

## Network Management System

The Network Management System (NMS) is a standalone WLAN management system that centralizes all configuration, performance monitoring, fault management, and troubleshooting functions for the Colubris Intelligent Mobility System (CIMS). Designed to simplify deployment and minimize network operational costs, the Colubris NMS features an embedded database, and scales easily from small WLANs to large networks servicing tens of thousands of client devices. Because it communicates with Colubris MultiService Controllers (MSCs) and Access Points (MAPs) using standard Internet protocols, NMS can manage any network topology, from a local campus network to a large, geographically-distributed network that spans hundreds of locations.



### Key Features:

- Automatically discovers Colubris Intelligent Mobility System (CIMS) components for fast, easy deployment
- Automates the configuration of over 200 settings, plus software distribution, eliminating the potential for human error
- Provides accurate troubleshooting data through real-time network and user-level monitoring
- Continuously audits security policies to ensure consistent enforcement
- Includes a reporting package that supplies detailed trending information to facilitate capacity planning
- Allows secure, remote management from any Web browser
- Supports unified LAN/WLAN management with an HP OpenView plug-in module and SNMP interface

NMS is offered as a turn-key appliance that is quick and easy to install. An intuitive browser-based GUI makes configuration and ongoing management easy. Licensing for the Colubris NMS is based on network size, making it a cost-effective management solution for networks ranging from a few to thousands of access points.

### Minimizing Downtime Through Automated Discovery and Configuration

The Colubris NMS automatically discovers new network elements on the WLAN and enables the administrator to organize them into groups for easy configuration and management. Elements are classified as MultiService Controllers or MultiService Access Points to protect against mis-configuration, and multiple groups can be established for each element type, enabling customized configurations by location. NMS uses standard IP protocols for discovery, backed up by TCP/IP port mapping, ensuring that the system can reach every element in the network, including those connected by NAT gateways.

Using the grouping capability, administrators can implement configuration changes in a matter of seconds. NMS handles all multiservice controller, access point and client bridge settings. It automates complex tasks, such as provisioning new services or implementing firmware updates, eliminating the potential for human error and minimizing downtime.

Once the network is deployed, NMS continuously audits the configuration of each device to ensure policies are consistently enforced. If it detects a mis-configured MAP or MSC, it can automatically correct the configuration and generate an alert. The audit also produces an inventory report for accurate asset tracking.

## Comprehensive WLAN Monitoring and Troubleshooting

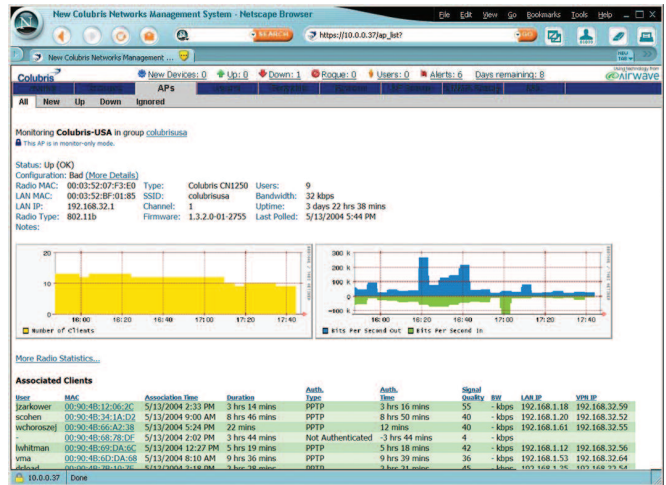
The Colubris NMS features a high-speed data collection engine that aggregates and correlates vital performance and security information in real-time. It produces an accurate and comprehensive view of the network and all associated client devices, enabling administrators to quickly troubleshoot problems. For networks that span wide-area links, the system also provides the ability to configure polling intervals by group for optimum bandwidth efficiency.

The Colubris NMS features a client data rate matrix that helps administrators quickly identify performance problems. A single poorly performing client device can degrade throughput for all the users associated with the same access point. The client data rate matrix enables administrators to compare data rates for all clients associated with an access point and quickly identify those that are disproportionately consuming bandwidth. Corrective actions, such as improving signal strength or coverage can then easily be taken.

NMS' intuitive browser-based interface facilitates a range of tasks, from network deployment and management, to help desk operations and capacity planning. User authentication and integrated SSL allows secure remote access using any Web browser.

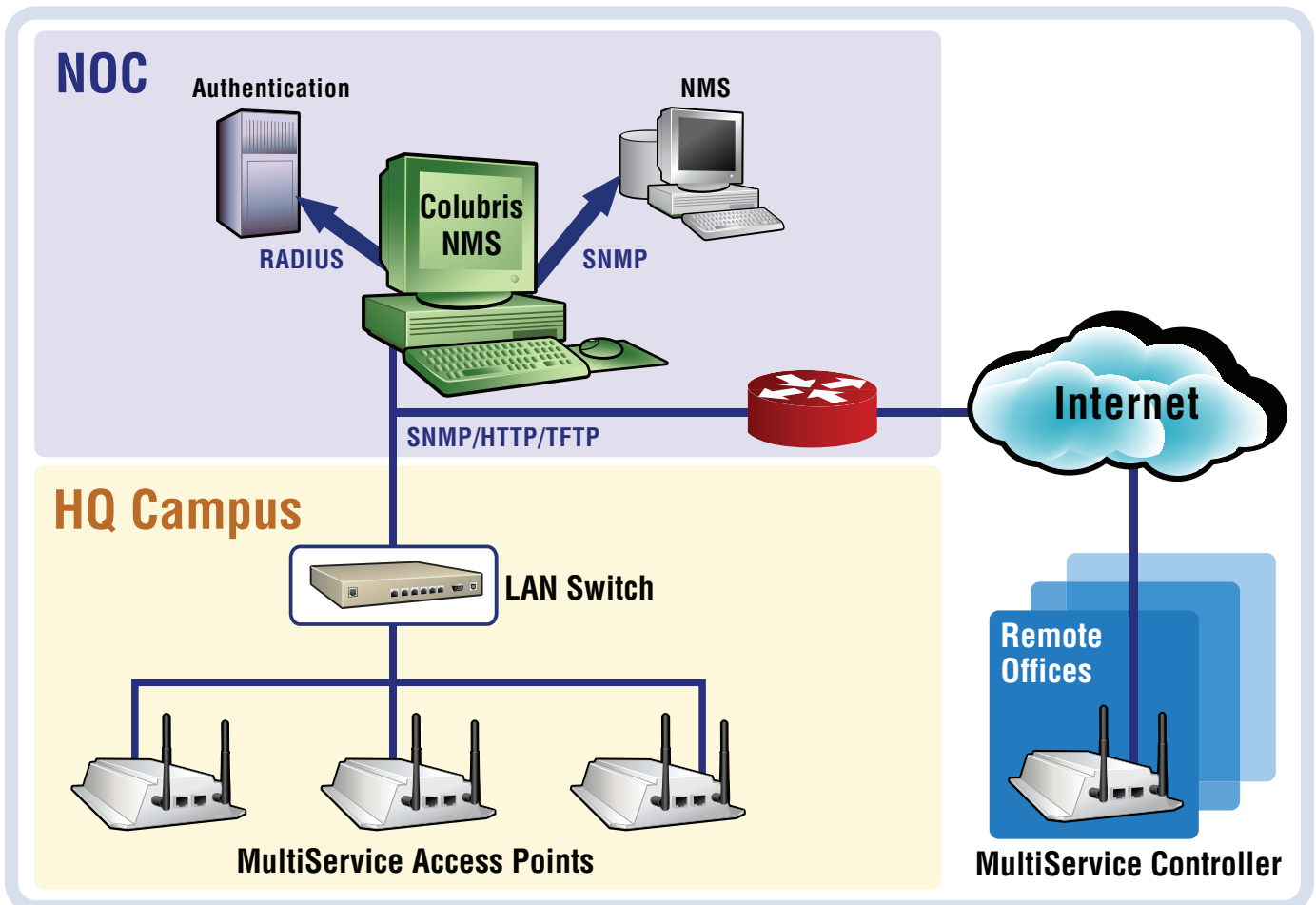
## Radically Simplified Client Troubleshooting

To facilitate help desk operations, NMS provides an integrated view of user status. By correlating RADIUS authentication transactions with detailed client device information and then providing a single consolidated screen of diagnostic information that includes dozens of key data points, NMS radically simplifies the troubleshooting process.

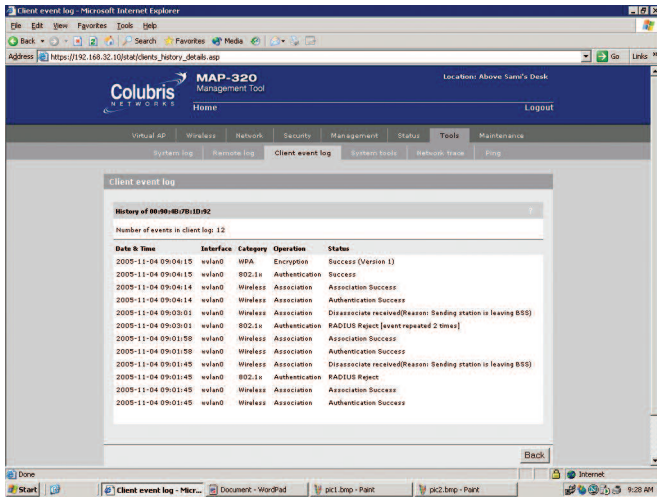


NMS presents a wealth of information at a glance, from signal strength and packet performance statistics to user roaming history and security configuration

An alerts screen displays real-time event notifications received from any element in the network, enabling network operators to take immediate corrective action. Alerts can also be triggered when a configurable threshold is exceeded, so operators can monitor specific operational parameters, such as traffic load or user count.



NMS uses IP-based protocols to efficiently manage thousands of devices connected via local and wide-area networks. It combines RADIUS accounting messages with client device monitoring information to produce a comprehensive view of client status, and its SNMP interface integrates the WLAN into an enterprise NMS



Convenient drill-down navigation provides access to embedded device management information, including the client event log that is resident in each MAP.

To help network administrators quickly resolve user log-in problems, NMS provides a client event log that provides a detailed history of 79 different association, authentication, security and DHCP handshake events for each client device. The client event log provides status and a plain English explanation for each event that can be used to pinpoint and resolve problems ranging from RADIUS/LDAP security permissions to client driver incompatibilities. It fills the gap left by cryptic error messages provided by operating systems used in wireless PCs and other mobile devices.

The Colubris NMS ensures network integrity by continuously monitoring the network for rogue access points using both advanced wireline scanning techniques and RF scanning. It works together with MAPs to monitor the RF environment, detecting and classifying rogue devices. A range of alert mechanisms enables network operators to take immediate action against legitimate threats.

Advanced RF security and intrusion prevention is provided by the Colubris RF Manager, a separate WLAN intrusion prevention system that not only detects rogue devices, but also blocks unauthorized WLAN activity.

## The Key to Managed Growth: Reporting and Network Planning

Detailed reporting is key to capacity planning and managed growth. NMS addresses this need with reports that graphically display detailed network performance statistics that can be analyzed on an enterprise-wide, per-location or per-AP basis. Comprehensive, historical performance reports assist network administrators with capacity planning. Administrators can also use NMS to periodically audit the configuration of each device to ensure consistency and reconcile equipment status against inventory lists.

The Colubris NMS also integrates seamlessly with enterprise management frameworks such as HP OpenView and other SNMP-based solutions.

## Setting A New Standard: The Colubris Family of WLAN Management Products

NMS is just one component of the Colubris family of ultra-advanced WLAN management products. Other products include:

- Colubris RF Manager, which provides strong intrusion prevention, RF security and location detection functionality; and
- Colubris RF Planner, which allows organizations to model RF coverage and security for access points and sensors.

NMS is offered as a pre-configured turnkey appliance that is sold in a range of capacities based on the maximum number of managed access points.

### NMS Appliance Models

	Entry	Enterprise
Base Managed APs*	200	500
Maximum AP Capacity	200	1000
Platform	1300	1500
<b>Model</b>	<b>1300</b>	<b>1500</b>
CPU	Xeon	Dual Xeon
Memory	1GB	2GB
Storage	80 GB SATA	80 GB SATA
Power Requirements (max.)	450W	600W

\*Separately orderable enterprise upgrade key adds 500 AP capacity.

### NMS Platform Specifications

Power Inputs	100-240 VAC, 50/60 Hz
Network Ports	(2) auto-sensing 802.3 10/100/1000 BASE-T (1) RJ-45 serial port with DB-9 adapter
Status LEDs	Power, storage activity, Ethernet activity
Temperature Range	Operating: 0°C to 50°C
Humidity	5% to 95% typical (non-condensing)
Regulatory Approvals	FCC Part 15-Subpart B (Class A), CSA NRTL (C22.2 No 950, UL 1950), Canada Class A ICES-003, Industry Canada ICES03, Australia and New Zealand, Class A, United Kingdom NS/G/1234/J/100003, EU EMC Directive 89/336/EEC, Class A CISPR 22/EN55022, EN6100-3-2, EN 6100-3-3, EN 55024, Japan VCCI
Overall Physical Dimensions	H: 4.4 cm (1.73 in.); L: 43.7 cm (17.2 in.); W: 42.8 cm (16.87 in.); Shipping Weight: 18 Kg (35 pounds)

## Technical Specifications

### Device Discovery

- Layer 2 Discovery (OSU, CDP, WNMPP IAPP)
- SNMP & HTTP Scans
- Manual entry

### Comprehensive AP and MultiService Controller Configuration

#### Radio Settings

- VSC and SSID
- Broadcast SSID On/Off
- Channel settings
- Transmission power
- Antenna configuration
- Excluded autochannels

#### Security Settings

- Required security (VPN, WPA, WEP etc.) per VSC
- RADIUS Server (Primary, Secondary, etc.)
- VLAN tagging
- Access Control Lists

#### Software Management

- Minimum firmware version
- Automated firmware upgrades
- Scheduled firmware distribution
- AP Configuration Auditing
- Configurable, automated AP auditing period
- Onscreen discrepancy report
- Auto-repair function

#### General

- Logical AP and Controller Groups
- Group-based policy management
- Job Scheduler
- LAN Settings
- "Management" vs. "Monitor Only" AP

### Monitoring

#### General

- Multiple views (Network, Group, AP)
- Real-time performance data
- Configurable SNMP polling interval (by Group)
- Graphical onscreen reports

#### User-based Monitoring

- Username
- IP & MAC Address
- Signal strength
- Authentication time/status
- Bandwidth utilization
- Roaming history

#### Network Monitoring

- Real-time AP status
- Total users
- Bandwidth utilization
- Uptime

#### Alerts & Triggers

- Standard SNMP alerts
- Advanced "synthetic" alerts
- User-configurable alerts
- Configurable severity codes
- Multiple delivery options (email, pager, console, SNMP trap)

#### Reporting

- Daily reporting package (network utilization)
- Ad hoc reports (by AP Group, time period)
- Graphical reports
- Rogue & client history reports
- Exportable via XML

#### NMS Integration

- AML™ certified plug-in with HP OpenView NNM
- SNMP traps

#### Rogue AP Detection

- Wireless RF scanning using APs
- Wireline discovery across subnets
- Integrated rogue detection list
- Ad hoc or scheduled rogue AP scans
- Rogue data includes MAC, SSID, RSSI, security settings, IP address (if available)
- Rogue history report

#### System Details

- Password-based security
- "Management, Monitoring and Operator" permission levels
- Web-based UI
- Unlimited simultaneous admin users
- Context-sensitive help

#### Interoperability

- 802.11b/g, 802.11a
- WEP, WPA, WPA2
- Wireless AP gateway

RADIUS server support list available at <http://www.colubris.com>



Colubris Networks, Inc.  
200 West Street  
Waltham, MA 02451

Tel: 781.684.0001  
Fax: 781.684.0009

[info@colubris.com](mailto:info@colubris.com)  
<http://www.colubris.com>

Copyright © 2007, Colubris Networks, Inc. Colubris Networks, the Colubris Networks logo, The Intelligent Wireless Networking Choice, and TriPlane are trademarks of Colubris Networks, Inc. All other products and services mentioned are trademarks of their respective companies.