

## **Monitoring of the Plant, by the Plant, for the Plant.**

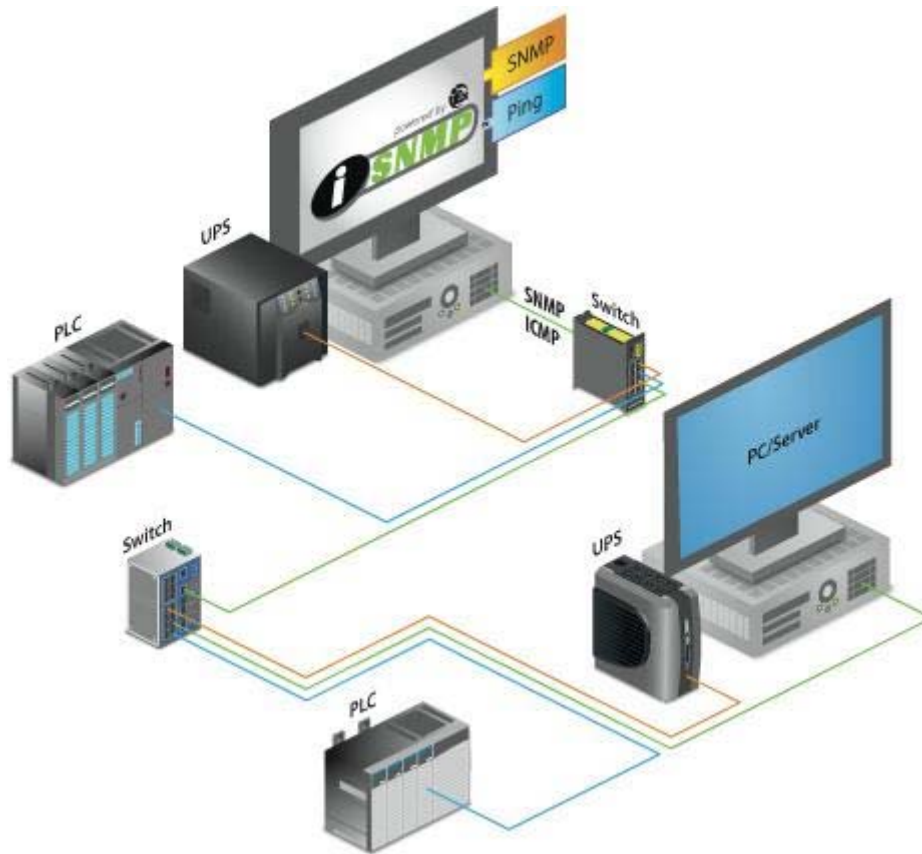
*by Kepware Technologies*

What is the most important thing on the mind of a manufacturing professional? Well, from most of the articles we read, it falls into two areas – improving manufacturing performance and reducing downtime. There are wide arrays of solutions available to assist you with both. You can focus on integration with your business systems to improve the real-time aspects of production management. You can focus on better production analytics to squeeze additional performance out of the equipment you are monitoring and both identify and resolve areas of production stress – the items that impact the reliability of your manufacturing equipment. These are all valuable pursuits and they will, no doubt, deliver improvements in your production and profitability. To know the savings, you should have quantified your cost of downtime, per machine, per line, per plant area, etc. Only then, will you really clearly know 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 Auto-Booting. 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?

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 we use in automation, virtually everything in the IT world supports SNMP communications. It is already there, waiting for your use. And, it is supported over the Ethernet you are already using.



So, what does this all mean? Well, it means you can both monitor and control most of the equipment making up your system infrastructure. You can monitor that printer and make sure it is on-line and has the resources it needs for this production shift. You can monitor for media left in drives or measure the UPS reserve power to make sure it is ready for that power interruption. And your network – monitor the normal bandwidth so that you can alarm on abnormal situations. 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 your IT personnel. They have tools such as HP OpenView – enabling them to discover and monitor the various bits that make up your business infrastructure. Ah yes, but 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 do you do? You know now that 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.

Well, the solution comes in the form of an Industrial SNMP (iSNMP) driver, not too unlike your RSLinx, ProfiNet, Modbus, etc. automation driver. An iSNMP Driver will let your automation system both monitor and manage your automation infrastructure. In addition to monitoring your PLCs and Field Devices, you will be able to communicate with all the pieces that make up your automation network, the backbone of your plant.

Here's SNMP 101. Devices that support SNMP are described as having an SNMP Agent capability. The Agent communicates with the device and exposes information based on 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 (Uninterruptable Power Supply) may deliver these variables:

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

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

Now, getting into real IT equipment can be very interesting. Wireless Access Points, your 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 monitor the quality of connections. There can be as many as 200 variables that can be accessed from a Wireless Access Point, from Web Encryption Keys to Authorized 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

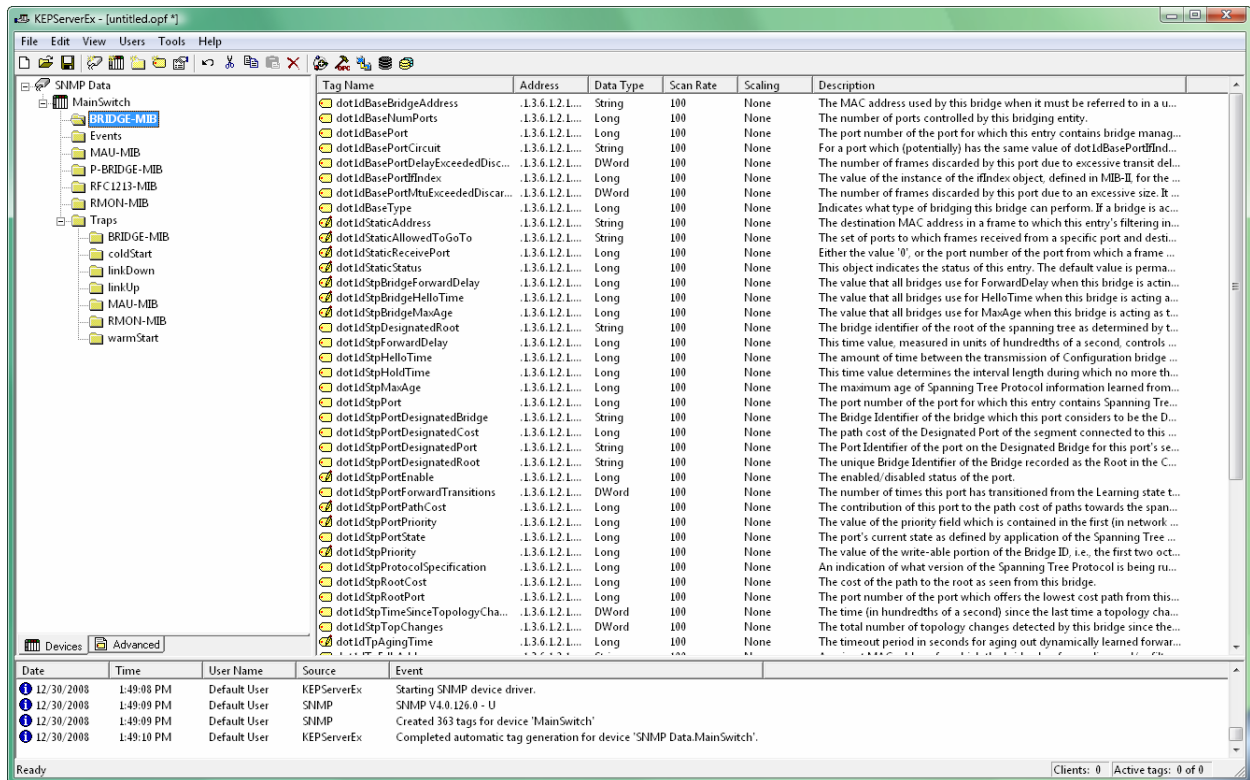
communication degradation – enabling you to alarm on pending trouble. And, there are variables that help you understand the type of network traffic currently flowing through the switch.

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, 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.

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 standard, OPC, provides for 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](http://www.opcfoundation.org).

These Drivers deliver both auto-discovering 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.



The display above highlights the KEPServerEX configuration environment and an auto-generated list of Tags typical of an SNMP Managed Switch.

This is all pretty straightforward 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 your existing HMI/SCADA. The return on this investment is likely to be the lowest hanging fruit that you'll find for a long time.

## Sidebar

Kepware is the leading provider of communications for Automation. Founded in 1995, and having developed a focus on communications for the automation industry, Kepware Drivers have become the most widely OEM'd product among both software and hardware vendors with-in the automation space.

In 2007, Kepware acquired the products of COI Software, the company that pioneered SNMP communications for automation. In 2008, Kepware redeveloped the iSNMP product, bringing it up to date with industry standards and adding the iSNMP and PING Driver to its current suite of over 130 protocols.

KEPServerEX, and all communication protocols, including iSNMP and Ping, are available for download at [www.kepware.com](http://www.kepware.com) and will offer full operation in a two-hour demonstration mode.