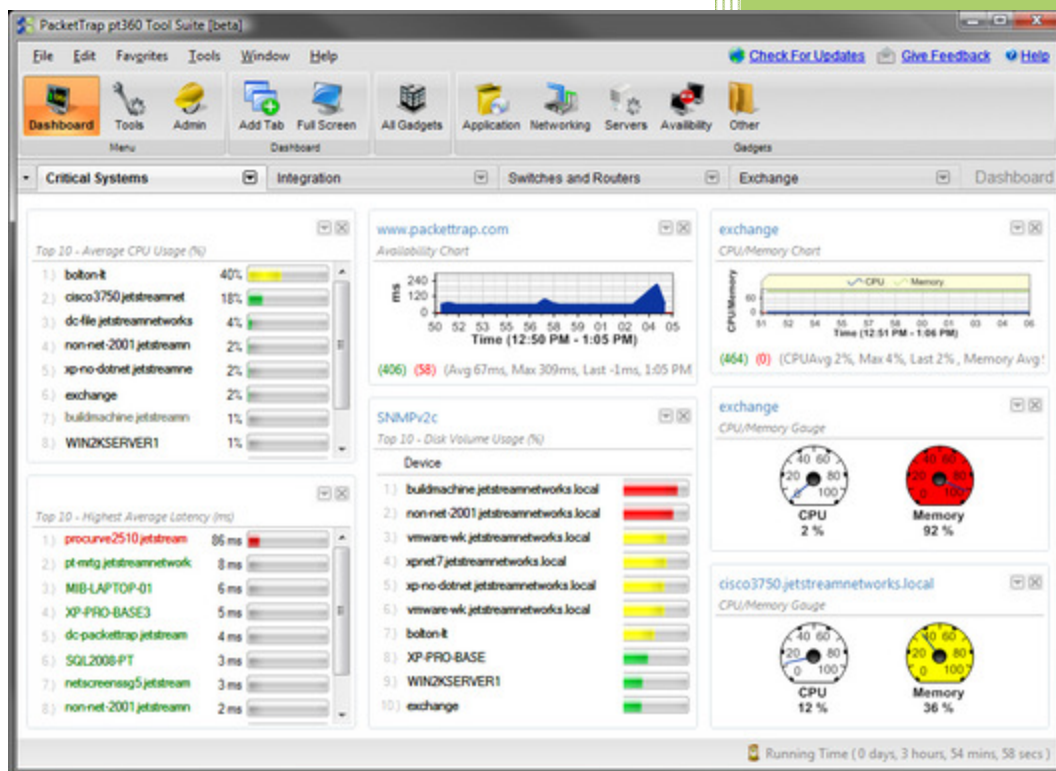


pt360 FREE Tool Suite

Networks are complicated. Network management doesn't have to be.



pt360 FREE Tool Suite - At a Glance

PacketTrap Networks

November, 2009

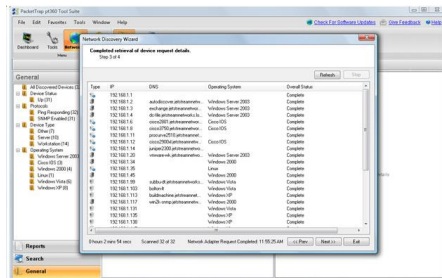
PacketTrap's **pt360 FREE Tool Suite** consolidates the PacketTrap free network management tools into a real time reporting solution and replaces disparate IT tools from multiple vendors. Why use individual point tools when you can exploit the value of these utilities in a consolidated suite that also includes integration with browser-based open source networking tools such as Nagios, OpenNMS, and others? Create custom dashboards, flow results between tools, and save network settings and favorites. The powerful, yet easy to use pt360 helps you tame your network. Networks are complicated. Network Management doesn't have to be.

pt360 FREE Tool Suite – At a Glance



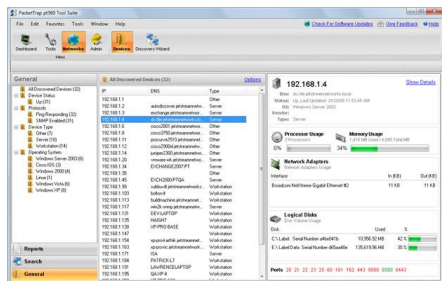
PacketTrap's iGoogle like **ptDashboard** is a “network management dashboard” with a summary display of key performance indicators (KPIs) and diagnostic metrics of network performance and availability. Managers and operations staff can continuously monitor key assets at chosen intervals with customizable gadgets.

- Monitor availability, CPU load, memory, disk space utilization, network interface traffic, network latency, and packet loss
- Manage and monitor each device or interface with SNMP and WMI
- Perform advanced monitoring of running services, process availability, and performance counters for MS Exchange, SQL, Active Directory
- Inventory of gadgets include charts, gauges, lists, text, and web links
- Drag and drop monitoring gadgets to create a custom view
- Full screen mode to maximize screen real estate and rotate multiple dashboards



PacketTrap **Network Discovery** performs a lightning quick scan of the entire network to discover all devices. Leveraging SNMP, the tool provides a complete set of attributes for each device that has been discovered and the results are piped into a cutting-edge iGoogle-like user interface.

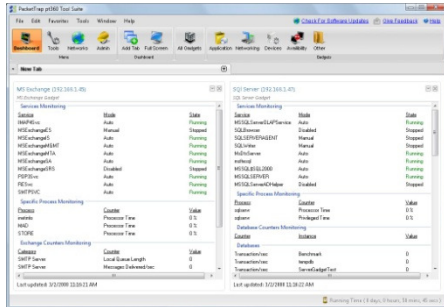
- Gather all technical data including hardware, software, and processes for each device.
- Identify devices by responding, status, protocols, type, and operating system
- Scan a single device, a subnet, or a range of subnets.
- Interact with PacketTrap Encrypted Credential Store for user access to devices.



PacketTrap **Network Inventory** creates a detailed repository of all devices on your network. It provides operating system, interface and port details, IP addresses, installed Windows software and many other details. The Network Inventory utility has robust searching and reporting capabilities as well.

- Take full control of all network assets you care about
- No special agents or data collectors are needed
- Store all inventory information locally for quick access
- Utilize SNMP protocols in the network discovery engine

- Search for granular information across all devices for additional analysis
- Generate reports for each or all devices and export to HTML or .CSV

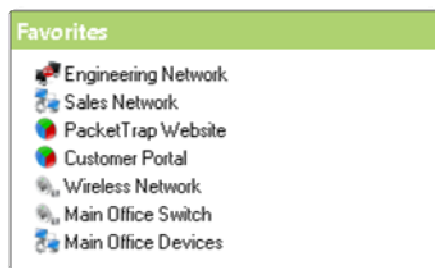


PacketTrap **Application Monitoring** provides in-depth visibility of running processes and performance counters for mission-critical applications **Exchange, SQL Server, and Active Directory**. Application failures are usually the most common problems that occur in IT infrastructure. These powerful real-time monitoring gadgets help IT Admins and network engineers prevent application failures and identify degradations early.

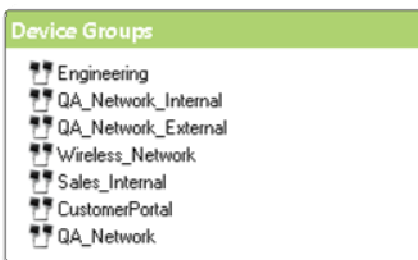
- Quickly determine the root cause of application performance issues before an end user is even aware that a problem exists.
- Perform advanced monitoring of running services, process availability, and performance counters for MS Exchange, SQL, Active Directory
- Advanced server monitoring of key indicators like CPU and memory utilization
- Visually track the performance of your applications by setting alert thresholds
- Create custom gadgets for each application



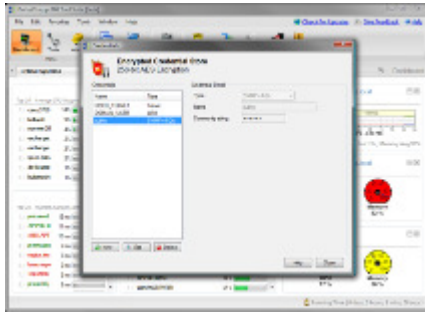
PacketTrap **Quick Launch** provides one-click access to all key areas of the FREE Tool Suite and allows for convenient flow of results between tools. Comprised of several components: Running Tools, Recent Tools, Favorites and Device Groups, the Quick Launch also has useful resources such as PacketTrap Help and Product Updates.



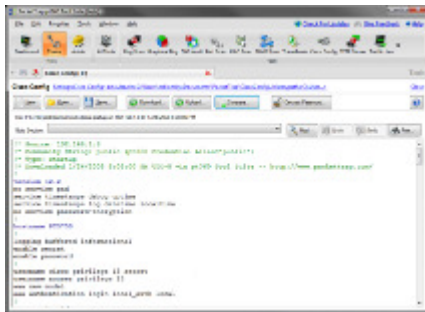
PacketTrap **Favorites** allows you to configure device groups, general criteria, and your favorite tool all wrapped as one custom tool. This gives you the ability to perform one-click runs of critical diagnostics specific to your network.



PacketTrap **Device Groups** allow you to treat selected network targets as one consolidated target of IPs and Subnets, grouped together for quick access when running a tool.

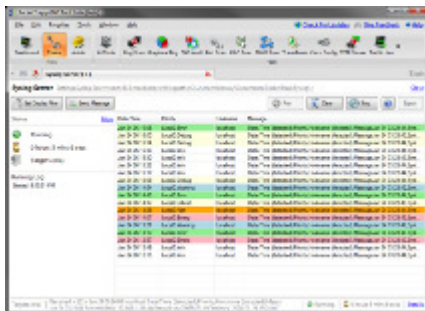


PacketTrap **Encrypted Credential Store** consolidates Windows, SNMP, and Telnet/SSH credentials in a single location for quick and simple diagnostics. The Credential Store utilizes 256-bit AES Encryption and provides password key access for additional protection.



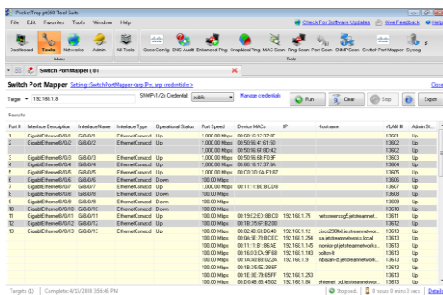
PacketTrap **Cisco Config** eases configuration and change management of Cisco® devices in lieu of one-off non-integrated point tools.

- Download device configuration files from a Cisco® devices
- Archive Cisco® router startup and running network configurations
- Upload configuration changes to routers or switches via SNMP or Telnet/SSH
- Compare the running config of a Cisco® router with the startup config or archive config
- Go To and Find any section within the config file quickly
- Decrypt any Cisco® type-7 passwords for routers and switches for lost password recovery



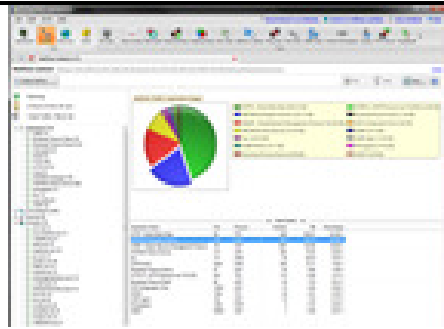
PacketTrap **Syslog Server** receives, logs, and displays syslog messages from hosts such as routers, switches, and any other syslog enabled device.

- Real-time display of syslog messages with date/time, host name, priority, and message.
- Archive messages for quick future reference
- Filter messages by Facility, Severity, date/time, host name, and key words
- Forward messages to another syslog server
- Export messages to HTML, .csv, and XML



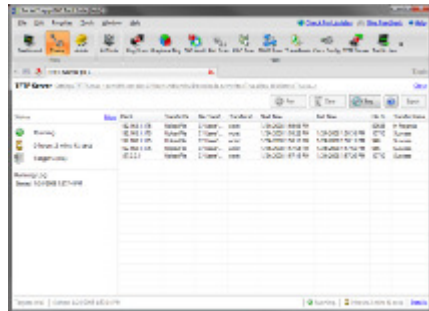
PacketTrap **Switch Port Mapper** helps network engineers discover the devices connected to each port on a switch quickly, thus eliminating the need to manually trace network cables.

- Discover all devices connected to each port on a switch
- Identify devices by MAC address, IP address, and host name
- View the operational status and port speed of each port
- Enable or disable a specific network interface
- Export tool results to CSV, XML, and HTML

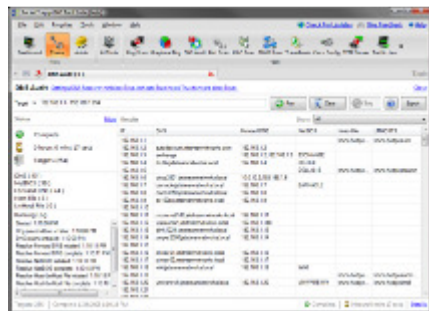


PacketTrap **NetFlow Listener** captures flow data from continuous streams of network traffic and converts raw data into useful charts, tables and tree hierarchy that quantify exactly how the corporate network is being utilized.

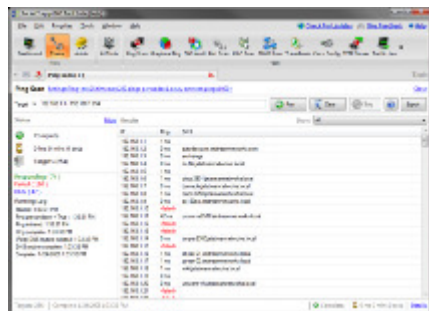
- Monitor network traffic by capturing flow data from network devices, including Cisco® NetFlow v1, 3, 5, 7 and 9
- Quickly identify which applications, conversations, devices, endpoints, and protocols are consuming the most network bandwidth
- Determine the cause of network over-utilization and highlight the conversations of the top talkers on the network, isolate suspicious traffic
- Provides historical trends for WAN and LAN bandwidth usage to determine whether additional bandwidth needs to be purchased
- Monitors Quality of Service (QoS) metrics to verify that Service Level Agreements (SLAs) are being met



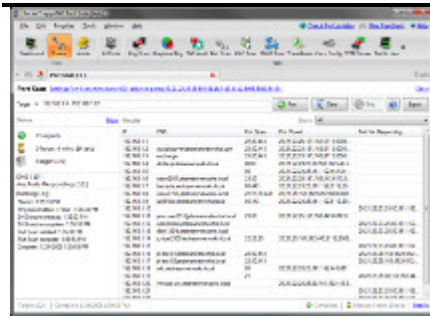
PacketTrap **TFTP Server** is a multi-threaded, highly scalable TFTP server. It supports unlimited simultaneous transfers and offers extended option negotiation between client and server, including clock size, transfer size, and timeout. Specify all and individual client connections for ultimate security. TFTP Server is commonly used to move executable images and configurations to and from routers, switches, hubs, XTerminals, and other network resources.



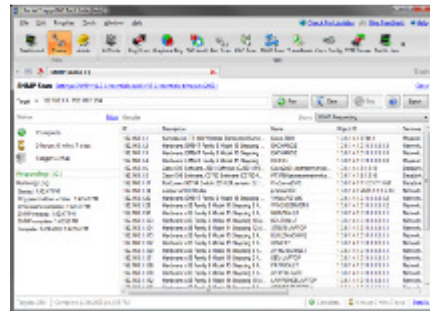
PacketTrap **DNS Audit** matches each IP Address in a specified range of IP Addresses to its domain name, and then checks back from the domain name to the IP Address to see if the resolution is the same forward and in reverse. DNS Audit also displays NetBIOS Host Name, Host, and LMHost for complete visibility.



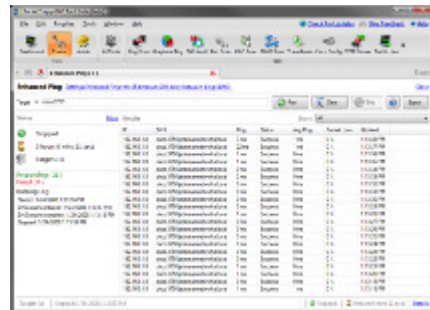
PacketTrap **Ping Scan** fires ICMP ECHO requests across a range of IP addresses and rapidly builds a spreadsheet for a quick visual display of which IP addresses are in use and which are not. DNS lookup information is provided by Ping Scan for each responding address.



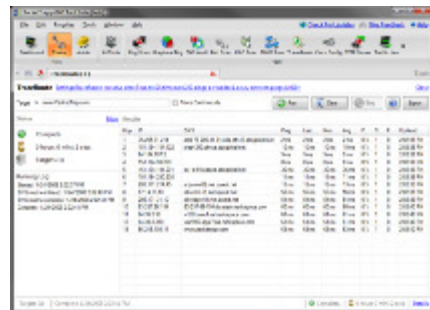
PacketTrap **Port Scan** tests for open TCP ports on specified individual machines and ports as well as within targeted ranges of IP addresses and ports. The most common port names are conveniently preloaded, but custom service names can be added easily. Port Scan is fast and easy to configure for a high degree of personal customization in the resulting view. Port scans can be scaled to match particular machine abilities, characteristics and firewall policies. Multiple export formats make for optimal presentation of the data in differing circumstances and situations.



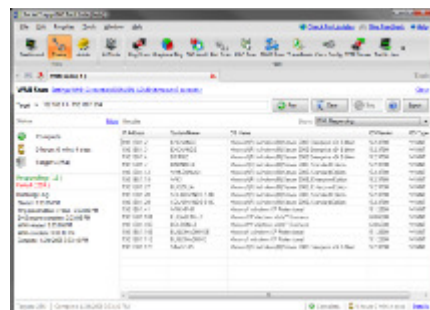
PacketTrap **SNMP Scan** discovers the contents of network subnets quickly and simply by combining SNMP discovery capabilities with a Ping Scan of a designated range of IP Addresses. Used and unused IP addresses are all identified and logged by SNMP Scan as well.



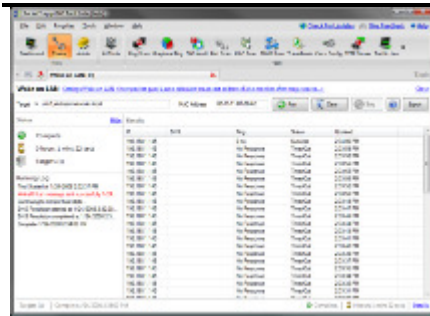
PacketTrap **Enhanced Ping** continuously logs running response times and exports data on demand to HTML, XML and CSV files. Enhanced Ping reports register current response time and running average response time in milliseconds as well as the current rate of packet loss.



PacketTrap **Trace Route** finds the route from an IP address to any other address by sending specially configured packets in a series of hops from node to node. By sending packets designed to time out and get returned after differing numbers of hops, and examining the ICMP and SNMP data returned, Trace Route can rapidly assemble a real-time display of resolved DNS, machine type, ISO level, boot and response time.



PacketTrap **WMI Scan** provides key information on the system and WMI Status for devices on the network. The results can be quickly and easily exported on demand from WMI Scan to HTML, XML and CSV files.



PacketTrap **Wake On LAN** will boot any networked machine with previously enabled capability in the BIOS by means of a “magic packet” from a remote location. Because an enabled network interface card is still receiving power, even on a shut down device, it keeps listening for the unique “magic” created for its MAC address. Upon reception, the network adapter alerts the computer to power on just as if the power button had been pressed. (Occasionally it will be necessary to reserve power for the card.) Wake On LAN is for those who have the thankless task of updating the many far flung machines of a large organization, for those who have left a digital asset on a shut down PC somewhere else, or for those who just need a little magic on the network.

About PacketTrap Networks

PacketTrap Networks118 Second Street, 6th Floor, San Francisco, Ca 95104

TEL: 415-348-0700 FAX: 415-348-0707

EMAIL: info@packettrap.comWEB: <http://www.PacketTrap.com>BLOG: <http://www.PacketTrap.com/blog>

PacketTrap Networks provides affordable enterprise-class network management solutions that allow network engineers to manage their networks from a single, centralized dashboard. The ptDashboard incorporates a proprietary suite of network tools to give users a graphical, global view of the IT environment for easy network monitoring and network diagnostics. It includes time-saving reporting and dataflow capabilities that are unmatched in the industry and also supports browser-based open source tools.

PacketTrap Networks was founded on the premise that existing network management offerings are point products lacking a central dashboard, integration and correlation and are too complex, expensive and/or poorly supported. We are committed to providing network engineers with management tools, platforms and other solutions that are developed by network engineers for network engineers. They provide the information network engineers need, when they need it, and how they want it. PacketTrap makes network management more affordable, effective and easier so network engineers can spend more time managing, predicting and preventing network problems and less time fixing them.