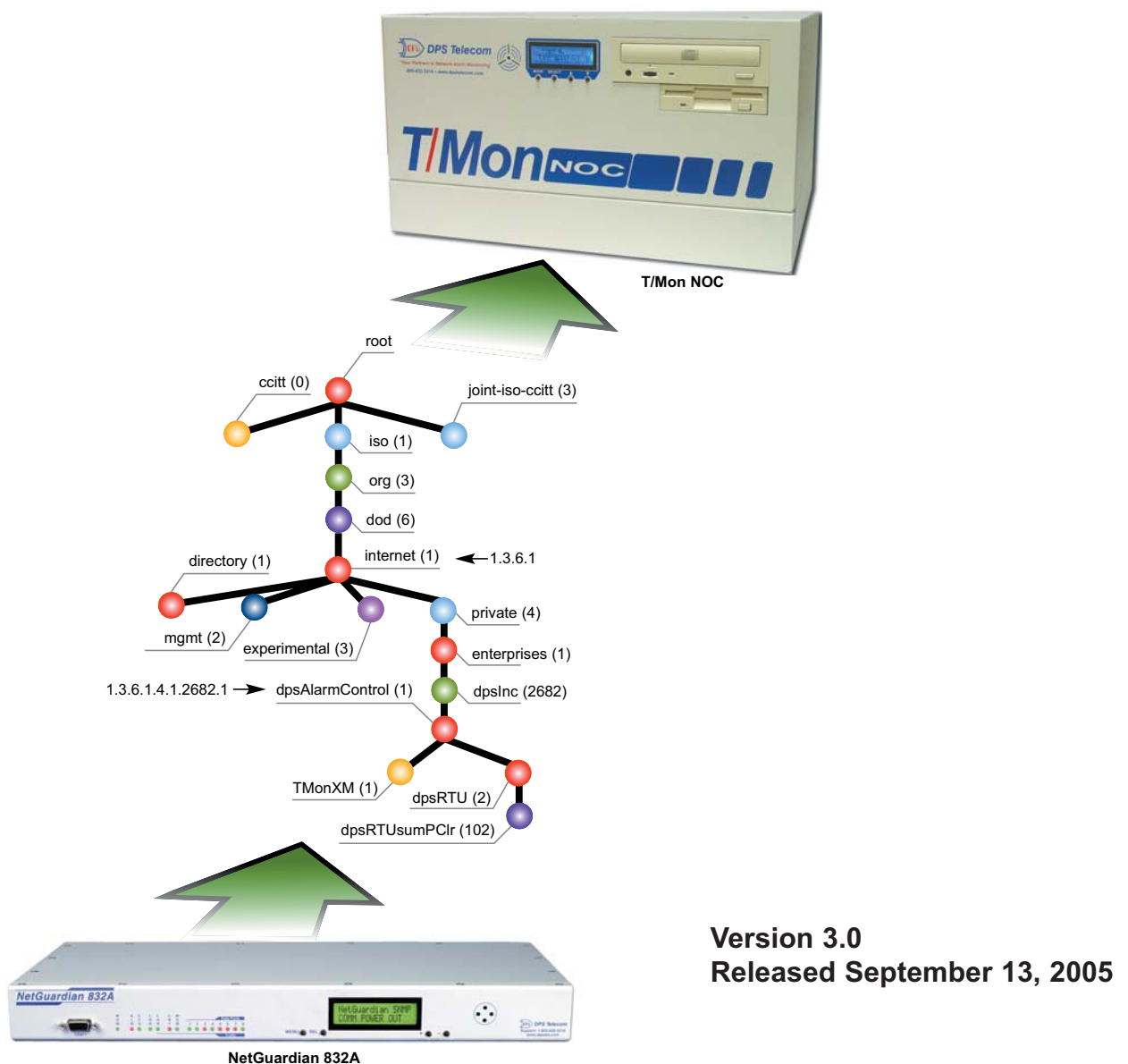


Demystifying the MIB by Marshall DenHartog

A complete guide to the SNMP Management Information Base:

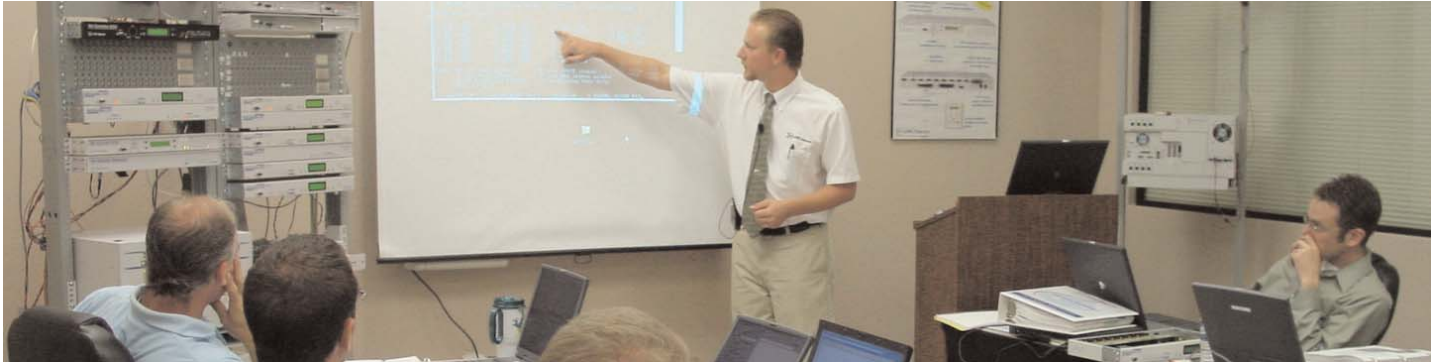
- Understanding the purpose and function of the MIB
- How to read the MIB
- Using the MIB to evaluate SNMP equipment



www.dpstelecom.com • 1-800-622-3314

"We protect your network like your business depends on it"™

Why Should You Come to DPS Telecom Factory Training?



Hands-on training in network alarm monitoring, taught by professional engineers.

DPS Telecom Factory Training is a fast, intense, 4-day crash course on the essentials of network alarm monitoring. You'll learn real-world telemetry fundamentals — knowledge that will save you hours of work and make your monitoring much more effective.



“This training is worth a lot more because it’s taught by the people who actually work with the system, not some corporate trainer.”

—Larry Hamilton, U.S. Telepacific

Personal Instruction in a Friendly Atmosphere

Anyone who's attended a DPS Factory Training Event will tell you it's not like any other training course. Here's the difference:

- **Personal instruction in small classes:** Classes are capped at nine people, so your instructor can focus on you. If you want to spend more time on a topic, your instructor or a DPS engineer will be happy to meet with you in a one-on-one breakout session.
- **Learn from engineers with real-world experience:** Your DPS instructors are skilled engineers who have worked on DPS product design and field implementations. They know your equipment and how you use it.
- **Work hands-on with real-world equipment:** At a DPS Factory Training Event, you'll work directly with the equipment — and you'll get the unique know-how that only comes with personal experience.
- **Complete access to DPS Telecom:** You'll talk to the engineers who design DPS equipment, tour the factory where it's built, and see the latest DPS products. If you've got a suggestion on how we can improve our products or services, we'll listen to you — and act to meet your needs.
- **Friendly, welcoming atmosphere:** The entire DPS staff will make you feel welcome. Hosted lunches and dinners will give you a chance to casually unwind with your classmates. You'll be able to share telemetry tips and experiences, and you'll get to know people you can relate to. Come to Fresno a day or two early and you can explore the splendors of nearby Yosemite, Sequoia, and Kings Canyon National Parks
- **Free tuition:** If you're a qualified telecom professional, there's no charge to attend a DPS Telecom Factory Training Event — that's a \$475 value. Call **1-800-622-3314** or go to www.dpstelecom.com/training and secure your place **today** — classes are small and they fill up quickly.

1-800-622-3314

www.dpstelecom.com/training

About the Author

Marshall DenHartog has seven 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 the SNMP Management Information Base.



Contents

| | |
|--|----|
| What is the MIB? | 4 |
| What does the MIB do? | 4 |
| Why do I need the MIB?..... | 4 |
| How do I get the MIB into my SNMP manager?..... | 4 |
| Why is the MIB important? | 4 |
| Why do I need to understand the MIB | 4 |
| How do I look at a MIB? | 5 |
| Will I need to edit the MIB?..... | 5 |
| How do I read the MIB?..... | 5 |
| What does a MIB look like?..... | 5 |
| Wow! What language is that? | 6 |
| How ASN.1 builds new terms out of existing terms | 6 |
| What terms are defined in the MIB | 7 |
| What is the function of an OID?..... | 7 |
| What does an OID look like? | 8 |
| OK ... but what does it mean?..... | 8 |
| When I look at my MIB files, I don't see long strings of numbers like that | 9 |
| So every MIB file needs to describe the entire OID tree? | 9 |
| How to avoid the most common cause of compile errors | 10 |
| So I'm reading the MIB What information am I looking for?..... | 10 |
| The MIB objects you need to know | 11 |
| 7 Reasons Why a Basic SNMP Manager is a Lousy Telemetry Master..... | 14 |

© Copyright 2004, 2005 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

What is the MIB?

The MIB, or Management Information Base, is an ASCII text file that describes SNMP network elements as a list of data objects. Think of it as a dictionary of the SNMP language — every object referred to in an SNMP message must be listed in the MIB.

What does the MIB do?

The fundamental purpose of the MIB is to translate numerical strings into human-readable text. 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, or OID. (OIDs are defined more fully later in this paper.)

The MIB provides a text label called for each OID. Your SNMP manager uses the MIB as a codebook for translating the OID numbers into a human-readable display.

Why do I need the MIB?

Your SNMP manager needs the MIB in order to process messages from your devices. Without the MIB, the message is just a meaningless string of numbers.

How do I get the MIB into my SNMP manager?

Your SNMP manager imports the MIB through a software function called compiling. Compiling converts the MIB from its raw ASCII format into a binary format the SNMP manager can use.

Why is the MIB important?

Because as far as SNMP managers and agents are concerned, if a component of a network device isn't described in the MIB, it doesn't exist.

For example, let's say you have an SNMP RTU with a built-in temperature sensor. You think you'll get temperature alarms from this device — but you never do, no matter how hot it gets. Why not? You read the RTU's MIB file and find out that it only lists discrete points, and not the temperature sensor. Since the sensor isn't described in the MIB, the RTU can't send Traps with temperature data.

Why do I need to understand the MIB?

As you can see, the MIB is your best guide to the real capabilities of an SNMP device. Just looking at the physical components of a device won't tell you what kind of Traps you can get from it. You might think it's strange that a manufacturer would add a component to a device and not describe it in the MIB. But the fact is, a lot of devices have sketchy MIBs that don't fully support all their functions.

When you're planning your SNMP monitoring, you need to be able to read MIBs so you can have a realistic idea of what capabilities you have. When you're evaluating new SNMP equipment, examine its MIB file carefully before you purchase.

What Features Do I Need in an SNMP RTU?



NetGuardian 832A SNMP RTU

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:** 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.
- 4. Control relays:** 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, plus many other advanced features.

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

How do I look at a MIB?

A MIB file is just ASCII text, so you can view it in any word processor or text editor, such as Microsoft Notepad. Some manufacturers provide precompiled MIBs in binary format, but those aren't readable. You want the raw ASCII version of the MIB file.

Note: MIB files are sometimes provided as Unix text files. Unix text format is significantly different from DOS/Windows text format. DOS/Windows text files have a carriage return and a line feed at the end of each line; Unix files only have a line feed. If you want to view MIB files on a Windows PC, ask your vendor for a DOS-formatted version, or you can use a conversion utility to convert between text formats.

Will I need to edit the MIB?

Generally speaking, no. MIB files aren't really designed to be edited by the end user. Theoretically, you could edit the text descriptions of managed objects to be more user-friendly, but it's better to use your SNMP manager's presentation software to create a useful display.

How do I read the MIB?

To read a MIB file, you have to understand just a little about how the MIB is structured. Don't worry — you don't have to master MIB notation in order to get useful information from the MIB. In this paper we're going to cover just the essentials you need to know to discover the telemetry capabilities of SNMP devices.

What does a MIB look like?

For an example, here are the first few lines of the standard DPS Telecom MIB file:

```
DPS-MIB-V38 DEFINITIONS ::= BEGIN
IMPORTS
    DisplayString
        FROM RFC1213-MIB
    OBJECT-TYPE
        FROM RFC-1212
    enterprises
        FROM RFC1155-SMI;
dpsInc OBJECT IDENTIFIER ::= {enterprises 2682}
dpsAlarmControl OBJECT IDENTIFIER ::= {dpsInc 1}
tmonXM OBJECT IDENTIFIER ::= {dpsAlarmControl 1}
tmonIdent OBJECT IDENTIFIER ::= {tmonXM 1}
tmonIdentManufacturer OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS read-only
    STATUS mandatory
    DESCRIPTION "The TMON/XM Unit manufacturer."
    ::= {tmonIdent 1}
tmonIdentModel OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS read-only
    STATUS mandatory
    DESCRIPTION "The TMON/XM model designation."
```

3 SNMP RTUs to Fit Your Spec

The NetGuardian RTU family scales to fit your needs ...



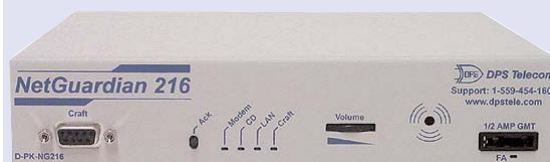
Full-featured NetGuardian 832A:

- 32 discretes, 32 pings, 8 analogs and 8 controls
- 8 terminal server serial ports
- NEBS Level 3 certified
- Dial-up backup
- Web browser interface
- Pager and email notification
- Dual -48 VDC, -24 VDC or 110 AC
- 1 RU for 19" or 23" rack



Heavy-duty NetGuardian 480

- 80 discretes, 4 controls
- Dual -48 VDC
- 1 RU for 19" or 23" rack



Economical NetGuardian 216

- 16 discretes, 2 analogs, 2 controls
- 1 terminal server serial port
- Single or dual -48VDC or 110 VAC
- 2 compact form factors for rack or wall mount

Wow! What language is that?

The MIB is written in ASN.1 notation. (The initials stand for Abstract Syntax Notation 1.) ASN.1 is a standard notation maintained by the ISO (International Organization for Standardization) and used in everything from the World Wide Web to aviation control systems.

A full description of ASN.1 is completely beyond the scope of this white paper — standard references to ASN.1 run up to 600 pages. For our purposes, there are only a few things to understand about ASN.1:

1. It's human-readable.
2. It's specifically designed for communication between dissimilar computer systems, so it's the same for every machine.
3. It's extensible, so it can be used for describing almost anything.
4. Once a term is defined in ASN.1, it can be used as a building block for making other terms. This is very important for understanding MIB structure — you'll see why later on.

How ASN.1 builds new terms out of existing terms

ASN.1 defines each term as a sequence of components, some of which may be sequences themselves. To give a simplified example, here's how you might describe a letter in ASN.1:

```
Letter ::= SEQUENCE {
    opening    OCTET STRING,
    body      OCTET STRING,
    closing    OCTET STRING,
    address    AddressType
}
```

Note that while most of the elements in this sequence are defined using a primitive element (the “octet string,” which is the equivalent of a byte), the address is simply defined as a text string, “AddressType.” You can do this because AddressType is defined in another sequence, like so:

```
AddressType ::= SEQUENCE {
    name       OCTET STRING,
    number     INTEGER,
    street     OCTET STRING,
    city       OCTET STRING,
    state      OCTET STRING,
    zipCode    INTEGER
}
```

For a computer parsing the sequence “Letter,” AddressType will be read as an instruction to insert the octet string and integer structures listed in the sequence that defines AddressType

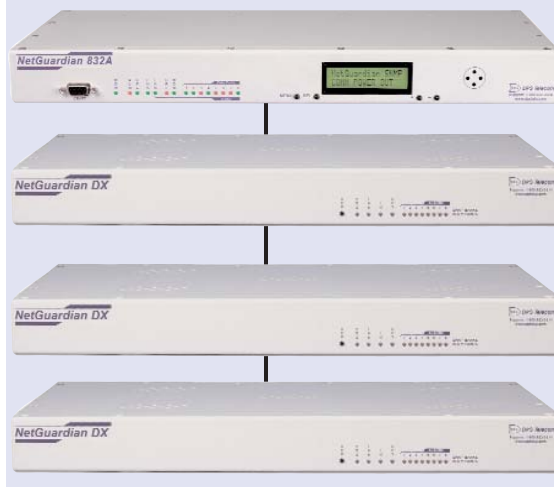
This RTU Grows with Your Network

When you're planning your alarm monitoring, think about the future. You don't want to get locked into an alarm system that's inadequate for your future needs — but you don't want to spend too much for alarm capacity you won't immediately use, either.

The NetGuardian 832A remote telemetry unit expands its capacity as your needs change. Install a NetGuardian at your remote site now, and get exactly the right coverage for your current needs.

Then, as your remote site grows, you can extend your alarm monitoring capabilities by adding NetGuardian DX Expansion units. Each NetGuardian DX adds 48 more alarm points, and you can daisy-chain up to three NetGuardian DXs off each NetGuardian 832A base unit.

| Unit | Capacity |
|-------------|----------|
| Base NG 832 | 32 |
| 1 DX | 80 |
| 2 DX | 128 |
| 3 DX | 176 |



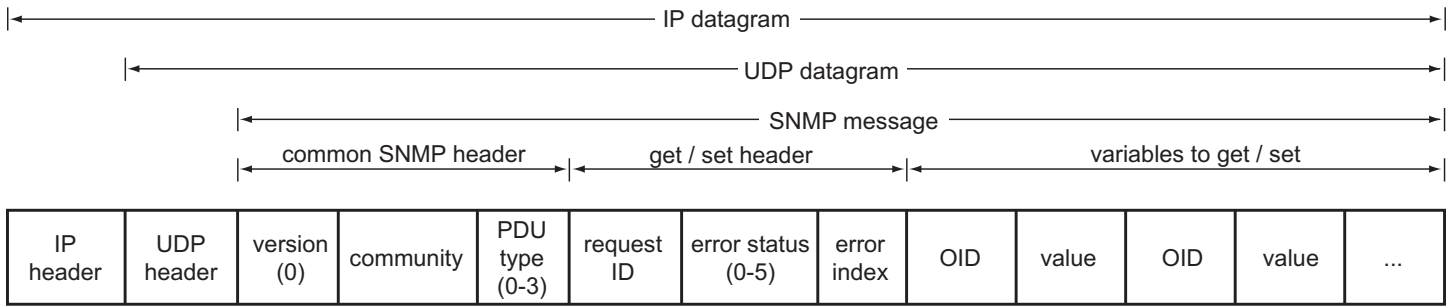


Figure 1. The OID identifies managed objects that can have assigned values

What terms are defined in the MIB?

The elements defined in the MIB can be extremely broad (for example, all objects created by private businesses) or they can be extremely specific (like a particular Trap message generated by a specific alarm point on an RTU.)

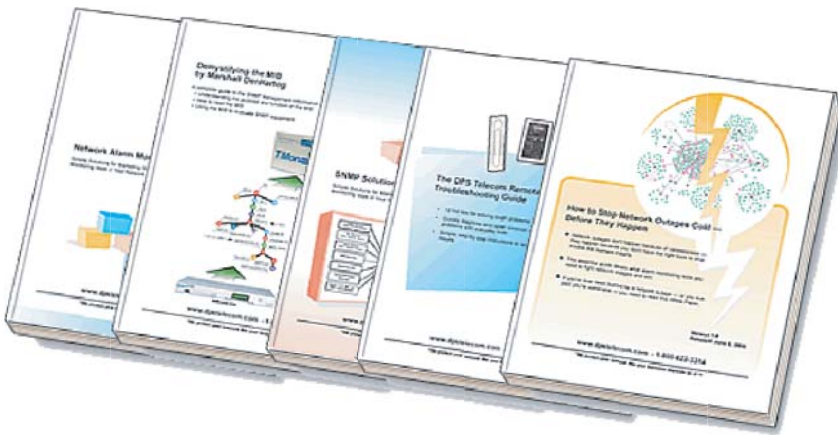
Each element in the MIB is given an object identifier, or OID. An OID is a number that uniquely identifies an element in the SNMP universe. Each OID is associated with a human-readable text label.

What is the function of an OID?

The OIDs identify the data objects that are the subjects of an SNMP message. When your SNMP device sends a Trap or a GetResponse, it transmits a series of OIDs, paired with their current values.

The location of the OID within the overall SNMP packet is shown in Figure 1.

More Info Resources on the Web



The DPS Telecom **White Paper Series** offers a complete library of helpful advice and **survival guides** for every aspect of system monitoring and control.

www.dpstelecom.com/white-papers

Let DPS Help You Survey Your Network — A Free Consultation at No Obligation to You

Determining your alarm monitoring needs can be tough. If you've got a busy job with lots of responsibilities, you don't have a lot of time to evaluate alarm systems and survey your remote sites.



Rick Dodd
Director of Sales
DPS Telecom

So why not get help from experts you can trust? DPS Telecom will help you survey your remote sites step-by step, making sure you don't miss any opportunities to make your network monitoring simpler, more effective — and easier on your budget.

A DPS expert consultant can help your figure out what alarm system will most effectively meet your needs without overloading your budget. Our goal is to help you maximize your return on investment while minimizing your expenditure — without pressuring you to buy a particular system.

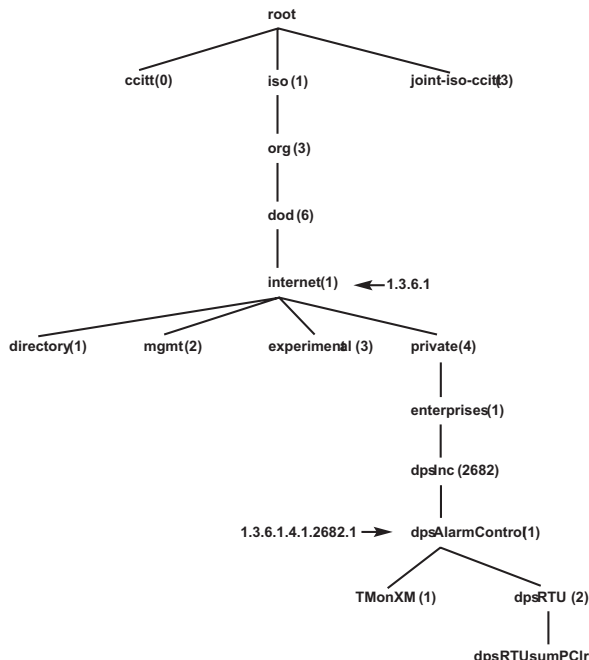


Figure 2. A branch of the MIB object identifier tree

What does an OID look like?

Here's an example: 1.3.6.1.4.1.2681.1.2.102

OK ... but what does it mean?

The OID is a kind of address. It locates this particular element within the entire SNMP universe. The OID describes a tree structure, as shown in Figure 2, and each number separated by a decimal point represents a branch on that tree.

The first few numbers identify the domain of the organization that issued the OID, followed by numbers that identify objects within the domain. Imagine if your home address started "Universe, Milky Way Galaxy ..." and ended with your house number. In a similar way, each OID begins at the root level of the OID domain and gradually becomes more specific.

Each element of the OID also has a human-readable text designation. From left to right, our sample OID reads:

1 (iso): The International Organization for Standardization, one of the two organizations that assign OID domains.

3 (org): An ISO-recognized organization.

6 (dod): U.S. Department of Defense, the agency originally responsible for the Internet.

1 (internet): Internet OID.

4 (private): Private organizations.

1 (enterprises): Business enterprises.

2682 (dpsInc): DPS Telecom.

1 (dpsAlarmControl): DPS alarm and control devices.

2 (dpsRTU): DPS remote telemetry unit.

102 (dpsRTUsumPCLr): A Trap generated when all the alarm points on an RTU are clear.

Alarm Master Choice: T/Mon NOC



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

- Detailed, plain English alarm descriptions** include severity, location and date/time stamp.
- Immediate notification of COS alarms**, including new alarms and alarms that have cleared
- Standing alarm list** is continuously updated.
- Text message windows** displaying specific instructions for the appropriate action for an alarm.
- Nuisance alarm filtering**, allowing your staff to focus its attention on serious threats.
- Pager and email notifications** sent directly to maintenance personnel, even if they're away from the NOC.
- 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.dpstelecom.com/tmon.

When I look at my MIB files, I don't see long strings of numbers like that

That's because each element of an OID only needs to be defined once. Remember, in ASN.1 notation, once a term is defined, it can be used as a building block to define other terms. The last number of an OID — its most specific element — refers back to the more general elements defined earlier in the MIB.

Here's how the last four elements in our sample OID are defined in the DPS Telecom MIB:

```
dpsInc OBJECT IDENTIFIER ::= {enterprises 2682}
dpsAlarmControl OBJECT IDENTIFIER ::= {dpsInc 1}
dpsRTU OBJECT IDENTIFIER ::= {dpsAlarmControl 2}
dpsRTUsumPClr TRAP-TYPE
    ENTERPRISE dpsRTU
    VARIABLES { sysDescr, sysLocation, dpsRTUdateTime }
    DESCRIPTION "Generated when all points clear."
    ::= 102
```

Look at how each term is defined as the term that came immediately before it in the OID, plus one more element. For example, `dpsInc` is `enterprises (1.3.6.1.4)` plus one more element, called `2682`. The next term, `dpsAlarmControl`, is `dpsInc (1.3.6.1.4.2682)`, plus one more element, called `1`. And so on. Each term in the OID is defined as an extension of earlier terms, going all the way back to the root term, `iso`.

An OID is meaningless unless every element it refers to is specifically called out and identified in the MIB. So when you're compiling your MIB files on your SNMP manager, you need to supply not only the OIDs defined by your equipment vendor, but also OIDs for public entities: `iso`, `org`, `dod`, `internet`, and so on.

So every MIB file needs to describe the entire OID tree?

Fortunately, no. The upper levels of the OID tree — the parts that define the general OID structure — are defined in a series of standard reference MIB files called RFCs.

(The initials stand for Request for Comment. The RFCs that define SNMP OIDs are part of a larger group of RFC documents that define the Internet as a whole.)

Learn SNMP the Easy Way: Attend DPS Telecom Factory Training



"I had heard of SNMP, but I never knew what SNMP was until I learned it at DPS Factory Training. I'm not at all scared about SNMP now." —Derek Willis, Paul Bunyan Telephone

Learn SNMP in-depth and hands-on, in a totally practical class that will teach you how to get the most from your network monitoring. At a DPS Factory Training Event, you'll learn how to turn SNMP theory into a practical plan for improving your network visibility.

The 4-day training course covers SNMP alarm monitoring ASCII alarm parsing and processing, configuring and using derived alarms and controls, and automatic e-mail and pager notifications. It's the easiest and most complete way to learn SNMP alarm monitoring from the technicians who have designed hundreds of successful SNMP monitoring implementations.

For Factory Training Events dates and registration information, call **1-800-693-3314** today or see us on the Web at www.dpstelecom.com/training.

The RFC MIB defines a basic dictionary of terms that vendors use to write their own equipment-specific MIBs. So a vendor-created MIB doesn't have to define the entire OID tree. The vendor's MIB file only has to define the unique OIDs that describe the vendor's equipment.

At the beginning of every MIB file is an IMPORTS line that calls out the terms used in the MIB and the RFC MIB that defines those terms.

Let's take another look at the very beginning of the DPS Telecom MIB:

```
DPS-MIB-V38 DEFINITIONS ::= BEGIN
IMPORTS
    DisplayString
        FROM RFC1213-MIB
    OBJECT-TYPE
        FROM RFC-1212
    enterprises
        FROM RFC1155-SMI;
```

From this IMPORTS line we can read that the DPS MIB is written using three terms defined in other MIBs — DisplayString, OBJECT-TYPE and enterprises — and these terms are defined in the RFC MIBs listed.

How to avoid the most common cause of compile errors

Your SNMP manager can't compile your MIB files correctly unless it also compiles the RFC MIBs that your MIB files refer to. For example, to compile the DPS Telecom MIB, you need to compile RFC1213-MIB, RFC 1212 and RFC1155-SMI. Compile errors are often caused by missing RFC MIBs.

RFC MIBs are publicly available on the Internet, or your vendor can supply the RFC MIBs you need.

All MIB files are written as extensions of the master RFCs. For this reason, you'll sometimes hear people say that there's only one MIB for all SNMP devices, and that individual MIB files are merely subsections of the unified Management Information Base.

That may be true in theory, but in real life, you only need to worry about the equipment you use, the MIBs that support your equipment, and the RFCs that support those MIBs.

So I'm reading the MIB. What information am I looking for?

You don't need to carefully read over every last line of the MIB file. For your purposes, you're only looking for particular items that will tell you what elements of the device you can monitor and control.

A well-written MIB will be divided into sections. Sections will be

How to Get Better Visibility of Your SNMP Alarms

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.

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.

If you want these features, you need the T/Mon NOC Remote Alarm Monitoring System. T/Mon is a multi-protocol, multifunction alarm master with advanced features like programmable custom alarms, automatic alarm correction, e-mail and pager alarm notification and more.

To learn more about T/Mon, call **1-800-622-3314** today to register for a live Web demonstration or register on the Web at:

www.dpstelecom.com/webdemo.

identified by comment lines. (In MIB notation, comments lines are identified by two hyphens.) So if you find a line that reads something like:

```
-- TRAP definitions
```

You know you've found what you're looking for.

There are also text labels that identify the MIB objects you're interested in. For example, in SNMP v1 MIBs, Traps are identified by the text label "TRAP-TYPE." If you know the text labels for the kinds of objects you're looking for, you can scan the MIB in a series of Ctrl-F searches.

The MIB objects you need to know

From the perspective of a telemetry manager, what you need to know from the MIB is:

1. What other RFC MIBs you need to support this device
2. What event reports (Traps) the device can send to the SNMP manager
3. What information you can request from the device (the SNMP equivalent of an alarm poll)
4. What characteristics of the device you can control via SNMP

RFC MIBs

The first thing you should look for in the MIB is what RFC MIBs are required to support this device. The necessary RFCs will be called out in the IMPORTS line at the beginning of the MIB.

Traps: Event Reports

For telemetry purposes, the MIB elements you're most interested in are what Traps the device can send. Traps are often described as alarms, but it's better to think of them as event reports.

When a Trap is called out in the MIB, it means that the device is configured to generate a report whenever the element listed changes state. This doesn't mean that the event is necessarily important. Many Traps are merely status messages.

In SNMP v1 MIBs, Traps are always designated with the text label TRAP-TYPE. Here's an example from the MIB for the DPS Telecom NetGuardian RTU::

```
dpsRTUp8005Set TRAP-TYPE
    ENTERPRISE dpsRTU
    VARIABLES { sysDescr, sysLocation,
dpsRTUdateTime,
dpsRTUAPort, dpsRTUCAddress, dpsRTUADisplay,
dpsRTUAPoint, dpsRTUAPntDesc, dpsRTUASState }
    DESCRIPTION "Generated when discrete point 5 is
set."
 ::= 8005
```

Price is Only the First Part of Cost Justification — Make Sure Your Vendor Offers Guaranteed Results

In my experience, clients who think hard about cost justification have a more important concern than just price. They want to make sure that they're not spend-



By Bob Berry
Chief Executive Officer
DPS Telecom

T/Mon NOC Can Monitor All Your Network Equipment

Most alarm systems support only the vendor's own devices or just one protocol. But T/Mon NOC monitors all your equipment — no matter who made it, or what protocol it uses — and display all your alarms on one screen.

T/Mon NOC can monitor nearly all your network equipment — DPS remotes, other manufacturers' remotes, switches, routers, PBXs, SONET equipment, multiplexers, battery plants, microwave radios, and more.

Why is this so important? Integrating all your alarms on one system gives you capabilities you can't get from separate, isolated systems:

- Know absolutely, 100% for certain if you have an alarm
- Monitor every essential piece of equipment in your network
- Correlate alarms across your entire network
- Integrate older, incompatible monitoring equipment
- Simplify training, maintenance and databasing

Fortunately, you can ignore a lot of this gobbledygook. Here are the elements that you're interested in:

TRAP-TYPE: This tells you it's a Trap.

DESCRIPTION: This is a human-readable description of the Trap. It should give you a good basic indication of what the Trap signifies.

VARIABLES: This tells you actual information will be included in the Trap. When an actual Trap is sent, each of these variables will be paired with a numerical value that indicates its current state. A variable-and-value pair is called a variable binding.

The variables look pretty cryptic, but it's easy to find out what they mean. Each variable is a text label for an OID defined elsewhere in the MIB. You can do a

Ctrl-F search for any variable term and find its definition. For example, "dpsRTUAPort" is defined in the DPS MIB like this:

```
dpsRTUAPort OBJECT-TYPE
    SYNTAX      INTEGER
    ACCESS      read-only
    STATUS      mandatory
    DESCRIPTION "RTU port number."
    ::= {dpsRTUAlarmEntry 1}
```

Trap variables are your best guide to what alarms you'll get from an SNMP device. Depending on the device, the variables can be highly detailed or they can be vague summary alarms.

Object-Types: Data you can read and sometimes write

When reading the MIB, you'll also want to know what information you can directly request from the device, and what information you can send to the device. These functions are controlled by the SNMP commands GetRequest and SetRequest.

If you want to translate these commands into classic telemetry terms, you can roughly think of a GetRequest as an alarm poll and a SetRequest as a control command.

GetRequests and SetRequests operate on a type of element called an object-type. Object-types are called out in the MIB like this:

```
tmonAState OBJECT-TYPE
    SYNTAX      DisplayString (SIZE (8))
    ACCESS      read-only
    STATUS      mandatory
    DESCRIPTION "The current alarm state."
    ::= {tmonAlarmEntry 4}
```

There are many different kinds of object-types. The specific object-types you might find in a MIB depend on the type of device, what kind of components it has, what the functions of those components, are, etc.

You're probably not going to be interested in every object-type listed in the MIB, because you're not going to be interested in everything about the device's functions.

T/Mon NOC Can Monitor All Your Network Equipment



Most alarm systems support only the vendor's own devices or just one protocol. But T/Mon NOC monitors all your equipment — no matter who made it, or what protocol it uses — and display all your alarms on one screen.

T/Mon NOC can monitor nearly all your network equipment — DPS remotes, other manufacturers' remotes, switches, routers, PBXs, SONET equipment, multiplexers, battery plants, microwave radios, and more.

Why is this so important? Integrating all your alarms on one system gives you capabilities you can't get from separate, isolated systems:

- Know absolutely, 100% for certain if you have an alarm
- Monitor every essential piece of equipment in your network
- Correlate alarms across your entire network
- Integrate older, incompatible monitoring equipment
- Simplify training, maintenance and databasing

To learn more about T/Mon, call **1-800-622-3314** today to register for a live Web demonstration or register on the Web at:

www.dpstelecom.com/webdemo.

When searching for object-types, it's helpful to start with a plan of what functions of the device you want to manage. What information do you want to retrieve? What controls do you want to set? Knowing the device's functions and how you want to use them will help you narrow down what object-types you should look for in the MIB.

Access

The most important entry in an object-type description is the ACCESS line. This controls whether you can read and write the data described in the object-type.

There are three access settings: not-accessible, read-only and read-write.

Not-accessible means the object-type is there, but you can't request the data in a GetRequest.

Read-only means you can request the data in a GetRequest, but you can't write new data for the object-type in a SetRequest.

Read-write means you're free to retrieve the data in a GetRequest and write new data for the object-type in a SetRequest.

In the example of the alarm state object-type:

```
tmonAState OBJECT-TYPE
    SYNTAX DisplayString (SIZE (8))
    ACCESS read-only
    STATUS mandatory
    DESCRIPTION "The current alarm state."
    ::= {tmonAlarmEntry 4}
```

The access here is read-only, because the alarm state is set by the alarm input on that alarm point.

Here's an example of an object-type with read-write access:

```
dpsRTUdateTime OBJECT-TYPE
    SYNTAX DisplayString (SIZE (23))
    ACCESS read-write
    STATUS mandatory
    DESCRIPTION "The RTU system date and time."
    ::= {dpsRTUIDent 4}
```

Here the access is read-write, because this is a value that you can set from your SNMP manager. You can retrieve the current settings from the RTU's internal clock through a GetRequest. And if the clock needs to be reset, you can write new data in a SetRequest.

Quick Primer on SNMP Messages

In SNMP v1, there are only 5 basic PDUs (program datagram units):

GetRequest: a manager-to-agent message requesting the current value of a managed object.

GetNext: a manager-to-agent message requesting the current value of the managed object one number after the one named in the request. (This is a way of walking down a table of values.)

SetRequest: a manager-to-agent message that writes a new value to a managed object

GetResponse: an agent-to-manager message in response to a GetRequest or a SetRequest. In either case, the message reports the current value of the managed object named in the manager's request

Trap: an agent-to-manager message reporting a change in the value of a managed object

I want to use a device feature that isn't described in the MIB. What can I do?

You can ask the vendor to extend the MIB to include this feature. DPS Telecom has extended its MIB to support client needs. But you need to understand that extending a MIB is actually a software development project. The MIB is not just a text file. It's also a software interface document to the embedded firmware of your SNMP device. Making additions to the MIB requires rewriting the device firmware.

This is a serious project, involving writing code, debugging it, and undergoing a thorough quality assurance process.

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.

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

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.
2. Immediate notification of changes of state (COs), including new alarms and alarms that have cleared.
3. A continuously updated list of all current standing alarms.
4. Text message windows displaying specific instructions for the appropriate action for an alarm.
5. Nuisance alarm filtering that eliminates meaningless status alarms and oscillations 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

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 multi-user 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?

T/Mon NOC Automatically Troubleshoots and Corrects Alarms

The same alarm can instantly go from minor to critical if something else goes wrong. For example, a low battery might not be a big deal until AC power and the backup generator both fail, and then it's an emergency.

T/Mon NOC's Derived Alarms feature gives you the power to instantly track these kinds of changing alarm conditions. Derived Alarms combine inputs from multiple alarm points into a single, software-configured alarm, using simple Boolean logic.

Let's say your low battery is a minor alarm. Low battery **AND** an AC power failure **OR** generator failure is a major. Low battery **AND** AC power failure **AND** generator failure is a critical alarm.

Derived Alarms can also include date/time factors, so they're great for filtering nuisance alarms. You don't have to be pestered by an alarm every time a door is opened in a busy facility during business hours — but you will be notified if the door is opened by an intruder at night.

Correct Alarms Instantly With No Human Intervention

T/Mon NOC's Derived Controls are even more useful, correcting problems before any human operator even knows something is wrong.

If critical network equipment fails, T/Mon NOC can automatically start backup equipment and notify a service tech. If a security door is breached after-hours, T/Mon NOC can automatically lock security gates, turn on lights, and page security staff.

DPS Telecom Guarantees You Won't Fail — 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.

Call or email Rick Dodd at **1-800-622-3314** or rdodd@dpstele.com and ask for a free, live Web demonstration of SNMP monitoring solutions with the T/Mon NOC 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 Rick at **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.

Why You Need Help With Your SNMP Implementation

Implementing an SNMP network alarm monitoring system can seem deceptively easy, but 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's Sales Department: Monitoring Consultants Who Put You First

"We're not your typical sales department," says Rick Dodd, DPS Telecom's Director of Sales.

"We don't rush the client. We don't recommend solutions until we have a good understanding of the client's requirements and ultimate goal. We're design consultants."

What makes Dodd and his sales staff different is their sincere, no-nonsense commitment to putting their clients first.

Dodd's primary goal is making sure you have the right solution to meet your needs — and if that means a smaller sale, that's OK with Dodd.

"A lot of the time we propose solutions that have a smaller sales volume, if it's the right solution for the client," said Dodd.

"That goes back to the DPS philosophy of creating complete client satisfaction. We customize our solutions to make it the right fit without the client having to buy a lot of extraneous hardware and software.

"The bottom line is, if you're not 100% happy with the solution we've provided, we've done something wrong. My personal promise is that when you order from DPS, you'll get the exact solution you're looking for, or you'll get your money back," said Dodd.

The DPS Telecom sales process is a systematic guarantee of Dodd's promise. With every client, Dodd and his sales staff follow a standard procedure that's designed to safeguard the client's best interests at every step.

Step 1: Consultation

When he first talks to a client, Dodd's only immediate goal is to determine the client's real needs, both for the present and the future.

"First we look the challenges you're facing right now. What are you currently working with, and why isn't it working for you? What are your current solutions shortcomings and pitfalls?"

"We have an extensive site survey we work from to understand your network — what equipment do you monitor, what alarm equipment do you currently have, what protocols and interfaces do you use," said Dodd.

"But we also look at where you want to be in the future, five or ten years down the road. We want to find out what a perfect long-term system for you would look like. We don't want to provide you with something you'll have to re-do two years from now."

Step 2: Design

The next step is to design an alarm monitoring application that will serve as a bridge between the client's current state and future objective. The goal here, Dodd said, is to create a "perfect fit" solution.

"A perfect fit solution is different for everybody's application. It might mean visibility of network systems you haven't been able to monitor before. It might mean consolidating visibility of your whole network to one console. The key is creating a solution that's simpler for you to manage, from your operational standpoint," said Dodd.

In most cases, the client's needs can be served with an existing DPS product. But if current products don't provide that perfect fit solution, Dodd will work with the DPS Engineering Department to develop a custom solution that meets the client's exact requirements.

"From a design aspect, perfect fit means we match our existing products against your requirements. A lot of times, an off-the-shelf solution will meet your needs. But if it doesn't, we modify our hardware and software so it fits your needs exactly. Our hardware is modular and the intelligence is built into the software, so we can tweak it pretty easily until it's the absolute best fit for you," Dodd said.



Rick Dodd
DPS Telecom
Director of Sales

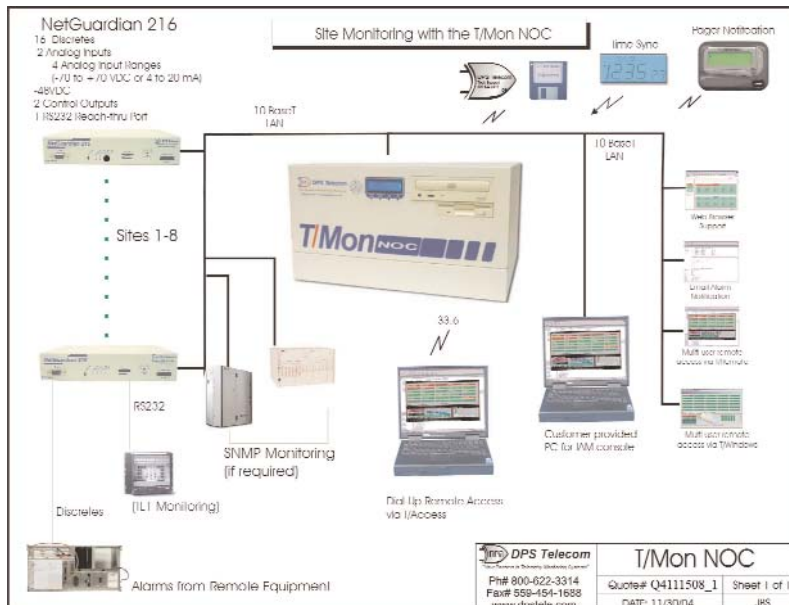
Step 3: Web Demonstration

When a preliminary design has been created, Dodd contacts the client for a Web demonstration. Using a shared browser connection and a conference call, Dodd explains the basics of the application and familiarizes the client with the technical features of the equipment that will be used.

The Web demo is a convenient, no-pressure way for the client to get a very personalized demonstration of the proposed alarm monitoring solution, covering both the broad application and the fine technical details.

Step 4: Quote

If the client approves the initial presentation, Dodd's staff prepares an in-depth written quote that details the client's existing situation, how the proposed solution will improve that situation, and the technical functionality of the equipment.



Sales quotes to clients are illustrated with detailed technical drawings.

“First we reiterate our understanding of your as-is situation, and we explain how where going to take you from where you are right now to your desired end results. Then we get into the nuts-and-bolts aspect of how it’s going to work in your network,” said Dodd.

“We also provide extensive application drawings with the quote. We spend a lot of time creating the drawings, because they really help you connect the dots and see what we’re proposing.

“The quote also includes a price page that breaks down the cost on a line-by-line basis, and a list of referrals to existing DPS clients. These are companies in your industry, sometimes even in your geographical area, that use similar equipment to what you have now and similar equipment to what we’re proposing. We want you to see you’re not buying something that’s untested or unproven.”

Step 5: Installation, Training and Support

Dodd emphasized that DPS clients aren’t on their own after they purchase. DPS Telecom continues to support the client with installation services, training and 24/7 tech support.

“Our installers are subject-matter experts in the product they’re installing — in fact, they’re the same guys who teach classes at DPS Factory Training Events. For a full-system install, your installer will make sure everything is working right and he’ll train you and your staff on the system,” said Dodd.

“We provide training with installation so that you have full control over your own alarm monitoring system and your own destiny. We want you to be as self-sufficient as possible — but we also provide a high level of support. For the lifetime of your DPS alarm monitoring solution, you’re entitled to 24/7 technical support.”

Step 6: Evaluation, Backed by a Money-Back Guarantee

Every alarm monitoring solution from DPS Telecom, including custom-engineered solutions, is backed by a 30-day, no-risk, money-back guarantee.

“Clients love this, because it basically removes all risk from buying our equipment. And that’s only right. If you’re going to commit a portion of your budget, you should be sure the product delivers a huge amount of value,” said Dodd.

“We guarantee that your alarm monitoring solution will work as promised, and if it doesn’t, you’re not on the hook for anything. After your system is installed, you can try it for 30 days, and if you’re not happy for any reason, you can send it back and you’re not on the hook for the equipment, for the training, for the shipping, for anything. It’s just 100% money back.”

T/Mon NOC

The only alarm system that supports all your equipment, no matter what protocol, no matter what manufacturer



How many different kinds of devices do you monitor? How many different screens do you have to watch? If you're tired of the confusion and clutter of multiple alarm consoles, you need T/Mon NOC.

T/Mon NOC is uniquely designed to monitor all your equipment, no matter what protocol, no matter what manufacturer. T/Mon shows your whole network on one screen, so problems can't hide.

With T/Mon NOC you can:

- Monitor alarms in 25 protocols, including: ASCII, Badger, Cordell, DCM, DCP, DCPf, DCPx, DCM, E2A, Larse, Modbus, NEC, Pulsecom, SNMP, TABS, TBOS and TL1.
- Display your entire network on one screen and know the status of your network with 100% certainty.
- Mediate alarm data to different protocols.
- Forward alarm data to other masters.
- Send pager and email alarm notifications to multiple users automatically.
- Connect multiple Remote Access users simultaneously via LAN, dial-up or serial port.
- Control remote site equipment manually or automatically in response to alarm inputs.
- Administer a centralized configuration database for your whole network.
- Maintain alarm history logs and create reports of alarm events.

"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."

—Todd Matherne, NCC System Admin

Because of its multiprotocol capability, T/Mon NOC is the perfect system to:

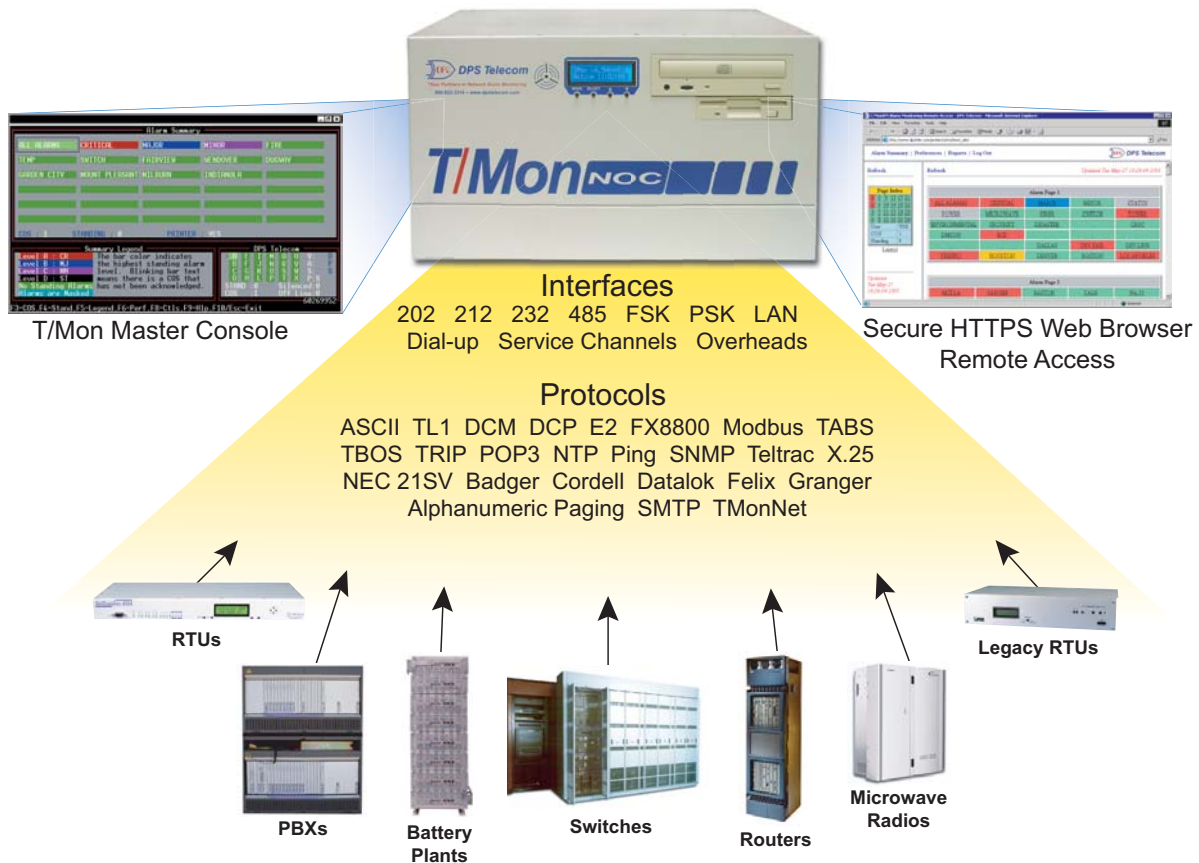
- Integrate diverse equipment to your SNMP or TL1 manager.
- Save your older equipment instead of replacing it — at huge cost savings to you.
- Manage large, complex networks from one T/Mon station, dramatically reducing staff and training costs
- Never miss an alarm — if there's a problem **anywhere** in your network, T/Mon will see it. And T/Mon's advanced notification features will make sure you know about it.

More T/Mon advantages:

- Easy-to-maintain system, so **any company** can monitor in-house.
- T/Mon's ASCII Alarm Processor extracts detailed information from switches, routers, SONET gear,, email, Web and FTP servers — and just about any other network device
- Monitor 24/7/365 — even when no one's in the office. Companies around the world safely rely on T/Mon's pager and email notification for after-hours monitoring. It's a 24/7 NOC without the hassle or expense.

“Looking at one map and knowing it shows every piece of equipment you’re monitoring in the field — when you see green on there from everywhere, all your sites, that’s piece of mind.”

—Brian Krest, Senior Telecom Engineer



More ways T/Mon NOC speeds repairs and makes maintenance easier

- **Pinpoint the exact location and description of alarms**
Monitor proactively, not reactively. T/Mon tells you everything you need to know to fix problems on the very first site visit — which site, which device, alarm severity and a plain English description of the alarm. You’ll eliminate unnecessary and overtime truck rolls, for a dramatic reduction in windshield time costs.
- **Tell system operators exactly what to do when an alarm happens**
T/Mon’s customizable text messages enable you to database detailed explanations and instructions for handling every alarm. Everyone on your staff, no matter what their skill or training, will know exactly what to do when an alarm happens.
- **Control nuisance alarms**
T/Mon gives you three ways to filter nuisance alarms: alarm tagging (ignore alarms until user un-tags them), alarm silencing (temporarily ignore alarms for specified time) and alarm qualification times (ignore momentary and self-correcting alarms).
- **Create custom alarms from multiple alarm inputs**
T/Mon’s Derived Alarms help you track complex events by combining alarm inputs and date/time statements. If you need to know when a site’s generator and battery have both failed ... or you want to know if a generator doesn’t run its weekly self-test ... or any other combination of events ... Derived Alarms will tell you.
- **Use these and all other T/Mon features on all alarms**
All your alarms from all your devices — no matter what protocol — can access all of T/Mon’s advanced features. Even your oldest devices can use pager and email alerts, Derived Alarms and Controls and nuisance alarm filtering. T/Mon NOC is a complete upgrade of your alarm monitoring in just one unit.

NetGuardian 832A



“It’s just a fantastic product. The NetGuardian does what it says it can do, and actually a lot more.” —Mark Renne, Program Manager

Powerful, high-capacity, versatile SNMP alarm collector covers all your remote monitoring needs

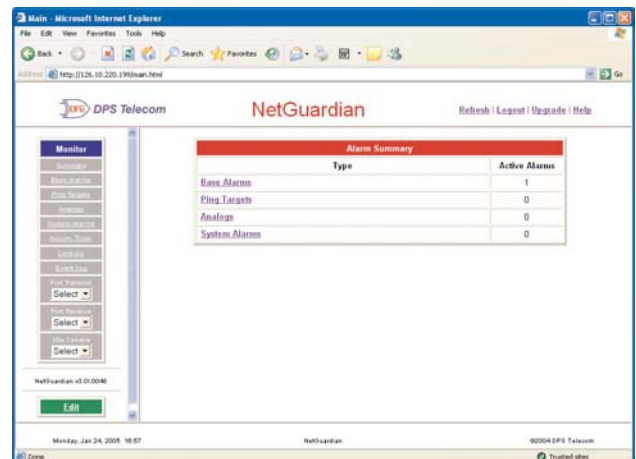
The NetGuardian 832A does as much as an RTU can ... and then it does a whole lot more.

The NetGuardian’s primary function is to **mediate contact closures and analog voltages to SNMP traps** — but it also serves as a **reach-through terminal server**, a **self-contained all-in-one alarm monitoring system**, a **24/7 email and paging system**. — and then there’s still more functionality ...

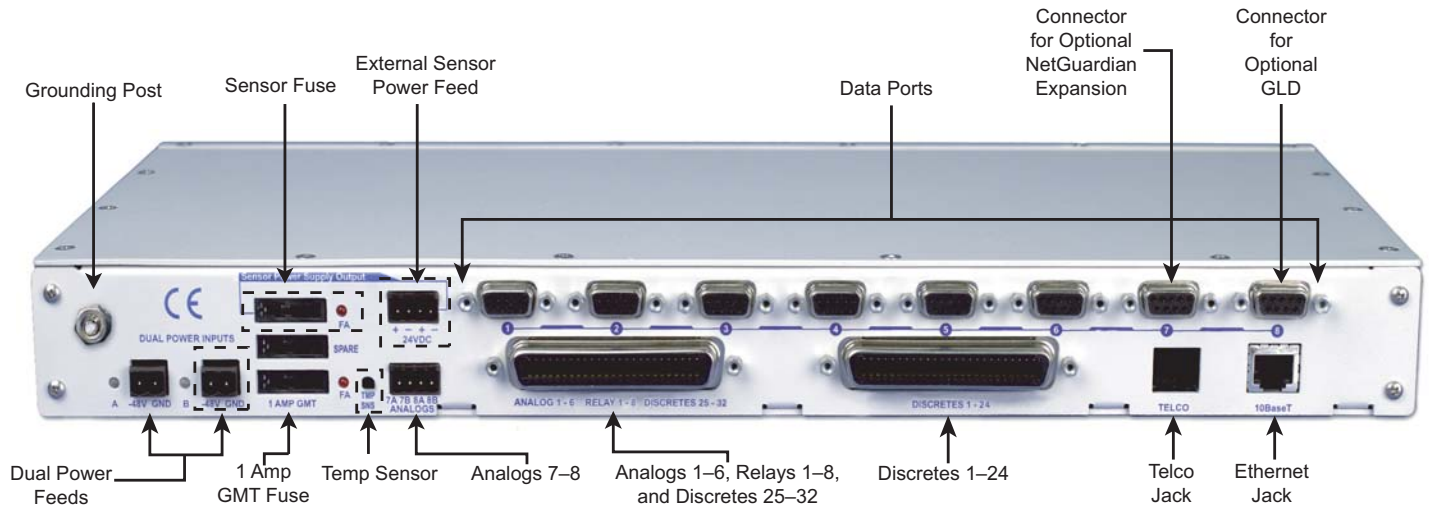
The NetGuardian 832A provides all the tools you need to for complete remote site management:



- Mediate **32 discrete inputs, 32 ping alarms, and 8 analog alarms** to SNMP traps.
- Report alarms to **multiple SNMP managers** or T/Mon NOC
- Supports **LAN or dial-up transport** — immediately implement SNMP monitoring without LAN or use dial-up as a backup path in case of LAN failure.
- Monitor legacy telephony gear, battery plants, generators, security locks, temperature sensors, and all your other remote site equipment.
- Expand your monitoring capacity up to 176 discrete inputs with the NetGuardian Expansion Unit.
- 4-threshold analog monitoring (Major Over, Minor Over, Minor Under and Major Under).
- Control site equipment with 8 control relays.
- Control switches, routers, PBXs and other telecom gear through the NetGuardian’s 8 terminal server reach-through ports.
- Integrated Web Browser interface for stand-alone alarm monitoring.
- Email and pager alerts for 24/7 alarm monitoring without a master.
- Live streaming video surveillance of remote sites with the NetGuardian SiteCAM.
- Included Windows configuration utility.
- **Free** lifetime firmware upgrades.



The NetGuardian Web Browser Interface provides stand-alone local monitoring.



NetGuardian 832A Specifications

Protocols: SNMP and DCPx

Discrete Inputs: 32 (expandable to 176)

Alarm Detection Speed: User-defined (3 to 999 msec)

Analog Inputs: 8

Analog Input Range: (-94 to 94 VDC or 4 to 20 mA)

Control Outputs: 8 Form C relay contacts

Maximum Voltage: 60 VDC/120 VAC

Maximum Current: 1 Amp, AC/DC

IP Address Ping Targets: 32

Interfaces:

8 DB9 RS-232 ports

1 RJ45 10BaseT Ethernet port

1 RJ11 POTS jack

2 50-pin Amphenol connectors (discretives, controls, and analogs)

1 DB9 connector (analogs)

Modem: 33.6K internal

Visual Interface:

LCD display with descriptive text

16 bicolor LEDs

Audible Interface: Alarm speaker

Dimensions: 1.75"H x 17"W x 12"D

(4.5 cm x 43.2 cm x 30.5 cm)

Weight: 4 lbs. 3 oz. (1.9 kg)

Mounting: 19" or 23" rack

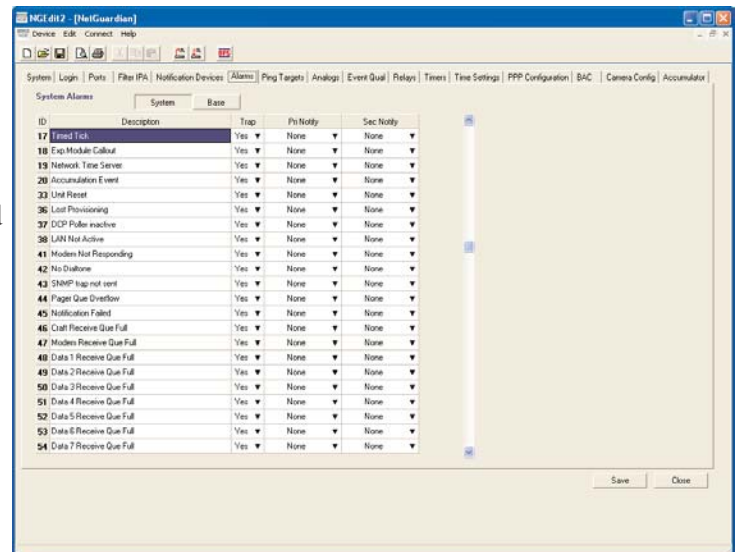
Power Input: -48VDC (-40 to -70 VDC) see options

Current Draw: 200mA

Fuse: 1 Amp GMT

Operating Temperature: 32°-140° F (0°-60° C)

Operating Humidity: 0%-95% noncondensing



The NetGuardian's included Windows configuration utility makes it easy to create standard configurations and upload them via LAN.

NetMediator T2S



Send TBOS Alarms Directly to Your SNMP Manager

The NetMediator is like an RTU on steroids - it does everything the NetGuardian 832A does, and then some. It's a full-featured alarm collector and protocol mediation device in one. You can mediate and monitor, saving you the expense of buying additional RTUs.

Protocols: SNMP, TL1, TBOS

Mediation: 8 TBOS displays to SNMP or TL1

Discrete Inputs: 32

Analog Inputs: 8 (voltage/current)

Analog Input Range: -70 to 94 VDC or 4 to 20 mA

Control Outputs: 8

Maximum Voltage: 60 VDC/120 VAC

Maximum Current: 1 Amp, AC/DC

Interface:

4 RS-422/RS-485 TBOS ports

4 RS-232 serial reach-through ports

2 50-pin connectors

1 4-pin connector

1 RJ45 10BaseT Ethernet port

1 RJ11 POTS jack

1 DB9F craft port

Visual Interface: 18 LEDs, LCD display

Dimensions: 1.75"H x 17"W x 12"D (4.5 cm x 43.2 cm x 30.5 cm)

Weight: 4 lbs. 3 oz. (1.9 kg)

Mounting: 19" or 23" rack

Power Input: +24 VDC

Current Draw: 200 mA

Fuse: 0.75 Amp GMT

Operating Temperature: 32°-140° F (0°-60° C)

Operating Humidity: 0%-95% noncondensing

Alarm Monitoring Solutions from DPS Telecom

Alarm Monitoring Masters



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

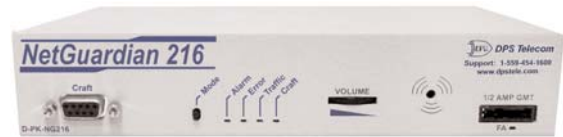


T/Mon SLIM: Light capacity regional alarm master. Supports up to 64 devices and 7,500 alarm points. Features pager and email alarm notification, Web Browser access, standing alarm list and alarm history logging.

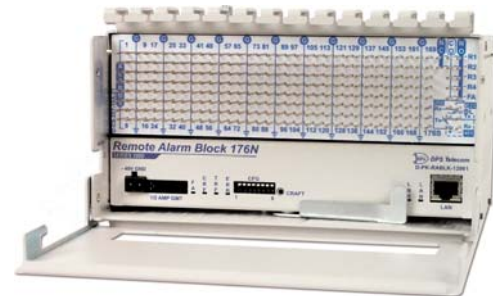
Remote Telemetry Units



NetGuardian 832A: RTU monitors 32 alarm points, 8 analog inputs, 8 control relays, 32 ping targets, 8 terminal server ports; reports to any SNMP manager, T/Mon NOC or T/Mon LT



NetGuardian 216: RTU monitors 16 alarm points, 2 analog inputs, 2 control relays, 1 terminal server port; reports to any SNMP manager, T/Mon NOC or T/Mon LT.



Remote Alarm Block 176N: Wire-wrap alarm block monitors 176 alarm points, 4 controls; reports to any SNMP manager, T/Mon NOC or T/Mon LT



NetGuardian 480: RTU monitors 80 alarm points, 4 control relays; reports to any SNMP manager, TL1 master, T/Mon NOC or T/Mon LT

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



"We protect your network like your business depends on it"