



Effective
Fault and Performance
Management
using
MG-SOFT's Solutions

Why Fault and Performance Management?

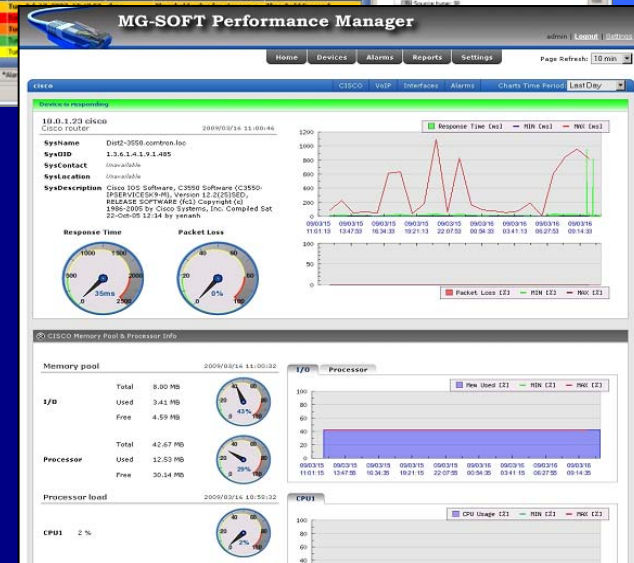
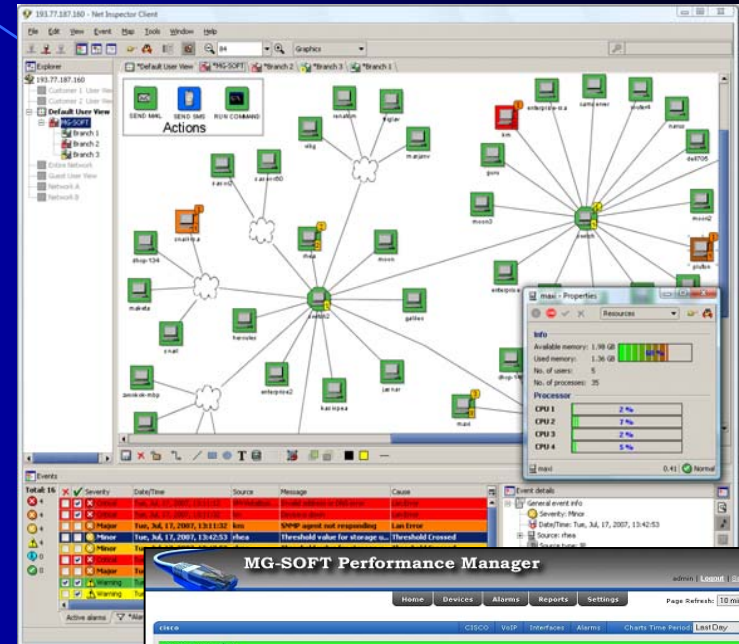
- It enables immediate detection of faults and failures on network devices, connections and services.
- It pro-actively monitors the usage of system resources (CPU, memory, storages) and links (bandwidth usage) --> it identifies bottlenecks, i.e., potential future problems.
- It generates alarms for existing and potential problems (e.g., web or e-mail server unavailability, network router or switch failure, excessive bandwidth usage, server overload, etc.).
- Alarms enable immediate corrective measures to be taken to minimize related costs.
- Quick mitigation of faults and failures as well as effective prevention of those let you do your business better. This has also a positive effect on the end-user and employee satisfaction and loyalty (your success).

Net Inspector™ & Performance Manager™

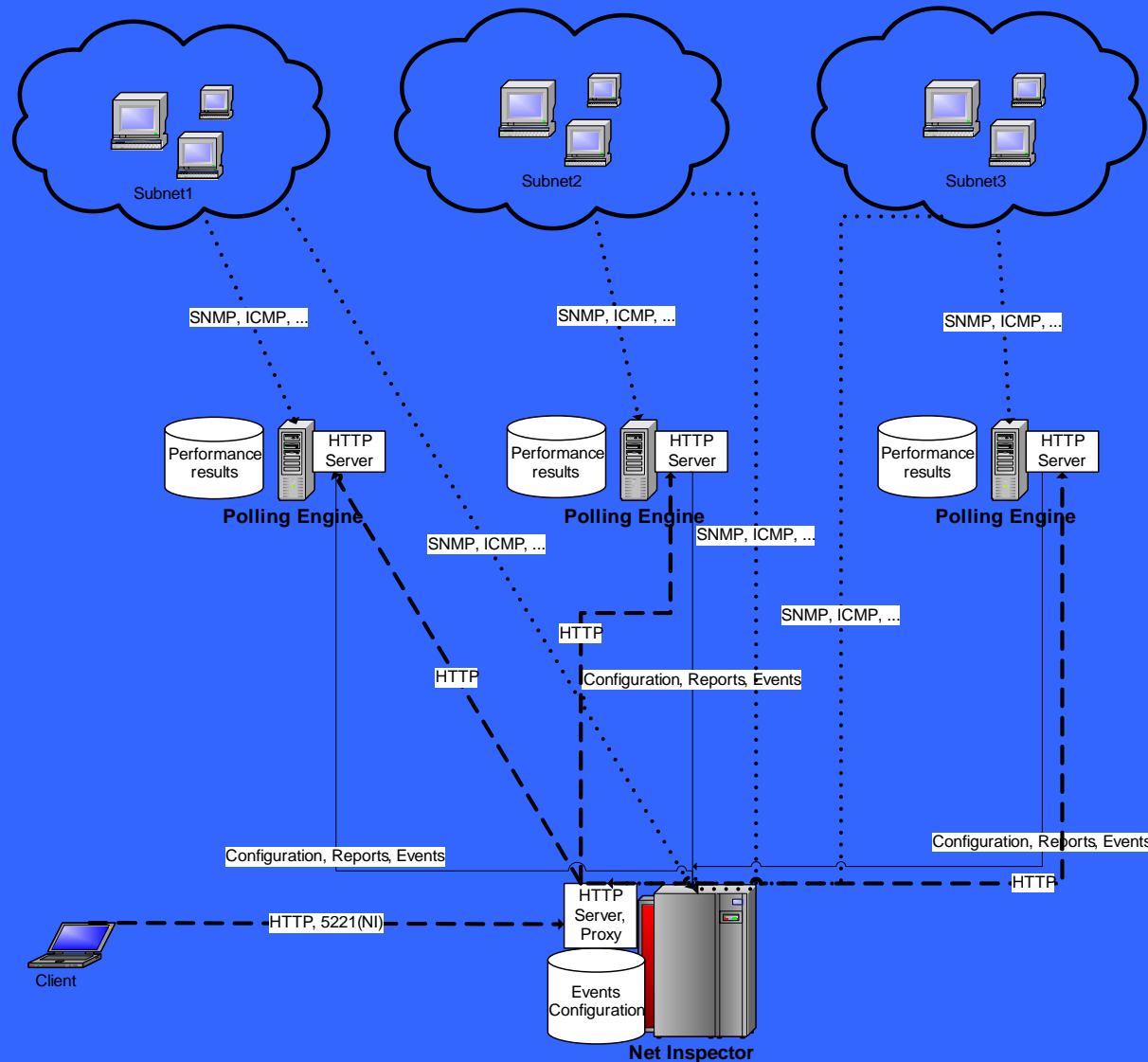


Integrated Network Management Solution

- It combines Fault and Performance Management
- Straightforward monitoring and management of system status and resources:
 - Immediate detection of faults
 - Monitoring resources usage
- Intelligent alarm management system
- Distributed polling with load balancing



Net Inspector + Performance Manager Scheme (Using Distributed Polling Engines)



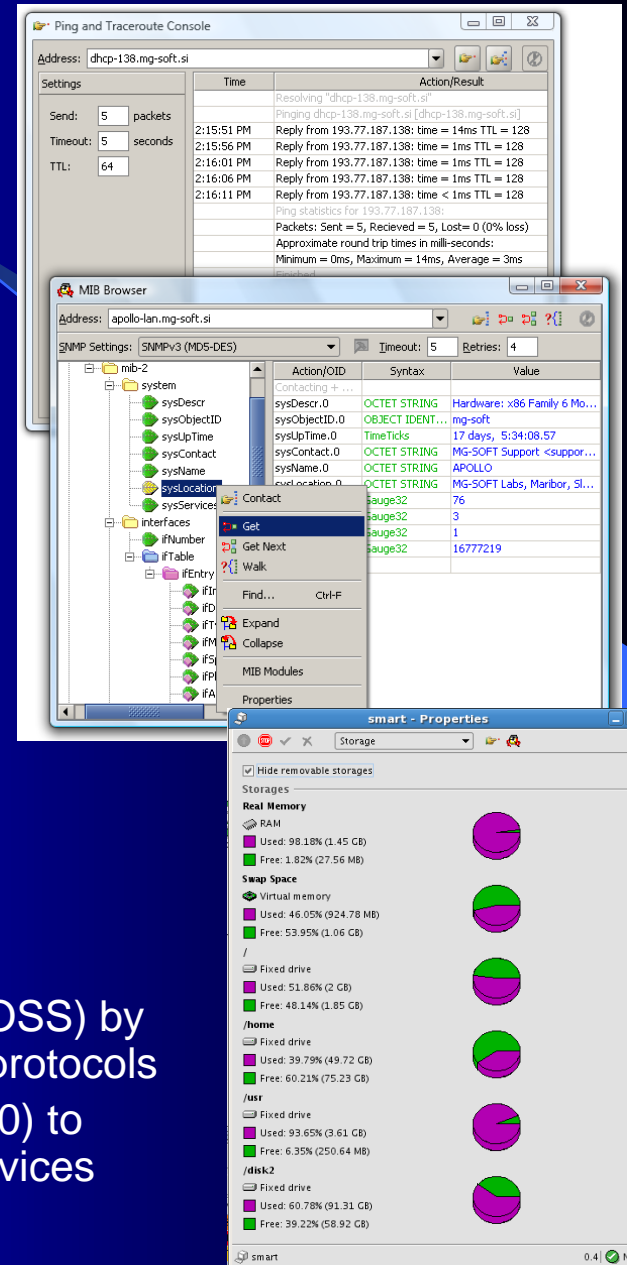
MG-SOFT Net Inspector (Fault Manager)

- Main Features

- Actively polls devices (ICMP Ping, SNMPv1, SNMPv2c, SNMPv3 (security))
- Receives event report messages (SNMP Trap and Inform)
- Monitors 19 well-known services (HTTP, HTTPS, FTP, DNS, SMTP, IMAP, IMAPS, POP3, SSH, Telnet, NNTP, NNTPS, LDAP,...) and user-defined TCP and UDP services
- Generates alarms (ITU X.733 compliant alarming system)
- Provides advanced alarm management features (propagation, filtering, searching, acknowledging, clearing, commenting, etc.)
- Stores events and alarms in SQL DB
- Discovery and auto network topology presentation with drill-down capabilities
- Customizable views of the network (user views) a means of access control
- Different types of users (admin, operator, guest) with different user-rights
- Performs actions on alarms:
 - Runs arbitrary commands or scripts (e.g., to automatically fix problems)
 - Sends e-mails and SMS messages (remote user notification)
 - Emits audible signals (plays sound files)
- Vendor-independent device monitoring, private MIB support (compiler included), private Traps support (trap-to-alarm mapping editor)
- Displaying device status and performance (CPU, memory, storages), latency and traffic statistics for network interfaces

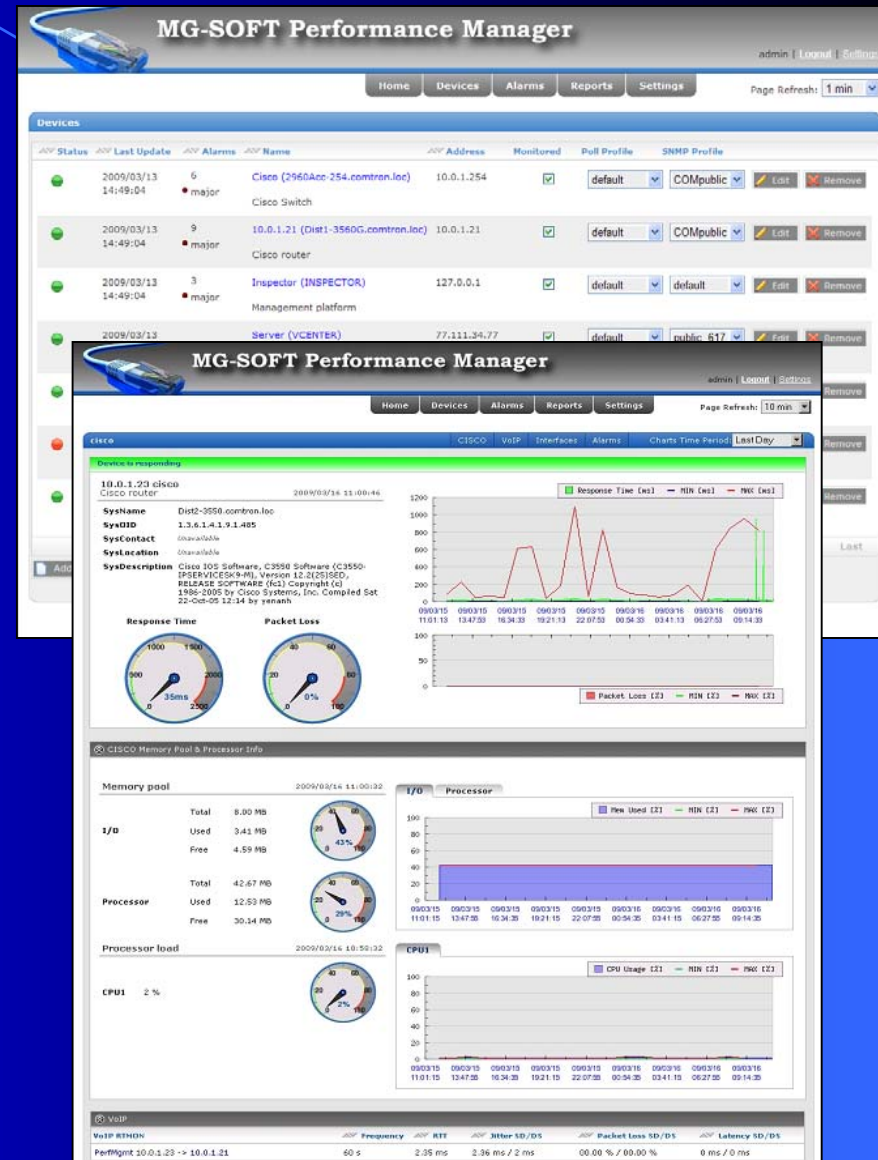
Net Inspector – Main Features (cont.)

- Integrated tools for manually troubleshooting faults:
 - Ping
 - Traceroute
 - MIB Browser (SNMP browser)
- Graphs (performance counters)
- User-defined commands on monitored objects (start node manager SW, Telnet, SSH...)
- Export alarms and device lists to HTML and CSV file formats for external use
- Client/Server architecture:
 - Server performs the polling, triggers, stores and manages alarms and performs actions on alarms
 - Client displays and lets you model the network, manipulate alarms and configure the system
 - Server is available for Linux in Win32/64 platforms
 - Java Client - platform independent
 - Java Web Start Client deployment and launching
- Remarkable performance (can monitor 1000s of objects, 80 alarms per second (real-time))
- Redundant cluster setup ready
- Can be integrated into higher-level management systems (OSS) by passing the configuration and alarms via SNMP and SOAP protocols
- Easily upgradeable from Lite (64 devices) to WorkGroup (500) to Enterprise Edition (1000) + support for additional Nx1000 devices can be bought (up to 16,000)



MG-SOFT Performance Manager

- It monitors device status and system resources (CPU, memory, storage), network interface status and statistics,...
- It can be integrated with Net Inspector (fault manager)
- SNMP as the base management protocol
- Can monitor any metric available through SNMP (GUI configurator included)
- Built-in reports for typical devices (e.g. Cisco) and performance statistics with history
- Monitors Quality of Service statistics for IP telephony (VoIP) on Cisco routers
- Generates alarms based on configurable threshold values
- Web-based access,...



Main Advantages of Net Inspector (compared to competition)

- Remarkable performance (concurrent monitoring of 16,000 NE, processes 80 alarms/s (real-time); new version: 64,000 NE, 160 alarms/s)
- Easy to install and use (auto topology discovery, out-of-the-box events, intuitive GUI)
- Stable and reliable solution - proven in real-life productive use (major telecommunications providers in Slovenia, Russia, Ukraine, some major insurance companies, Slovenian Armed Forces,...)
- Broad platform support (Java client - platform independent, server for Linux and Windows)
- Distributed network management (distributed polling engines)
- Scalability of the system (easily upgradable licenses and performance)
- Cascading and integrability into higher-level management systems (OSS/BSS)
- Cost-effective Fault Management and (optional) Performance Management solution

Integrability

Northbound Interfaces:

- Passing aggregated events to Operations Support Systems (OSS) applications via the standard management protocol (SNMP Traps) - Net Inspector SNMP proxy agent module (X.733-compliant)
- OSS can retrieve status and alarm information for individual device over SOAP
- Net Inspector can import configuration from configuration management database (CMDB) via HTTP or SOAP

Southbound Interfaces (SNMP, ICMP, any TCP or UDP-based protocol/service):

- Any vendor's device can be monitored either through its native SNMP agent or NI proxy agent (can synchronize alarms with NI Server) and ICMP Ping (availability, latency)
- Vendor-specific SNMP notifications (Traps, Infoms) are transformed to alarms using configurable trap-to-alarm rules
- Monitoring well-known services (HTTP, HTTPS, FTP, DNS, SMTP, IMAP, IMAPS, POP3, SSH, Telnet, NNTP, NNTPS, LDAP, LDAPS, IPP, LPD, MsSQL, MySQL and Oracle service) + arbitrary (user-configured) TCP and UDP network services