

TECHNICAL ARTICLE: SNMP: SOLUTION TO INFRASTRUCTURE PROBLEMS KNOWN AND UNKNOWN!

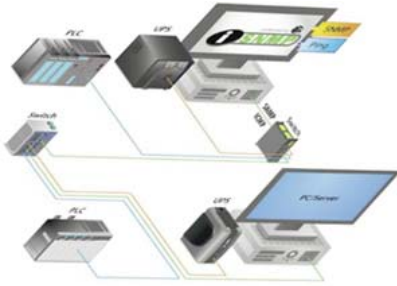
 Jump to Articles from: Issue 45 [GO](#)
[Request Further Info](#) [Print this Page](#) [Send to a Friend](#)

What is the most important thing on the mind of a manufacturing professional? Most discussions involve two areas - improving manufacturing performance and reducing downtime. There are many solutions available to assist with both. Simple Network Management Protocol is a major resource says Kepware's Roy Kok

A FOCUS ON INTEGRATION with the business systems can improve real-time aspects of production management. A similar focus on better production analytics can squeeze additional performance out of the equipment you are monitoring. Both identify and resolve areas of production stress, items that affect reliability of the manufacturing equipment. These are all valuable pursuits and they will, no doubt, deliver improvements in production and profitability.

To calculate the savings effectively, the cost of downtime should be quantified – per machine, per line, per plant area, etc. Only then, will you really gain a clear picture of the return on your investments. But as was said in a song... 'The real troubles in your life are apt to be things that never crossed your worried mind: the kind that blindsides you at 4pm on some idle Tuesday.'

What might they be? Let's start simple – that production printer that is left off-line or that ran out of ink or paper. The storage disk that filled up. On the more disruptive side – it's the CD left in a drive that stops a system from autobooting. The operator that started a video session and stole all available network bandwidth... It's the laptop plugged into an available switch port to access a plc needing maintenance (oops – yes, I let my kids use it to do homework the other night and hmmm – I guess they may have accidentally infected it). How do you monitor and protect against all this?


What SNMP can do

SNMP, Simple Network Management Protocol, is a communications protocol built into most of the IT infrastructure around us. From printers to UPS systems, routers and the PCs used in automation, virtually everything in the IT world supports SNMP communications. It is already there, waiting to be used. And, it is supported over the Ethernet you are already using.

So, what does this all mean? It allows both the monitoring and control of most equipment making up the network system infrastructure. It can monitor that printer and make sure it is on-line and has the resources it needs for this production shift. It can do the same for media left in drives, or measure the UPS reserve power to make sure it is ready to cope with a power interruption. It can also monitor your network for normal bandwidth and generate alarms when abnormal situations arise. You can even disable unused ports on a switch to ensure someone doesn't just plug-in a maintenance laptop without first following procedures to ensure the safety of your automation environment.

Monitoring devices via SNMP has typically been the domain of IT personnel. They use tools such as HP OpenView – enabling them to discover and monitor the various bits that make up the business infrastructure. But hold on! They can't tell a PLC from an SLC and you really don't want them performing a port scan of your automation network. No, that really wouldn't be a good idea, unless you like the idea of a Tuesday evening infrastructure troubleshooting session...

So, what should one do? Since you already have most of what you need in terms of devices that can give you SNMP results, all that's missing is the integration of SNMP data with your existing HMI/SCADA solution.

The solution comes in the form of an Industrial SNMP (iSNMP) driver, similar to your RSLinx, Profinet, Modbus, etc. automation driver. An iSNMP driver will let the automation system both monitor and manage the automation infrastructure. In addition to monitoring PLCs and field devices, you will be able to communicate with all the pieces that make up your automation network, the backbone of the plant.

Introducing SNMP 101

Devices that support SNMP are described as having SNMP Agent capability. The Agent communicates with the device and exposes information based on, and in the format of, the SNMP Communications Standard. The SNMP Standard however, does not describe the data that is available from a device. That is handled by a separate definition called a MIB (Management Information Base) file. Devices that include an SNMP Agent will have a corresponding MIB File, either available with the device or easily accessible from the manufacturer. The MIB describes the information that is available, and how to interact with the device. Some data is read-only; other data can be read or written to.

SNMP commonly supports two types of connections, one for the polling of data (A GET command) and another for the generation of unsolicited messaging based on triggers – called TRAPS. A SET command also exists for the management of a device – writing information to a device.

Let's have a look at some MIB Variables – for common devices used in Automation.

A typical UPS (Uninterruptible Power Supply) may deliver these variables:

- BatteryCapacity
- OutputFrequency
- OutputVoltage
- OutputLoad
- BasicOutputStatus (On-line)
- BasicTimeonBattery
- ReplaceBattery

OPTIONS

- [Technical Articles](#)
- [Case Studies](#)
- [New Products](#)
- [Search Articles](#)

PROTOCOLS

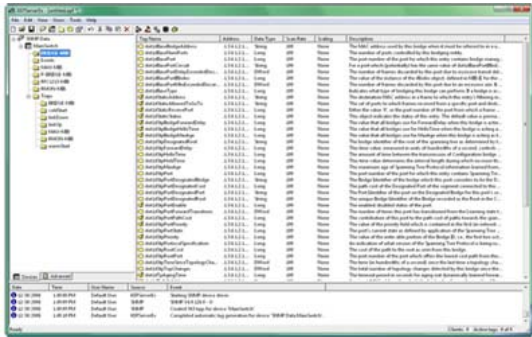
- [Ethernet I/P](#)
- [Profinet](#)
- [Powerlink](#)
- [EtherCAT](#)
- [Modbus TCP](#)
- [SERCOS](#)
- [FF HSE](#)

Printers offer a great deal of information, from on-line status to toner and paper levels:
 hrDeviceStatus – running, warning, testing, down;
 hrPrinterStatus – idle, printing, warmup
 hrPrinterDetectedErrorState – lowPaper, noPaper, lowToner , noToner , doorOpen, jammed, offline, serviceRequested

Getting into real IT equipment can be interesting. wireless access points, the greatest vulnerability in an automation infrastructure, offer a wealth of data . You can be monitoring or controlling who has access, how long connections have been active, and the quality of connections. As many as 200 variables can be accessed from a wireless access point, from web encryption keys to authorised MAC addresses. There is frequency (channel) information, communication traffic statistics, and current connection statistics. The use of SNMP connectivity can allow you to automatically manage security procedures and control access, right from an HMI/SCADA that delivers user friendly controls, operator logs and procedural tracking.

Bridges, switches, and routers, offer equally as much information. Most of this information is not valuable for continuous monitoring, however, there are variables that can enable and disable ports not currently in use. Standard procedures can require an operator to give access to a switch port, rather than leaving ports available to anyone who walks by with an Ethernet cable. There are indicators of communication degradation – enabling you to alarm on pending trouble, and there are variables that help you understand the type of network traffic currently flowing through the switch.

Some industrial automation equipment and sensors support SNMP in addition to other protocols. SNMP communications can open a wide range of new functionality for the control engineer. Common IT products exist for server farm automation. Products deliver HVAC monitoring and control and power distribution management. You can easily control a remote power receptacle, perhaps triggering a remote boot via SNMP. These products can now be easily installed with and incorporated into your automation environment.



The display above highlights the KEPServerEX configuration environment and an auto-generated list of Tags typical of an SNMP managed switch. (source Kepware)

No SNMP? No problem...

But what about Ethernet devices that are not SNMP compliant? Well, they can still be monitored. Most likely they'll respond to a PING network command. A PING is a simple network command used to test whether a particular device is reachable across an IP network. It can be used to determine the accessibility of the device, and can also be used to determine the responsiveness of a device – by measuring the response time (although other factors such as network latency may also be a factor). An additional driver (imaginatively called PING) provides this connectivity.

These drivers (iSNMP and PING) have been developed, adhering to automation communication standards, enabling use with virtually any automation software product. The OPC standard provides the transfer of data between various software applications, in this case a communications Driver and an HMI/SCADA solution. For more information on OPC, visit www.opcfoundation.org.

These drivers deliver both auto-discovery and auto-configuring functionality for quick and easy setup. Devices may be set manually or an IP range may be scanned to uncover items to monitor. Once identified, the driver will import the associated MIB and will display all available TAG data for the device. It is then up to the Client application to make use of this new information.

This is all pretty straight forward stuff for the plant engineer. He or she has been leveraging this type of functionality with automation equipment for years! All that is needed is the addition of another communication driver or two, enabling the integration of IT infrastructure equipment via SNMP, with the other protocols currently being monitored by the existing HMI/SCADA. The return on this investment is likely to be the lowest hanging fruit that you'll find for a long time.

Roy Kok is VP, Sales and Marketing, Kepware Inc

Source: Industrial Ethernet Book Issue 53:39

[Request Further Info](#)

[Articles Menu](#)