How to Successfully Implement SNMP In Your Network

A Practical, Step-by-Step Guide

• Learn The 5 Key Steps to SNMP Implementation...

• See How Controlled SNMP Migration and Protocol Mediation Can Modernize Your Network...

• Understand The 4 Most Common SNMP Pitfalls - And How To Avoid Them...

www.dpstelecom.com  • 1-800-622-3314
How This White Paper Will Help You

How much do you need to know about SNMP to implement SNMP alarm monitoring on your communications network?

Fortunately, you don’t need to study SNMP on a theoretical level to make your implementation successful. But there are some SNMP issues that are potential pitfalls, and you need to know how to avoid them.

This paper is a step-by-step guide to SNMP alarm monitoring implementation, focusing on the practical problems that can arise and how to solve them.

Contents

Introduction ......................................................... 3
Preliminary Planning: Assess Your Existing Network Before You Budget ......................................................... 3
Learn SNMP the Easy Way: Attend DPS Telecom Factory Training ................................................................. 3
Step One: Plan Your SNMP Reporting ................................................. 4
All SNMP Is Not Equal ................................................................. 4
Step Two: Survey Your Existing Equipment - What Do You Want to Monitor? ................................................. 5
DPS Telecom Remote Site Survey ................................................................. 5
Step Three: Survey Your Existing Data Transport ................................................. 7
What Equipment Can Be Mediated to SNMP? ................................................................. 8
Step Four: Collect MIB Files for Your Equipment ................................................. 9
Step Five: Plan Your Migration Budget ................................................. 10
Choose Your SNMP Manager With Care ................................................................. 11
How You Can Migrate to LAN, Without Killing Your Budget ................................................................. 11
How LAN Migration Works ................................................................. 12
Potential Pitfall #1: High Costs of Migrating Remote Sites to LAN ................................................................. 12
Potential Pitfall #2: High Costs of Replacing Non-SNMP Equipment ................................................................. 13
Potential Pitfall #3: Losing Valuable Monitoring Capabilities ................................................................. 13
No-Risk, Custom Engineering ................................................................. 13
Potential Pitfall #4: Manpower Costs ................................................................. 14
Learn More In A Live Meeting Room ................................................................. 14

© Copyright 2004, 2005, 2006, 2008 DPS Telecom
All rights reserved, including the right to reproduce this white paper or portions thereof in any form without written permission from DPS Telecom. For information, please write to DPS Telecom 4955 E. Yale Ave., Fresno, CA 93727-1523 1-800-622-3314 • info@dpstele.com
Printed in the U.S.A
Introduction

You’ve just been put in charge of implementing SNMP alarm monitoring on your network. Maybe you just inherited a system. How do you know it was built right in the first place? What do you really need to know about SNMP to make this transition work?

You could spend months studying protocol architecture or MIB structure, but that’s not necessary to get a monitoring project off the ground.

You don’t need to know SNMP on a theoretical level to make your SNMP deployment successful. SNMP telemetry is still telemetry, and most of what you already know still applies.

In fact, your telemetry experience is going to be highly valuable during your SNMP implementation. Even though it uses an IP protocol, SNMP equipment is not plug-and-play simple. You still have to deal with all the usual issues of a telemetry deployment, like data transport, interface compatibility, configuration, and debugging.

But there are also some SNMP-specific issues that you need to be aware of. These issues can potentially turn into pitfalls that can stop your SNMP implementation in its tracks, stretch your project over time and over budget, even reduce your overall visibility of your network. We’ll flag the problems you may run into and offer some suggestions for solving them.

Preliminary Planning: Assess Your Existing Network Before You Budget

Before you start any work on your deployment—even budgeting—you need to begin with a thorough assessment of your existing network, to determine how much of your existing transport and network equipment is compatible with SNMP monitoring.

You certainly want to identify any potential replacement issues before you budget, or you may be caught short by unexpected problems. But equally, you want to take advantage of opportunities to reduce your capital expenditures by continuing to use existing transport and equipment.

Network surveys can be complex. A software survey tool can help make sure you don’t miss any essential network elements.

For some ideas on how to evaluate your network, see “DPS Telecom Remote Site Survey,” on page 5.

Learn SNMP the Easy Way: Attend DPS Telecom Factory Training

“DPS Factory Training is a big help in not feeling intimidated by your network monitoring system. It’s excellent — presented in the right way and tailored to the needs of the class.”

— Bill Speck, 3 Rivers Telephone

Learn network alarm monitoring in-depth in a totally practical hands-on class. The DPS Telecom Factory Training Event will show you how to make your alarm monitoring easier and more effective. You’ll learn SNMP alarm monitoring, ASCII alarm processing, derived alarms and controls, and how to configure automatic email and pager notifications. DPS training is the easiest way to learn alarm monitoring, taught by technicians who have installed hundreds of successful alarm monitoring deployments.

For dates and registration information, call 1-800-693-3314 today or go to www.dpstelecom.com/training.
Step One: Plan Your SNMP Reporting

Before diving into MIBs, traps, and all the technical aspects of SNMP, you’ll need a solid plan to get you to your ultimate goal of successful SNMP implementation. This step involves taking a closer look at your network as a whole to just how SNMP reporting will tie everything together.

Here are a few important questions you’ll need to answer during this planning phase:

1. Where are your alarm masters? Are they located at a single NOC or do you have a backup master at another site?
2. If you have equipment that natively supports SNMP, what version(s) can they use? Remember that not all SNMP versions are the same. (See “All SNMP Is Not Equal” below.)
3. What kind of visibility do your alarm masters need? For certain masters that are rule-based, you may not want total visibility. Writing and adding rules for this filtering could become expensive in a hurry. Adding a sub-master to act as an SNMP filter may be the more cost-effective choice for downstream alarm filtering.

A master needed for regional use has a few visibility options. It can be used to filter only certain types of alarms, such as power alarms, that are forwarded on to your MOM (Master of Masters.) In another scenario, you may want only critical alarms, regardless of type, to be forwarded. You filter alarms by type or level of severity.

All SNMP Is Not Equal

There are 3 main versions of SNMP, with each one offering more and more capabilities. The 3 versions are SNMPv1, SNMPv2c, and now SNMPv3. Over time, security enhancements and other features were added to versions of SNMP, and it’s important to understand the differences between them.

SNMP v2c offers a variety of improvements over v1. One significant advantage is the ability to use the new Inform notification in place of traps.

Trap notifications, supported in SNMP v1 and later, are considered non-robust because the SNMP manager doesn’t send an acknowledgement in response to the Trap. The device sending the Trap sends it only once. The sending device has no confirmation that the Trap has been received, so there’s no guarantee that the alarm information has been successfully sent to the SNMP manager.

Inform notifications, supported in some SNMP v2c implementations or SNMP v3, are designed for confirmed deliv-
ery. When an SNMP manager receives an Inform, it sends a confirmation response back to the SNMP agent device. A well-designed SNMP agent device doesn’t receive a response to its Inform, it resends it until the SNMP manager sends the confirmation response or the specified number of retries is exhausted. Other managers not designed as well are not as robust in their re-try attempts.

SNMPv3 features several enhancements over earlier versions, but **security is the most significant SNMPv3 enhancement**. SNMPv3 messages may be protected in 2 ways, including encryption to protect the content of any intercepted communication.

SNMPv3 encrypts messages using CBC-DES encryption, a part of the Universal Security Model (USM). It 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.

It is important to know which version(s) of SNMP is supported by the equipment currently in your network, as well as any other equipment you plan on integrating into your network.

**Step Two: Survey Your Existing Equipment - What Do You Want to Monitor?**

The next step in your network assessment is determining how much of your existing network elements support SNMP.

As in Step One, your goal here is to collect information about your existing network so you can systematically plan what upgrades will be necessary for SNMP monitoring.

If you’re lucky, much of your current equipment will already support SNMP. A lot of recently manufactured equipment is built with native SNMP support, so your newer equipment may already be SNMP-ready, even if you’ve never used that capability before.

Now let’s look at your network elements that don’t support SNMP. Some of these may be upgradable. Check with the manufacturer of your equipment to see if there is an SNMP upgrade option.

The upgrade could be as simple as installing new firmware on the equipment, but you may have to replace your existing equipment with a later model that supports SNMP.

Unfortunately, for some of your equipment, upgrade options just won’t be available. The manufacturer may no longer sup-

---

**Questions to Ask: Your Remote Site Survey**

**RTU Capacity and Function**

1. How many remote sites do you need to monitor?
2. Do you want video surveillance at those sites?
3. Do you want a building access control system to manage entry to those sites?
4. How many alarm points do you need to monitor at each site?
5. How much growth, in sites and alarms at each site, do you anticipate over the next 5 years?
6. Do you need any analog inputs (e.g., voltage, temperature, humidity, signal strength)?
7. How many ASCII device (e.g., switches, routers, etc.) will you monitor at your remote sites?

**Installation**

1. How do you currently connect to your remote sites? (LAN, overhead, digital or analog circuit, terminal server, microwave?)
2. Do any of your sites support an alternate path communications link?
3. What type of power do you have at the master and remote sites? (–48 VDC, 110 VAC, other?)
4. How do you want to mount your RTUs? (23” rack, 19” rack, wall, tabletop?)
5. Who will install your RTUs?

This is just a small sample of the DPS Telecom Remote Site Survey. The full Remote Site Survey is a complete 5-page guide to evaluating your network alarm monitoring needs. For your copy of the Remote Site Survey, call DPS Telecom at 1-800-622-3314.
port your model, or, in some cases, the manufacturer may no longer be in business.

In those cases, you’re going to have to consider replacing the equipment with something entirely new. But you have to be careful about replacing equipment — it can involve unnecessary costs.

Another potential problem is that new SNMP equipment may not be equivalent to your older equipment. Replacement may mean giving up useful features of your legacy equipment.

Besides your SNMP-native equipment, consider what else in your network you also need to monitor. These may be things you have not yet tied into your network. Do you want to monitor doors? Temperature at remote sites? Legacy gear? Use the following survey to determine how they can be monitored using SNMP.

After completing your equipment survey, you can divide your equipment into four categories:
1. Equipment that natively supports SNMP.
2. Equipment that can be firmware upgraded to support SNMP.
3. Equipment that can be swapped out for a later SNMP model.
4. Equipment that cannot be replaced with a direct SNMP equivalent. (This is the most dangerous equipment-related pitfall — for solutions, see “High Costs of Replacing Non-SNMP Equipment,” right, and “Losing Valuable Monitoring Capabilities,” pages 12-13.)
Using this information, you can create a conversion plan for implementing SNMP monitoring on your network. You now have a list of what needs to be upgraded to use SNMP, and how it can be upgraded.

When you combine this list with the transport network map you created in Step One, you should now have a complete diagram of how your network needs to be adapted to put SNMP monitoring into place.

**Step Three: Survey Your Existing Data Transport**

The big challenge in your SNMP implementation is making sure that you have enough bandwidth for SNMP traffic going to all your remote sites.

So this step in your network assessment is to examine your present telemetry network map. You need to identify the existing transport that’s currently in place and determine if any adjustments need to be made for SNMP monitoring.

Your goal here is to collect the information you need to create a new network drawing that represents the transport you’ll need to deploy in order to support SNMP monitoring. This new map will be your guide to planning your transport upgrades.

The ideal transport for SNMP data is LAN (10/100/1000 BaseTen are all ideal, however, DSL is also a viable choice)–but in many cases, your LAN is not going to extend to all your remote sites. Another option is transport via T1.

If no LAN connection is available, you do have other options. You can also send SNMP data over an order wire, a radio overhead channel, a channel bank, or PPP over a dial-up or direct link.

The key question for all of these alternative transports is this: Do they provide sufficient bandwidth?

---

**Your Migration RTU Solution: The NetGuardian 832A G5**

- Wireless connection option - GSM or CDMA
- High Capacity: 32 discrete alarms (expandable to 176), 32 ping alarms, 8 analog alarms, 8 controls, and 8 serial ports
- **SNMPv3 compatible**
  - Dual 10/100 NIC
  - RoHS 5 or 6
  - 8-port terminal server for multiple-user LAN access to PBXs and switches

- Fiber interface option (100BaseFX)
- Internal modem for dial-up backup path
- Configure and monitor via Web browser
- E-mail and pager notifications
- Free lifetime firmware upgrades
- Free Windows-based utility for off-site editing and LAN-based remote provisioning
- Multiple customization and expansion options
- **HTTPS option (SSL)**

For more information, check out the NetGuardian on the Web at [www.DpsTelecom.com/RTUS](http://www.DpsTelecom.com/RTUS)
UDP packets are small, and most SNMP traps are small, so you don’t need a huge amount of bandwidth, but there has to be enough for your probable amount of network traffic. Insufficient bandwidth is going to increase latency and reduce response time. Medium-bandwidth transport might be OK, but smaller bandwidths are going to be clearly inappropriate for mission-critical network alarm monitoring.

You should be very careful about using lower-bandwidth transports like 202 channels or serial links. These connections should be analyzed for their speed and capacity before being certified for SNMP traffic.

You should also watch out for communications links that involve multiple conversions from one type of transport to another. These will also increase the latency of your SNMP monitoring, the complexity, and cost as well.

At any site where the currently available data transport is less than optimum, you’re going to have to consider upgrading to a higher-bandwidth connection. There are often other benefits to extending your LAN that help with project justification purposes. Perhaps the most significant of which is to be able to communicate faster and administer remote equipment in the field. Also, in many cases, you can save cost by decommissioning higher maintenance circuits and canceling third party contracts associated with them.

When you complete your transport survey, you’ll be able to divide your sites into four categories:

What Equipment Can Be Mediated To SNMP?

- Switches
- Microwave radios
- Routers
- SONET equipment
- Channel banks
- Channel Service Units (CSUs)
- Digital Access Cross-Connect Systems (DACS)
- Digital Service Units (DSUs)
- Network Interface Units (NIUs)
- Multiplexers
- Muldems
- Modbus devices
- ASCII printer and logger devices
- Any equipment that generates alarms in ASCII, DCM, DCP, DCPf, DCPx, E2A, TABS, TBOS, or TL1
1. Sites that have transport that is already adequate for SNMP traffic.
2. Sites whose data traffic can be re-routed from low-bandwidth transport to high-bandwidth transport.
3. Sites that can be economically upgraded to bandwidth adequate for SNMP traffic.
4. Sites that cannot be easily or cheaply upgraded to high-bandwidth or LAN traffic. (This is a serious potential pitfall; please see “High Costs of Migrating Remote Sites to LAN,” in the adjacent sidebar.)

Using this information, you can now redraw your telemetry network map to represent how your transport network needs to look for SNMP monitoring. This updated map will be your guide to systematically and efficiently upgrading your transport network.

Step Four: Collect MIB Files for Your Equipment

After completing Steps One and Two, you should now have a plan for:

1. How you’re going to transport SNMP data from your remote sites.
2. How you’re going to ensure SNMP compatibility for your telemetry equipment.

Your next step is to make sure that you have the correct Management Information Base (MIB) files for all of your equipment.

MIB files have an elaborate inner structure, but you don’t need to know too much about it to use them. The important thing to know about a MIB file is that it’s a kind of dictionary or code book that is used to assemble and interpret SNMP messages.

Each type of device on your network has its own specific MIB file. The MIB file defines the device as a set of managed objects — values that can be read or changed by the SNMP manager.

The MIB file enables the SNMP manager to interpret trap messages from devices. To make sense out of a trap that’s sent by a network element, the SNMP manager needs to have access to the MIB that describes the format and content of the possible traps that the element can send.

To be available for the SNMP manager, the MIB file for each of your equipment types needs to be installed on the SNMP manager, a process that’s called “compiling.”

The Building Access System (BAS) is a comprehensive building management system that integrates into an existing alarm management platform. With the system in place, a log of all site access, including the time of day and location that access was granted, is maintained. In addition, alarms such as intrusions and excessive access attempts are reported to a T/Mon on a per door basis.

- Centralized entry-management and control
- Controls and regulates up to 16 door entry points
- Supports up to 1,300 users
- Users can be granted access by day of the week, time of day and location
- Supports up to 16 doors per site
- Units function independent of master
- System can withstand connectivity losses to the local NetGuardian and T/Mon
- Entry Control Unit (ECU) passes on access codes to the NetGuardian for validation
- Proxy card reader eliminates the chance of forgotten keycodes and increases your level of access control
The network administrator in charge of the SNMP manager can handle the chore of compiling. All you need to do is ensure that the correct MIB file for each equipment type is collected and provided to the network administrator.

This is relatively simple, because MIB files are created and supplied by equipment vendors. The MIB file should have been provided on disk with your equipment; if it can’t be located, contact your equipment vendor for assistance. 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. This information should be documented by your equipment vendor. In some cases a vendor may supply multiple MIB files.

For more information on the MIB see our white paper “How To Read and Understand the SNMP MIB,” at www.dpstele.com/white-papers.

**Step Five: Plan Your Migration Budget**

Now that you’ve gone through the preliminary planning in Steps One through Three, you can now begin planning the budget for your SNMP implementation.

Hopefully, examining your existing data transport and telemetry equipment has helped you identify areas of your network that can be preserved without upgrading.

Using migration and mediation solutions, considerable portions of your network can be made SNMP ready without the costs of wholesale replacement. This can go a long way to keeping your capital expenditure budget within reasonable limits.

But you also need to watch out for costs related to installation manpower. A complete changeover of entire systems, or “forklift swapout,” can strain your personnel budget as well as your Cap-X budget.

Trying to replace large portions of your network at once can take more man-hours than you have personnel — or overtime budget — to cope with.

And buying equipment that you can’t install can hurt your projects finances as well. Equipment that’s sitting in a warehouse instead of operating in the field generates no return on investment.

A migration solution can help with this problem as well. You don’t have to purchase more equipment than your available manpower can conveniently install within any budget period. When you decommission your old alarm masters you’ll be saving yourself from the support headaches, maintenance time, downtime, and service agreements associated with them.

When planning your migration it’s important to not forget the big picture. Installing a state of the art element manager with impressive monitoring capabilities provides numerous benefits. See page 10 for some examples of the benefits unified alarm monitoring visibility of your entire network can provide.
Choose Your SNMP Manager With Care

An efficient SNMP manager will offer different strategies for determining “keep alive.” The idea behind this process is to continually check that your network equipment is online. The absence of traps and alarms isn’t always a good thing. What if your device loses power, or your LAN to that site goes down? The T/Mon NOC master, for example, issues “Get” commands and ICMP pings to answer the question, “Are you still there?”

Also beware of any ongoing costs associated with buying a new SNMP master. Particular things to be on the lookout for are continuing licensing fees. Some vendors may charge licensing fees per device or device type. Other licensing fees are wide open, so you may only have to pay them once. Make sure you understand all the terms before such fees eat up your OpEx cost.

Keep in mind that different SNMP managers will report alarms differently. One reason is the interpretation of MIB files. Some SNMP managers support add-ins that are installed in the framework. Some of these frameworks have an attractive interface - but don’t get blindsided by bells and whistles. These add-ins may use a colorful display to show alarms, but can disappear once you ack the event. This can be very misleading since the alarm’s condition still stands and nothing has been done yet to fix the problem. Since you need alarms to propagate to multiple points of visibility, you may have to make a choice between style and substance.

How You Can Migrate to LAN, Without Killing Your Budget

Installing LAN connections at remote sites is a significant cost—it can be the single biggest expense of your SNMP implementation. Many remote sites are distant and isolated, making them difficult to be integrated into your corporate network.

Fortunately, you don’t need a LAN connection at every remote site. SNMP data can also travel over an alternative transport, like PPP over a dial-up connection or dedicated line. The answer is controlled migration to LAN transport.

Alarm Master Choice: T/Mon NOC

T/Mon NOC has many features to make your alarms more meaningful, including:

1. Detailed, plain English alarm descriptions include severity, location and date/time stamp.
2. Immediate notification of COS alarms, including new alarms and alarms that have cleared.
3. Standing alarm list is continuously updated.
4. Text message windows displaying specific instructions for the appropriate action for an alarm.
5. Nuisance alarm filtering, allowing your staff to focus its attention on serious threats.
6. Pager and email notifications sent 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.

For more information, check out T/Mon on the Web at www.dpstele.com/tmon.
Remote access to sites with LAN

How LAN Migration Works

Step One: Install an SNMP RTU with Dial-Up or Dedicated Line Capability

In a controlled LAN migration strategy, you first integrate your remote sites into your SNMP-based monitoring system, using existing transport.

To do this, all you need is an SNMP-based remote telemetry unit (RTU) or proxy device that supports both LAN transport and your existing transport.

Alarm data is collected by the RTU, reported via dial-up to a PPP server which connects to the SNMP manager.

Step Two: Install a LAN Connection

Later, a LAN connection is installed at the remote site. The same SNMP RTU installed in Step One can be immediately transferred to LAN transport with minimal configuration—and without disconnecting alarm inputs. (Figure 2).

A dial-up connection can be retained as backup secondary connection in case of LAN failure.

You don’t have to cut over all your sites at once—you can gradually migrate different sectors of your network to LAN, as your budget and installation manpower allows.

Benefits of LAN Migration

- **Spread the expense of installing LAN over several budget cycles.** Completing a major installation in one budget cycle can strain your Cap-X and staffing budgets. With controlled migration, you control the pace of migration, so it happens as quickly or as slowly as you like.

- **Minimize equipment costs.** With LAN migration, you only have to buy one SNMP RTU for each of your remote sites, and it’s compatible with both your old and your new transport.

- **Implement SNMP monitoring now at all your remote sites.** Without LAN migration, you’d need to maintain a separate legacy alarm monitoring system to monitor your non-LAN sites. Operating two unintegrated alarm systems is a bad idea—it means higher maintenance costs, higher training costs, and watching multiple screens to monitor your network.

Installing LAN transport at these sites can be a significant cost item, one that can cause your SNMP implementation project to go over budget in the first stages.

You could decide simply to not implement SNMP monitoring at these sites for the time being, and go back to them at a later budget cycle.

But postponing your SNMP migration not really a viable solution, either. It will mean an extended transition period, and during that time you’ll have to maintain your legacy monitoring platform to support those sites. Operating two unintegrated platforms is a headache in itself — it means higher maintenance costs, higher training costs, and having to watch multiple screens to stay on top of your network.

But there is a solution. You can install SNMP network elements that can support both LAN and your existing legacy transport. These elements can access your LAN through a dial-up connection to a PPP server, either over a public switched network or a dedicated line.

4 Most Common SNMP Pitfalls - And How to Avoid Them

Potential Pitfall #1:

High Costs of Migrating Remote Sites to LAN

The first speed bump you may hit in your SNMP implementation are remote sites that can’t be gracefully migrated to LAN.

After you’ve completed your transport survey, you may find that you have some remote sites that don’t fit into Category 4: the existing transport is inadequate for SNMP; there’s no available alternative high-bandwidth route; and they can’t be economically upgraded to LAN.

Installing LAN transport at these sites can be a significant cost item, one that can cause your SNMP implementation project to go over budget in the first stages.

You could decide simply to not implement SNMP monitoring at these sites for the time being, and go back to them at a later budget cycle.

But postponing your SNMP migration not really a viable solution, either. It will mean an extended transition period, and during that time you’ll have to maintain your legacy monitoring platform to support those sites. Operating two unintegrated platforms is a headache in itself — it means higher maintenance costs, higher training costs, and having to watch multiple screens to stay on top of your network.

But there is a solution. You can install SNMP network elements that can support both LAN and your existing legacy transport. These elements can access your LAN through a dial-up connection to a PPP server, either over a public switched network or a dedicated line.
This solution lets you immediately implement SNMP monitoring at these sites, but you can postpone a LAN upgrade at the site until a later budget cycle. And you’re still minimizing equipment costs, because the same equipment supports both LAN and dial-up connections.

**Potential Pitfall #2:**

**High Costs of Replacing Non-SNMP Equipment (If replacement is possible!)**

Another place where your SNMP implementation budget can get derailed is the sheer expense of replacing a lot of equipment.

It takes a lot to make a remote site run — not just the primary equipment, but also essential secondary equipment such as battery plants, rectifiers, generators.

And to keep full visibility of your remote site, you also need to monitor environmental factors: temperature, humidity, fire, flooding.

Your telephony gear can possibly be replaced with SNMP native equipment — at considerable expense.

But your essential secondary monitoring equipment probably has no SNMP native equivalent. You could maintain a second legacy telemetry system to monitor power and environmental factors, but again, splitting your monitoring across two or more screens is not the best solution.

Fortunately, in many cases, replacement is simply unnecessary. Your equipment does not have to natively support SNMP for you to monitor it using SNMP.

A proxy device can accept standard discrete and analog alarm inputs and convert them to an SNMP trap.

**Potential Pitfall #3:**

**Losing Valuable Monitoring Capabilities**

Even if your budget will cover it, replacing your existing equipment with SNMP-native equipment is not always your best course of action. There’s no guarantee that your new SNMP equipment will have the same functions, or be as capable, as the equipment it replaces.

Being locked into one telemetry protocol is just as dangerous as being locked in to one equipment vendor — it severely limits your equipment choices. And in network monitoring, not having all the features you need can limit your visibility of network problems, and possibly leave your network more vulnerable to a service-affecting outage.

---

**No-Risk Custom Engineering**

Need a new master that supports your orphaned legacy remotes? Need a mediation solution for incompatible protocols or communication interfaces? Need a single-unit solution that includes all the capabilities and features you choose?

If your network has unique needs, we’ll create a custom design system just for you. At DPS Telecom, custom design is standard service. Our business has been built on continuous innovation, and we embrace opportunities to design new network monitoring solutions.

**Guaranteed perfect fit solutions**

You’re never taking any risks when you purchase DPS Telecom products. We built our business by following a client-first philosophy, and our primary goal is creating the highest level of security for your network.

Every system we make is customized for the specific needs of the client who orders it. Additionally, all DPS products, including custom solutions, are backed by our 30-day no-risk money-back guarantee.

Put DPS Telecom’s custom engineering process to work for you. Call 1-800-622-3314 and ask about no-risk custom engineering.
You can integrate many different types of equipment into your SNMP monitoring by using a protocol mediation solution.

With protocol mediation, you can select the equipment you want, confident that it will work with your SNMP monitoring. You can still use valuable features from existing equipment and other telemetry protocols.

And not least, protocol mediation offers a way of preserving existing equipment in place, saving your budget.

Potential Pitfall #4:

Manpower Costs

Forklift swapouts place a huge strain on budgets: they create high capital expenditure costs, they require many years of billable time to install, and warehoused equipment generates no ROI.

A controlled migration to SNMP monitoring from your existing system can stretch these costs over several budget cycles, ensuring a positive balance sheet during each budget cycle.

Here’s how controlled migration works:

In first phase, alarm outputs from existing telemetry equipment is re-routed to a combined telemetry master/protocol mediation device. The protocol mediation device converts the incoming data to a single stream of SNMP data, which is forwarded to an upper-level SNMP manager.

Depending on your network’s individual needs, you can stop right here or you can start migrating your network to SNMP.

If you choose the migration option, non-SNMP network elements are gradually replaced by SNMP devices. Sections of the network can be cut over to SNMP as your Cap-X and purchasing budget permits, without interfering with your network monitoring.

Learn more in a Live Meeting Room

In a Live Meeting Room, you’ll see the full range of customized DPS solutions for network reliability management, including T/Mon NOC, the NetGuardian 832A, and more. Your Applications Engineer will help you find the legacy integration solution with the right capacity, protocol, and data transport for you. You can view presentations & application overviews from Applications Engineers and ask questions for more details on the topics you’re most interested in.

Call 1-800-622-3314 today to schedule your free Web demo of legacy support solutions – or register at www.dpstele.com/tmon-webdemo.
Get the Facts Before You Purchase Your Next Network Monitoring System

If you found the information in this white paper useful, you’ll also be interested in the other white papers in the DPS Telecom Network Monitoring Guide series. Each paper is a complete guide to an essential aspect of network monitoring. These are the facts you need to know to make an informed purchase of your next network monitoring system.

Perfect-Fit Alarm Monitoring
Do you have a specialized monitoring need that no off-the-shelf product can solve? Does it seem like you need to buy several products just to get the job done? At DPS, we design and build custom products to suit our clients’ unique needs. In this white paper, we’ll walk you through our time-tested development process that can give you exactly what you need. To receive this report, visit: http://www.dpstelecom.com/white-papers

Practical Guide to SNMP Troubleshooting
Your are you encountering problems with your SNMP implementation? Are you planning to expand your SNMP deployment? This white paper is a guide to troubleshooting SNMP. Get valuable tips for identifying and solving problems with MIBs, firewalls, traps, IP routing, and more. To receive this report, visit: http://www.dpstelecom.com/white-papers

Monitoring Alarms Over T1
Monitoring sites outside of your existing LAN used to be difficult, expensive, and time-consuming. Now, new technology allows you to effectively monitor sites when T1 is the only available connection. This new white paper will show you how to monitor your outside plant sites, cost-effectively provide Ethernet to site equipment, and maximize your ROI. To receive this report, visit: http://www.dpstelecom.com/white-papers

Give Us Your Feedback
Send your comments to feedback@dpstelecom.com

This all sounds great, but where can I get product details?
If you would like to know more about the products and services mentioned in this white paper, visit www.dpstelecom.com and click “Applications.” or “Products.”

Turn to DPS Telecom Tech Support for Your SNMP Questions
The NetGuardian, T/Mon NOC and other SNMP products offered by DPS include comprehensive technical support. If you’ve purchased DPS products to implement SNMP in your existing network and have questions, contact DPS Tech Support today at 559-454-1600.

At DPS Telecom, the representative who answers your call isn’t an intern reading from a script. **DPS Tech Support representatives are engineers** who contribute to product development. And, if your problem requires additional expertise, the DPS Engineering Department that designed your product is right down the hall.
“As a telecom provider, uptime is becoming more critical every day. A 99.9% uptime is considered bad. In order to achieve 100% we turned to DPS. The whole experience was very impressive.”

—Rich Abalos
Calaveras Telephone

“I was looking for a way to integrate our local ILEC region into HP OpenView without a major network change. T/Mon’s SNMP responder was the answer. The 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

Written by Marshall DenHartog and Andrew Erickson

About the Author

Marshall DenHartog has over ten 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.

Andrew Erickson is Lead Writer for The Protocol, the monthly alarm monitoring ezine from DPS (www.TheProtocol.com). Experience writing web content and product documentation have prepared him to capture the expertise of the DPS Engineering team in a clear, concise white paper.

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

“We protect your network like your business depends on it”™