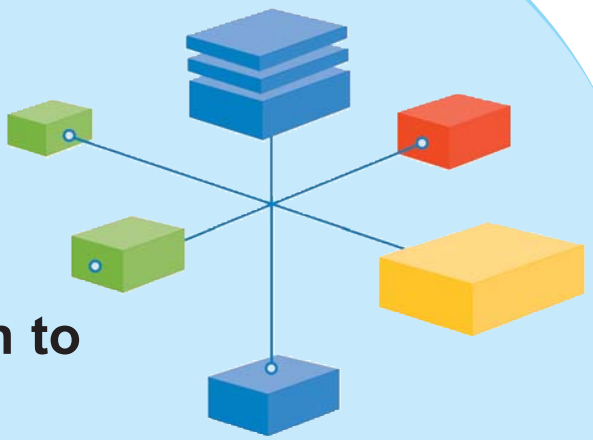
DPS Telecom

"Your Partners in Network Alarm Monitoring"



SNMP Tutorial:

The Fast Track Introduction to SNMP Alarm Monitoring

by Marshall DenHartog

Simple Network Management Protocol for real-world telecom network alarm monitoring . . .

- Fast, complete introduction to SNMP
- Effective telecom alarm monitoring with SNMP
- Integrating legacy equipment to SNMP monitoring
- Overcoming the limitations of SNMP
- Enhanced security with SNMPv3

Updated for SNMPv3

Version 2.0
Released July 21, 2010

www.dpstelecom.com · 1-800-622-3314 US $36.95

Printed in the U.S.A

How This Guidebook Will Help You

Most SNMP reference books aren't written for you, the telecom professional who needs to monitor network alarms with SNMP. Instead, most SNMP books are written for IT techs. That's great if you want to manage a computer network, but it's useless if you need carrier-grade network visibility of telecom equipment and remote sites.

This guidebook has been created to give you the information you need to successfully implement SNMP-based alarm monitoring in your network. It's an introduction to SNMP strictly from the prospective of telecom network alarm management, with fast specific answers to help you make SNMP monitoring work in your network.

Contents

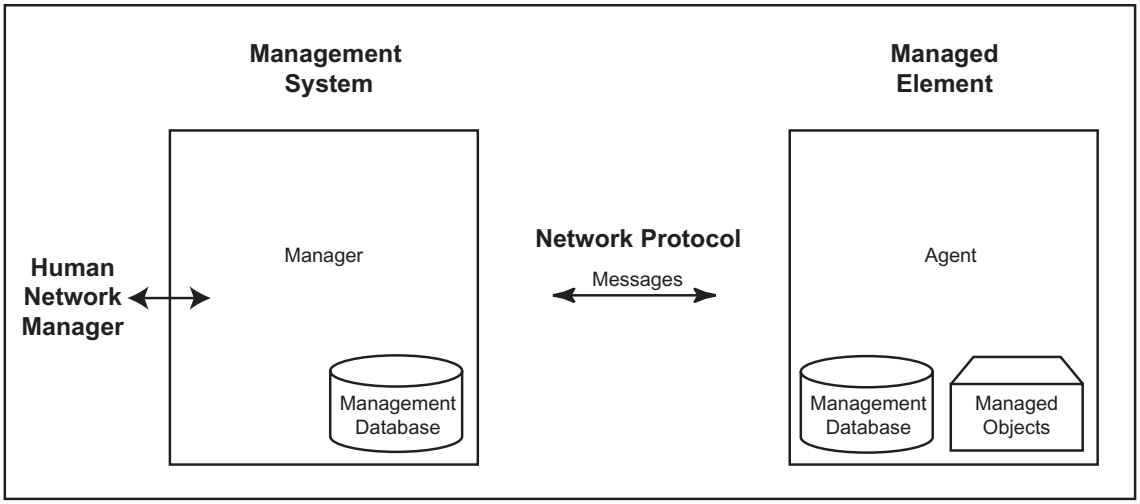


Figure 1. SNMP uses a manager/agent architecture. Alarm messages (Traps) are sent by the agent to the manager.

Part 1: An Introduction to SNMP

SINCE ITS CREATION in 1988 as a short-term solution to manage elements in the growing Internet and other attached networks, SNMP has achieved widespread acceptance.

SNMP was derived from its predecessor SGMP (Simple Gateway Management Protocol) and was intended to be replaced by a solution based on the CMIS/CMIP (Common Management Information Service/Protocol) architecture. This long-term solution, however, never received the widespread acceptance of SNMP.

SNMP is based on the manager/agent model consisting of a manager, an agent, a database of management information, managed objects and the network protocol. The manager provides the interface between the human network manager and the management system. The agent provides the interface between the manager and the physical device(s) being managed (see illustration).

The manager and agent use a Management Information Base (MIB) and a relatively small set of commands to exchange 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 in SNMP messages.

Reality Check: What Can SNMP Do For Me?

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**. Moving your alarm monitoring off dedicated copper lines and onto existing LAN/WAN infrastructure creates significant savings. LAN data transport reduces 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.

That's what's good about SNMP — but there's also some pitfalls that you have to watch out for. If you're not careful, it's easy to wind up with a system that costs too much and does too little. For a full report on 8 pitfalls to avoid, call DPS at 1-800-622-3314.

You can avoid the risks (and guarantee the benefits) of your SNMP implementation by working with an experienced vendor who can help you accurately determine your network monitoring needs. To learn more, call **1-800-622-3314** and ask for your free Network Monitoring Needs Analysis.

Part 2: How SNMP Handles Alarm Messages

SNMP USES FIVE basic messages (Get, GetNext, GetResponse, Set and Trap) to communicate between the manager and the agent.

The Get and GetNext messages allow the manager to request information for a specific variable. The agent, upon receiving a Get or GetNext message, will issue a GetResponse message to the manager with either the information requested or an error indication as to why the request cannot be processed.

A Set message allows the manager to request a change be made to the value of a specific variable in the case of an alarm remote that will operate a relay. The agent will then respond with a GetResponse message indicating the change has been made or an error indication as to why the change cannot be made.

The Trap message allows the agent to spontaneously inform the manager of an "important" event.

As you can see, most of the messages (Get, GetNext, and Set) are only issued by the SNMP manager. Because the Trap message is the only message capable of being initiated by an agent, it is the message used by DPS Telecom remote telemetry units (RTUs) to report alarms. This notifies the SNMP manager as soon as an alarm condition occurs, instead of waiting for the SNMP manager to ask.

The small number of commands used is only one of the reasons SNMP is simple. The other simplifying factor is its reliance on an unsupervised or connectionless communication link.

This simplicity has led directly to its widespread use, specifically in the Internet Network Management Framework. Within this framework, it is considered robust because of the independence of the managers from the agents; that is, if an agent fails, the manager will continue to function, or vice versa.

Reality Check: What Features Do I Need in an SNMP RTU?

HOW DO YOU find the right SNMP RTU? Look for more features than just SNMP support. Many devices can output SNMP Traps — when you're evaluating an RTU, look instead at how many alarm monitoring functions it can perform.

Here are 5 essential features that your SNMP RTU must have:

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:** While discrete alarms monitor on/off conditions, analog alarms measure continuously variable levels of voltage or current. Analog alarms monitor 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:** Don't waste time and money sending 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 NOC.
5. **Terminal server function:** Your RTU 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 offer stand-alone local visibility through any web browser, expandable alarm capacity, LAN access via dial-up connection and more.

To learn more about DPS RTUs, request a live Web demo at www.dpstelecom.com/webdemo.

Essential SNMP: What is a Trap?

An SNMP Trap is a change-of-state (COS) message — it could mean an alarm, a clear or simply a status message. You often have to parse variable bindings to decode a Trap. To make sure the meaning of a Trap is understood, all DPS Telecom SNMP equipment transmits a unique Trap ID for both alarm and clear for each alarm point. Unlike a classic telemetry master, basic SNMP managers don't keep a standing alarm list, so it's difficult to tell what's happening in your network by looking at a list of Traps.

Part 3: Understanding the MIB (Management Information Base)

EACH SNMP element manages specific objects with each object having specific characteristics. Each object/characteristic has a unique object identifier (OID) consisting of numbers separated by decimal points (e.g., 1.3.6.1.4.1.2682.1). These object identifiers naturally form a tree as shown in the below illustration. The MIB associates each OID with a readable label (e.g., dpsRTUAState) and various other parameters related to the object. The MIB then serves as a data dictionary or codebook that is used to assemble and interpret SNMP messages.

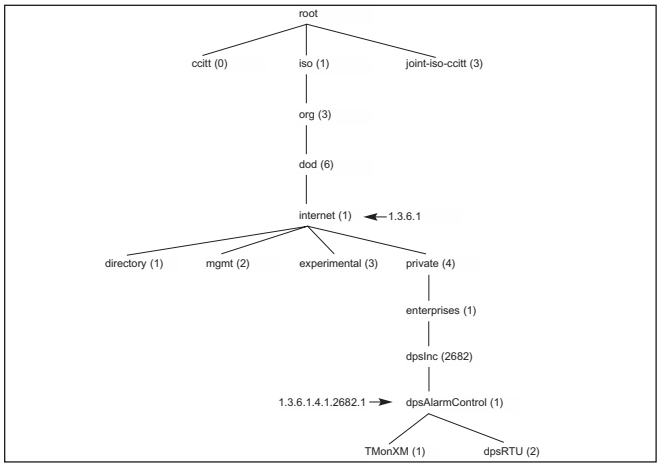


Figure 2. The branch of the MIB object identifier tree that represents managed elements used by DPS Telecom equipment.

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 element uptime, it will assemble a GET packet that includes the OID for each object/characteristic of interest. The element receives the request and looks up each OID in its code book (MIB). If the OID is found (the object is managed by the element), 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.

When an element sends a Trap packet, it can include OID and value information (bindings) to clarify the event. DPS remote units send a comprehensive set of bindings with each Trap to maintain traditional telemetry event visibility. Well-designed SNMP managers can use the bindings to correlate and manage the events. SNMP managers will also generally display the readable labels to facilitate user understanding and

Essential SNMP: What is the MIB?

The MIB lists the unique object identifier (OID) of each managed element in an SNMP network. Your SNMP manager can't monitor your devices unless it has compiled their MIB files. The MIB is also a guide to the capabilities of your SNMP devices. For example, if your device's MIB lists OIDs for Traps but not for GetResponse messages, you know it will report alarms, but will not respond to alarm polls. Learning to read MIBs is difficult, but it's worth the trouble.

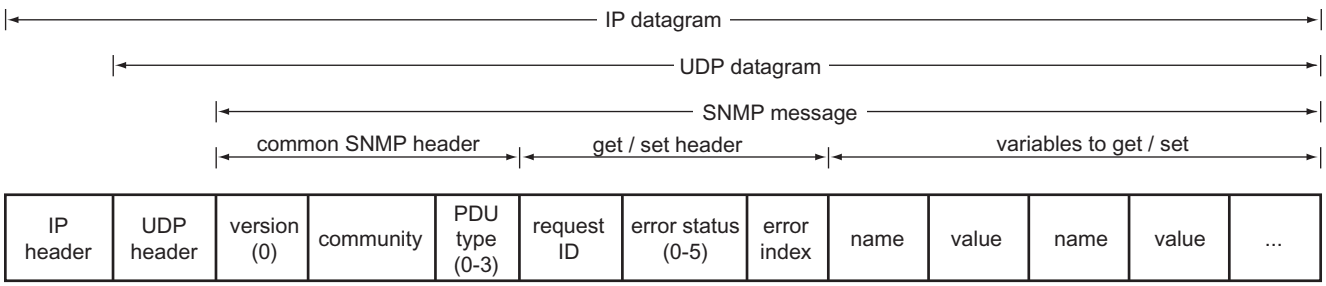


Figure 3. The SNMP data packet is enclosed in the UDP data packet, which is enclosed in the IP data packet.

decision-making.

Part 4: Understanding Packet Types and Structure

Let's examine the communication between managers and agents. 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 with the following SNMP v1 packets (Protocol Data Units or PDUs) used to communicate:

Get
GetNext
Set
GetResponse
Trap

The manager sends a Get or GetNext to read a variable or variables and the agent's response contains the requested information if managed. The manager sends a Set to change a variable or variables and the agent's response confirms the change if allowed. The agent sends a Trap when a specific event occurs.

Figure 3 (above) shows the packet formats. Each variable binding contains an identifier, a type and a value (if a Set or GetResponse). The agent checks each identifier against 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

Reality Check: 4 Signs You Need Protocol Mediation

1. **You have a lot of non-SNMP equipment:** Before planning your SNMP implementation, do a site survey and find out how much non-SNMP equipment you have in your network. Changing out a large number of non-SNMP devices can add hundreds of thousands of dollars to your project costs. Protocol mediation saves you money by keeping your non-SNMP equipment in place.
2. **You want to gradually migrate from your old system:** It's time to replace your older system - the master is starting to fail, and it's hard to get new remotes. But you can't afford a forklift swapout of your whole system. Protocol mediation lets you integrate your old remotes to an SNMP manager, so you can replace your legacy system step by step.
3. **You inherited someone else's incompatible system:** If your company has merged with another, you might find yourself responsible for a whole new network of incompatible equipment. You can't afford to replace this network, but you need to integrate it into your existing operations. Protocol mediation will merge your two networks at minimal expense.
4. **You don't want to pay license fees:** You may have to pay a separate license fee for every device you monitor with your SNMP manager. If you have a large network, that can get real expensive real fast. A protocol mediator can take input from your whole network and consolidate it to one SNMP input, at only one license fee.

Essential SNMP: What is UDP?

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 variable and sometimes interpret its value.

Part 5: Understanding Layered Communication

A Critical Tool for Troubleshooting Communication Problems

WE CONTINUE to examine the Simple Network Management Protocol (SNMP) focusing specifically on the layered communication model used to exchange information. The last section focused on the structure of SNMP messages, however an SNMP message is not sent by itself. It is wrapped in the User Datagram Protocol (UDP), which in turn is wrapped in the Internet Protocol (IP). These are commonly referred to as layers and are based on a four-layer model developed by the Department of Defense (you may recall the DoD origins of the Internet).

SNMP resides in what is called the Application layer, UDP resides in the Transport layer and IP resides in the Internet layer (somewhat obvious). The fourth layer is the Network Interface layer where the assembled packet is actually interfaced to some kind of transport media (for example, twisted pair copper, RG58 co-axial or fiber). While this multi-layer model may seem a bit confusing, it effectively isolates the tasks of

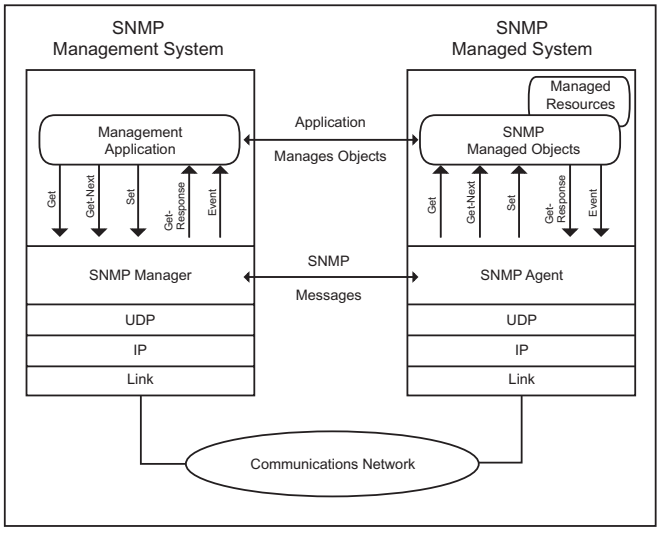


Figure 4. An SNMP message passes through the protocol layers at both the manager and agent. Each layer does a specific communication task.

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

Reality Check: How Protocol Mediation Works

PROTOCOL MEDIATION converts legacy alarms to SNMP Traps, enabling you to monitor all your equipment from your SNMP manager.

Mediating other protocols to SNMP

For remote-site mediation, DPS Telecom offers the NetGuardian 832A and the NetMediator. The NetGuardian is an SNMP-based remote telemetry unit that accepts inputs from discrete, analog and ping alarms, then forwards the data as SNMP Traps (v1, v2c, or v3) to multiple SNMP managers. The NetMediator includes all the local site monitoring capabilities of the NetGuardian, plus it can mediate TBOS and TABS alarms to SNMP.

NetGuardian 832A

NetMediator

For central-office mediation, the T/Mon Remote Alarm Monitoring System serves as a general protocol mediation solution. T/Mon 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.

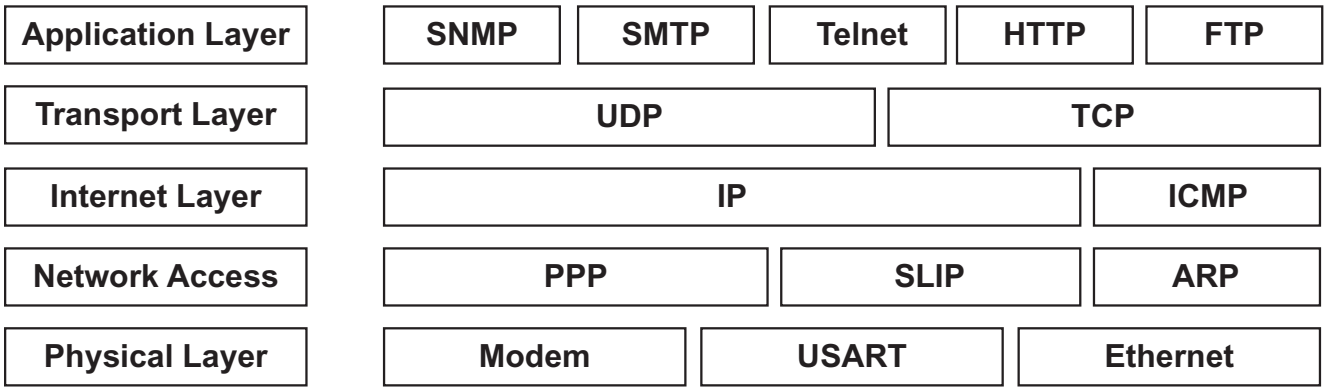


Figure 5. SNMP's location in the TCP/IP protocol stack. SNMP is an applications-layer component of the TCP/IP suite of protocols

perspective. The SNMP manager wants to know what the Agent's System Name is and prepares a GET message for the appropriate OID. It then passes the message to the UDP layer. The UDP layer adds a data block that identifies the manager port to which the response packet should be sent and the port on which it expects the SNMP agent to be listening for messages. The packet thus formed is then passed to the IP layer. Here a data block containing the IP and Media Access addresses of the manager and the agent is added before the entire assembled packet gets passed to the Network Interface layer. The Network Interface layer verifies media access and availability and places the packet on the media for transport.

After working its way across bridges and through routers (the modern equivalent of over the rivers and through the woods) based on the IP information, the packet finally arrives at the agent. Here it passes through the same four layers in exactly the opposite order as it did at the manager. First, it is pulled off the media by the Network Interface layer. After confirming that the packet is intact and valid, the Network Interface layer simply passes it to the IP layer. The IP layer verifies the Media Access and IP address and passes it on to the UDP layer where the target port is checked for connected applications. If an application is listening at the target port, the packet is passed to the Application layer. If the listening application is the SNMP agent, the GET request is processed as we have discussed in previous articles. The agent response then follows the identical path in reverse to reach the manager.

Troubleshooting IP Communication Problems

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.

Part 6: 7 Reasons Why a Basic SNMP Manager Is a Lousy Telemetry Master

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.

The typical off-the-shelf SNMP manager is not designed for displaying and processing telemetry data, especially not for the kind of real-world monitoring tasks network managers most need performed. These capabilities can be added to an SNMP manager, but it may require substantial custom software development.

Using an off-the-shelf SNMP systems for mission-critical telemetry is disappointing at best and disastrous at worst. If you're used to the standards of classic telecom telemetry, 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.

Before you buy … check for these 7 essential telemetry features:

1. **Basic SNMP managers don't provide complete, precise alarm descriptions**
   A basic SNMP manager doesn't record location, time, severity or descriptions 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. **Basic SNMP managers can't identify cleared alarms**
   Even more work is required to identify whether a Trap represents an alarm or a clear condition. Creating this addition to the Trap association database often requires analyzing multiple variable bindings within the Trap packet.

Reality Check: 7 Features That SNMP Managers Can't Match

1. **Detailed alarm notifications in plain English that your staff will immediately understand and take action on.** Every notification includes full information about the alarm, including its severity, location, date/time stamp, and a user-defined description.
2. **Immediate notification of changes of state (COSs)**, including new alarms and alarms that have cleared. You don't have to hunt to find out what's changed in your network — T/Mon lists it for you.
3. **A continuously updated list of all current standing alarms.** Even if the system operator acknowledges the alarm, it remains in the Standing Alarms screen until it is cleared.
4. **Text message windows displaying specific instructions for the appropriate action for an alarm.** System operators, even without extra training, will know precisely what to do and who to call in case of an alarm.
5. **Nuisance alarm filtering.** Unimportant alarms that generate meaningless status notices or oscillate between alarm and clear conditions subconsciously train your staff to ignore the alarm monitoring system. T/Mon filters out nuisance alarms, allowing your staff to focus its attention on serious threats.
6. **Pager and e-mail notifications.** Send alarm notifications directly to maintenance personnel, even if they're away from the NOC.
7. **Derived alarms and controls** that combine and correlate data from multiple alarm inputs and automatically control remote site equipment to correct complex threats.

The T/Mon NOC Remote Alarm Monitoring System provides total visibility of your network status and automatically notifies the right people to keep your network running.

Sign up for a Web demo of T/Mon NOC at www.dpstelecom.com/webdemo

3. **Basic SNMP managers don't maintain 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. **Basic SNMP managers don't identify 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. **Basic SNMP managers are insufficiently secure 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. **Basic SNMP managers don't sort or filter alarms**
   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. **Basic SNMP managers don't provide the alarm notification you need**
   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.

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.

For details about an alarm management system that overcomes these 7 barriers , send an email to:

solutions@dpstelecom.com

Case Study: KMC Telecom saves $2 million per year through in-house monitoring

WHY PAY someone to do something you can do yourself? That was the question KMC Telecom, a fast-growing integrated provider of voice, data, and Internet services, asked itself in 2001. Until last year KMC relied on an outsource provider to monitor its fiber optic network, which stretches over 30,000 miles across 35 states. KMC decided it could save money by monitoring their network themselves. KMC created a highly successful network operations center in Huntsville, Ala. Since the Huntsville NOC began operation, KMC has saved substantially on operations costs while creating a real-time monitoring capability that proved itself during November's tornado strike.

"It's really added to our peace of mind to be able to see what's going on real-time"

KMC's move from outsourced to in-house monitoring was one more milestone in the telecom's growth from start-up to major-league CLEC. KMC had outsourced network monitoring since the foundation of its fiber optic network in the mid-1990s. The growth of the company and its network had by 2001 created a situation where it was both possible and necessary to use economies of scale to cut operational costs.

In reliable hands: KMC Telecom's team now has total control at their finger tips. They no longer have to pay for outsourced monitoring and are finding their response times to network outages have improved now that they can view alarm events in real-time.

"We'd outsourced our monitoring since we deployed our facilities network," says Harold Moses, director of operations for KMC in Huntsville. "For most start-ups, it's not economical to do these things for yourself. But as the network grew, it became more and more practical for us to take monitoring in house. We're looking at cost savings and how to integrate costs."

Moses says that operating its own NOC has saved KMC millions. "We've cut the operational expenses significantly. The total project resulted in about $2 million a year in savings. The NetGuardian equipment was a part of that." The Huntsville NOC relies on the alarm collection capacity of DPS Telecom's NetGuardian. KMC has NetGuardians in 48 different locations across the United States, where they monitor the integrity of KMC's fiber optic network as well as environmental, power, and security alarms in KMC's numerous remote sites.

KMC has deployed 60 NetGuardians and 120 NetGuardian Expansions. This should give you some idea of the scope of KMC's operations; altogether, the Huntsville NOC monitors approximately 3,000 alarm points. Monitor data from the NetGuardians is sent as SNMP Traps to the Huntsville NOC, where it is displayed using HP OpenView internet usage manager software. Moses says the decision to use the NetGuardian came from knowledge of the quality of older DPS Telecom products and research into current alarm monitoring offerings

"DPS Telecom gives us a reliable way of accessing a variety of equipment, regardless of the brand or provider. We now have a common interface for our existing system."

from a number of vendors. The deciding factor was that the NetGuardian gave KMC a cost-effective means of using its existing equipment.

"DPS Telecom gave us a reliable way of accessing a variety of equipment, regardless of the brand or provider. We now have a common interface for our existing system. We did quite a lot of research of what was available. We thought that the NetGuardian had a lot of flexibility, in terms of the various software options and terminal capacity," says Moses. According to Dale Stinson, manager of the Huntsville NOC, the NetGuardian was the solution that made the most sense for cost and capability.

"NetGuardian was the only solution that met both our technical and our budget needs," Stinson says. "The NetGuardian is tightly integrated with the way we work, in how it handles SNMP Traps and its tight integration with HP OpenView." Monitoring the network in-house has also improved KMC's monitoring visibility in ways that are impossible to accomplish with a third-party provider, Stinson adds.

"The NetGuardian is tightly integrated with the way we work, in how it handles SNMP Traps and its tight integration with HP OpenView."

"It's really added to our peace of mind to be able to see what's going on real-time. Outsourced monitoring can't see problems in real time," Stinson says. The real-time monitoring capability was of great service on the morning of Nov. 11. Tornados had ripped through Alabama, Mississippi, Ohio, Pennsylvania, and Tennessee, knocking out the commercial power supply to several KMC Telecom sites. "Nine out of 10 of these sites are unmanned," says Stinson. "We have automatic backup generators, but we still need to send a technician to the site. It would have taken us several minutes longer to respond if we were still using outsourced monitoring. Being able to do real-time in-house monitoring probably shaved 30 minutes off our response time."

Understanding SNMPv3

SNMPV3 FEATURES several enhancements over earlier versions, but security is the most significant in the majority of SNMP applications. SNMPv3 messages may be protected in 2 ways, including encryption to protect the contents of any intercepted traps. SNMPv3 encrypts messages using CBC-DES encryption, a part of the Universal Security Model (USM).

The "EngineID" Unique Identifier
The EngineID in SNMPv3 uniquely identifies each SNMP entity. Conflicts can occur if two SNMP entities have duplicate EngineID's. The EngineID is used to generate the key for authenticated messages.

Authentication
Authentication is one of two types of security available in SNMPv3. It is used to ensure that traps are read by only the intended recipient. As messages are created, they are given a special key that is based on the EngineID of the entity. The key is shared with the inteneded recipient and used to receive the message.

Privacy
The other of the two SNMPv3 security types, Privacy encrypts the payload of the SNMP message to ensure that it cannot be read by unauthorized users. Any intercepted traps will be filled with garbled characters and will be unreadable. Privacy is especially useful in applications where SNMP messages must be routed over the Internet.

The Cost of Security Nothing is free. SNMPv3 can be the secure network management solution you need, but you must be prepared for the additional processing time required to calculate EngineID's during authentication and encrypting/decrypting Privacy-enabled messages. Ultimately, you must decide if the enhanced security of SNMPv3 is worth the cost in your application. If you don't need the security, you're probably best running an earlier version that is simpler to maintain.

SNMPv4?
In an effort to reduce the need for future versions of SNMP, the SNMPv3 protocol was designed with greater flexibility than previous versions. This is expected to make the lifespan of SNMPv3 longer than its predecessors.

Quick and Dirty SNMP Checklist

5 Steps You Can Take Today to Start Your SNMP Monitoring Project

☐ Assess Your Existing Network

Start with a thorough assessment of your exiting network equipment and data transport, checking for what you already have that's compatible with SNMP. The more you can keep, the more you'll save on capital expenditures.

☐ Survey Your Existing Data Transport

The biggest challenge in your SNMP implementation is ensuring you have enough bandwidth for SNMP traffic. Examine your present telemetry map. Identify existing transport and identify what adjustments need to be made.

- ☐ **Check for SNMP-ready transport: LAN, overhead channel, channel bank, order wire or PPP over a dial-up or direct link**
- ☐ **Make sure transport has adequate bandwidth for UDP traffic**
- ☐ **Check if low-bandwidth transport can be rerouted to high-bandwidth**

☐ Survey Your Existing Equipment

Determine how much of your currently existing network elements support SNMP, so you can plan systematically what upgrades will be necessary for SNMP-based monitoring

- ☐ **Equipment that natively supports SNMP**
- ☐ **Equipment that can be firmware upgraded to support SNMP**
- ☐ **Equipment that can be swapped out for a later SNMP model**
- ☐ **Equipment that cannot be economically replaced with a direct SNMP equivalent (Don't replace this equipment — look for a protocol mediation solution instead)**

☐ Collect MIB Files for Your Equipment

Make sure that you have the correct Management Information Base (MIB) files for all of your equipment. The MIB file enables the SNMP manager to interpret Trap messages from devices. MIB files are equipment specific, so it's important to make sure that you have the correct MIB for your equipment type, model, and version number.

☐ Plan Your SNMP Implementation Budget

Watch out for the capital expenditure and installation manpower costs of a forklift swapout. Use protocol mediation solutions to make your existing network SNMP ready. This will avoid the costs of a systemwide replacement, keeping your budget within reasonable limits

SNMP Troubleshooting Guide

Not getting Traps from your SNMP RTU? Here's some quick troubleshooting steps to isolate the problem:

- ☐ **Check RTU configuration**
  - ☐ **Is the Trap address set to the correct IP address for the SNMP manager?**
  - ☐ **Is the RTU configured to send Traps to Port 162? (Port 162 is the standard port for receiving SNMP Traps — if your SNMP manager uses a different port, make sure all devices are configured for the same port)**
  - ☐ **Are all alarm points on the RTU configured to send Traps?**
  - ☐ **Does the Trap community string on the RTU match the Trap community string on the SNMP manager?**
- ☐ **Use packet sniffer at RTU end to make sure Trap PDUs are sent.**
  If no packet sniffer is available, proceed to the next step. If your RTU is a DPS Telecom unit, use the Analyze mode of your included configuration software.
- ☐ **If RTU configuration is correct, check network communication between the SNMP manager and the RTU**
  - ☐ **Ping the RTU from the SNMP manager**

  If the ping is unsuccessful, check the firewall configuration. Reconfigure firewall to allow UDP traffic at Port 162 (or port used by your SNMP manager)
  - ☐ **Use packet sniffer at SNMP manager end to make sure Trap PDUs are arriving at the manager.**
- ☐ **If Trap packets are arriving, check SNMP manager configuration**
  - ☐ **Double-check Trap community string settings**
  - ☐ **Make sure that the right MIB file for the RTU has been compiled on the SNMP manager**
- ☐ **If no Trap packets are arriving at the SNMP manager, there is an error in the network settings. Consult your network administrator.**

SNMP Glossary

Agent: A hardware device or software program that reports to an SNMP manager. In network alarm management, an SNMP agent is typically an RTU, but other network devices like switches, routers and hubs can also act as SNMP agents. An SNMP agent can also be a subsection of a larger device, like the SNMP Agent software module in T/MonXM, which mediates T/Mon alarms to SNMP traps.

Authentication: An SNMPv3 security measure that ensures that only the intended recipient receives the SNMP message. Secret authentication keys are generated based upon the EngineID of the SNMP entity.

Community string: An SNMP security password. There are three kinds of community strings:

Read Community: Allows an SNMP manager to issue Get and GetNext messages.

Write Community: Allows an SNMP manager to issue Set messages

Trap Community: Allows an SNMP agent to issue Trap messages.

Compiling: The process of importing a MIB file into an SNMP manager. To compile properly, a MIB file must be formatted in a text file according to the Structure of Management Information (SMI) standard.

COS (Change of State) alarm: A telemetry alarm that is clearly labeled as reporting a change in status from clear to alarm or from alarm to clear.

EngineID: In SNMPv3, a unique identifier for each SNMP entity. An entity may send an empty message to another entity to request its EngineID prior to initiating communication.

Event: In SNMP terms, any change of status in a managed object in the network. SNMP equipment can generate traps for many different kinds of events, not all of which are important for telemetry. The ability to filter unimportant events is essential for high-quality SNMP alarm management

Get: An SNMP message issued by a manager that requests the status of a managed object.

GetNext: An SNMP message issued by a manager, used to walk down a range of OIDs. The GetNext request retrieves the value of the managed object one number after the OID listed in the request.

GetResponse: SNMP message issued by an agent in response to a Get, GetNext or Set request from the SNMP manager.

Inform Notification: An SNMP message (supported in some v2c and v3 implementations) that is similar to a trap- but requires a confirmation response from the manager. This is more robust than a standard trap and offers better reliability, but it also consumes more network resources.

Internet Protocol (IP): the network layer datagram protocol of the TCP/IP protocol suite. SNMP runs over UDP, which in turn runs over IP.

Managed Objects: Values of network devices that can be read or overwritten by the SNMP manager, like alarm status, control relay status, system uptime, etc. In SNMP terms, every network device is defined in the MIB as a set of managed objects.

Management Information Base (MIB): The MIB is a data structure that describes SNMP network elements as a list of data objects. To monitor SNMP devices, your SNMP manager must compile the MIB file for each equipment type in your network.

Manager: A top-level SNMP master system (hardware or software) serving as the human interface to the SNMP network. The manager can issue Get, GetNext and Set requests to agents and receives GetResponse and Trap

messages.

MD5: One process for generating authentication/privacy keys in SNMPv3 applications.

NMS: Network Management Software or Network Management System. Another term for SNMP manager software or hardware.

Object Identifier (OID): A number that uniquely identifies a managed object in an SNMP network. An OID consists of a series of numbers separated by decimal points. Each decimal point represents a leaf node in the tree structure of the MIB. For example, all OIDs for DPS Telecom equipment begin with the numbers 1.3.6.1.4.1.2682. This sequence represents: iso (1); org (3); dod (6); internet (1); private (4); enterprises (1); dpsInc (2682).

Ports 161 and 162: The virtual ports most commonly used to transmit SNMP messages. Port 161 is used for messages
sent by the manager, and Port 162 carries messages sent in the opposite direction from agents.

Privacy: An SNMPv3 security measure. Privacy encrypts the message contents using a key, so the contents of intercepted messages will not be readable.

Protocol Data Unit (PDU): An SNMP message. There are 5 types of PDU in SNMP v1: Get, GetNext, Set, GetResponse and Trap.

Packet Internet Gopher (PING): An ICMP (Internet Control Message Protocol) echo request to determine whether a device on an IP network is online.

Proxy agent: An SNMP agent that translates non-SNMP messages and inputs to SNMP. In network alarm monitoring, a proxy agent is usually an RTU that converts contact closure inputs to SNMP traps, like the NetGuardian 832A. Devices that mediate other alarms in other protocols to SNMP, like the NetMediator T2S (TBOS to SNMP) is also a proxy agent.

Referenced (RFC) MIBs: MIBs that are required by the main MIB during compiling. If any of these referenced MIBs are missing, the main MIB will not compile properly.

Set: An SNMP message issued by a manager instructing an agent to change a Managed object to a new value

SHA: One process for generating authentication/privacy keys in SNMPv3 applications.

Simple Network Management Protocol (SNMP): the standard TCP/IP protocol for managing IP network devices.

Standing alarm list: A list of all uncleared alarms, as maintained by a full-featured network alarm management system. Standard SNMP managers automatically delete all acknowledged traps, but a standing alarm list displays every alarm that has not been reported as cleared by the monitoring equipment.

Structure of Management Information (SMI): the standard that defines the MIB structure.

Transmission Control Protocol (TCP): the more common transport layer protocol in the TCP/IP suite. TCP is considered a “reliable” protocol because it establishes a connection between the host and the recipient, guaranteeing delivery. UDP, the transport protocol used for SNMP does not establish a connection or guarantee delivery.

Trap: An SNMP message issued by an SNMP agent that reports an event.

User Datagram Protocol (UDP): the transport layer protocol used to send SNMP messages. Unlike TCP, UDP is a connectionless protocol that does not guarantee delivery of the data packet. However, UDP uses fewer network resources than TCP, making it more suitable for transporting a large number of status messages.

Variable Binding: the data field of a GetResponse or Trap PDU. Each variable binding lists a managed object and its current value.

SNMP Monitoring Solutions from DPS Telecom

Trap Processors

T/Mon LNX: Full-featured alarm master for up to 1 million alarm points. Features support for 25 protocols, protocol mediation, alarm forwarding, pager and e-mail alarm notification, Web Browser access, multi-user access, standing alarm list, alarm history logging. Available SNMP software:

T/MonXM SNMP Agent Software Module: Forwards T/Mon alarms in SNMP.

T/MonXM SNMP Trap Processor Software Module: Receives SNMP traps; displays as standard T/Mon alarms.

T/Mon SLIM: Light capacity regional alarm master. Supports up to 64 devices and 7,500 alarm points. Features pager and email alarm notification, Web Browser access, standing alarm list and alarm history logging.

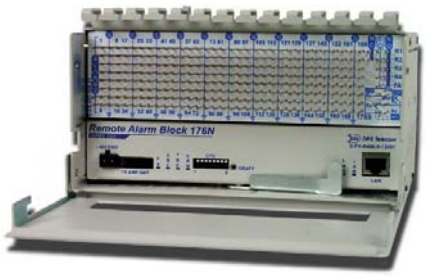
Remote Telemetry Units

NetGuardian 832A: RTU monitors 32 alarm points, 8 analog inputs, 8 control relays, 32 ping targets, 8 terminal server ports; reports in SNMP

NetGuardian 216: RTU monitors 16 alarm points, 2 analog inputs, 2 control relays, 1 terminal server port; reports in SNMP.

NetGuardian 480: RTU monitors 80 alarm points, 4 control relays; reports in SNMP.

NetMediator T2S: Protocol mediator converts 8 TBOS ports, 32 alarm points, and 8 analog inputs to SNMP; 8 control relays, 4 terminal server ports.



Remote Alarm Block 176N: Wire-wrap alarm block monitors 176 alarm points, 4 controls; reports in SNMP.

Call 1-800-622-3314 for price and ordering information

Reality Check: Why You Need Help With Your SNMP Implementation

IMPLEMENTING AN SNMP network alarm monitoring system can seem deceptively easy — you just look on the Web, find a few vendors, compare a few features, add some configuration and you're done, right?

The truth is, developing a network monitoring system on your own is one of the riskiest things you can do. Here are some of the typical problems you might face if you don't get expert advice when you're designing your system:

1. **Implementation time is drawn out:** It's going to take longer than you think. Network monitoring is a highly technical subject, and you have a lot to learn if you want a successful implementation. And anytime you are trying to do something you've never done before, you are bound to make mistakes — mistakes that extend your time and your budget beyond their limits.
2. **Resources are misused:** If you're not fully informed about your options for mediating legacy protocols to SNMP, you may replace equipment that could have been integrated into your new system. Rushing into a systemwide replacement when you could have integrated can cost you hundreds of thousands of dollars.
3. **Opportunities are missed:** If you install a new network monitoring system today, you're committing your company to that system for as long as 8 to 10 years. Many telecoms design what they think is a state-of-the-art monitoring system — and then find that their technology is actually a generation behind.

DPS Telecom Guarantees Your Success — or Your Money Back

When you're choosing a network monitoring vendor, don't take chances. Be skeptical. Ask the hard questions. Above all, look for experience. Don't take a sales rep's word that his company can do custom development. Ask how many systems they've worked with, how many protocols they can integrate to SNMP, and check for client testimonials.

DPS Telecom has created hundreds of successful SNMP monitoring implementations for telecoms, utility telecoms, and transportation companies. (Check out www.dpstelecom.com/case-studies for some examples.) DPS Telecom monitoring solutions are proven performers under real-world conditions.

You're never taking any risk when you work with DPS Telecom. Your SNMP monitoring solution is backed by a 30-day, no-risk, money-back guarantee. Test your DPS monitoring solution at your site for 30 days. If you're dissatisfied for any reason, just send it back for a full refund.

What to Do Next

Before you make a decision about your SNMP monitoring, there's a lot more you need to know. There's dangers you want to avoid — and there's also opportunities to improve your remote site maintenance that you don't want to miss.

Get the information you need — register now for a free, live Web demonstration of SNMP monitoring solutions with the T/Mon Remote Alarm Monitoring System. There's no obligation to buy — no high-pressure salesmen — just straightforward information to help you make the best decision about your network monitoring. You'll get complete information on hardware, software, specific applications, specifications, features and benefits . . . plus you'll be able to ask questions and get straight answers.

Call 1-800-622-3314 today to schedule your free Web demo of SNMP monitoring solutions — or register on the Web at www.dpstelecom.com/tmon-webdemo.

"I would personally like to let you know how beneficial the installation of the SNMP responder was to the mission of our department. We were looking for a way to integrate our local ILEC region in HP OpenView without a major network change. The SNMP responder was the answer. This migration will allow us not only to monitor all alarms in one spot but also build extensive collection reports of our whole network."

—**Todd Matherne**, EATEL

"It is hard to find companies with the intelligence and aptitude to meet the customer's exact needs, and I believe that is what DPS is all about."

—**Lee Wells**, Pathnet

About the Author

Marshall DenHartog has 12 years' experience working with SNMP, including designing private MIB extensions, creating SNMP systems for multiple platforms, and developing SNMP-based monitoring for several nationwide networks.

DenHartog's experience with both the theoretical and practical sides of SNMP have equipped him to write a straightforward guide to SNMP for real-world use.

www.dpstelecom.com
1-800-622-3314

DPS Telecom
"Your Partners in Network Alarm Monitoring"

US $36.95