	
10.0.0.239	Location Service (135)	Aug 18, 2007 11:26:40
	SMB NetBIOS Session (139)	
	SMB (445)	
	SMTTP (25)	
	HTTP (80)	
10.0.0.237	Location Service (135)	Aug 23, 2007 14:18:08
	SMB NetBIOS Session (139)	

Report Manager

New Tracker

Transport Protocol: TCP

IP Address: 10.0.0.245

Friendly Name: HTTP

Port: 80

Interval: 60 second(s)

Timeout: 1 minute(s)

Logging Threshold: Service DOWN (Recommended)

Add Tracker

Edit/Copy a Basic Alert

Basic Alerts | 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 :

- 10.0.0.100
- 10.0.0.245
- 10.0.0.4
- 10.0.0.50
- DV9000T
- DV9000VPC1
- FSM726
- HP6BD7AE
- HPLJ4000N
- NITIX
- NOSTROMO
- NV01
- NVSRV1
- nx9600.aci.local
- nx9600srv1
- NX9600SRV2
- VIRTUALMOTHER

Home | Trackers | Networks | Devices | Event Logs | Reports | Files | Settings | Log Off

Setting Up Alert from Tracker | Version 4.6 | Current User: Netmon Administrator

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

IP/Host	Service	Count	Time
DV9000T	SMB NetBIOS Session	139	Aug 24, 2007 10:34:42
alenc.com	HTTP	80	Aug 14, 2007 11:25:26
65.162.99.97	Telnet	23	Aug 14, 2007 11:24:48
65.162.99.125	HTTP	80	Aug 14, 2007 11:26:02
65.162.99.124	HTTP	80	Aug 14, 2007 11:25:57
65.162.99.123	HTTP	80	Aug 14, 2007 11:25:52
65.162.99.122	HTTP	80	Aug 14, 2007 11:25:47
65.162.99.121	HTTP	80	Aug 14, 2007 11:25:41
65.162.99.120	HTTP	80	Aug 14, 2007 11:25:36
65.162.99.119	HTTP	80	Aug 14, 2007 11:25:31
65.162.99.117	HTTP	80	Aug 14, 2007 11:25:21
65.162.99.116	HTTP	80	Aug 14, 2007 11:25:16
10.0.0.50	SSH	22	
	HTTP	80	
	Sun-RPC	111	Aug 14, 2007 11:26:41
	5001 (5001)		
	6001 (6001)		
10.0.0.4	HTTP	80	Aug 14, 2007 11:26:10
10.0.0.25	SMB NetBIOS Session	139	Aug 18, 2007 17:25:10
	SMB	445	
10.0.0.245	Discard	9	
	Daytime	13	
	Time Synch	37	
	HTTP	80	Aug 14, 2007 11:28:04
10.0.0.239	Location Service	135	Aug 18, 2007 11:26:40
	SMB NetBIOS Session	139	
	SMB	445	
10.0.0.237	SMTP	25	
	HTTP	80	
	Location Service	135	
	SMB NetBIOS Session	139	Aug 23, 2007 14:18:08

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

Label: Ping failed

Recipient: Administrator, Netmon

Media: Email

Max Latency: Service Down

Conditional: -

Alert Commands

Command: Start IIS

The following command(s) will run when the alert is triggered:

None

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.

The screenshot shows the Orion Network Summary Home page. At the top, there is a navigation bar with links for Home, Top 10, Events, Alerts, Syslog, Overview, Reports, Admin, Logout, Help, and N. The main content area is titled "Network Summary Home" and includes a "Network Map" section. The map shows a world map with several nodes marked: New York, London, Bangalore, Singapore, and Sydney. A large "SAMPLE MAP" watermark is overlaid on the map. Below the map, there is a text box that says "This map is not live." To the left of the map, there is a list of nodes grouped by type of device. The list includes:

- unknown
 - 10.0.0.100
 - 10.0.0.245
 - 10.0.0.4
 - 10.0.0.50
 - DV9000T
 - NITIX
 - NVSRV1
 - nx9600.aci.local
 - NX9600SRV2
- HP
 - HP6BD7AE
 - HPLJ4000N

The screenshot shows the Orion Node Details page for the node NITIX. The page includes a navigation bar and a "Node Details" section. The node status is "Down". The IP address is 10.0.0.1. The machine type is "Unknown" and the DNS is "NITIX". To the right of the node details, there is a gauge showing "100 % Packet Loss". Below the gauge, there is a line graph titled "Average Response Time & Packet Loss" for "TODAY". The graph shows "Response Time in milliseconds" on the left y-axis (0 to 100 ms) and "% Packet Loss" on the right y-axis (0% to 100%). The x-axis shows time from 24 Fri to 2pm. The graph shows a red line for "% Packet Loss" at 100% and a green line for "Response Time" at 100 ms. Below the graph, there is a text box that says "No Data for Selected Time Period".

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.

The screenshot displays the Netmon Visual Network Explorer (VNE) interface. At the top, there is a navigation menu with icons for Home, Trackers, Networks, Devices, Event Logs, Reports, Files, Settings, and Log Off. The current user is identified as 'Netmon Administrator' and the version is 4.6. The main window is titled 'Visual Network Explorer' and contains several configuration options: Source Interface (Local IP Packet Analyzer), Traffic View (Relative), Conversations (Top 32), View Hosts By (Host Name), and Apply Traffic Filter (All Traffic). A 'Selected Host(s)' dropdown shows '10.0.0.245'. The central area is a network map showing various hosts and their connections. The map includes nodes like 10.0.0.245, 10.0.0.4, 10.0.0.50, 10.0.0.119, 231.4.2.0, NVSRV1, nostromo, FSM726, NV01, and nx9600. A central node is highlighted with a purple box and labeled 10.0.255.255. The right-hand panel contains a 'Tools' section with buttons for DNS Lookup, Traffic Capture, and Traceroute. Below this, there is a 'Host (Name or IP)' field with '10.0.0.245' and a 'Record Type' dropdown set to '[ANY] All Records'. A 'Lookup' button is present. Below the lookup section, there is a table of DNS records:

.	900	IN	SOA	A.ROOT-SERVERS.NET.	NSTLD.VERISIGN-GRS.COM.	2007082500	1800
---	-----	----	-----	---------------------	-------------------------	------------	------

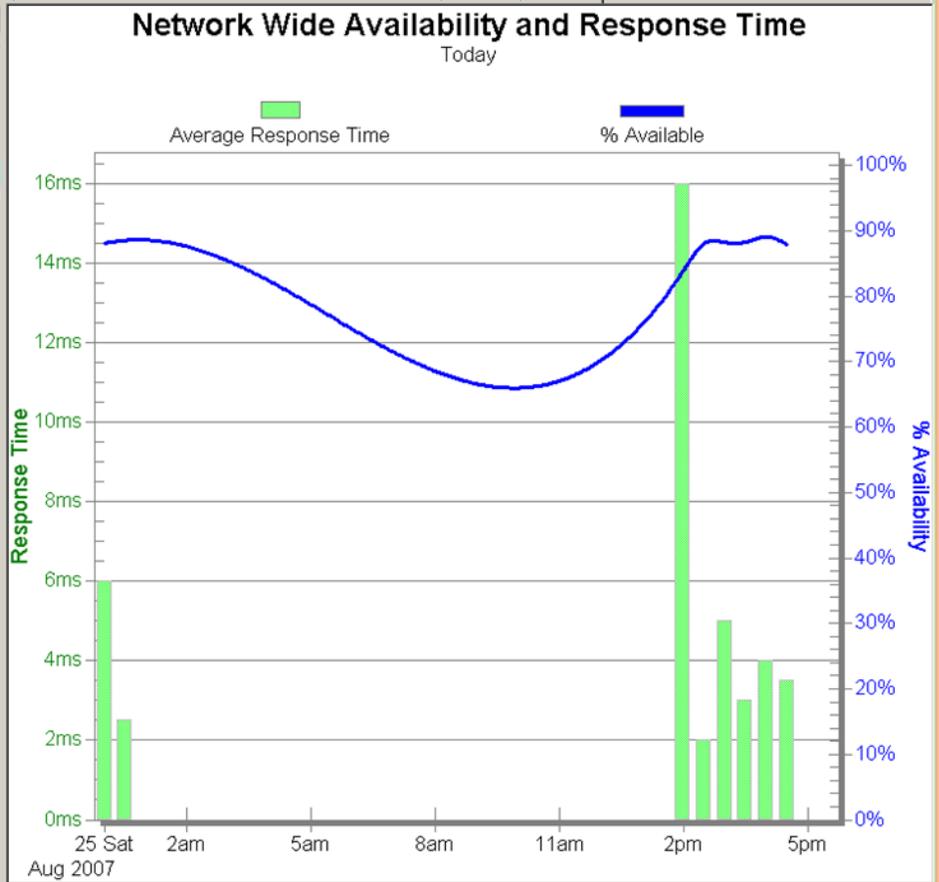
The bottom of the right panel has a 'Help & Resources' section.

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 than 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 I
 - Total Bytes Transferred 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
 - rx9600.aci.local
 - NX9600SRV2
- public
 - DV9000VPC1
 - NG FSM726
 - HPBD7AE
 - HPLJ4000N
 - NOSTROMO
 - NV01
 - rx9600srv1
 - VIRTUALMOTHER



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/Down 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	100.000%	4 weeks, 22 hours, 55 minutes, 8 seconds	None
6002	100.000%	4 weeks, 22 hours, 55 minutes, 8 seconds	None
6004	100.000%	4 weeks, 22 hours, 55 minutes, 8 seconds	None
8081	100.000%	4 weeks, 22 hours, 55 minutes, 8 seconds	None
DNS	100.000%	4 weeks, 22 hours, 55 minutes, 8 seconds	None
esi-dc	100.000%	4 weeks, 22 hours, 55 minutes, 8 seconds	None
FSM726	100.000%	4 weeks, 22 hours, 55 minutes, 8 seconds	None
Host Name Server	100.000%	4 weeks, 22 hours, 55 minutes, 8 seconds	None
HTTP	100.000%	4 weeks, 22 hours, 55 minutes, 8 seconds	None
HTTP	100.000%	4 weeks, 22 hours, 55 minutes, 8 seconds	None
Kerberos5	100.000%	4 weeks, 22 hours, 55 minutes, 8 seconds	None
LDAP	100.000%	4 weeks, 22 hours, 55 minutes, 8 seconds	None
Location Service	100.000%	4 weeks, 22 hours, 55 minutes, 8 seconds	None
resurrection	100.000%	4 weeks, 22 hours, 55 minutes, 8 seconds	None
resurrection80	100.000%	4 weeks, 22 hours, 55 minutes, 8 seconds	None
resurrectionRDP	100.000%	4 weeks, 22 hours, 55 minutes, 8 seconds	None
SMB	100.000%	4 weeks, 22 hours, 55 minutes, 8 seconds	None
SMB	100.000%	4 weeks, 22 hours, 55 minutes, 8 seconds	None
SMB NetBIOS Session	100.000%	4 weeks, 22 hours, 55 minutes, 8 seconds	None
SMTP	100.000%	4 weeks, 22 hours, 55 minutes, 8 seconds	None
VPC Mail Scanner	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? **Hot!**](#)
- [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

