



**netSENTINEL™**  
when uptime is critical

## Table of Contents

netSENTINEL - Introduction .....	3
Mapping and Modeling the Infrastructure. ....	3
Measuring, Monitoring and Alerting .....	4
Diagnostic Support.....	6
Asset Management.....	12
Incident and Change Management .....	14
Reporting.....	15
Administration .....	16
netSENTINEL Deployment .....	16
Conclusion.....	17

## **netSENTINEL - Introduction**

Today's highly automated business services are revenue generators that rely on IT services for availability and performance. netSENTINEL provides the link between IT performance and critical business needs by providing an integrated management platform to monitor, manage and maintain the IT infrastructure that business services rely on.

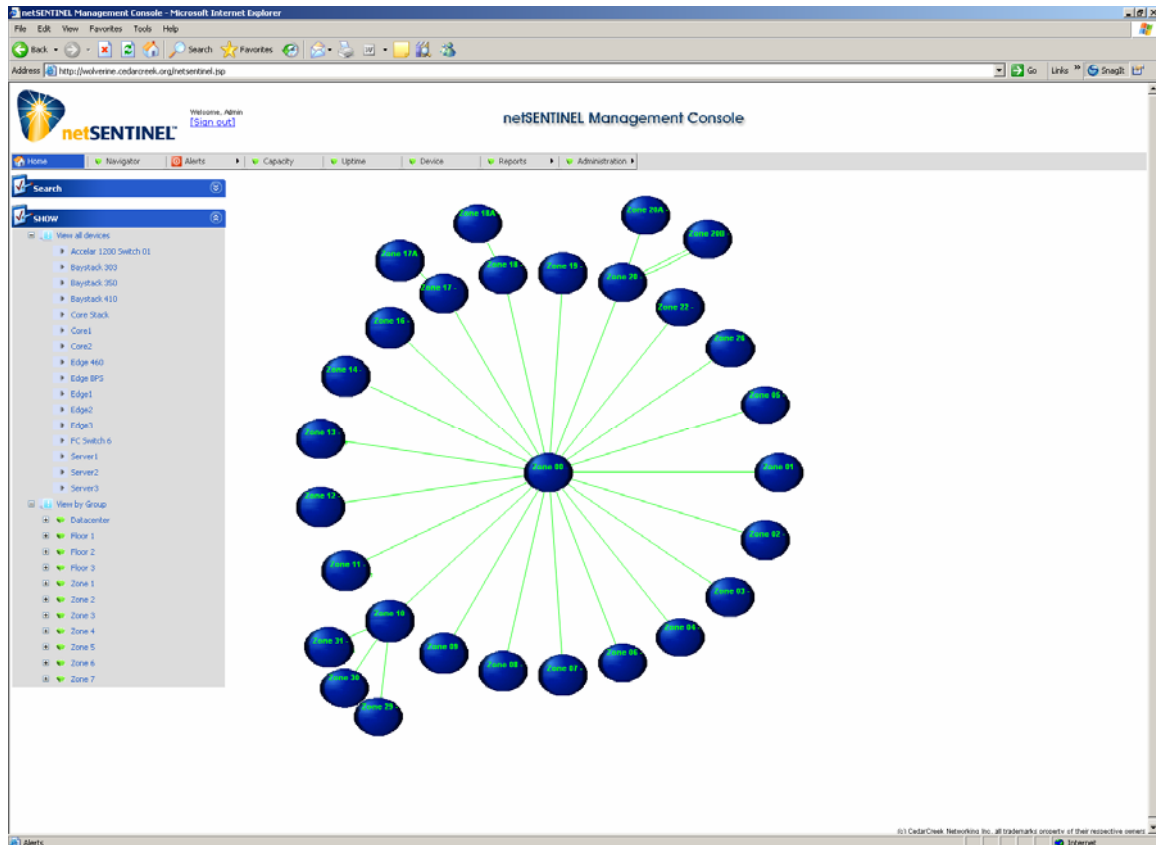
As a managed service, netSENTINEL delivers the network management and monitoring results you want without the time and expense of purchasing and maintaining hardware and software. Instead of spending weeks or even months learning and deploying software tools, you're up and managing quickly, while your staff and resources can stay focused on strategic business initiatives. You also gain access to a team of trained IT Infrastructure Professionals with extensive experience in monitoring, managing and maintaining enterprise networks. With some of the most powerful remote management technology available today, our certified systems engineers tailor the implementation of your netSENTINEL to your needs, quickly and effectively. Once you're up and managing, our involvement doesn't stop. We are available to support you and to work with you to ensure you get the most from your netSENTINEL investment. Whether it's a small change you'd like help with or a major extension of netSENTINEL in your infrastructure, our commitment is to provide you with the highest level of service and support. With netSENTINEL it's like having a team of network management professionals on your staff and at your disposal.

### **Mapping and Modeling the Infrastructure.**

Like all successful management processes, netSENTINEL begins by developing accurate map of the components in your environment and their relationships. netSENTINEL can employ powerful network scanning tools and processes to discover the devices in your network at a detail level, or alternately our deployment engineers work with you to develop this information from your documentation. Network connection information for all significant devices in your infrastructure is documented in the netSENTINEL link table and devices are analyzed according to their type, manufacturer, hardware and software assets.

The next step is to model the infrastructure according to your view of your business. User defined groups can be created to identify the significant similarities and differences in your infrastructure or your business. For example, devices can be grouped by type, like servers or switches, devices may be grouped by location or by the business processes they support. Devices can be members of multiple groups. The value of a precise, living, infrastructure map is to provide the basis for measuring the infrastructure at various levels and to quickly understand issues, their impact, and their root cause when they occur.

The figure below illustrates a logical infrastructure map of a larger facility. In this example the map has been developed around the concept of device location and the manufacturing processes that the devices in each group support.



## Measuring, Monitoring and Alerting

netSENTINEL is a powerful service that provides the tools and processes to monitor, measure and manage the broadest range of IP devices. netSENTINEL can monitor any IP enabled device using industry standard protocols. The following is a representative list of the types of devices netSENTINEL monitors and measures.

- Servers
- Workstations
- Switches - Core, Edge
- SAN's
- Firewalls
- Routers
- Wireless devices, AP's, Bridges
- Printers
- VoIP systems
- Laptops
- Robotics
- Programmable logic controllers
- UPS
- WAN Circuits
- VPN's
- Temperature

Once the infrastructure and the devices are discovered, netSENTINEL provides a full flexible approach to measuring your entire infrastructure. Out of the box, netSENTINEL provides standard monitoring templates for most devices with the ability to expand or change the templates for any device at any time. While the list of available metrics is exhaustive, typical monitoring metrics include:

- Bandwidth - Speed / Utilization
- Bandwidth - Traffic / Utilization
- Port - Status / Traffic / Performance
- Module - Status / Traffic / Performance
- Device - Status / Traffic / Performance
- Fan - Status
- Power Supply - Status
- Temperature / Threshold
- Disk - Size / Usage / Threshold
- Services - Running / Stopped
- Software - Applications Installed
- Hot-Fixes / Patches Installed
- Memory - Usage / Processes Executed
- Link - Status / Performance
- Interface - Status / Traffic / Performance
- CPU - Capacity / Load / Threshold

The netSENTINEL polling agent remotely polls your entire network every 60 seconds, using industry standard protocols ( SNMP, ICMP, TCP and WMI ) to monitor and measure your infrastructure. The polling agent collects thousands of data points throughout your infrastructure for availability, status, performance, and utilization metrics. Each metric is compared for critical conditions and stored in the database for tracking and reporting. Critical conditions are immediately recorded, alerted and communicated through a variety of user defined methods providing the ability to quickly act upon issues before they become problems for your customers. Alerts contain device, time and location information along with a summary of the specific issue and can be immediately communicated by e-mail, pager, SMS, cell, PDA, etc. Alert information can be managed and assigned to individuals, groups, support providers or third party systems.

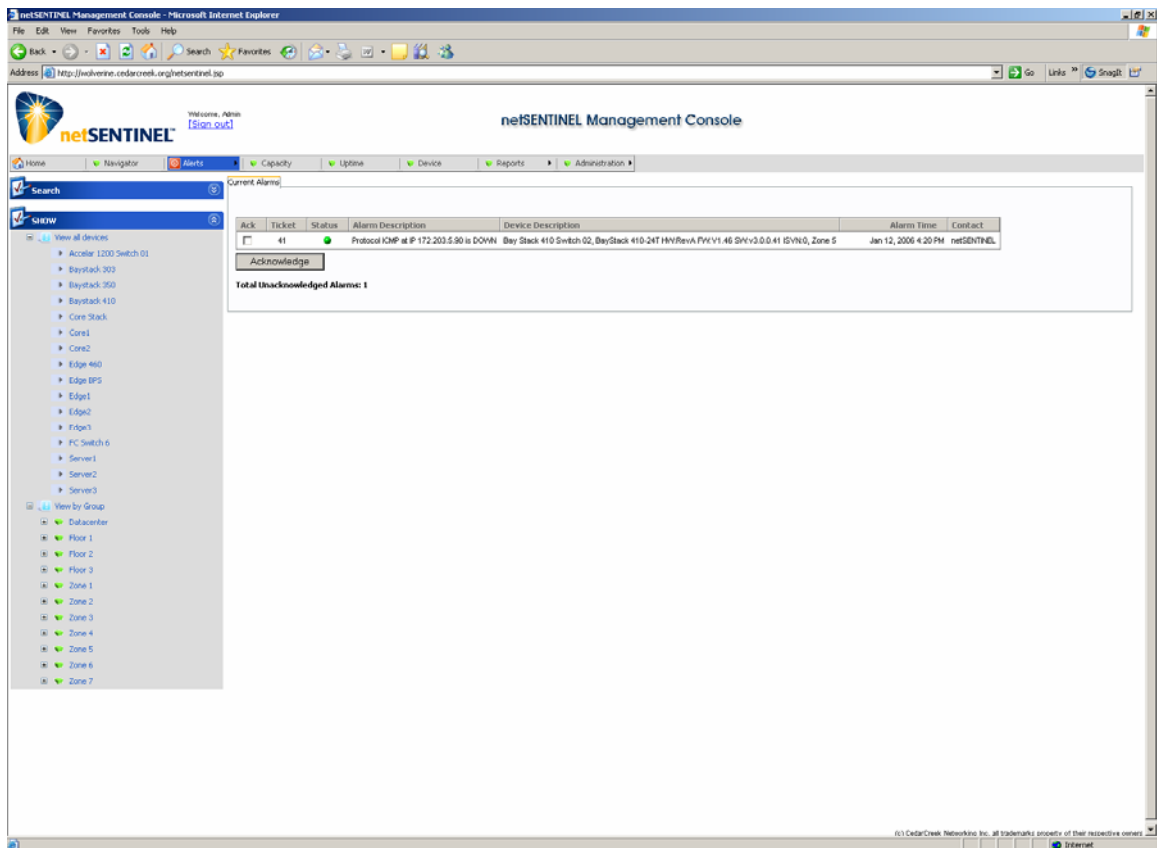
netSENTINEL measures and monitors your entire infrastructure without loading invasive agents on your servers or devices. In addition, while rarely required, netSENTINEL can provide custom monitoring processes for a range of specialized customer requirements like fire or security systems.

## Diagnostic Support

netSENTINEL's unique graphical interface provides a high level, business view of the status of your IT environment. The Navigator also provides support to quickly isolate faults and pinpoint trouble areas. While all alerts are conveniently listed in one screen with details and a direct link to the affected device, the graphical Navigator provides intuitive alert information showing fault status at a glance. The drill-down Navigator expands each sub-level to expose devices within a group that are impacted by the Alert condition and identify the specific area of failure or threshold condition.

All Alerts are captured, listed and stored indefinitely. Alerts include an assigned sequential number, current status information, a fault or threshold description, device details, time stamp and contact information. Each Alert has an embedded link to the affected device for quick navigation. Alerts are considered Current until they are acknowledged. Once acknowledged, they are moved from the Current Alerts screen to the Historical Alerts screen.

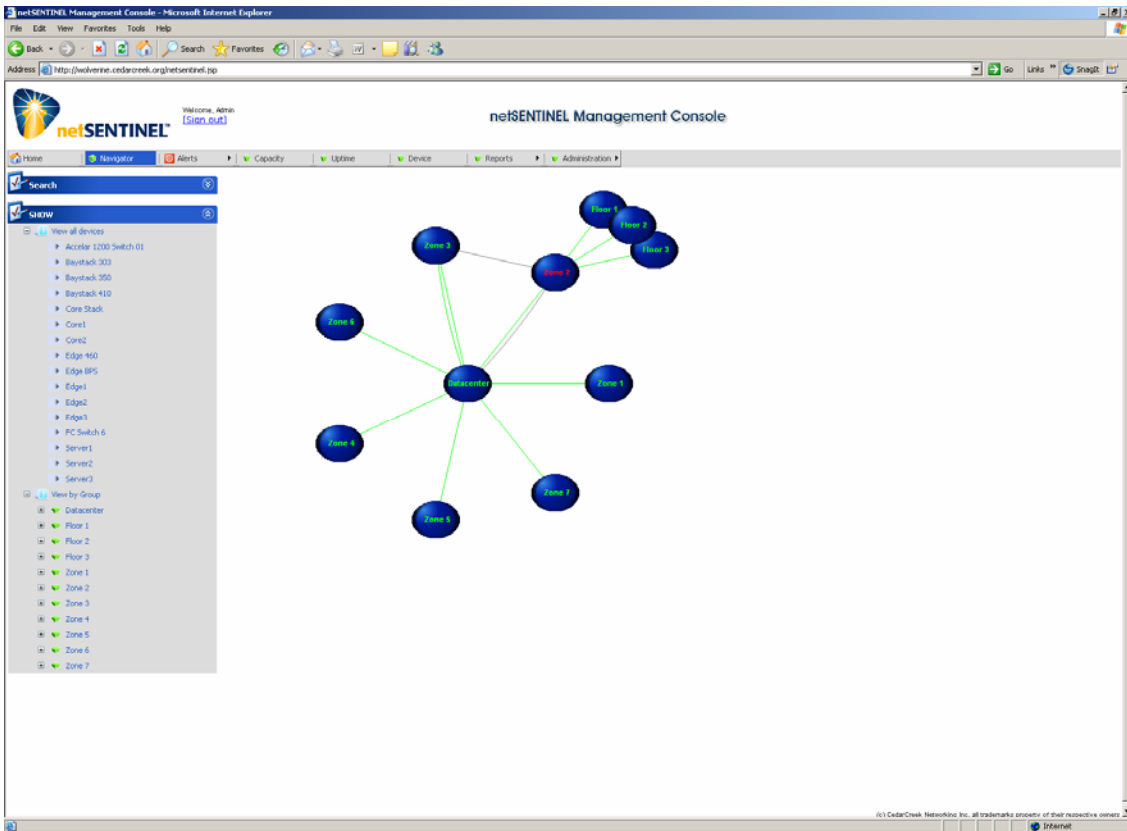
### Current Alerts Screen



The screenshot displays the netSENTINEL Management Console interface within a Microsoft Internet Explorer browser window. The browser's address bar shows the URL <http://wslvmme.endacreek.org/net Sentinel.sp>. The console header includes the netSENTINEL logo, the user name 'Welcome, Admin', and a 'Sign out' link. The main navigation bar contains tabs for Home, Navigator, Alerts, Capacity, Uptime, Device, Reports, and Administration. The 'Alerts' tab is active, showing a 'Current Alerts' section with a table of alerts. The table has columns for Ack, Ticket, Status, Alarm Description, Device Description, Alarm Time, and Contact. One alert is listed with Ticket #41, Status 'OK', and Alarm Description 'Protocol ICMP at IP 172.203.5.90 is DOWN'. Below the table is an 'Acknowledge' button and a summary 'Total Unacknowledged Alarms: 1'. A left-hand navigation pane shows a tree view of devices, including 'View all devices', 'Accelar 1200 Switch 01', 'Baystack 303', 'Baystack 350', 'Baystack 410', 'Core Stack', 'Core1', 'Core2', 'Edge 460', 'Edge BP2', 'Edge1', 'Edge2', 'Edge3', 'PC Switch 6', 'Server1', 'Server2', 'Server3', and 'View by Group' with sub-items like 'Datacenter', 'Floor 1', 'Floor 2', 'Floor 3', 'Zone 1' through 'Zone 7'. The footer of the console contains the text '©2007 DataCreek Networks Inc. All trademarks property of their respective owners.' and an 'Internet' icon.

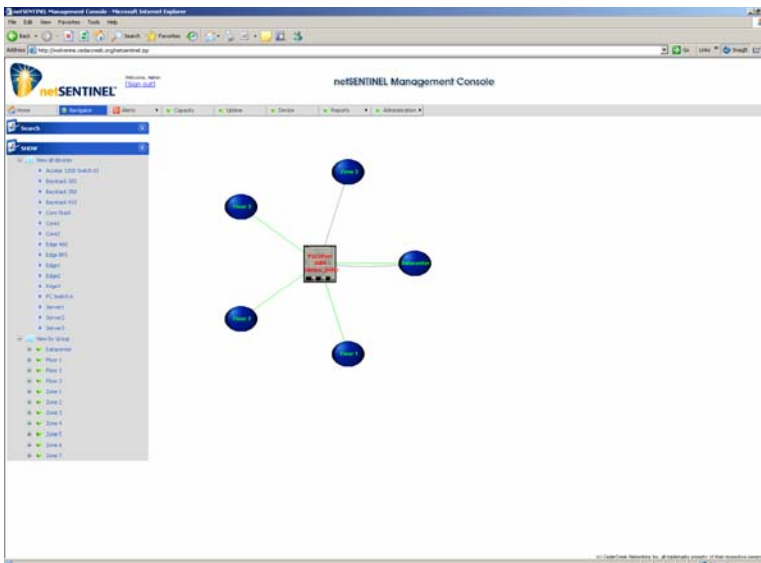
Ack	Ticket	Status	Alarm Description	Device Description	Alarm Time	Contact
<input type="checkbox"/>	41	OK	Protocol ICMP at IP 172.203.5.90 is DOWN	Bay Stack 410 Switch 02, BayStack 410-24T1HYRevA.PHY.V1.46 SN:V2.0.0.41 ISV:0, Zone 5	Jan 12, 2006 4:20 PM	netSENTINEL

## Navigator – Top Level – All Zones



The Navigator also indicates alerted conditions through the graphical drill-down interface. Alerts are indicated in red through the layers of the navigator to provide information on the location of the Altered device relative to the infrastructure and the business services impacted.

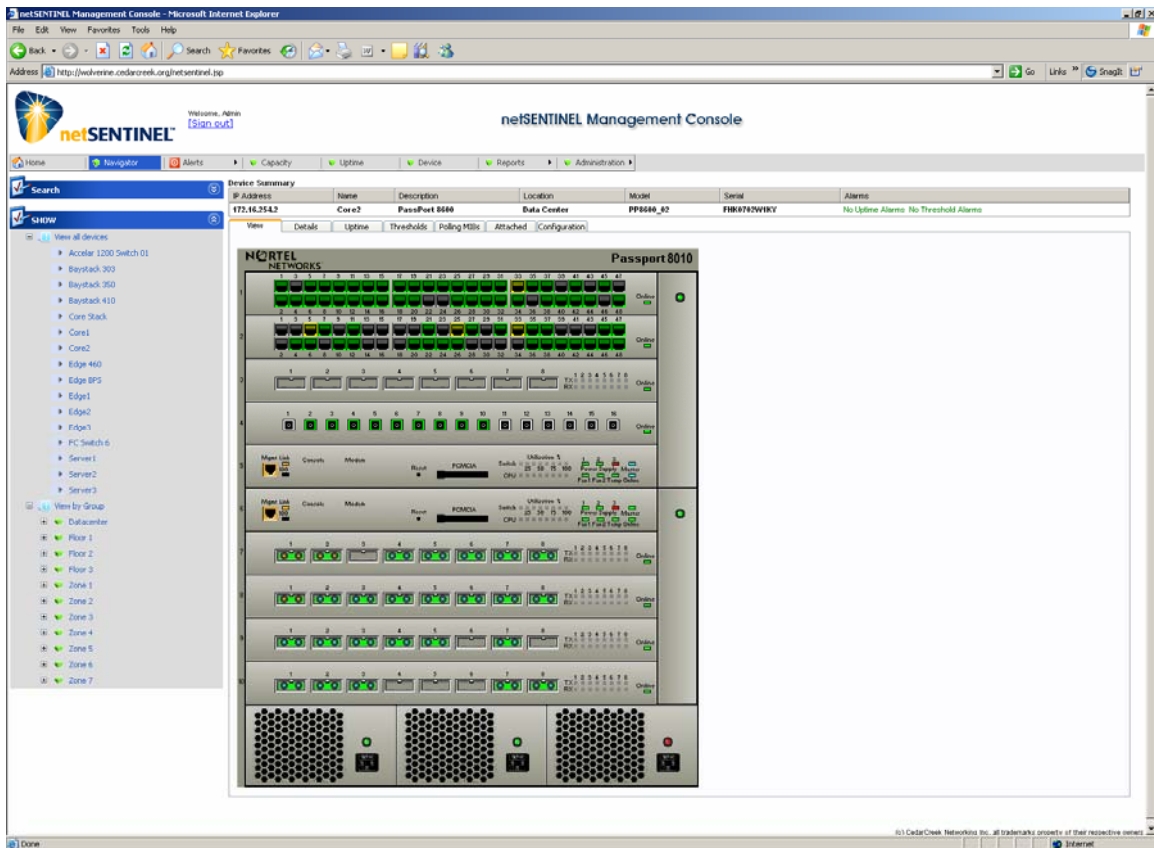
## Navigator – Zone Level Drill-Down



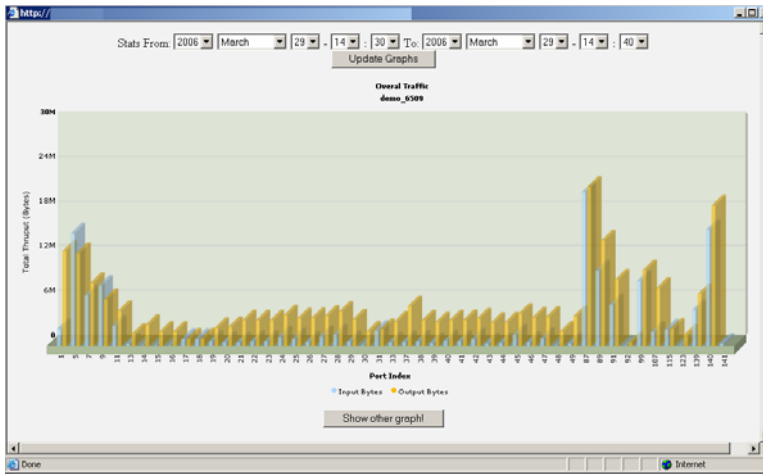
Detailed current status and historical information is available to support root cause analysis. Time selectable network traffic, bandwidth utilization, port / link speeds and up/down metrics are all available at the click of a mouse through the intuitive representation of each network device. Performance metrics for the Core Switch shown below are available at the switch level by clicking on the device, at the blade level by clicking on the blade, or at the port level clicking on a port. Performance metrics are selectable by user defined time periods.

The Network Device Interface for a switch Administration shows used and unused ports, with drill down from aggregate to port level performance metrics.

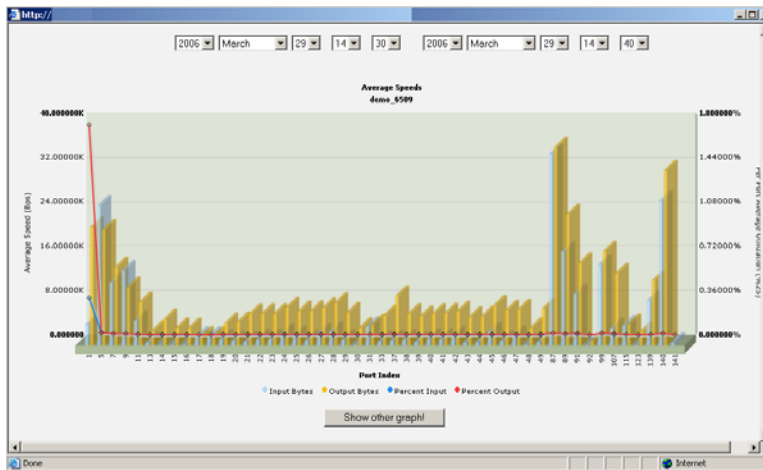
### Network Device Drill-Down



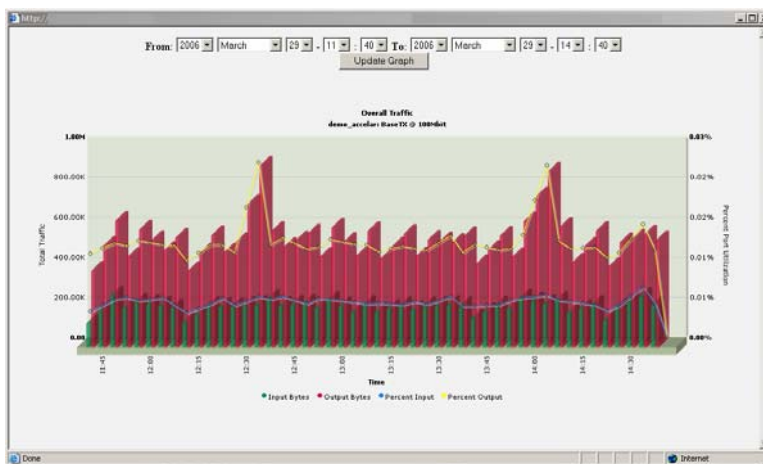
## Aggregate Device Port Traffic Drill-Down – All Ports



## Average Switch Port Speed Drill-Down – All Ports

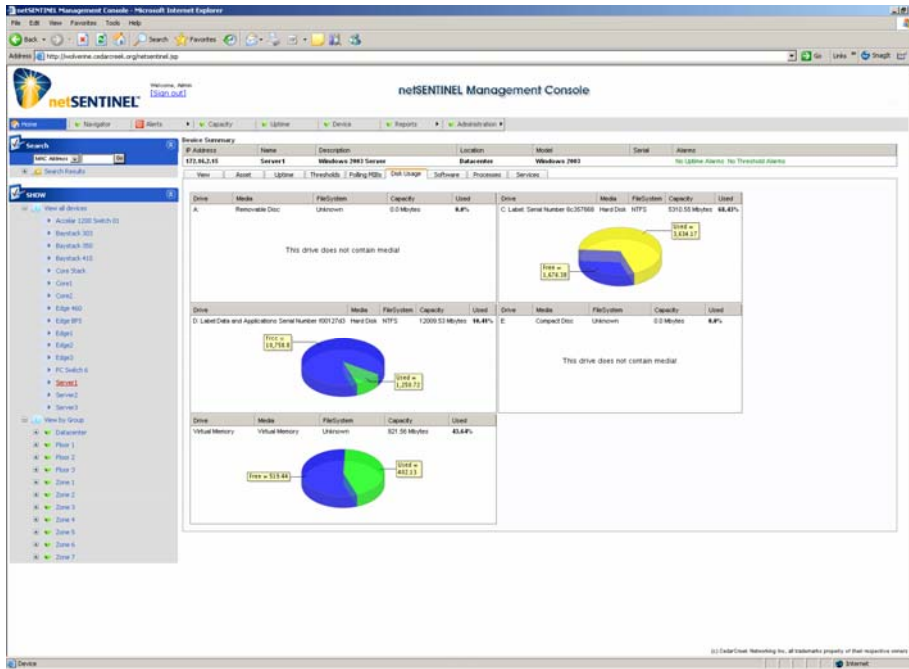


## Port Traffic Drill-Down

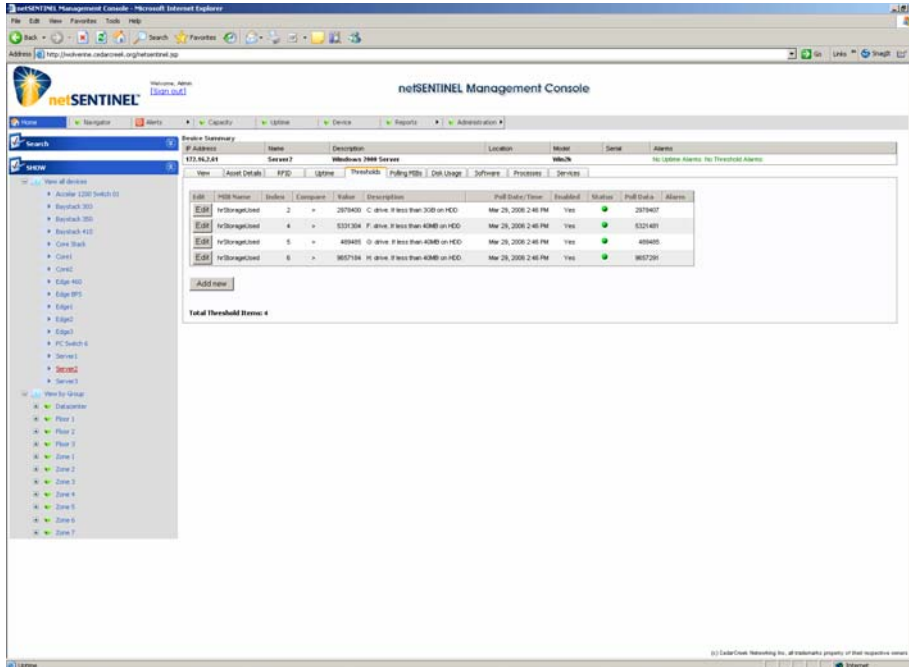




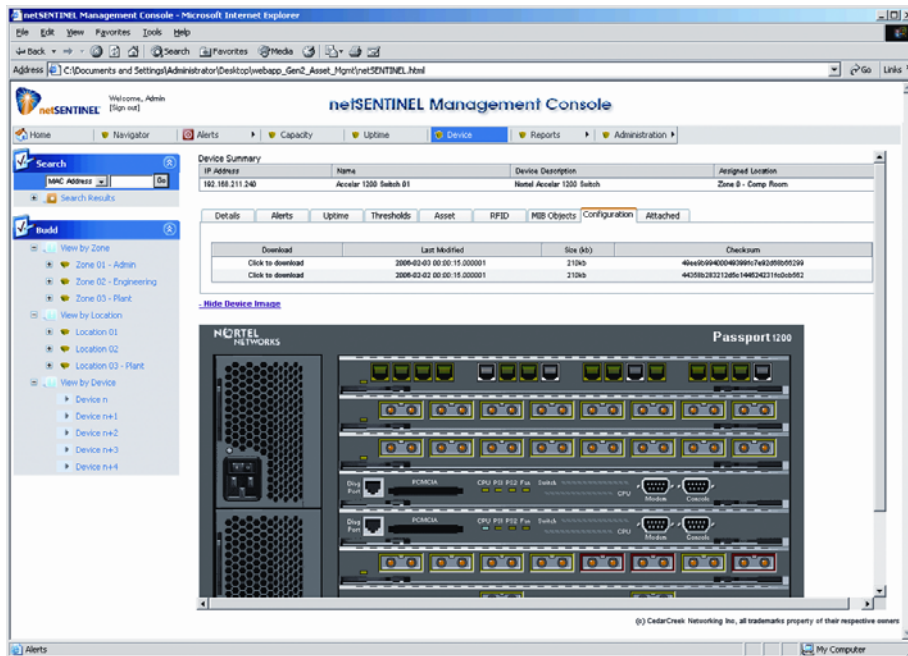
# Hard Disk and Virtual Memory Utilization



Thresholds for poll data are easily added, configured or modified for each device from a single screen.



Device configurations are automatically backed up, compared, and stored for 5 versions. They can be quickly downloaded in the event that a configuration roll-back is required, or a replacement device needs to be quickly configured.



## Asset Management

netSENTINEL's Asset Management Module provides complete automation of computer inventory and audits. The asset discovery and asset identification feature identifies hardware and software assets for Microsoft Windows 2000, XP, ME and 2003 operating systems. Hardware detection includes available manufacturer, product and serial information for all major components along with BIOS, processor, drive, interface and video and monitor information. Software OS detection includes OS product, version number and service pack information. Installed software detection includes software name, version, and license information. Computer inventory audits can be scheduled against selected devices or groups of devices to provide a continuous update of the status of your computer assets. Current audits can be compared with previous audits to identify and report changes to your inventory.

# Device Asset Management

The screenshot displays the netSENTINEL Management Console interface. The browser address bar shows the URL: <http://wolverine.cndereek.org/net Sentinel>. The console header includes the netSENTINEL logo, a user greeting "Welcome, Admin", and a "Sign out" link. The main navigation bar contains tabs for Home, Navigator, Alerts, Capacity, Uptime, Device, Reports, and Administration.

The central area is titled "Device Summary" and displays a table of assets:

IP Address	Name	Description	Location	Model	Serial	Alerts
172.16.2.15	Server1	Windows 2003 Server	Datacenter	Windows 2003		No Uptime Alerts No Threshold Alerts

Below the table, there are tabs for "View", "Asset Details", "IPID", "Uptime", "Thresholds", "Polling MHz", "Disk Usage", "Software", "Processes", and "Services". The "Asset Details" tab is active, showing a tree view of hardware components and a table of disk usage.

The hardware tree view includes:

- Processor & BIOS
- Hard Drives
- Optical Drives
- Network Adapter
- Video & Monitor
- Sound
- Keyboard & Mouse
- Printers
- Software
- Services
- Users & Groups
- OS Settings

The disk usage table shows the following data:

Letter	Mountable	Filesystem	Name	Size	Used	Free
C:	Yes	NTFS	Home	80,000 MB	19,000 MB	42,000 MB
D:	No	NTFS	Data	40,000 MB	38,000 MB	2,000 MB

The left sidebar provides navigation options, including "View all devices" and "View by Group". The "View all devices" section lists various network devices like switches and edge routers. The "View by Group" section lists physical locations such as Datacenter, Floor 1-3, and Zone 1-7.

At the bottom of the console, there is a footer with the text: "(C) CdeCreek Networks Inc. all trademarks property of their respective owners".

## **Incident and Change Management**

netSENTINEL's integrated trouble-ticket management system provides enterprise support for incident and change management. netSENTINEL Alerts can be configured to create incident tickets for forwarding and assignment to support personnel, or tickets can be created separately from the netSENTINEL interface by users with access to the ticketing module. Priority and status can be assigned for managing and tracking purposes. Updates to the ticket thread are captured and recorded and can be automatically forwarded by e-mail to relevant individuals or groups. All ticket detail, current and resolved is stored indefinitely for reference, reporting and trend analysis and provides auditable change and incident management records for regulatory compliance. For customers with existing or preferred third-party ticket management systems, netSentinel can be configured to pass Alert information to the third-party system through the management system API.

## netSENTINEL's integrated trouble-ticket management system netAssist

The screenshot shows a web browser window displaying the netAssist interface. The browser's address bar shows the URL [http://netassist.cedarcreek.ca/new\\_ticket.php](http://netassist.cedarcreek.ca/new_ticket.php). The page features the netSENTINEL logo and the ASSIST logo. A navigation menu includes links for Home, Submit Ticket, Open Tickets, Closed Tickets, and Logout. The main content area is titled "Submit New Ticket" and contains a form with the following fields:

- Your E-mail:** demo.customer@mycompany.ca
- Send to:** CedarCreek Support
- Subject:** XYZ Application is responding slowly
- Problem Description:** The xyz application is taking .....
- Impact Severity:** Support organization partially affected
- Onsite Visit Required:** (dropdown menu)
- Pager Alert:**  (for after hours, weekends, or holidays)
- Pager Message:** Call 519-xxx-xxxx, ticket opened by democustomer1, demo customer

A "Send Ticket" button is located at the bottom right of the form. At the bottom of the page, the copyright information reads: Copyright 2003, CedarCreek Networking Inc. [www.cedarcreek.ca](http://www.cedarcreek.ca) 519-571-9394.

## Reporting

netSENTINEL's extensive reporting capability provides one of the leading infrastructure report generators. Reports can be created for four main areas of infrastructure management; Availability, Response, Capacity, and Alert & Events. Reporting can be defined by any combination of devices or group(s) of devices and generated by a user-defined time period. The flexibility to generate reports on demand allows you to report on precise areas of your business, infrastructure, or equipment.

Availability reports provide key for Service Level Agreements (SLA) or process improvement initiatives (CPI). The Availability report provides aggregate uptime measures for the devices or groups selected over the time period along with a breakdown of availability changes over the time period selected. Availability trend analysis is reported and the trend forecast is displayed using trend extrapolation. A detailed report for each device is available and includes scheduled and unscheduled availability, outage count, and downtime results.

Response reports support SLA and CPI initiatives, but they also provide insight into the user experience by exposing critical infrastructure response / performance metrics. The Response report provides three levels of response for each device selected, fastest response, slowest response and average response, along with a breakdown of response changes over the time period selected. Response trend analysis is reported and the trend forecast is displayed using trend extrapolation.

Capacity reporting supports infrastructure planning and provides information to highlight capacity opportunities and / or early warning of issues. The Capacity report provides three levels of information for each device selected, average capacity utilization, peak capacity utilization and remaining capacity. A breakdown of capacity changes over the time period selected is provided. Capacity trend analysis is reported and the trend forecast is displayed using trend extrapolation.

Alert and Event reporting provides a historical analysis of tickets generated by netSENTINEL and recorded in netASSIST. This information provides the basis for understanding the type and number of alerts or events being generated and the service level of the individuals, groups, or organization responding. Tickets are analyzed by status, time, response, assignment, completion, and logged hours to provide management insight into infrastructure issues and responses.

## **Administration**

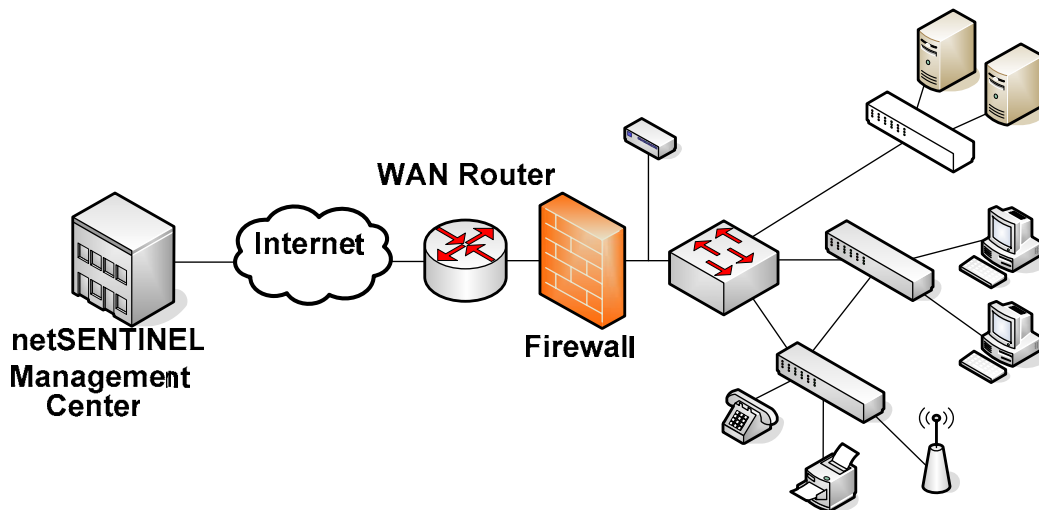
netSENTINEL includes managed administration as part of the basic netSENTINEL service to provide administrative support for your netSENTINEL. Whether it's a small change or a major extension in your infrastructure, our team of network engineers will update your netSENTINEL configuration quickly and expertly, according to your needs.

For those who prefer to configure netSENTINEL themselves, the administrative functions may be accessed through the netSENTINEL interface. Administrative and user access levels are customer defined and assigned against user credentials to expose the administrative functions of the service to authorized users. Administrative users have full control of their netSENTINEL configuration to create, edit, or delete individual components of the configuration. Administration of netSENTINEL is powerful and intuitive. Devices, groups, and links can be defined, and uptime and threshold scan settings can be created, deleted or modified at a granular level. So whether you prefer to administrate netSENTINEL or have our specialists provide configuration maintenance on your behalf, we make it easy for you to stay current with your management needs.

## **netSENTINEL Deployment**

netSENTINEL's remote management technology is the foundation of our delivery service. Our integrated platform is built on an architecture that allows for the rapid delivery of services designed to match your internal processes. Capabilities include infrastructure polling, monitoring, availability and threshold alerting, ticketing, root-cause diagnostics, asset management, asset tracking, reporting, and administration, each fully visible through our web-based customer portal.

With netSENTINEL there's no need to install software connectors or agents on your equipment. netSENTINEL delivers a self contained appliance ( netSENTINEL Agent ) to your location which is simply and easily installed on your network, behind your firewall, under your control at all times. The netSENTINEL agent requires access to the devices to be monitored and internet access to communicate with the netSENTINEL Management Center.



Simplified netSENTINEL remote-management deployment.

Once the netSENTINEL Agent is installed in your network, it automatically establishes a secure 3DES VPN connection to the netSENTINEL Management Center where it receives customized instructions for the polling of your network. The netSENTINEL agent continuously monitors your network, collecting and forwarding the data to the netSENTINEL Management Center where the data is automatically analyzed and correlated with predefined thresholds to determine if the status is within pre-defined thresholds to determine if the status is within acceptable operating tolerances or if further action in the form of an alert, ticket or report is required. The data is then stored to provide historical benchmark and trending information for troubleshooting, reporting or analysis. This information is delivered within seconds and is fully visible through our web-based customer portal.

## Conclusion

**netSENTINEL provides your business with a single tool to effectively monitor, manage and maintain the local, national or international corporate network infrastructure 24 hours a day, 365 days a year.**

**netSENTINEL provides a single web based repository that can be accessed from anywhere, allowing your business to store and access all asset, support and critical information with one web based tool.**



285 Fountain St. South  
 Cambridge, On N3H 1J2  
 P: 1.866.440.0312  
 F: 1.866.643.0365  
 www.netsentinel.ca