Network Management System (NMS) FAQ

Q: How does the NMS work?
A: The Cooper NMS is a powerful, flexible and highly scalable wireless and fixed network management solution for thousands of network nodes that enables administrators to cost effectively plan, deploy, monitor, control, troubleshoot and report on fixed and wireless networks from a centralized location.

It retrieves node information by polling all network gateways at a regular interval, which is configurable by the user. Depending on the configuration, the NMS may also poll repeaters and remote field stations to gather all the desired information. Upon polling responses the NMS evaluates the status of every node and checks any preconfigured services thresholds. If any of the nodes or services indicating a Warning or Critical status the NMS will send immediately an alert via SMS or email to the designated maintenance personnel to follow up. A dashboard on the NMS will provide a comprehensive overview of the status of the entire wireless and fixed network. For more information please refer to our website at www.cooperbussmann.com/wireless

Q: What Operating System should I use for the NMS?
A: You can use the Windows or Linux operating system. The NMS uses VM Player, which makes the NMS independent from the operating system.

Q: Why do I need to install VM Player?
A: The VM Player software separates the Operating System of your computer from the NMS application. Independent of what Operating System your computer is using the NMS application can be installed on any Windows or Linux computer.

Q: Can I use my day-to-day PC to run the NMS application?
A: The NMS application can run on your day-to-day PC depending on the size of your network. However it is recommended to use a stand-alone computer so that the processing power is solely dedicated to the NMS application. It is therefore not subjected to any underperforming software application or software crashes.

Q: How can I install the NMS into an existing wireless network?
A: The NMS is designed to be integrated seamlessly into an existing wireless network without having any impact on the network operation. The installation process will not impact the operation of your network.
Q: What software and hardware are required to use the NMS?
A: The NMS is self-contained and only requires access to the internet over your local area network. A free version of the VM Player needs to be downloaded during the installation process. The only customer-supplied equipment is a PC, Laptop or Server and possibly a Router to connect to multiple wireless Gateways.

Q: Can I use any commercial Router to connect to the gateways?
A: Yes. Any commercially available Router or Bridge can be used.

Q: How many gateways can I connect to the NMS?
A: There is no limit to the number of gateways that can be connected to the NMS system. The only limitation will be the physical network connectivity of your system. Gateways can be connected in either bridged or routed networks. If routed networks are used, you should ensure the gateways have the correct routing configuration to allow communication back to the NMS system.

Q: How much bandwidth does a Gateway require, and will this affect my network operations?
A: During normal operation, a gateway is being polled by the NMS every five minutes, which is configurable. It transfers approximately five kilobytes of data across the connection contributing a small amount to your total bandwidth utilization. Depending on which items are configured for monitoring, additional data may be polled from other repeaters and field devices contributing another five kilobytes per remote device. Remote diagnostics and firmware upgrades will transfer significantly more data, but can tolerate very slow transfer rates.

Q: Can the NMS database be backed up?
A: Yes, the NMS database can be backed up manually by the user at any time, which is highly recommended. It also allows the user to restore the NMS to any previously backed-up version.

Q: How many wireless devices can the NMS handle?
A: The NMS is very scalable from monitoring just 1 device to up 1,000 devices. Future versions will be able to handle over 10,000 devices.

Q: Can I use the NMS for monitoring my other LAN equipment as well?
A: The NMS is designed to allow monitoring of wireless and wired LAN equipment. It can be used to monitor your IT equipment as well as your wireless network all at once.
Q: Does the NMS provide an alarm escalation procedure?  
A: The NMS can be configured to escalate alarms that are not resolved by first line response. Alarm escalation can be configured individually, or for groups. The user will be notified via SMS and/or email.

Q: Can I monitor a wireless network with devices from different manufacturers?  
A: Cooper NMS is especially designed to efficiently monitor ELPRO devices. However, the NMS has the capability to allow monitoring of devices from a variety of manufacturers but it requires SNMP MIBs to be available for the implementation.

Q: Why would I need an NMS installed for my small wireless network?  
A: The NMS will save you time and effort. At one view you can see the status of your network and devices. You would not have to travel to the remote sites to see the status of a device. From the NMS you have direct access each device for status monitoring or configuration purposes.

Q: What happens if a Gateway fails?  
A: The NMS will issue an alert notifying you of missed heartbeat signals. This indicates the NMS is no longer receiving its signal from the Gateway. The system will identify the failed device, and other devices that are unreachable due to its failure. This simplifies troubleshooting and isolation of the problem in the network.

Q: What happens if the Internet is interrupted or a data cable accidentally cut? Are there alternate communications means for the NMS to get an alert to my maintenance personnel?  
A: If the disruption happens before an alert signal is sent out the NMS cannot issue an alert notification until the disruption has been fixed.

Q: We have a remote location, but there is neither wireless nor Ethernet connectivity available.  
A: Depending on the specific details of your location, monitoring of the location may be possible by installing a Gateway where there is an Ethernet drop or using additional wireless nodes to extend the monitoring coverage to the desired area.

Q: My LAN network is unreliable. Is there any redundancy built into the path from the NMS to the Gateway?  
A: The NMS software uses standard IP routing and Ethernet bridging techniques to communicate to the gateway devices. There are a variety of techniques available to improve network reliability, including spanning tree protocol (bridging) and Virtual Router Redundancy Protocol (IP).
Q: Can I use my laptop to log into the NMS remotely?
A: The NMS is designed to allow for up to 64 local or remote users. Remote connectivity need to be coordinated with your IT department for security reasons. If you are allowed to establish an http session with the NMS then you will be able to log into the system from anywhere worldwide.

Q: How does the NMS affect my network traffic?
A: The NMS generates minimal network traffic by polling the gateway devices, and only polling network nodes when necessary. The polling cycles are configurable by the user and can be adjusted depending on the data rate of the device.

Q: Can I use my Smartphone to access the NMS?
A: There is no application currently available to use your Smartphone to access the NMS. However, it will be available in an upcoming release.

Q: How is the NMS licensed?
A: The NMS can be licensed by the number of nodes. There are three base system licenses available: 50 Node license, 100 Node license and an Unlimited Node license. Additional add-on node licenses can be purchased in increments of 100 nodes.

Q: How can I upgrade the demo version of the NMS to the licensed version?
A: To upgrade to the licensed version of the NMS you need to install a special License Key, a License File and a USB dongle. No new software is required. These items can be ordered through your Sales representative.

Q: Can nodes connected to wireless Access Points be detected and mapped?
A: There is no issue if using ELPRO Wireless Access Points. If using a third-party Access Point and the wireless Access Point is configured as a bridge, then the NMS will be able to map the nodes connected to it. If the wireless Access Point (or any router) is configured to use network address translation (NAT), then no network analysis tool will be able to go beyond the device to examine the nodes connected to it.

Q: What devices can be monitored with the NMS?
A: The NMS version 1.0 supports the following devices:
   - 915U-2: firmware version 1.2.1
   - 245U-E: firmware version 2.16
   - 945U-E: firmware version 2.16
   - 455U-D: firmware version 3.03
In a future release it will also support the 450U-E, 615M-1 and both WirelessHART devices 315WH-GT and 315WH-DC.
Q: How much faith can I have in the system?
A: The NMS has been designed for maximum uptime expected by data center professionals and telecom engineering standards.

Q: What happens during a power failure – does my NMS need my attention to get it going again?
A: Depending on your system configuration, the NMS may need to be restarted after a power failure. To ensure automatic restart, we suggest that you purchase VMware’s VM Server product in place of the free VM Player application.

Q: Can the NMS interface with DCS or SCADA systems?
A: The NMS is designed to be open and flexible regarding the interoperability with external systems. However, no existing interface application currently exists. It is the intention to provide such an interface at a later time upon customer requests.

Q: I can’t allow an Internet connection to your server; it opens up a security leak in my network.
A: The architecture of the NMS System was carefully designed following industry best practices, and its communication poses no new risks to your network security. If your facility currently contains no Internet connection, one can be established for the sole use of the NMS System such that it is isolated from the rest of your network and therefore poses no security risk to it.

Q: What kind of security measures does the NMS have to avoid intrusion of my network and having sensitive data leaving my network?
A: The NMS supports 128 bit SSL encryption, outbound-only communication requiring no need to open incoming firewall ports, user and device password authentication for all network communications, user rights and restrictions, user activity auditing, SSL client and server certificate authentication, remotely managed security updates, and firewall at the Command Center.

Q: What security measures are in place for accessing the NMS?
A: Access to the NMS is by username and password only. Your administrator has full control to add and delete users and change passwords to protect access to your NMS information and assign user restricted policies.

Q: If my system needs servicing, who do I need to contact?
A: Cooper Bussmann has two service centers, one in Vancouver, Canada and another one in Brisbane, Australia. They can be contacted via phone or email during regular business hours.
Q: Is training my employees going to be difficult?
A: No. Initial training can be performed via WebEx and the system will come with access to
documentation for basic troubleshooting procedures.

Q: Where can I obtain more information on the NMS?
A: Visit the Cooper Bussmann website at www.cooperbussmann.com/wireless

Technical Support:
United States: +1 866 713 4409
Australia: +61 7 3352 8624

Email:
ELPRO-Support@cooperindustries.com
ELPRO-US-Support@cooperindustries.com