Predictive Monitoring and Alerting in Heterogeneous IP Networks
AdRem NetCrunch 4 White Paper
©2006 AdRem Software, Inc.

This document is written by AdRem Software and represents the views and opinions of AdRem Software regarding its content, as of the date the document was issued. The information contained in this document is subject to change without notice.

ADREM SOFTWARE MAKES NO WARRANTS, EITHER EXPRESS OR IMPLIED, IN THIS DOCUMENT. AdRem Software encourages the reader to evaluate all products personally.

AdRem Software and AdRem NetCrunch are trademarks or registered trademarks of AdRem Software in the United States and other countries.

All other product and brand names are trademarks or registered trademarks of their respective owners.

AdRem Software, Inc.
410 Park Avenue, 15th Floor
New York, NY 10022
USA

Phone: +1 (212) 319-4114
Fax: +1 (212) 832-4114
Email: adrem@adremsoft.com
Web site: http://www.adremsoft.com
GAIN A GLOBAL VIEW OF YOUR NETWORK ................................................................. 5

FUNCTIONAL OVERVIEW ........................................................................................... 6

NETCRUNCH IN A NUTSHELL ..................................................................................... 6
NETWORK DISCOVERY AND VISUALIZATION .......................................................... 7
Wizard-driven network discovery ............................................................................. 7
Map views of logical and physical network layers................................................... 7
Custom and filtered network views ......................................................................... 9
Graphic routing maps ............................................................................................... 10
Monitoring dependencies map ................................................................................. 11
Node information ..................................................................................................... 11
Easy map administration and customization ............................................................ 12
Remote access via a web browser ............................................................................. 13
Customizable GUI .................................................................................................... 15

SERVER MONITORING ............................................................................................. 16

NETWORK MONITORING ......................................................................................... 18
Device monitoring .................................................................................................... 18
Performance Monitoring via WMI ........................................................................... 19
Bandwidth monitoring ............................................................................................ 19
UPS systems monitoring ......................................................................................... 20
Network diagnosis tools .......................................................................................... 20

APPLICATION AND SERVICE MONITORING .......................................................... 22
Windows .................................................................................................................. 22
NetWare .................................................................................................................. 22
SNMP-aware applications ....................................................................................... 22
Network services ...................................................................................................... 23

SNMP-BASED MANAGEMENT .................................................................................. 24
Viewing and modifying SNMP parameters ............................................................... 24
Customizing SNMP views ....................................................................................... 25
MIB browsing .......................................................................................................... 25
MIB compiling ......................................................................................................... 26

EVENT MANAGEMENT ............................................................................................. 27
Alert-releasing events ............................................................................................. 27
Event notifications .................................................................................................. 27
Response actions ..................................................................................................... 28
Alert escalation and delay ....................................................................................... 28
Event logging .......................................................................................................... 29
SNMP trap handling ............................................................................................... 30
Syslog handling ...................................................................................................... 30

TRENDING AND REPORTING .................................................................................. 31
Performance trending ............................................................................................. 31
Trend Export .......................................................................................................... 32
Browser-based reports ............................................................................................ 32

CONTROLLING LARGE NETWORK ENVIRONMENTS ................................................. 35
Monitoring optimization ........................................................................................ 35
Monitoring prioritization ....................................................................................... 35
Event suppression ................................................................................................. 36
Efficiency on high-performance systems ............................................................... 37

CONCLUSION ............................................................................................................ 38

APPENDIX 1: NETCRUNCH AUDIENCE .................................................................... 39
APPENDIX 2: SYSTEM REQUIREMENTS ........................................................................... 40
APPENDIX 3: EDITIONS AND LICENSING ....................................................................... 41
ABOUT ADREM SOFTWARE ............................................................................................. 42
Gain a Global View of Your Network

Studies reveal that the majority of small and midsize IT teams have no monitoring solution implemented. If they have, usually the solution is inadequate and covers the IT infrastructure only in 30%.

In today’s corporate reality, the network drives the business. A company’s success is inextricably linked with its revenue-producing IT processes and services such as e-mail, Web site or order entry and billing systems. Even in small-to-midsize IT infrastructures with up to several thousand users, daily business operation relies on the seamless and uninterrupted interaction of a wide array of software and hardware components coming from many vendors. However, the growing demand for superior service and the evolution of business models constantly pushes the limits of the existing IT investments. This puts a heavy strain on network administrators who need powerful tools that would help achieve superior network visibility and streamline key service assurance duties.

In this situation IT shops can no longer manage various servers, routers, switches and other assets separately. They must take a more integrated approach that consolidates workloads and maps to business priorities. To achieve that, they need is a true fact-based picture into the health and relationships within their network infrastructures.

Providing cost-effective support in these administrative challenges is AdRem NetCrunch from AdRem Software. This easy-to-use program combines powerful topology visualization, agentless monitoring, alerting and troubleshooting with real-time performance trending and historical reporting. NetCrunch provides administrators with a multi-dimensional view of their network environment, allowing them to visually monitor, navigate and correlate diverse sources of data. This way the can minimize the time detect, to diagnose and repair problems. Using NetCrunch they can also become reliable participants in the running of an organization by creating business-relevant policies, predicting demand, reallocating resources in time, and reporting on service level compliance.

With NetCrunch, IT organizations in small-to-midsize enterprises get the functionality breadth and integration comparable to high-end solutions. At the same time, they can benefit from low acquisition costs, quick deployment, ease of use, and minimum resource usage they’ve come to expect from narrow-focused point tools. As a result, network, application and service uptime can be increased while expenses on training, consulting, deployment and maintenance can be kept to a minimum.
**NetCrunch in a Nutshell**

**Network visualization**
The core capability delivered by NetCrunch is the power to visually display an anatomy of the entire network infrastructure. As a result, administrators gain multiple perspectives on what is in the network and how all vital component parts are interconnected. This is possible via:

- Auto-discovery and display of logical and physical network topologies
- Periodic updates of the logical network views
- User-defined views of managed assets grouped by location, host type, vendor, IP address, business process, and several other criteria
- Remote access via a web browser to the program’s network data.

**Monitoring**
With NetCrunch, users can probe into the dynamically changing network behavior by accessing current, easy-to-read information. This way, they can tell at a glance what is and isn’t working inside hosts’ system resources, network services or applications. In some cases, it is even possible to anticipate impending problems. To that end, the program provides:

- Host/service availability and response time tracking
- Threshold-based monitoring of host and application performance using SNMP, Windows NT, and NetWare performance counters
- Detailed real-time diagnostic information
- Full-fledged SNMP management.

**Alerting and corrective actions**
NetCrunch early detects malfunctions in managed objects providing several ways to restore IT operations to the optimum level. With automated problem identification and event responses, users can react quickly and efficiently ensuring that service levels and users are not compromised. Key features in this functionality area include:

- Event notifications delivered to predefined users or groups via e-mail, modem, pager, ICQ, SNMP trap, syslog message, cell phone text message
- Automatic corrective actions, including NT service restart, system reboot, running of Windows commands, Linux scripts, Novell NLMs
- Flexible event management with customizable event logs, alert escalation and alert delay via monitoring dependencies
- Prepackaged diagnostic tools (graphical ping, traceroute, bandwidth scanner, service/port scanner, SNMP browser/editor).

**Trending and reporting**
Apart from the real-time information, NetCrunch delivers a wealth of historical performance data. In this manner, users can go beyond current issues taking up strategic activities such as capacity forecasting or consolidation of the existing assets. This can be done via:

- Collection of performance trends
- Real-time and long-term trend visualization
- Daily, weekly and monthly reports for various platforms, applications, and services
- Report customization and scheduled distribution via email.
Network Discovery and Visualization

Wizard-driven network discovery

NetCrunch can scan your network infrastructure discovering all subnetworks, servers, routers, switches, bridges, printers and other IP devices within it. It will also detect network services and applications running on each individual host.

Typically, the program scans network assets using SNMP and ICMP protocols; however, for a more accurate picture of the network, it can also use Active Directory, Windows Workgroups, and eDirectory.

To ease network discovery, you can use a special wizard where you can determine whether the program should use pre-defined discovery parameters (automatic mode) or ones specified by you (manual mode).

In the manual discovery mode, the program will scan only hosts matching your criteria. You can also specify SNMP community string, scanning range, scanning frequency, and services to be monitored. This gives you fine-grained control over the scope of discovery and monitoring.

At that stage, you can also configure the simplified monitoring. Then NetCrunch will only ping the status of less important hosts without monitoring their performance and generating alerts or reports. This way you can save resources for full-fledged monitoring of critical hosts.

Map views of logical and physical network layers

Having scanned the network, NetCrunch determines whether the discovered asset is a server, router, switch, printer, or any other device, assigns a device-specific icon to it, and arranges the icon on relevant network views. By default, the program identifies the following devices types:

- Windows NT, 2000, XP; Windows Server 2003
- UNIX/Linux (Linux, AIX, FreeBSD, Solaris)
- NetWare from 3.x to 6.x; Novell OES
- Switches
- Routers
- Bridges
- Network printers
- Wireless Access Point

However, you can freely extend this list with many more device types.

The most fundamental type of network view in NetCrunch is a graphical map that provides a synthetic overview of the status of network connections, hosts, services and applications. The most common type of a map display created by NetCrunch represents the logical network topology based on the IP addresses of different nodes. This map variety can be periodically updated to accommodate nodes and services added or removed from the network after the last discovery.
Another way of illustrating the network environment is a map of the physical topology that documents the actual structure of the network. By clicking on a particular switch in a top level summary view of the entire physical topology, you can easily access a more detailed view of the selected segment. This way you can easily check which devices are connected to specific ports on a switch or a wireless access point.
NetCrunch provides a true-to-life picture of Cisco switches in networks where multiple remote networks and VLANs are configured. In this case, the program reads a switch list in a given VLAN and then retrieves information from forwarding tables for all configured VLANs.

**Custom and filtered network views**

With NetCrunch, you can tailor graphical representations of your network to suit your needs by manually creating customized maps. You can do this by opening a blank map and adding any number of nodes to it.

A custom view created in this manner may illustrate a business process. You can for example visualize your company’s web services by creating a map populated with a router, firewall and web servers. Thus, critical resources can be controlled without sorting through a large number of devices.

![Figure 3. Example of a custom network view](image)

A more advanced variety of a custom view is a dynamically updated filtered view of the network. In this case, NetCrunch uses predefined filtering criteria to automatically pool together specified network nodes in a separate dynamic view. Filtering criteria available in NetCrunch include:

- Node type (router, email server, switch, etc.)
- Windows Domain/eDirectory
- Location
- IP address
- DNS name
- Last alert time
- Node state
- Network service list
- Number of minutes since node insertion
- Number of minutes since last node state change
- Number of unacknowledged alerts
- Simplified monitoring

* Feature available only in the Premium XE edition of AdRem NetCrunch 4.x
You can also create your own filtering criteria by assigning descriptions to managed objects. Importantly, each filtered view may be configured with its own monitoring, alerting and reporting policy, enabling you to quickly respond to and diagnose events in critical business operations.

Apart from map views, the program offers other ways to present network data. It can show a bar chart or pie chart summary of the node state or side-by-side display of ten best/worst nodes in terms of availability. It can also present a separate chart view grouping real-time trend charts displaying selected performance counters retrieved via SNMP or from Windows or NetWare systems.

Another common view type is a table that lists an index of all or selected network nodes (e.g. only Windows, NetWare or SNMP-enabled nodes) along with a summary of real-time status and usage statistics about each node.

With customized and filtered network maps and other types of network views, NetCrunch provides the way to see their complex networks in an easy to grasp manner. You can conveniently perform at-a-glance checks of multiple functional and organizational aspects of your IT environment.

**Graphic routing maps**

NetCrunch can also be used to create informative routing maps that reflect connections between particular nodes on the network. These maps are generated by discovering routing tables held on hosts and help to monitor the availability and reliability of all routing connections. For example, if you need to monitor any Website running on an external provider, NetCrunch allows you to view all the intermediate hops and determine if a problem lies with the host provider system, or anywhere within the intermediate hops.
Figure 5. A routing map

Monitoring dependencies map

Another vital map variety available in NetCrunch is related to the idea of node monitoring dependencies. Namely, the program builds a map of node monitoring dependencies that were discovered by the program as well as configured by the user. In other words, a map of this kind shows parent nodes along with ones that have been found or configured to be depending on them.

Node information

Map objects in NetCrunch are color-coded, which means you can check at a glance if for example your email and backup servers (or any other critical devices and services) are functioning properly. With an easy-to-read timely indication of problems, users can quickly diagnose emergencies by accessing detailed results of real-time network measurements.

Right clicking on the problem node on the map or in the table brings up a handful of critical information such as node operational status and uptime, last response, binding interfaces, average and maximum response time, percentage of packets lost or summarized SNMP and system-specific information.

The node summary view may also display a list of non-responding services, the number of interfaces down, and unacknowledged alerts. For each network service on a node, a history window can be opened showing a summary of service events, last 24 hour distribution and hourly averages of service response time, packet loss and availability. In case of Windows NT/2000/XP nodes, users can also quickly diagnose the status Windows services.

Another useful function is the Node Notes option that allows users to add their own notes to each node.
Easy map administration and customization

For easy selection of specific objects and navigation between network views, NetCrunch views are displayed as a directory tree. Individual maps, node objects and their properties can be easily assembled into larger entities called atlases. Maps can be easily printed. Maps and atlases can be saved, backed up, restored, exported, and thus eases historical analysis of topology changes. In addition, NetCrunch provides sophisticated data sorting, filtering, search and drill-down techniques. The bottom line is that you can meaningfully order and view the relevant graphical information about network hosts no matter where these hosts are located, what platform they're running, or what vendors they represent.

The NetCrunch mapping mechanism is highly configurable. You can personalize map and atlas layout and graphics by adding, removing and repositioning map objects, importing custom shapes and images (such as building plans, floor plans, geographic maps, etc.), and changing the background, icons, colors and sizes of almost every element. In addition, to easily switch between multiple map views you can add links from one map to another.
Remote access via a web browser

For convenient remote network administration, NetCrunch can also be used from a Web browser. The program’s Web interface supports SSL encryption and policy-based access to NetCrunch data and functionality. This way, multiple operators with unique read/write or read-only remote access profiles can simultaneously use NetCrunch to securely access different segments (views) of the network and different program operations. This can be especially important in large multi-location organizations with multiple in-house or outsourced network supervisors, where there’s a need to enforce secure administrative hierarchy and collaboration.

<table>
<thead>
<tr>
<th>Program object</th>
<th>Permission type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program</td>
<td>● Change Web access options</td>
</tr>
<tr>
<td></td>
<td>● Change Web access password</td>
</tr>
<tr>
<td></td>
<td>● Add node to monitor</td>
</tr>
<tr>
<td></td>
<td>● Use iTools</td>
</tr>
<tr>
<td>Atlas Map</td>
<td>● View alerts</td>
</tr>
<tr>
<td></td>
<td>● View reports</td>
</tr>
<tr>
<td></td>
<td>● View map</td>
</tr>
<tr>
<td></td>
<td>● Discover network services</td>
</tr>
<tr>
<td></td>
<td>● View node monitoring properties</td>
</tr>
<tr>
<td></td>
<td>● View node properties</td>
</tr>
<tr>
<td></td>
<td>● View node status</td>
</tr>
<tr>
<td></td>
<td>● View Windows NT services</td>
</tr>
<tr>
<td>Node</td>
<td>● View reports</td>
</tr>
<tr>
<td></td>
<td>● View node monitoring properties</td>
</tr>
<tr>
<td></td>
<td>● View node properties</td>
</tr>
<tr>
<td></td>
<td>● View node status</td>
</tr>
<tr>
<td></td>
<td>● View Windows NT services</td>
</tr>
</tbody>
</table>
By properly distributing Web-enabled access to NetCrunch, the Administrator can transfer administrative responsibility for specific program resources and tasks from a central higher authority to a lower authority.

Unlike in many other solutions, NetCrunch’s web interface is provides the same methodology and graphical lay-out as the Windows client instance of the program. Because the program ships with a built-in Web server, you can access NetCrunch via a Web browser without configuring an additional HTTP server.

Another useful capability available in NetCrunch’s remote access is the option to log all remote access sessions. As a result, network supervisors can easily determine what users connected remotely to NetCrunch, at what time, from what address and what tasks they performed.

The following is a list of remote access operations available in NetCrunch:

- View a NetCrunch atlas
- View a NetCrunch event log
- Generate/view reports
- Access diagnostic tools
- Delegate access rights to program objects and operations to multiple users
- Establish 3 or unlimited concurrent remote connections
- View current remote users and log them off
- Use Web browsers such as Internet Explorer, Firefox, Mozilla and Netscape
Customizable GUI

NetCrunch ships with a highly customizable GUI. With the window docking capability, users can freely configure multiple program windows in a single docking site. When combined with the program’s multi-display capability, this can used to display one docking site – containing for example the Network Atlas and Network View windows – in one monitor, and another docking site with other network view windows in another monitor (in maximized size) or on an overhead projector. If more display devices are setup on the machine where NetCrunch is running, users can create additional docking sites with selected program windows in each.
Server Monitoring

Using NetCrunch, you can retrieve and graph performance information about Microsoft Windows or Novell NetWare servers using operating system-specific performance counters. This way you can visually monitor and configure alerts on many crucial counters available in Windows or NetWare systems, especially ones related to:

- Server performance (CPU, memory, disk)
- Bandwidth utilization
- Network services (POP3, HTTP, FTP, Telnet, etc.)
- System applications
  - Windows NT services and applications (e.g. MS SQL, Oracle, MS Exchange, MS IIS, and Active Directory)
  - NetWare Loadable Modules (percentage utilization, allocated memory, corrupted nodes, memory free, memory used, total memory)

However, you can also control other server systems, including critical UNIX-based server platforms such as Linux, FreeBSD, HP-UX, Solaris and AIX, by utilizing the program’s powerful SNMP management capabilities. NetCrunch uses SNMP v1, v2 and v3 standard to allow you to track and manage vital performance and resource utilization parameters on virtually any network server instrumented with SNMP agents. On each monitored server counter, you can set up proactive thresholds, which when breached will initiate an alert notification or corrective action (See "SNMP – based Management" on page 24).

For prioritized server control, you can place all or selected Windows, NetWare or SNMP-aware servers in separate network views and define system-specific monitoring and alerting policies on a per group basis. You can also create chart views showing real time trends of selected performance counters as well as display their history graphs.

In addition, NetCrunch can monitor connectivity and response time of 60 predefined network services and application services running on top of your servers. This is extremely useful, as many vital applications depend on various application services for their faultless operation. This way you can track crucial business-relevant application services, such as directory services, web services, email services, database services and network services.

The following is a list of server monitoring and management capabilities available in NetCrunch:

- Check device operational status based on SNMP agent availability and response time
- Retrieve, monitor and chart SNMP, Windows and NetWare performance counters
- Modify any writeable SNMP v1, v2 and v3 counter
- Create customs views of servers
- Import vendor-specific MIBs to extend server manageability
- Capture SNMP traps and syslogs sent by your server, and subsequently log, redirect or convert them into a NetCrunch event
- Setup complex alerting rules using proactive performance thresholds
- Schedule remote program and script execution on your server
- Print SNMP data about your servers and export it to XML, HTML, Microsoft Excel, or comma delimited files
Figure 10. Performance view of Windows server charts
Network Monitoring

Device monitoring

NetCrunch uses information from ICMP, SNMP, Network Neighborhood, eDirectory to identify, map and manage a wide selection of network devices instrumented with SNMP v1, v2 and v3 agents (See “SNMP Management” on p.). These include routers, switches, hubs, wireless access points, gateways, printers and firewalls from a wide array of multiple vendors such as Cisco or 3Com. Apart from discovering network devices, the program detects over 60 network and application services running on these devices.

The program is preconfigured with a list of devices that it can identify automatically, however, you can freely extend this list of using the program’s Device List Editor. As a result, NetCrunch can correctly recognize, map and monitor virtually all the devices that reside in your network.

A snapshot view of any device’s performance is possible via real-time gauges or charts. All devices monitored with SNMP can be presented in a single table, so that their utilization can be compared in real time on a single screen. The advantage is that instead of having to compare several summary views from different monitoring applications, users can view disparate resources and metrics consolidated in a single console view.

You can leverage vendor-specific SNMP monitors to track and setup alerting thresholds on virtually any host-related variable available via SNMP. The following are examples of key parameters that can be tracked and alerted on for routers, switches and printers:
Application and Service Monitoring

### Device type

<table>
<thead>
<tr>
<th>Device type</th>
<th>Sample monitored parameters</th>
</tr>
</thead>
</table>
| Router      | • CPU utilization
             • Errors and discards
             • Memory utilization
             • Voltage and Temperature
             • Buffer statistics (hits, misses, failures)
             • Service response times
             • Interface status |
| Switch      | • CPU utilization
             • Errors and discards
             • Memory utilization
             • Port traffic
             • Port utilization and errors
             • Connection load |
| Printer     | • Interface traffic
             • Paper out/low
             • Paper jam
             • Toner out/low |

You can perform a variety of monitoring and management operations of your devices such as:
- Check device operational status based on SNMP agent availability and response time
- Retrieve SNMP v1, v2, and v3 performance data and graph SNMP performance counters
- Modify any writeable SNMP performance counter
- Browse a library of over 450 most widely used third-party MIBs to create personalized SNMP views of device MIB data
- Import and add vendor-specific MIBs to the program’s MIB database
- Capture SNMP traps and syslogs sent by your devices and subsequently log, redirect or convert them into a NetCrunch event
- Define proactive performance threshold alerts that indicate degrading device performance
- Schedule a remote program and script on a Windows, NetWare or Linux devices
- Report on any monitored device performance parameter
- Print SNMP data and export it to XML, HTML, Microsoft Excel, or comma delimited files

### Performance Monitoring via WMI

NetCrunch comes predefined with the AdRem WinTools application. WinTools use Microsoft’s Windows Management Instrumentation (WMI) to provide extensive monitoring of nodes running the Windows operating system. Specifically, it allows users to:
- examine basic information about the Windows computer one is connected to
- display and terminate processes running on the computer
- perform system shutdown, log off or restart of the local or remote Windows computer
- view, start, stop and pause Windows services currently installed on the Windows computer
- manage Windows log files on the computer (namely: Application, Security and System)
- inspect hardware and software inventory on the Windows computer to which you are connected
- to explore all namespaces and WMI (Windows Management Instrumentation) classes on the computer and create new queries for information on desktop systems, applications, and other components.
Bandwidth monitoring

Using NetCrunch, you can easily analyze the network traffic on your switches or on any other SNMP-enabled device (router, workstation, wireless access point). The program makes it easy to set up thresholds on switch performance, interface utilization (packets transmitted, error rates, collisions, discards for each interface), through traffic or any other variable available via SNMP v1, v2 and v3. As a result, you can determine the up-to-the-minute load on a machine, or its peak and average activities, which can ease base lining and making informed upgrade decisions.

UPS systems monitoring

By way of SNMP NetCrunch can be used to supervise vital environmental monitors and Uninterruptible Power Supply (UPS) systems. It can also capture syslogs and SNMP traps coming from these systems. As a result, you can monitor and be alerted on a variety of crucial functions, including: UPS load, battery status, output voltage, output current, voltage, temperature, power supply, fan performance.

When critical conditions occur in these crucial functions, NetCrunch can notify users via a wide range of methods such as e-mail, modem, pager, ICQ, SNMP trap, or cell phone text message. It can also execute a predefined script or program.

Network diagnosis tools

For in-depth analysis of the network situation, NetCrunch offers a package of handy IP and SNMP toolset that includes utilities such as: Ping, bandwidth scanner, reliability test, Traceroute, network scanner, SNMP Info, MIB Browser, and DNS Lookup.

Ping allows you to verify the connectivity of a remote computer by sending and receiving test ICMP (Internet Control Message Protocol) echo packets to it, and measuring its response time (in milliseconds).

Trace Route is used primarily to trace a route from a local computer to any other computer on the Internet. In other words, it determines how many hops there are between the local and target machine, and displays response time, name, and IP address of each intermediate hop. This tool can be used to detect routing anomalies, and verify if a specific connectivity delay is local or global.

With Bandwidth, you can graph transfer rate (number of packets received, sent, and lost) between your and other computer in the network. On the other hand, the Reliability tool is ideal for verifying the quality of the link between local and other device in the network. It sends a series of packet samples, incrementing the size of each successive sample. This way you can check the bandwidth for packets of differing sizes.

NetCrunch's network scanner is used to discover open ports and services running on a given host, check their current status and response time, and scan the whole local network to detect nodes within it. You can restrict the list of services or ports to be checked to specific or well known ones, or to ports usually used by trojans.
AdRem NetCrunch 4.x

Application and Service Monitoring

![Figure 12. Service scanner](image)

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
<th>Protocol</th>
<th>Port</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP</td>
<td>SSL/TLS Secure Shell</td>
<td>TCP</td>
<td>22</td>
<td>OK</td>
</tr>
<tr>
<td>FTP</td>
<td>&lt;10 Simple Mail Transfer Protocol</td>
<td>TCP</td>
<td>21</td>
<td>OK</td>
</tr>
<tr>
<td>POP3</td>
<td>&lt;10 Post Office Protocol - Version 3</td>
<td>TCP</td>
<td>110</td>
<td>OK</td>
</tr>
<tr>
<td>PING</td>
<td>&lt;10 Ping (Internet Control Message)</td>
<td>ICMP</td>
<td></td>
<td>OK</td>
</tr>
<tr>
<td>TFTP</td>
<td>15 File Transfer Protocol</td>
<td>TCP</td>
<td>20</td>
<td>OK</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Server</td>
<td>UDP</td>
<td>53</td>
<td>OK</td>
</tr>
<tr>
<td>Web</td>
<td>Windows Internet Name Server</td>
<td>UDP</td>
<td>80</td>
<td>OK</td>
</tr>
<tr>
<td>WINS</td>
<td>Windows Internet Name Server</td>
<td>TCP</td>
<td>67</td>
<td>OK</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
<td>TCP</td>
<td>25</td>
<td>OK</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
<td>TCP</td>
<td>21</td>
<td>OK</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
<td>TCP</td>
<td>465</td>
<td>OK</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
<td>TCP</td>
<td>21</td>
<td>OK</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Server</td>
<td>UDP</td>
<td>53</td>
<td>OK</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
<td>TCP</td>
<td>80</td>
<td>OK</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol</td>
<td>TCP</td>
<td>443</td>
<td>OK</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol</td>
<td>UDP</td>
<td>5060</td>
<td>OK</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
<td>TCP</td>
<td>389</td>
<td>OK</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
<td>TCP</td>
<td>22</td>
<td>OK</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
<td>UDP</td>
<td>5000</td>
<td>OK</td>
</tr>
<tr>
<td>SFTP</td>
<td>Secure File Transfer Protocol</td>
<td>TCP</td>
<td>22</td>
<td>OK</td>
</tr>
<tr>
<td>Telnet</td>
<td>Text Terminal Protocol</td>
<td>TCP</td>
<td>23</td>
<td>OK</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
<td>UDP</td>
<td>5000</td>
<td>OK</td>
</tr>
<tr>
<td>SFTP</td>
<td>Secure File Transfer Protocol</td>
<td>TCP</td>
<td>22</td>
<td>OK</td>
</tr>
</tbody>
</table>

Figure 12. Service scanner
Application and Service Monitoring

Windows
NetCrunch allows you to conveniently monitor performance of applications running on top of Windows-based nodes. Firstly, you can setup application-related events on network services. For example, to track Microsoft Exchange applications, you can have NetCrunch monitor – as well as chart and report on – % Packets Lost or Round Trip Time for POP3 and SMTP network services.

Secondly, you can configure the program to monitor Windows-specific application counters available for the server and define threshold conditions on these counters. Many useful vital performance counters can be monitored this way. For example, in the case of Exchange servers, you can monitor counters such as:
- SMTP Server\Remote Queue Length
- MSExchangeIS Mailbox\Send Queue Size
- MSExchangeIS Mailbox\Receive Queue Size
- MSExchangeIS\RPC Requests
- MSExchangeIS\RPC Average Latency

Apart from monitoring and reporting on server-related application services, NetCrunch can also track and control Windows NT services. You can use the program to define events that will indicate the change of state of a selected Windows service. This way you can have the program notify you, or perform a corrective action, when any specified NT service changes state, in other words, when it is stopped, run, or paused. In response to one of any of these NT service state changes, you can have the program start, stop, pause, restart or continue a given NT service.

NetWare
NetCrunch provides an easy way to monitor, alert and report on the performance of the NetWare Loadable Module (NLM) programs that run on your NetWare operating system. To do that NetCrunch reads native NetWare counters. The following NLM-related performance objects can be tracked, trended and alerted upon via NetCrunch:
- Percentage utilization
- Allocated memory
- Corrupted nodes
- Memory free
- Memory used
- Total memory

SNMP-aware applications
NetCrunch provides extensive monitoring for many of the business-critical network services and applications that support SNMP polling and traps. This way you can use the program to track crucial application services, such as directory services, web services, email services, database services and network services, antivirus and backup.

By handling SNMP traps and retrieving information from application-related SNMP monitors, NetCrunch can monitor and alert on critical application performance metrics such as:
- Traffic utilization
- Conversations
- Error conditions
- Resource utilization
- Response time
- Data captures
Network services

The program delivers out of the box availability and response time monitoring for over 60 TCP/UDP network services. Moreover, you have an option to create/configure third party network services to be monitored.

The program's network service monitoring mechanism is highly configurable and each node service can have a separate polling interval. Because all network services can be configured to be checked at regular intervals, you can detect at a glance interrupted connections or malfunctions in services. You can conveniently modify polling parameters such as timeout, time restriction, frequency or number of packets sent.

To minimize polling traffic, the program can be set not to monitor services enabled on a node when this node is down. Similarly, if a router goes down all the underlying devices will not be polled. In addition, you can view real-time/ historical statistics about each monitored service in chart views.

The following is an example of Internet service functions that you can track via NetCrunch's network service monitoring capability:

- HTTP (availability of HTTP and HTTPS sites)
- FTP (availability of an FTP server/site)
- ICMP ping (monitors a remote host's availability)
- DNS (DNS server)
- SMTP (mail server)
- POP3
- NNTP
- TCP port function (Checks if a port is responding and verifies its response)
- NTP (status of time servers)

Figure 13. Service editor window
SNMP-based Management

Viewing and modifying SNMP parameters

With NetCrunch, advanced SNMP management is possible without in-depth expertise in this network management standard. You can access extensive SNMP information without navigating MIB trees (database containing device parameters) or knowing specific Object Identifiers (OIDs). Particularly notable is the program’s full support for SNMPv3 Authentication and Encryption – this way NetCrunch ensures that only authorized operators are able to monitor and configure SNMP-aware nodes across your entire IT organization.

There are several options for viewing SNMP data in the program. The easiest one is a tabular view displaying all SNMP-aware nodes along with the data on their configuration, status and performance. To gain a more exhaustive view, you can right click a specific node and access a wealth of SNMP information. Alternatively, detailed SNMP information can be accessed via the program’s SNMP View module that allows you to examine predefined SNMP snapshots of a specific device. The data within SNMP View is organized in a user-friendly, collapsible tree hierarchy. You can easily define new groups, forms and sections thus creating your own SNMP snapshots of the device. In case of parameters in read/write mode, you can remotely set their values, which can be useful for remotely reconfiguring and troubleshooting routers, switches, or network printers.

All SNMP information presented by NetCrunch can be exported to a file (XML, HTML, Microsoft Excel, or comma delimited) and printed. The latter option can serve as a powerful method for creating a thorough inventory of owned assets and for identifying underutilized resources. For example, an analysis of all switches in a network may reveal that many of them run an insufficient number of cards and connections, and thus can be consolidated into fewer assets.
Customizing SNMP views
Importantly, the variables displayed in SNMP View can be fully customized using another built-in tool called SNMP View Editor. The module allows users to define/add simple values and derived expressions to a given SNMP view. This is especially important because OID values are just counters and, in fact, to become meaningful statistics (such as Percent Errors, Volume, Percent Used) they need to be aggregated. As a result, SNMP View can display the result of a simple expression calculated from two SNMP variables/columns or convert an ambiguous form of an SNMP variable/column into a more human-readable form, for example by converting a device status numerical value to an icon or to a textual format.

MIB browsing
Another vital part of NetCrunch SNMP management capability is MIB Browser. It allows you to load a MIB file of an SNMP device and traverse its collapsible tree in order to view all available tables and variables, and read OID descriptions. Just like in the case of the SNMP View part of the program, if an object value in a MIB structure of a device is writeable, it can be remotely modified.

SNMP Manager's MIB Browser ships with a comprehensive MIB library containing customizable definitions for over 450 of the most widely used third-party MIBs. MIB file is a sort of a gateway to a device – it stores descriptions of the object hierarchy and attributes on the device. As a result, walking a MIB tree and setting values via MIB Browser can greatly enhance your device monitoring and management efficiency.
SNMP-based Management

MIB compiling

NetCrunch ships with a MIB compiler utility that provides a useful way to extend device manageability. You can use it to import vendor-specific MIB, edit their contents and compile them. As a result of the compiling operation, the new MIB is added to the program’s MIB database. This way you can use all the forms, tables, panels, and traps defined in vendor specifications to monitor and control significantly more aspects of all SNMP-enabled devices defined by this MIB.

Another useful feature on AdRem’s MIB Compiler is the ability to edit and recompile existing MIBs, which allows you to troubleshoot MIBs or create private extensions to better suit your management needs. During editing, you can quickly search for a specific string within the MIB file using the Find option.
Event Management

Alert-releasing events

The main purpose of monitoring in NetCrunch is to detect events that indicate faults or malfunctions in connections, devices, systems, services or applications. Once NetCrunch generates an event, the event is logged in the program's event database for further fault analysis. Events are usually configured to notify users and automatic actions aimed at diagnosing and resolving the problem.

A special type of NetCrunch event is a breach of a threshold condition. Typically, thresholds are configured to detect an undesirable condition and generate an event. The following advanced alerting threshold conditions are available: rise/fall, unexpected rise/fall, no value/received value, state is equal/is different. Interestingly, NetCrunch allows you to assign thresholds to "virtual performance counters". Virtual counters are specific for NetCrunch and are defined as an expression using real counters retrieved from devices. Virtual counters may be displayed in real time performance charts, or an alert policy may be configured to notify the administrator when a threshold has been crossed. Using them you can for example create an interface bandwidth utilization counter calculated from three different factual counters: "bytes received/second", "bytes sent/second" and "interface speed".

Typical alert-releasing events in NetCrunch include:
- SNMP threshold broken
- Windows performance threshold breached
- Novell NetWare performance threshold broken
- Network service availability threshold breached
- Host up/down
- Host interface up/down
- Network service up/down
- Reception of an SNMP trap
- Change of the node state within a specified time frame
- Reception of a syslog message
- Windows service stopped, running, paused
- NetCrunch Hearbeat (this event is generated on an ongoing basis at specified time intervals)
- Map action (node is discovered, deleted, enabled, disabled)

Event notifications

In response to any of the above event, NetCrunch can immediately issue a notification or set of notifications to specified recipients (See "Alert escalation and delay" on page 27). This way you gain the assurance that you will be the first to know of any problem in the network. The following are available notification options:
- Desktop notifications (alert bar, alert dialog, sound alert, speech alert)
- SNMP trap
- Syslog message
- Beeper via modem
- ICQ message
- SMS (via ICQ, Internet, modem)
- Pager (via modem or SSNP)
- GSM modem
- E-mail (via built-in server or external SMTP server)
Response actions

NetCrunch events can also trigger the automatic execution of local or remote corrective actions. These include:

<table>
<thead>
<tr>
<th>Control actions</th>
<th>Diagnostic actions</th>
<th>Logging actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Run a remote program/script on Windows, NetWare and Linux machines</td>
<td>● Perform Traceroute and add test results to an alert message</td>
<td>● Write to file</td>
</tr>
<tr>
<td>● Set an SNMP variable</td>
<td>● Add network service status to an alert message</td>
<td>● Write to Windows Event Log</td>
</tr>
<tr>
<td>● Restart/shutdown a computer (Windows, NetWare, Linux/Unix)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Control a Windows service (Start, stop, pause, restart, continue)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Terminate a process</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Set node monitoring state (enable/disable node monitoring)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Start a computer via a Wake on LAN network command</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

One of the most powerful features of NetCrunch is the ability to write and schedule remote scripts to be executed as responses to events. This provides you with virtually unlimited options of extending the program's management functionality. The script types available in NetCrunch include Windows programs, Windows scripts, Linux/Unix scripts and NetWare scripts. Some of these scripts are already predefined in the program. These are:

- Start Windows SNMP service
- Reboot Linux node
- Restart Linux SNMP service
- Down NetWare server
- Shutdown Linux node
- Restart NetWare server
- Load FTP NLM
- Unload FTP NLM

For prioritized control over the entire network, you can institute alert policies on four separate levels, going from the top multi-map atlas level, through a map or a submap, an individual node (a server, router, etc.) down to a particular service running on a node. The bottom line is that you don’t have to configure alerts one by one, which can save a considerable amount of your time.

Alert escalation and delay

NetCrunch provides the facility to escalate alerts to higher levels of support. This means that one NetCrunch event may generate a specific set of actions at different times and issue different types of notifications to different recipients. This system allows you to assign responsibility for handling events to other staff members in a way that matches their qualifications and the times they are on call.

Example:

- You may configure one type of action to happen immediately after the event happens, for example “send a desktop warning message to a junior administrator”.
- You may schedule another action to occur after 5 minutes, for example “send an SMS to an administrator”.
- After 30 minutes – if the issue is still unresolved – yet another action may be initiated, for example “send an email to a supervisor”.

You can setup the last action to be repeated at user-defined time intervals to ensure that the problem will be finally addressed by the right person.

Additionally, you can setup delays on specific events. As a result, NetCrunch will not fire an alert immediately on detecting the event (for example “device down”) but only after the emergency condition (device inaccessibility in this case) continues for a specified time. However, if within the specified time window another event happens that cancels the condition – in this case “device up” – the alert will be automatically suppressed. This way, NetCrunch eliminates many false alarms that might indicate temporary spikes ensuring that you address only real threats.

Figure 17. Example of an alert escalation policy for a Host DOWN event

**Event logging**

When a specified event happens on a particular node, NetCrunch can store it in its own SQL event database for further analysis. With a click of a mouse, you can access a number of crucial details about events for an individual node or for the whole view or atlas, including data such as:

- Event severity
- Time and date
- Host name and IP address where the event occurred
- State of the host
- Event resolution
- Alert message
- Owner, source, category, and more.

For example, seeing event for a particular host can provide information whether a current problem is recurring or intermittent one. Logged events can be easily grouped in custom views, filtered, deleted, printed or exported to XML, HTML and Excel. With a consolidated, tabular display of network and system events, you can easily track IT support activities and identify stress points that require additional attention.
SNMP trap handling

AdRem NetCrunch delivers a SNMP trap processing engine. Incoming SNMP traps from any SNMP-enabled device in the network can be captured, logged, converted into a NetCrunch alert and sent as notifications to predefined administrators, or forwarded to third-party management systems and SNMP devices (Cisco, 3COM, Nortel routers and switches.)

Syslog handling

AdRem NetCrunch can act as a syslog server receiving, storing, sending and forwarding syslog messages generated by network devices (routers, switches) and Unix systems. Specified sylogs are stored in the event database where they can be filtered, processed, converted into alerting actions (e.g. email notifications) just like common NetCrunch event logs, or forwarded to third-party management systems and SNMP devices.
Trending and Reporting

Performance trending

NetCrunch provides powerful trending capabilities by allowing you to analyze real-time and historical performance trend data. Real-time trend charts for any monitored performance counter can be placed in a separate performance view for selective control. This way you can graph response time, availability, utilization and performance across servers, devices, network services and applications.

Another vital part of the program's trend analysis capability is the Trend Viewer utility. It allows you to specify the time frame for the trended counter as well as choose to analyze daily, weekly, and monthly distribution of selected counters by hours and weekdays. You can also choose to view average, maximum, and minimum values of a counter and compare the history of a single counter across multiple servers. This way you can quickly determine under- and over-utilized hosts.

All trend graphs and tables can be printed and exported to HTML and XML. Trend visualization is an essential administrative technique helping administrators detect emerging usage patterns, identify stress points, or readjust thresholds and policies.
Trend Export

All performance trend data gathered in NetCrunch can be exported to external SQL databases. Most popular databases are supported such as:

- MS SQL Server 2000/2005
- MS Access 2000 or higher
- Oracle 9i/10g
- DBISAM 3.x/4.x
- MySQL 5.x
- Interbase 7.x
- ODBC Data Sources
  - MySQL 5.0.18 via MySQL ODBC 3.51 Driver
  - PostgreSQL 8.0 via PostgreSQL ANSI Driver
  - MaxDB (SAP DB) 7.6 via MySQL MaxDB 7.06 driver

Browser-based reports

AdRem NetCrunch can store relevant data from user-defined sources. Based on collected statistics, the program can generate multi-chart performance reports that offer a historical perspective on the behavior of high-demand network servers, devices, services and applications.

All key parameters, including availability, response time and performance can be reported on critical resources, which can help you track service levels. Reports can be enabled for a single host, a map, or an entire network.

Common preconfigured report types include:

- Nodes availability (Top 10 network services in terms of availability)
- Node interfaces availability
- Network traffic on node interfaces
- Network service availability, think time and uptime (DNS, FTP, HTTP, MSSQL, POP3, ORACLE, SMTP, SNMP)
- SNMP counters (e.g. processor and memory utilization, processor bottleneck analysis)
- NetWare file server
- Windows NT server (network performance and capacity planning, disk usage and performance, memory usage analysis, network interfaces usage)
- Processor bottleneck analysis
Another useful feature of NetCrunch’s reporting module is the ability to create own report templates by grouping any number of counter charts in a single document. This way you can freely customize your reports by selecting counters to be trended, report styles, descriptions, time scope and chart types.

The program's reporting engine can use stand-alone databases such as SQL event log database. Reports can be viewed – also via a web browser – in easy-to-read graphical formats such as
Trending and Reporting

graphs, distribution charts or gauges. They can also be printed, or exported to a wide array of output formats, including .PDF, .XLS, .HTML, .XHTML, .TXT, .RTF, .QRP, and .JPEG files.

Report scheduling is another useful report management capability offered by NetCrunch. Daily, weekly, or monthly program reports can easily be scheduled to run at regular intervals on an automated basis, and subsequently distributed via email to profiled users or groups. In this manner, vital information may be quickly distributed to interested parties.
Controlling Large Network Environments

NetCrunch ships with a variety of techniques and that allow for meaningful control of large network environments. Using these techniques, you can selectively and efficiently monitor your network while sparingly utilizing bandwidth and available system resources.

Monitoring optimization

NetCrunch provides a Monitoring Optimization Wizard that allows you to determine the depth and frequency with which selected nodes will be monitored. In other words, nodes of varying significance will be monitored in varying depth and scope.

Depending on the user’s selection in the wizard, NetCrunch grades all discovered network nodes in terms of their importance and based on this determines what data to poll on selected nodes and how often. For example, nodes recognized as “critical” (servers, routers, firewalls, or nodes with more than two monitored network services) can be tracked in a full-fledged way. This means that:

- all the network services running on those nodes will be monitored at short intervals
- system counters will be monitored at short intervals
- status and performance events and alerts will be stored and generated for services and system counters
- reports will be generated for services and system counters.

On the other hand, all nodes found to be less important will be monitored with lesser depth. This allows you to conserve program and network resources for detailed monitoring of crucial resources.

Monitoring prioritization*

Apart from tailoring monitoring depth, the program allows you to decide which nodes and services should be monitored first. By retrieving information available in routers NetCrunch automatically builds a hierarchy of monitoring dependencies among network nodes (this hierarchy is presented on a Monitoring Dependencies map; see figure 22 below). What’s more, the monitoring dependencies can also be configured by the user on a per-node basis. As a result, certain nodes are treated by the program as depending on others and thus take precedence in the monitoring process.

Based on this hierarchy the program prioritizes its monitoring and event generation strategy giving prominence to parent nodes that are on top of the dependencies hierarchy. What’s more, in the case of a failure of a superior node, the program suspends monitoring and trend collection for all dependent nodes and the network services running on them.

In this “first things first” approach the program reduces the polling of unresponding assets and available network bandwidth and system resources are utilized in a meaningful way. This way NetCrunch can help control large network environments.

* Feature available only in the Premium XE edition of AdRem NetCrunch 4.x
Event suppression

Using the dependencies among mapped network hosts NetCrunch provides an alert suppression mechanism for “down” events occurring on child nodes and node services. This eliminates situations when a single occurrence – for example “router down” – triggers a massive flood of alerts from dependent nodes instead of a single meaningful alert. As a result, administrators can quickly focus first on crucial issues and do not need to sift through excessive amount of redundant information.

For example, when the HTTP service on a node is detected as being “down”, NetCrunch will generate the “HTTP service down” event only after determining that the event was not caused by the outage of the service’s node (in other words only when the node is up, that is when at least one network service on this node responds correctly). However, if it turns out that the HTTP service is down because the node itself is down, the “HTTP service down” event will be suppressed (just like all the “down” events for other services on this node).

In another example, when the program detects that an HTTP server is down because of the outage of a router, it will suppress the “server down” event, generating only the “router down” event. This capability allows you to quickly find out that the true cause of a server problem is the outage of a router link. As a result, in an event log you will find – instead of an excess of insignificant events – only one intelligent event that clearly indicates the underlying cause of the issue.

* Feature available only in the Premium XE edition of AdRem NetCrunch 4.x
Efficiency on high-performance systems

NetCrunch is designed for top-of-the-line processor technology and implements advanced mechanisms that are used on extremely fast computers. By fully utilizing the performance characteristics of multi-core and multi-processor machines, the program achieves maximum responsiveness and speed that such systems allow. As a result, NetCrunch can poll and process large amounts of data allowing you to control several thousand nodes in a heterogeneous TCP/IP network.

* Feature available only in the Premium XE edition of AdRem NetCrunch 4.x
As evident from the above description of the program's functionality, AdRem NetCrunch goes a long way to redefine the common perception of core or standard network management functionality based on agentless monitoring, to include features such as physical and logical topology mapping, fault and performance management, and capacity planning, to name a few. With reasonable purchase costs, quick deployment and extensive cross-platform functionality that can be used instantly to deliver the business value, NetCrunch offers a compelling solution for managing IT infrastructures according to business and cost control priorities.

For global enterprises, NetCrunch appeal lies in its ability to complement large frameworks in cost-efficient and secure network monitoring in local and remote offices or overseas operations. In this capacity, the program can meaningfully monitor up to a few thousand network nodes without using agents. For small and medium-sized organizations where there is not enough time, and manpower to deploy expensive management systems, NetCrunch can become a critical tool for deep yet labor-efficient monitoring. In both scenarios, IT shops equipped with NetCrunch can move away from the reactive management mode thus creating a more agile and responsive IT infrastructure, and achieving rapid returns in revenue enhancements and cost savings.

An estimated 50% of management framework clients admit they intend to complement their existing architectures with management solutions from third-party vendors.
Appendix 1: NetCrunch Audience

AdRem NetCrunch is a highly versatile solution that can be used in environments of many sizes by users with differing skill levels and job descriptions. Specifically, NetCrunch is recommended to:

**Administrators in small and mid-size companies**
AdRem NetCrunch is a perfect single-point infrastructure management solution for small and mid-size companies with up to 1,000 network users, where it can be used for optimizing performance of business-critical resources and checking the ongoing status of network servers, devices, applications, and systems.

**Administrators in large, dispersed environments**
In mission-critical divisions of global corporations, NetCrunch can serve as a monitoring solution for overseeing particular remote and local networks and specific network components, services and applications restricted via the program’s remote access rights management capability. In this role, NetCrunch can also complement high-end management frameworks and function as a component of a global IT support strategy.

**Capacity planners**
With NetCrunch, capacity planner can easily locate over or under utilized resources, assess systems historical performance, allocate budgets, as well as anticipate and justify upgrade decisions. With the program’s comprehensive data presentation capabilities, users can display the program’s console in overhead projectors.

**IT managers**
For IT managers, high level summary views of the quality of service delivered by IT support personnel will prove of considerable value. With NetCrunch, they can regularly communicate clear system performance information to senior-level executives and business stakeholders making it easy to plan and start new business initiatives driven by IT.

**Network consultants**
NetCrunch can be a great help for consultants who want to troubleshoot customer networks in different remote or onsite locations. NetCrunch can be installed on a laptop which gives consultants unrestricted mobility in their jobs. It can also be securely accessed from a variety of web browsers by users with strictly defined remote access policies. Another advantage that appeals to consultants is the program’s ability to backup and save atlases documenting IT environments of diverse customers.

**VARs, networking services firms, and system integrators**
AdRem NetCrunch enables the unified management of mid-size infrastructures by delivering a compelling package of functions so far unavailable for a similar price range such as proactive network visualization, monitoring, troubleshooting, alerting and reporting. Therefore, it is only natural that NetCrunch presents new revenue opportunities for companies looking to secure profitable consulting contracts or to deliver superior service their customers with minimized resources and costs.
# Appendix 2: System Requirements

<table>
<thead>
<tr>
<th>Minimum system requirements</th>
<th>Recommended system requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Processor</strong></td>
<td></td>
</tr>
<tr>
<td>Intel Pentium or compatible 1 GHz</td>
<td>Intel Pentium 2.4 GHz or faster</td>
</tr>
<tr>
<td><strong>Memory</strong></td>
<td></td>
</tr>
<tr>
<td>256 MB of RAM</td>
<td>512 MB of RAM; generally, more memory improves responsiveness</td>
</tr>
<tr>
<td><strong>Available Hard Disk Space</strong></td>
<td></td>
</tr>
<tr>
<td>80 MB for program files after installation, 100 MB for collecting trend data</td>
<td>80 MB for program files after installation, 1 GB for collecting trend data</td>
</tr>
<tr>
<td><strong>Display</strong></td>
<td></td>
</tr>
<tr>
<td>Super VGA (800 x 600 pixels) High Color (16 bit)</td>
<td>Super VGA (1280 x 1024 pixels) True Color (24 bit)</td>
</tr>
<tr>
<td><strong>Web Browser</strong></td>
<td></td>
</tr>
<tr>
<td>Internet Explorer 5.5</td>
<td>Internet Explorer 6.0 or higher</td>
</tr>
<tr>
<td>Firefox, Mozilla, Netscape</td>
<td>Firefox, Mozilla, Netscape,</td>
</tr>
<tr>
<td><strong>Operating System</strong></td>
<td></td>
</tr>
<tr>
<td>Windows 2000</td>
<td></td>
</tr>
<tr>
<td>Windows XP</td>
<td></td>
</tr>
<tr>
<td>Windows Server 2003</td>
<td></td>
</tr>
</tbody>
</table>

**Monitored platforms and protocols:**
- Windows 9x (only via an SNMP agent), Windows NT/2000/XP/2003
- NetWare 4.x, 5.x, 6.x, Novel Open Enterprise System (OES)
- UNIX (Linux, FreeBSD, HP-UX, Solaris, AIX)
- any platform or device supporting SNMP
- TCP/IP
- SNMP v.1, v.2, v.3
Appendix 3: Editions and Licensing

NetCrunch Editions
NetCrunch ships in two editions – Premium XE and Premium – that differ in functionality and management purposes. It should be noted that both versions are licensed per monitoring station. NetCrunch Premium XE is the more scalable version of the program. It is designed to be run on the dedicated machine and is recommended for monitoring networks containing up to a few thousand nodes. On the other hand, NetCrunch Premium may run on non-dedicated machine and performs best in a few hundred nodes' environment.

NetCrunch Premium XE provides a selection of unique performance capabilities. When running on dedicated high-performance systems, it can perform at the maximum speed that such systems allow. It also offers advanced physical network topology maps, with support for VLANs on Cisco switches. What's more, this edition ships with monitoring prioritization and alert suppression based on node dependencies capabilities. As a result, administrators can effectively monitor more network nodes and collect considerably more network data from a single point of control.

Note

NetCrunch Licensing Model
AdRem NetCrunch 4.x Premium XE and AdRem NetCrunch 4.x Premium are licensed per monitoring station. This means that single license allows you to install NetCrunch on a single station and monitor any number of hosts in your IP network. No additional licenses are needed for monitoring hosts added after the purchase of the program.

For pricing information, please go to http://www.adremsoft.com/netcrunch/pricing-prm.php.

Further Information
To view an animated product tour, in-depth product documentation or to download a fully-functional 30-day trial version, please visit the NetCrunch website at www.adremsoft.com/netcrunch.
About AdRem Software

AdRem Software (www.adremsoft.com) provides rapidly-deployable software solutions for monitoring, managing, troubleshooting and securing enterprise networks. The company's products target mid-size companies, VARs, system integrators, and network management services firms that seek to maximize returns on heterogeneous IT infrastructures by boosting network/systems performance and availability, optimizing IT asset utilization and reducing maintenance overhead. The company's solutions are deployed on over 400,000 servers worldwide.

AdRem Software was founded in 1998 as a privately held corporation. The company’s efforts to create scalable, multi-task, easy-to-use solutions were quickly noticed and appreciated, resulting in the prestigious "Best Commercial Application" award from the Novell Developers’ Contest in 1999 for AdRem Server Manager.

With AdRem Software’s flagship solution, AdRem NetCrunch, businesses can automatically visualize and monitor their multi-technology networks and proactively ensure system, application and service availability to customers, employees, and partners. AdRem NetCrunch is noted for delivering a mid-tier enterprise-class solution that offers full-fledged proactive network and systems management at the price of a point product.

AdRem Software serves a diverse global customer base, including small, medium and large enterprises from all industries, government and public sector organizations, non-profit organizations, and educational establishments. The company’s solutions are sold through AdRem’s online store, resellers, distributors, and system integrators in more than 60 countries.