A Fast Track Introduction to SNMP and its Practical Use in Network Alarm Management

Case Study: Nova Scotia Power Upgrades Obsolete SNMP Manager To T/Mon, Looks To Prevent Site Visits

7 Fatal Mistakes Network Engineers Make When Implementing SNMP

Top 10 Ways to Tell if your SNMP gear makes the cut

3 Factors that Prove Your Network Needs a Protocol Mediation Solution
Contents

Tutorials

4 SNMP 101 - Learn SNMP Basics Quickly

10 MIB 101 - What is a MIB and how is it used?

Case Study

12 Nova Scotia Power Upgrades Obsolete SNMP Manager To T/Mon, Looks To Preventing Site Visits

Network and Gear

14 5 Basic Capabilities to Look for in an SNMP Remote Monitoring Device

16 7 Fatal Mistakes Network Engineers Make When They Attempt to Integrate SNMP and Non-SNMP Systems

22 Top 10 Ways to Tell if Your SNMP Gear Makes the Cut

Protocols

9 The Pros and Cons of SNMP v1, v2c, v3

18 Three Factors that Indicate You Need a Protocol Mediation Solution

19 Mediating Protocols and Inputs/Outputs to SNMP

Contributors

Sergey Dub
Engineering Manager

Reinier Jugao
Engineer

Mark Parreira
Engineer

Harshan Samra
Engineer

Jerry Yang
Engineer

Andrew Erickson
Marketing Manager

Ashley Pappas
Marketing Writer

Angel De La Cruz
Sales Team

Billy Chansombath
Quote Tech

Contact Information

www.dpstele.com
Sales: 800-622-3314
Support: 559-454-1600
Fax: 559-454-1688
Email: questions@dpstele.com
SNMP 101

SNMP was created in 1988 (based on Simple Gateway Management Protocol, or SGMP) as a short-term solution to manage elements for growing networks - like the Internet. Since then, SNMP has achieved widespread acceptance and become a standard protocol for tons of applications.

The Manager-Agent Model
SNMP is based on the manager/agent model. The model consists of the following pieces:

- **Manager**: The manager provides the interface between the management system and the network techs responsible for the system.
- **Agent**: The agent provides the interface between the manager and managed objects.
- **Managed objects**: Managed objects are logical objects in the software that generally correspond to physical things, like inputs and outputs.
- **Database**: The data base acts as a sort of dictionary to help your devices communicate. It's called a MIB and will be discussed later in more detail.

A MIB database and a few simple commands
The manager and agent use a Management Information Base (MIB) and a relatively small set of commands to swap information. The MIB is organized in a tree structure with individual variables, such as point status or description, being represented as leaves on the branches. A long numeric tag or object identifier (OID) is used to distinguish each variable uniquely in the MIB and SNMP messages. (See MIB 101 on page 10 for more information.)

How SNMP Handles Alarm Messages
SNMP uses five basic messages (GET, GET-NEXT, GET-RESPONSE, SET, and TRAP) to communicate between the manager and the agent.

GET: Ask for Information at Any Time
To get status information from the agent, the manager can issue GET and GET-NEXT messages to request information for a specific variable. Once a GET or GET-NEXT message is received, the agent will issue a GET-RESPONSE message to the manager with either the information requested or an error explaining why the request cannot be processed.

SET: Control Your Remote SNMP Devices
A SET message allows the manager to request a change be made to a managed object (i.e. a control relay). The agent will then respond with a GET-RESPONSE message if the change has been made or an error explaining why the change cannot be made.

TRAP: The Most Common SNMP Message
TRAP messages are unique because they are the only message type that is initiated by the agent.
TRAP messages are used to inform the manager when an important event happens. This makes TRAPs perfect for reporting alarms to the manager rather than wait for a status request from the manager.

**Why is SNMP “Simple”?**
Aside from the small number of commands SNMP uses, it is considered “simple” because of its reliance on an unsupervised or connectionless communication link. This simplicity has led directly to its widespread use, especially in internet applications. SNMP is considered “robust”, because of the independence of the managers from the agents. Because they are typically separate devices, if an agent fails, the manager will continue to function, or vice versa.

**Understanding Packet Types and Structure**
Basic serial telemetry protocols, like TBOS, are byte-oriented with a single byte exchanged to communicate. Expanded serial telemetry protocols, like TABS, are packet-oriented with packets of bytes exchanged to communicate. The packets contain header, data and checksum bytes. SNMP is also packet-oriented. The packets are composed of the message types discussed earlier: Get, GetNext, GetResponse, Set, and Trap.

Each packet, or variable binding, contains an identifier, a type and a value (if a Set or response). The agent uses its MIB to determine whether the object is managed and changeable (if processing a Set). The manager uses its MIB to display the readable name of the variable and sometimes interpret its value for any techs who may need to take corrective action.

**The Layered Communication Model of SNMP**
To send information, SNMP uses a layered communication model.

Layer 1 - Application layer (SNMP)
Layer 2 - Transport layer (UDP)
Layer 3 - Internet layer (IP)
Layer 4 - Network Interface layer (i.e., twisted pair copper, RG58 coaxial or fiber)

While this multi-layer model may seem a bit confusing, it effectively isolates the tasks of communication and ultimately assists in designing and implementing a network.

**Traversing the Layers**
To illustrate the function of this layered model, let’s look at a single SNMP GET request from the agent’s perspective.

**Step 1:** The SNMP manager wants to know what the Agent’s System Name is and prepares a GET message for the appropriate OID.

**Step 2:** It then passes the message to the UDP layer. The UDP layer adds a data block that identifies the manager port that the response packet should be sent to.
Step 3: The packet is then passed to the IP layer, where the data block containing the IP and Media Access addresses of the manager and the agent are added.

Step 4: The entire assembled packet gets passed to the Network Interface layer. The Network Interface layer verifies media access and availability. It then places the packet on the media for transport.

Step 5: After working its way across bridges and through routers based on the IP information, the packet finally arrives at the agent.

Step 6: Here it passes through the same four layers in exactly the opposite order as it did at the manager.

Understanding layers makes troubleshooting easier
Understanding this layered model makes it easier to troubleshoot communication problems. When there is a problem, you can simply trace it down, out one end, into, and up the other. LAN/WAN link and activity status indicators provide some visibility to the Network Interface layer.

ICMP echo requests and responses (Pings) provide some information regarding the proper functioning of the IP layer. SNMP processing indicators can be used to verify the passage of the packet through the UDP layer and the functioning of the Application layer. Each step can be verified independently until all steps are working correctly for end-to-end communication.

SNMP Inform The most under-utilized SNMP command - ever.
SNMP v2c was created to fill in some of the holes that SNMP v1 had. One such fix was the Inform Command. Unlike Traps, which are simply received by a manager, Informs are positively acknowledged with a response message. If a manager does not reply to an Inform, the SNMP agent will resend the Inform.

Informs are similar to a trap, with the exception of the confirmation response it requires from the manager that the inform is sent to. This makes it more robust than a standard trap and offers better reliability, but it also consumes more network resources.

Because the Inform command is newer to the SNMP game than Traps, it seems to be horribly under-utilized. If you have SNMP v2c or v3 and aren’t using Inform commands, then you are losing out on a valuable delivery guarantee that could prevent a major outage or other problem.
What can SNMP do for me?

SNMP has grown beyond its IP roots to play an important role in remote alarm monitoring of telecommunications networks. SNMP can do a lot to make your network alarm monitoring more cost-effective and your network more reliable - if you clearly identify your network monitoring goals and have the right tools to achieve them.

The advantages of SNMP are:

- **It’s LAN-based.** The long-term trend in the telecom industry has been to move support functions like alarm monitoring off dedicated copper lines and onto existing LAN/WAN infrastructure. This saves significantly on installation and operation costs and transports alarm data more reliably.
- **It’s an open standard.** SNMP is non-proprietary, fully documented, and supported by multiple vendors.
- **It can be easily extended.** SNMP is simple, but it’s also flexible enough to describe almost anything. Vendors and users of SNMP equipment can add to the Management Information Base (MIB) to include nearly any kind of device.
- **It provides a common management platform for many different devices.** If it’s supplied with the right MIB file, an SNMP manager can correctly interpret alarm data from any device that supports SNMP, creating greater interoperability between different parts of your network.

How can you best integrate SNMP into your network monitoring? Let us help you. DPS Telecom is the industry leader in hardware and software alarm monitoring solutions. We’ve helped many companies successfully implement SNMP-based monitoring, and we can do the same for you. We can help you find the right implementation strategies, avoid the pitfalls, and use SNMP effectively to increase your network’s reliability. (To read more on “8 Pitfalls When Integrating Incompatible Network Monitoring Systems and Protocols” - visit http://www.dpstele.com/network-management/guides/8-pitfalls.php)

You can find out more about what you can do with SNMP by checking out our SNMP Applications Knowledge Base (www.dpstelecom.com), a unique step-by-step guide to finding the right SNMP applications and products for your needs. And if you want to learn more, call 1-800-622-3314 to talk to a DPS Telecom Application Engineer about SNMP.

---

**UDP Isn’t Always Reliable**

UDP (User Datagram Protocol) is the IP transport layer protocol that supports SNMP messages. Unlike TCP, UDP is a connectionless protocol. A UDP host places messages on the network without first establishing a connection with the recipient.

UDP does not guarantee message delivery, but it’s a lightweight protocol that can transport a large number of status messages without using too many network resources.
The T/Mon LNX SNMP Manager:

A multiprotocol, multifunction network alarm manager designed as a single-platform solution for all alarm monitoring applications.

T/Mon collects alarm data from different equipment and protocols from hundreds of manufacturers.
The Pros and Cons of SNMPv1, v2c, v3...

As SNMP has evolved, each new version has included major feature modifications to improve functionality over the previous version. But, that doesn’t mean that older versions of SNMP don’t have their merits or that you should stop using and older version and upgrade. Each version of SNMP has its pros as well as cons (yes, even v3 isn’t perfect!). Here is a list of the pros and cons of each version, to help you choose which version is best for you.

<table>
<thead>
<tr>
<th>SNMP v1</th>
<th>SNMP v2c</th>
<th>SNMP v3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pros</strong></td>
<td><strong>Pros</strong></td>
<td><strong>Pros</strong></td>
</tr>
<tr>
<td>Open, standard protocol</td>
<td>SNMP Inform</td>
<td>Newest version</td>
</tr>
<tr>
<td>Only version supported by some smaller/older SNMP devices</td>
<td>Improved error handling (over v1)</td>
<td>Improved security with encryption</td>
</tr>
<tr>
<td></td>
<td>Improved SET commands (over v1)</td>
<td>Also has SNMP Inform</td>
</tr>
<tr>
<td><strong>Cons</strong></td>
<td><strong>Cons</strong></td>
<td><strong>Cons</strong></td>
</tr>
<tr>
<td>No encrypted security</td>
<td>Not all devices are SNMP v2c compliant</td>
<td>Not all devices are SNMP v3 compliant</td>
</tr>
<tr>
<td>No inform command available</td>
<td>No encrypted security</td>
<td>Inform is more complicated than v2c</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Problems can occur if two SNMP entities have the same EngineID</td>
</tr>
</tbody>
</table>

How to locate the correct MIB file in a ZIP.

When downloading a .zip file full of .mib files, it can be hard to determine which MIB you actually need. What's the difference between each file? Do I need all of them, or just a few for my specific device? If you don't know the answers to these questions, then downloading a .mib file can become a tedious process.

Have no fear! We spoke with Jerry Yang, DPS Engineer, to help you better understand MIB zip files and locate the correct one (or more) for you.

First, some companies provide a readme.txt (or similar) file as part of the .zip bundle. Because it is not a .mib file, it usually goes unopened. Mistake number 1. Believe it or not, this file is actually there for a reason and can help you decipher the rest of the .zip bundle. These files contain a list of what devices each .mib file relates to. There's no need to download files for a master if all you have is an RTU, and this readme.txt file can be key in sorting out those details.

Perhaps the .zip file doesn’t include a readme.txt file. Your next option is to check any device documentation that may have been provided with your RTU or master. The bottom line is that you should be able to find some sort of documentation that draws a figurative map of what you need.

Of course, if all else fails, you can always call their tech support line and ask. Any good company worth purchasing from should at least be able to assist you in determining which .mib file is right for you.
MIB 101
Decoding the Management Information Base

Understanding the Management Information Base (MIB)

An SNMP MIB (“Management Information Base”) is a simple file that is required for SNMP to function. It’s an ASCII text file that describes every data object (ex. “Temperature Sensor 2”) within a physical SNMP agent device (ex. “NetGuardian RTU”). It’s essentially a agent-to-manager dictionary of the SNMP language, where every object referred to in an SNMP message is listed and explained. In order for your SNMP manager to understand a device that it’s managing, a MIB must first be loaded (“compiled”).

If you’ve ever loaded driver files onto a PC for an external accessory (ex. USB device), you understand the concept of MIBs. Your SNMP device’s manufacturer should include a MIB with your purchase. You then simply have to compile it into your SNMP manager. The manager uses the MIB as a “reference chart” to understand traps, or messages, sent from SNMP devices in your network.

Going a little deeper, the function of the MIB is to translate numerical strings into readable text for humans. When an SNMP device sends a Trap or other message, it identifies each data object in the message with a number string called an object identifier (OID). This is great for a computer, but not easily readable for a human being. The MIB provides a text label for each OID. This is very much like DNS servers on the internet that translate numerical IP addresses (“216.58.194.206”) into domain names that you can read and easily remember (“google.com”).

Object Identifiers

Object identifiers, or OIDs are used to describe SNMP network elements by using a number string. Each segment in the number string denotes a different level in the order, starting with one of the two organizations that assign OIDs, all the way down to a unique manufacturer, a unique device, and a
unique data object. An OID may look like this: 1.3.6.1.4.1.2682.1

How OIDs are sent via SNMP
SNMP agents include OIDs with every Trap message they send. This allows the SNMP manager (by using the appropriate pre-compiled MIB) to understand what the agent is saying.

Similarly, when an SNMP manager wants to know the value of an object/characteristic, such as the state of an alarm point, the system name, or the agent uptime, it will assemble a GET packet that includes the OID for each object / characteristic of interest.

The agent receives the request and looks up each OID in its MIB. If the OID is found (because the object is managed by this agent), a response packet is assembled and sent with the current value of the object / characteristic included. If the OID is not found, a special error response is sent that identifies the unmanaged object. This tells the SNMP manager that it “has the wrong number”.

TRAPS: OIDs vs. variable bindings
When an agent sends a TRAP packet, it can optionally include value information (“variable bindings”) to clarify the event. Some RTUs use OIDs exclusively to encode event information (one unique OID for every conceivable TRAP event). Others use a single OID for most TRAP messages, then explain the event in variable bindings. Both schemes work. Just make sure you understand the difference so that you can configure your system correctly.

Well-designed SNMP managers can use variable bindings or OIDs to better correlate and manage network events. SNMP managers will also generally display detailed information (extracted from either variable bindings or MIB labels) to improve your understanding and decision-making.

MIB Manager Recommendations
MIB Managers are software applications that make it easy to explore your MIB files. They take the text file supplied by your device manufacturer and present them in a human-readable format.

Their features can vary, making it hard to know which one to use. That’s why we asked a couple of our engineers which ones they recommend and why.

“iReasoning MIB Browser is my top recommendation for MIB management. It’s free for SNMP v1 and v2c. The only downfall is you have to pay if you want to use it for SNMP v3.”
-Jerry Yang, Engineer

“If you have SNMP v3 I would recommend ManageEngine. It’s free and easy to use!”
-Reinier Jugao, Engineer
Case Study:
Nova Scotia Power Upgrades Obsolete SNMP Manager To T/Mon, Looks To Preventing Site Visits

Nova Scotia Power provides nearly 97 percent of the electricity for Nova Scotia, and has served as their main provider for over 80 years. This includes a growing base of some 483,000 commercial, residential, and industrial customers.

“Now we monitor the whole province, everything from power supplies, right through transportation equipment like the microwave and fiber.”

With the responsibility to produce and distribute over 13,000 gigawatt hours of electricity a year, a reliable network is priceless for Nova Scotia techs. Throughout the province, thousands of kilometers of transmission and distribution lines are used to deliver power. With their current SNMP manager becoming obsolete, it was time for Nova Scotia Power to hunt for a new, reliable monitoring system to serve on the front lines of their network. Richard Boutilier and Richard Itiveh share how Nova Scotia Power turned to DPS monitoring for the answer.

“I inherited the old system from the guy that retired,” said Boutilier, an Electronics Technician. “He pretty much built it, and I had to maintain it.” Keeping pace with the growing network, approximately 80 NetGuardians are now deployed throughout the network. “It wasn’t quite so many when I first started. Now we monitor the whole province, everything from power supplies, right through transportation equipment like the microwave and fiber.”

“I can see what with T/Mon, we’ll be able to store data that will help us track the reliability of our system”

When taking over the “old system,” Boutilier didn’t anticipate their current SNMP manager becoming obsolete. Their concern was finding a suitable replacement that would maintain their current level of network monitoring, while leaving room to add more levels of protection. “We wanted more visibility - a more user-friendly system for our techs,” Itiveh said.
The Answer: T/Mon
With DPS NetGuardians already deployed in their network, Nova Scotia turned to DPS for a better look at the T/Mon Alarm Management System. “I can see what with T/Mon, we’ll be able to store data that will help us track the reliability of our system,” Itiveh said. “We’re now at DPS to complete training. We just purchased a T/Mon, and it’s going to replace our obsolete [SNMP manager].”

“With T/Mon, we’ll be able to have records that say this alarm keeps coming in from this system at this site, and happens for several days, months or years.”

Factory Training at DPS Headquarters helped Boutilier and Itiveh decide where they want to see this new alarm system go. One item on Boutilier’s list is to reduce truck rolls for basic maintenance items “With the implementation of the T/Mon, I’d like to start doing things like weekly or monthly maintenance on our generators,” Boutilier explained. “We physically have to go to the site and do that now, so it would be nice to have that kind of control.”

T/Mon History Reports Can Help Save Time and Money
Looking to help cut costs with T/Mon in place, Itiveh plans on using T/Mon historical data to pin down common network problems. “With T/Mon, we’ll be able to have records that say this alarm keeps coming in from this system at this site, and happens for several days, months or years,” Itiveh said. “Down the road, we’ll be able to see we’ve got a flaky link.” Trending analysis will help Nova Scotia Power identify and prevent network-affecting issues.
5 Basic Capabilities to Look for in an SNMP Remote Monitoring Device

AN SNMP RTU with the right set of features will let you monitor all of your remote site equipment on one integrated SNMP-based platform. Integrating your monitoring has lots of advantages. You can monitor your whole network from one screen, greatly reducing the chances of missing an alarm. You’ll save money, because you won’t be needlessly duplicating equipment.

And because each remote site is covered by one compact high-capacity RTU, you can save remote-site space for revenue-generating equipment.

Here’s the 5 basic capabilities to look for:

1. **Discrete alarm inputs**, also called digital inputs or contact closures. These are typically used to monitor equipment failures, intrusion alarms, beacons, and flood and fire detectors.

2. **Analog alarm inputs**. These measure varying levels of voltage or current (not just on/off conditions) and are used to monitor variable conditions like temperature, humidity, and pressure, all of which can critically affect equipment performance.

3. **Ping alarms**. An RTU that supports ping alarms will ping devices on your network at regular intervals. If a device fails to respond, the RTU will send an alarm as an SNMP trap, providing immediate notification that the device has failed or gone offline.

4. **Control relays**. It’s a senseless waste of time and money to send a technician to a remote site miles away simply to turn a switch. An RTU with control relay outputs will let you operate remote site equipment directly from your network operations center (NOC).

5. **Terminal server functions**. Your RTUs can also serve as a terminal server to remote-site serial devices. Your devices connect to the RTU’s serial ports, giving you immediate Telnet access via LAN from your NOC at any time.

DPS Telecom offers SNMP RTUs that meet all these requirements - and also have compelling extra features like stand-alone local visibility through any web browser, expandable alarm capacity, LAN access via dial-up connection and more.
NetGuardian 832A G5
Not Just an SNMP RTU

The NetGuardian 832A G5 is a large-capacity RTU that monitors 32 discrete alarms and 8 analog alarms, pings 32 network elements, controls 8 relays, provides LAN reach through access to 8 serial ports, and reports via SNMP v1, v2c, v3, DCPX, e-mail, or pagers.

Visit dpstele.com/rtu for more information.

Also Available:
NetGuardian 864A G5

With twice the capacity of the 832A, the NetGuardian 864A can handle alarms from even the largest networks - and it’s STILL just 1 RU.
7 Fatal Mistakes Network Engineers Make When They Attempt to Integrate SNMP and Non-SNMP Systems
And How You Can Avoid Them

SNMP IS A STANDARD protocol that has wide acceptance in the industry and is flexible enough to describe almost anything. Because of these advantages, many network managers have come to believe that SNMP should be used for all telemetry monitoring applications.

SNMP certainly has its place in an effective telemetry monitoring solution, but this doesn’t mean that any off-the-shelf SNMP manager can provide adequate visibility and control of your network. Typical off-the-shelf SNMP managers are not designed for displaying and processing telemetry data for effective alarm management, especially for the kind of real-world monitoring tasks network managers most need performed. These capabilities can be added to an SNMP manager, but it usually requires substantial custom software development.

Before you buy, make sure you avoid these 7 fatal mistakes
Relying on off-the-shelf SNMP systems for mission-critical telemetry is a major mistake. If you’re switching from traditional telemetry or integrating non-SNMP monitoring with an SNMP-based system, an off-the-shelf SNMP manager will not provide the detailed alarm data you expect. Before you commit to an SNMP monitoring solution, you need to make sure it supports essential telemetry functions. There are seven fatal mistakes network managers typically make when integrating SNMP and non-SNMP monitoring. Your SNMP implementation will be successfully only if you can avoid them.

1. Selecting a system that doesn’t provide detailed alarm descriptions
A basic SNMP manager doesn’t record the location, time, severity, or a precise description of alarm events. To adapt an off-the-shelf SNMP manager to monitor these factors, you must create and maintain a master alarm list representing all the monitored points in your network — and then also create and maintain a database associating all the traps that may be sent to the SNMP manager with the alarms on that list.

2. Settling for a system that can’t identify cleared alarms
Even more database work is required to identify whether a trap corresponds to an alarm condition or a clear condition. Creating this addition to the trap association database often requires analyzing multiple variable bindings within the trap packet.

Above: Using a proxy device is a good way to mediate legacy and non-SNMP gear to your SNMP Manager.
3. Not maintaining a history of standing alarms
Relying on a basic SNMP manager for alarm management can potentially result in completely losing visibility of threats to your network. A basic SNMP manager doesn’t maintain a list of standing alarms. Instead, the typical SNMP manager maintains an event log of newly reported traps and a history log of acknowledged traps. As soon as a trap is acknowledged, it is considered cleared. Imagine what might happen to your network if a system operator acknowledges an alarm, and then, for whatever reason, fails to correct the alarm condition. Who would know the alarm is still standing?

4. Not identifying system operators
Basic SNMP managers do not record the identity of the system operator who acknowledges an alarm. In the example of the negligent system operator, it would be impossible to determine who had made the mistake or to assign responsibility for the resulting problems.

5. Trusting a system that’s insecure for multiple users
Out of the box, the typical SNMP manager is not designed for multi-user security. All traps are posted to one alarm list; all users may view all alarms, and all users may acknowledge all alarms.

6. Broadcasting all alarms to all system users
Basic SNMP managers have no built-in functions for organizing alarms by logical category, posting the same alarm to multiple logical categories, or sorting which alarms the user wants to see. If Jones is in charge of all equipment for the Western region, and Smith is in charge of power plants, both need to know about a generator failure in Tucson, but neither one needs to know about all the alarms in the network. And if one manager corrects the alarm condition and acknowledges the alarm, the other manager needs to know it was acknowledged and by whom. Unfortunately, standard SNMP managers will not support these functions.

7. Allowing yourself to be bombarded by nuisance alarms
No SNMP manager supports the advanced features necessary for best quality telemetry monitoring, such as notifications escalation, legacy protocol mediation, nuisance alarm silencing, automatic control relay operation, and automatic notifications by pager and e-mail.

How Can I Get a Customized SNMP Solution without Making These Mistakes?
It is true that many, but not all, of these functions can be added to standard SNMP managers, but implementing telemetry monitoring in a basic SNMP manager usually involves a substantial amount of custom software module development. Even when pre-built software modules are available, they usually require custom tweaking to perform exactly as you want them to.

The need for extensive customization eliminates the advantage of using a simple open standard, and it is difficult to justify significant development costs after purchasing an already expensive SNMP manager. Why take the time, trouble, and expense to recreate capabilities that are already present in a high-quality, SNMP-capable network alarm management system? And in fact, it is much easier to adapt a traditional telemetry master to process SNMP traps than to adapt an SNMP manager to perform telemetry functions. There is no question that SNMP is right for many applications, and it is clear that SNMP will be increasingly used in the future.

SNMP is an effective tool, but it’s only one item in your telemetry monitoring toolkit, and it can be used more effectively when it is part of a total alarm management solution.
Three Factors that Indicate You Need a Protocol Mediation Solution

Protocol Mediation Makes Your Monitoring More Flexible and Preserves Your Existing Equipment

INTEGRATING SNMP into your network monitoring doesn’t mean you have to abandon existing equipment that uses other protocols. The right protocol mediation solution will allow SNMP to happily coexist on your network with TL1, TBOS, TABS, or even manufacturers’ proprietary protocols.

1 Your network uses many different types of equipment from different vendors: It makes sense to integrate your monitoring to one common platform. Your staff won’t have to divide their attention between different monitoring screens, greatly reducing the chances of missing an alarm. And because you won’t be needlessly duplicating monitoring systems, you’ll save on costs for equipment, maintenance and staff training.

2 You inherited legacy equipment: Today’s telecom networks often resemble geological strata, with successive generations of monitoring equipment laid on top of each other. This is especially likely if your company has merged with another. If you have a lot of legacy equipment, it’s cost-prohibitive to replace it all, and if it’s still functional, you shouldn’t have to. At the same time, you don’t want your legacy equipment to cut off your options for adding new equipment as you need it. Protocol mediation lets you use old and new together.

3 Your vendor dropped support for your monitoring equipment: Orphaned network monitoring platforms are increasingly common today. Small and large manufacturers have left the monitoring equipment business, or gone out of business altogether; or companies simply stop supporting their older products. Unfortunately, you, the client, are left holding the bag - but a protocol mediation solution.
Mediating Protocols and Inputs/Outputs to SNMP

If most of your equipment natively reports alarms as SNMP traps, but you have some equipment that uses other protocols, you’ll probably want to mediate the non-SNMP alarms to SNMP. Depending on the scale of your operation, you’ll want to either mediate alarms at the individual remote site, or mediate alarms from several sites at a central office.

Remote Site Mediation of I/O
For remote-site mediation, DPS Telecom offers the NetGuardian 832A G5. The NetGuardian is an SNMP-based remote telemetry unit that accepts inputs from discrete, analog, and ping alarms and forward the data as SNMP traps to multiple SNMP managers.

Remote Site Mediation of Protocols
The NetMediator T2S G5 includes all the local site monitoring capabilities of the NetGuardian, plus it can mediate TBOS and TAB alarms to SNMP.

Central Office Mediation
For central-office mediation, the T/Mon LNX Network Alarm Management System serves as a general protocol mediation solution. T/Mon LNX collects alarms from many different types of equipment and protocols, mediates all alarm data to a common format, and forwards alarm data to other devices in a wide variety of protocols, including SNMP traps.

Mediating SNMP to Other Protocols
Alternatively, you may have a non-SNMP master that is deeply embedded in your network, but you need to monitor native SNMP devices like switches, routers, and DACs. In that case the correct solution is to mediate traps from the SNMP devices into the protocols used by your existing master. This solution is more practical and less expensive than replacing your existing master, and also avoids the trouble and costs of installing and maintaining a specialized SNMP manager to monitor only SNMP equipment.

If you are mediating alarms from SNMP to other protocols, you most likely are collecting SNMP traps from diverse equipment at various sites. You need a central office mediation solution that will collect the incoming traps in one place and mediate them all to different protocols before forwarding them to the higher level master.
DPS Telecom
Two Ways We Can Help You

Attend Tuition-Free Factory Training

DPS Telecom offers a week-long, tuition-free, training course. The class covers several different topics, including **SNMP**, and is taught by the DPS Engineers that design the product.

- Day 1: RTUs
- Day 2: T/Mon
- Day 3: T/Mon
- Day 4: **SNMP**
- Day 5: ASCII (optional)

Visit [www.dpstele.com/training](http://www.dpstele.com/training) for more information or to sign-up for a class.

Call Tech Support For Free 24/7

Need help fast? DPS Telecom offers free tech support 24/7 to all of their clients.

When you call DPS you’re NEVER trapped in Voice Mail Hell. You’ll be connected to a live, competent human being who understands your equipment and can quickly solve your problem.

Get Help Now!
support@dpstele.com
Tech support: (559) 454-1600
After hours: (559) 744-3771
SNMP Alarms
Receiving Traps is Only the Beginning of Effective SNMP Monitoring

THERE’S A BIG DIFFERENCE between basic alarm monitoring and intelligent alarm management. Any basic system will give you some kind of notification of an alarm. But simple status reports don’t provide effective full visibility of your network.

Automated Correction
Your staff can’t hover around a screen watching for alarms with their full attention 24/7. A simple system cannot get alarm information to the people who can correct problems quick enough to make a difference. And some problems require immediate action far faster than any human being can respond.

Using a basic alarm monitoring system makes it more likely that faults will not be corrected, potentially resulting in serious damage to your network and your revenue.

Intelligent Notification
An intelligent alarm management system won’t just tell personnel there’s a problem; it will locate the problem, provide instructions for corrective action, route alarm information directly to the people who need it, and, if possible, correct the problem automatically. Advanced features like these can make the difference between a minor incident and major downtime, and that’s a crucial edge to have in today’s competitive telecom industry.

Why You Need Help With Your SNMP Implementation

AS PART of a trend towards real time autonomous reporting and LAN-based network alarm monitoring, SNMP has become one of the most important tools in the arsenal of network managers. It’s flexible, relatively robust, and has become the standard native management protocol for many kinds of network enabled equipment.

Because of these advantages, many network managers have come to believe that SNMP should be used for all telemetry monitoring applications, and that an SNMP manager is the most effective telemetry monitoring solution.

However, an off-the-shelf SNMP manager cannot give you the full visibility of your network that is required for best quality network monitoring. SNMP can be a highly effective network monitoring tool, but implementing SNMP effectively requires expertise and experience in creating network monitoring solutions.

DPS Telecom can help you find the right SNMP implementation for your network and your business. DPS solutions for SNMP-based network monitoring have proved their capability in the thousands of implementations we have designed for our clients.

For 17 years, the exclusive focus of DPS Telecom has been creating network alarm monitoring solutions for real-world business environments. Our goal is to develop a perfect fit solution that achieves your monitoring goals.

Visit www.dpstelecom.com for more information.
Does Your Gear Make the Cut?  
Top 10 Ways to Evaluate SNMP Gear

SNMP RTU

1. **Support multiple managers**
   It’s important to have a backup SNMP manager in case anything goes wrong. If your SNMP RTU only supports one manager, you’re in trouble. Look for one that supports at least 2. Since there’s no extra hardware required, some smart manufacturers have given you a larger number like 4 or 8. Why not have flexibility for the future?

2. **Support backup notifications**
   SNMP is great, but anything is vulnerable to failure. Your network could go down at a site. That will kill off your SNMP notifications instantly. In situations like that, you NEED TO HAVE a backup. Your RTU might send text messages. It might call you with an automated voice message. It could even use older technologies like serial or 202 if you happen to have those available. Whatever you use, your backup will give you important situational awareness when SNMP is unavailable.

3. **Allow SNMPv3 security**
   SNMPv3 security requirements are coming. If you work at a security-conscious organization (large utility, corporation, or government agency), you’re probably already facing them. If you’re not, it’s only a matter of time. Fortunately, more and more RTUs are capable of sending secure, encrypted SNMPv3 traps. It’s an important layer of security that you just don’t get with SNMP v1 or v2c.

4. **Mediate other protocols to SNMP**
   You probably have some older equipment in your network that supports a protocol other than SNMP. It may not even have contact closure outputs and be totally dependent on that legacy protocol. Even if contact closures are available, protocol messages generally offer more alarm detail. That’s why having a smart SNMP RTU pays off. You can mediate your legacy protocol messages to SNMP traps. Handling this function in the RTU (rather than your SNMP manager) eliminates the need for legacy transport to leave the building. You’ll get all possible detail out of your device and bring it into your SNMP management umbrella.

5. **Have a proven design**
   Your SNMP RTUs get more than their fair share of punishment. They’re forced to operate in remote, unmanned facilities. Temperatures might be extreme. By their very nature, they have to be wired into everything else. It’s absolutely critical that your choose a proven RTU. Ask vendors about their deployments. Do they have a global footprint of happy customers, or are you the guinea pig?
SNMP Manager

6. Gracefully integrate non-SNMP equipment
SNMP has revolutionized remote asset management, but that doesn’t mean it covers 100% of your systems. You have to be able to accommodate whatever equipment you have in your network. You can’t just throw everything out when a new technology emerges. You have to support both during the transition. Choose an SNMP manager that can handle the other protocols you use in your network.

7. Display alarms on a map
If there’s been one technological innovation that has improved situational awareness among SNMP-manager users, it has to be map displays. When you’re responsible for a network that covers a large service territory, there’s just nothing clearer than seeing alarms placed on a geographic map. Lists are helpful. Maps are better. Choose an SNMP manager that has one.

8. Have a modern web interface
Especially in security-intensive environments, installing software is a pain. As you jump around the network, do you have the right software installed on all of your workstations? Do you have enough licenses? Web interfaces eliminate all of that. You just enter the IP address of your SNMP manager in your web browser. Done. You’ll get a clean, simple interface that you can access anywhere. Good SNMP managers will also tidy up the interface when you view it on your smaller smartphone screen.

9. Send SNMP GET “pings”
ICMP pings have long been a way for monitoring systems to verify that a LAN device is online. Master stations, including SNMP managers, can send pings at a defined interval (ex. every 5 minutes) to a list of devices. If a device fails to respond, that can trigger an alert so you know the device is malfunctioning. Unfortunately, some devices still respond to traditional ICMP pings when their higher-level functions have failed. To accommodate this, smart SNMP managers are capable of sending a “ping” in the form of an SNMP GET message instead. Because responding to an SNMP message is more complicated, you can be confident that your device is truly online and fully functional.

10. Have a proven design
It should go without saying, but you’d be surprised what well-intentioned people have tried. Your SNMP manager is the core of your remote management system. Don’t hack something together from open-source software and a few devices you bought online. Your business is a serious enterprise. Choose a proven SNMP manager that will support your network uptime.
DPS Telecom is a manufacturer of Remote Monitoring Equipment - including SNMP managers, agents and environmental sensors. Every product is built to order with your specs in mind.

At DPS Telecom, we see ourselves as your partner in securing your network. We will never leave you with a monitoring problem unsolved. We will always put your needs first. We back that philosophy up with 24-hour tech support - which our clients rate the best in the industry - installation assistance, off-site databasing, Factory Training, and maintenance agreements.