The Essential TL1 Guide:  
A Quick Reference for Busy Professionals

You probably still have a sizeable investment in TL1, even though it's considered a legacy protocol. Your valuable gear, especially SONET and legacy equipment, depends on your TL1 knowledge.

This Essential TL1 Guide provides fundamental information in a quick summary format, allowing you to spend your valuable time managing revenue-generating infrastructure.

Version 1.0  
Released June 1, 2007

www.dpstelecom.com  •  1-800-622-3314

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

TL1 is one of the most widely used telecom network management protocols. Although it is considered today to be a legacy protocol, a TL1 is still an important tool in the monitoring field because of its popularity among SONET, legacy, and other network elements.

This doesn’t mean that you have to be a TL1 expert, but you must have a core working knowledge of the protocol to know what you can expect from TL1 telemetry reporting. And if your staff is telling you what can and can’t be done with your TL1 monitoring system, you must be able to assess their accuracy.

This white paper is not a complete reference guide to TL1 protocol. Instead, it is a guide to essential fundamentals, providing the information you need in a quick format.

Contents

What is TL1 ................................................................. 4
How Understanding TL1 Will Help You ........................................ 4
Is TL1 Easy to Understand? .................................................... 4
3 Benefits Shared by TL1 and SNMP ........................................ 4
The Most Common TL1 Message Types ..................................... 5
Basic TL1 Message Elements ............................................... 6
Common TL1 Message Format .............................................. 7
TL1 Message Samples ...................................................... 8
Understanding TL1 Error Messages ....................................... 10
TL1 via Command Line Interface ........................................ 11
Potential TL1 Pitfalls - and Solutions ................................... 11
Using RTRV-HDR to confirm that a TL1 device is online ............ 12
USing RTRV-ALM to request a report of standing alarms .......... 12
Case Study: Triple Play Provider EastLink Manages Rapid Network Growth with T/Mon NOC .... 14
Monitor a Complete SONET Ring with TL1 by Connecting to Just One Network Element .... 16
What is TL1?
Transaction Language 1 (TL1) is a set of ASCII-based instructions, or "messages". These messages enable a human user or an Operations Support System (OSS) to manage a network element (NE) and its resources.

A Standardized Protocol
Bellcore developed TL1 in 1984 as a standard (MML) man-machine language to manage network elements. Before the development of TL1, most vendors designed equipment around their own proprietary protocols. These incompatible protocols caused headaches for operators, programmers, and support technicians. Having multiple protocols means more training, more support issues, and more screens to monitor.

With the creation of TL1, Bellcore hoped to introduce a single, open protocol for managing network elements. It was intended to replace the diverse protocols used by different vendors.

A Man-Machine Language
In addition to being open, TL1 is powerful because it bridges the gap between human users and network equipment. It is structured enough to be parsed by machines, but also verbose enough to be read by human operators.

Since special decoders or debuggers are not necessary, TL1 is a frequent command line interface choice for equipment manufacturers. TL1 messages are also embedded with the database information required to interpret the meaning of an alarm.

How Understanding TL1 Will Help You
TL1 is a multi-vendor and multi-technology protocol with comprehensive management support. There's a very good chance that TL1 protocol plays a significant role in your network. A solid foundation of TL1 knowledge allows you to do your job more effectively. With this white paper, you're just a few pages away from the core understanding you need.

Is TL1 Easy to Understand?
TL1 is a set of ASCII-based instructions, or "messages". Because TL1 is text-based, you won't be intimidated by a jumble of code or hexadecimal protocols. This makes the learning curve for basic TL1 much shorter than with other protocols.

This doesn't mean, however, that you won't need a basic introduction to TL1 fundamentals. You must learn the basics before you can read, understand, and write TL1 commands. Fortunately, TL1 message formats are very well defined and documented, and you can learn about the most frequently used commands in this guide.

3 Benefits Shared by TL1 and SNMP
TL1 is a spiritual precursor to SNMP. Both were intended to be open standards and comprehensive languages. TL1 and SNMP protocols share the following three benefits:

1) Widespread implementation
2) Open standard makes it easier to connect networked devices with monitoring software
3) Verbose command responses
The Most Common TL1 Message Types

Although there is a wide range of standard TL1 messages, four types comprise the majority of TL1 communication:

1) **Autonomous messages**
Asynchronous messages (usually events or alarms) that are typically sent by network elements.

2) **Input/Command messages**
Commands sent by the user or OSS to a network element.

3) **Output/Response messages**
Replies sent by the network element in response to an input/command message.

4) **Acknowledgment messages**
Acknowledgments of the receipt of a TL1 input message, usually associated with a delayed report or action.

Connect 8 Streams of TL1 Messages to a Single Physical Port

The DPS TL1 MUX-8 combines eight incoming TL1 streams into a single stream of data, allowing you to connect 8 physical ports to a single port on your TL1 master. This prevents simultaneous TL1 messages from “colliding” and becoming unreadable.

The TL1 MUX-8 watches for the semicolon terminator at the end of each TL1 message. If the single stream is currently available, the message is forwarded to your TL1 master instantly. If the single stream is busy sending messages from another port, any other simultaneous messages are stored in the 256K buffer. Stored messages are sent to your master, in the order received by the MUX-8, at the next available opportunity.
Learn About Remote Site Monitoring From the SNMP Experts: Attend DPS Telecom Factory Training

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 (a tool for parsing TL1 messages), 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.

“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

“ASCII and TL1 commands... [were] presented very well, making the introduction to a new language enjoyable!”
— Dewayne Hamilton, Level 3 Communications

“[DPS Factory Training] really was the best training class I’ve been to in my telecom career.”
— Mary Steffen, National Grid

For dates and registration information, call 1-800-693-3314 today or go to www.dpstelecom.com/training
Common TL1 Message Format

Although TL1 messages may look intimidating to new users, commonly used messages include several clearly defined elements that are separated by colons:

\[
\text{verb \ [-modifier \ [-modifier]]::TID:AID:CTAG:generalblock;}
\]

The Verb and Optional Modifiers
The first section of this message is structured in the following way:

\[
\text{verb \ [-modifier \ [-modifier]]:}
\]

Verb
The verb refers to the type of action to be taken by the network element (in case of a command message) or the type of event that has occurred in the element (in case of an autonomous message).
(Ex. “ACT”, “RTRV”)

Modifiers
When they are used, Modifier 1 and Modifier 2 are used to identify and describe the object in the network element that the message will act on. Modifiers commonly refer to equipment type.
(Ex. “RTRV-ALM-ALL”, “RTRV-ALM-T1”)

The TID, AID, CTAG, and General Block
The second part of the message, known as the “staging block”, identifies the exact resource in the network element that will be acted on by the command. The staging block is constructed in the following format:

\[
: \text{TID:AID:CTAG:generalblock:}
\]

The Target Identifier (TID)
Every TL1 device is assigned a Target Identifier or (TID), which uniquely defines that device. The (TID) is the first command in the staging block sequence. The TID is subject to the following rules:

• The TID can be of maximum 20 ASCII characters and may only contain letters, numbers, and hyphens.
• In direct (or “point-to-point”) routing, where commands are sent to an element over a private line, the TID value can be null.
• In indirect routing, where commands are sent over a shared or public line, a valid TID value is essential. If multiple devices will see the same command, you must specify a TID so you can select the device you wish to “talk” to.

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 a lot of responsibilities, you don’t have a lot time to evaluate alarm systems and survey your remote sites.

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.

There’s no hard-sell sales tactics. No harassing sales calls. No pressure to buy. We won’t discuss specific equipment options until we’ve helped you plan the right monitoring strategy for your network.

Rick Dodd
Director of Sales
DPS Telecom
The TID value is also used to identify the source of a response message from a network element.

**The Access Identifier (AID)**
The Access identifier (AID) is found after the TID. It contains one or more simple or compound parameters. The parameters identify a specific entity within the associated target element to be acted upon by the input message.

In other words, the TID defines a network element (Switch Bay 1), and the AID defines the specific segment (Shelf 3, Card 4) of that network element. The AID is often the field that uniquely identifies the alarm.

**The Correlation Tag (CTAG)**
A correlation tag (CTAG) is used to correlates a response or an acknowledgement to an earlier input message. When a response message is sent, it uses the same CTAG to indicate the command to which it is responding. It is, therefore, the user’s responsibility to ensure that CTAGs are unique for each message. A replicated CTAG will not cause an error directly, but it will create uncertainty when responses are received with duplicate CTAGs.

CTAGs are also used as serial numbers for autonomous alarm messages. If a number in the sequence is skipped (ex. 0001,0002,0003,0005), the user can see that an autonomous message was missed and send a “retrieve all alarms” command.

**The General Block**
The General block holds the information of the message. It also denotes how its information will be used by the NE. Certain types of large network elements that engage in switching may make an extension to the basic TL1 message. The general block is required for commands that have a payload and varies depending on the command.

The General Block can also be used to specify delayed actions. To accomplish this functionality, the general block must contain an order number, date, and time for automatic execution. The delayed action feature of TL1 is helpful for busy operators who must perform service maintenance or run performance analysis. You may schedule actions that will be stored in a remote buffer and executed at a specific date and time.

**TL1 Message Samples**

**Autonomous Messages**

Autonomous messages, the most frequently used TL1 response type, are output messages sent by the NEs to report alarms, performance data, configuration changes, or condition changes. This means that alarms are sent immediately, instead of waiting until someone requests a status update. In this way, autonomous messages are the TL1 equivalent of the SNMP trap. In addition to receiving autonomous notification of alarms, TL1 operators can schedule messages that periodically report performance data values.

Sample Autonomous Message #1 (Critical Alarm):

```
<table>
<thead>
<tr>
<th>Code</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>*C</td>
<td>Critical</td>
</tr>
<tr>
<td>**</td>
<td>Major</td>
</tr>
<tr>
<td>*^</td>
<td>Minor</td>
</tr>
<tr>
<td>A^</td>
<td>Status</td>
</tr>
<tr>
<td>M</td>
<td>Response</td>
</tr>
</tbody>
</table>
```

These codes are used to indicate an alarm severity or a response message.
Sample Autonomous Message #2 (Alarm Clear):

```
FRESNO_NODE3 04-05-11 16:16:00
*C 000004 REPT ALM EQPT
"NEW ALARM2: CL ,, NULL ,, NEND , NA" ;
```

As you can see, this message is almost identical to the original Autonomous Alarm Message, but with a slight difference: The code for Critical Alarm (“CR”) has replaced by the code for Clear (“CL”). This indicates that the alarm condition described in the previous message has been cleared.

**Command Messages**
TL1 commands request an action to be executed by the recipient of the message

Sample Command #1 (Login to Network Element with “Activate” Command):

```
ACT:: USER :: USER1 2485 :: PASS1;
```

In this example, the UID is a username, and the PID is a password. They will be compared against the receiving element’s administrator list to determine the success of this login attempt. It’s also important to remember that some NEs will send you no response at all until you have logged in successfully. This is a security measure to prevent malicious users from discovering that the NE is present at all. NOTE: Some TL1 NE’s do not support any security, do not require a login, and do not support the “ACT-USER” command.

NOTE: The CANC-USER command is used to log off of a TL1 network element. Remember that some NE’s will automatically log you off after a certain period of inactivity.

**Response Messages**
The response message (or “output message”) is a reply sent by the NE in response to an input message. The response comes upon the completion of the task requested by the TL1 input message, and it states whether or not the requested task was completed successfully.

Sample Response (Response to User Login Attempt):

```
Response Message
FRESNO_NODE3 07-03-26 08:51:43
M 2485 COMPLD Status (Completed)
"USER1: 07-03-26 08:51:43, 0";
```
Acknowledgement Messages

An acknowledgement message is a special reply sent by the NE in connection with a delayed command. This special response is issued after the receipt of the command and indicates the status of the request:

An acknowledgement message begins with one of the following two-letter response codes:

- **IP** - “In Progress” - Sent if the NE cannot execute a request within 2 seconds.
- **PF** - “Printout Follows” - Command execution is in progress and a response will be sent upon completion.
- **OK** - “Current status is OK” - Command has been executed successfully
- **NA** - “No Acknowledgment” - Execution status is unknown (an error)
- **NG** - “No Good” - Valid command, but cannot be executed due to a parameters issue (an error)
- **RL** - “Repeat Later” - System resources are not currently available to process your command.

Immediately following this two-letter response code, a CTAG matches the acknowledgement message with its associated command message.

**Sample Acknowledgement (Delayed Command Execution Notification):**

![Status Code (In Progress)](image)

**Understanding TL1 Error Messages**

If a TL1 device encounters an error, it will respond directly with an error message containing four standard characters. Most monitoring systems support the same distinct code system. These codes tell you where you need to look to correct your command (TID, AID, etc.).

**Sample Error Message:**

![Timestamp](image)

**Other Four-Letter Error Codes:**

- **ICNV** - Input, Command Not Valid
- **IITA** - Input, Invalid Target Identifier (TID)
- **IIAC** - Input, Invalid Access Identifier (AID)
- **IDNV** - Input, Data Not Valid
- **INUP** - Input, Non-null Unimplemented
- **IISP** - Input, Invalid Syntax or Punctuation
- **PIFC** - Privilege, Illegal Field Code
TL1 via Command Line Interface

Human operators can interact directly with TL1 equipment through a command line interface via Telnet or serial connection. Commands may be typed manually to query and control network elements.

Entering TL1 commands manually via command line must be done carefully, however, as any syntax mistake will result in an error. This can be especially frustrating, because the message must be retyped from scratch. If your NEs have special editing capabilities, you might be able to scroll back to your previous message and correct your mistake, but this is not a core part of TL1.

On some network elements, an echo feature is available to help you minimize retyping. As you type, your characters will be “echoed” back to you by the NE. You’ll be able to see what you’ve typed as you compose your TL1 messages. Be sure to activate this option carefully, however. If multiple NE’s can “see” your keystrokes, you may get multiple echos (“AAACCCCTTT---UUUSSSEEERRR”).

When 2 machines are communicating, you’ll want to turn off any echo options, because machines always know what they typed. Echo can also cause confusion for alarm masters when it’s accidentally left on.

Another potential solution is to activate a “local echo” option in your terminal software. This will make commands you type appear within your terminal. Should you make a mistake, you can generally copy your original message, correct the error, then resubmit the command without retyping it completely.

Potential TL1 Pitfalls - and Solutions

High Bandwidth Requirement
One potentially significant TL1 challenge is the high bandwidth required for transmission of ASCII text. This becomes an issue if your are reporting over slower transports like dialup or 1200 baud.

Strict Message Formats
TL1 can also create issues for users because it is very structured. Any deviation in the command message will result in an error. Using an automated TL1 interface for day-to-day tasks will eliminate typing errors and increase your efficiency.

For the times you need to use the command line, you can decrease time spent retyping commands by becoming familiar with the most common TL1 message types, described earlier. The better you know your message formats, the fewer mistakes you will make.

Although it is useful to understand the command-line foundation of TL1, it’s best to use a high-quality alarm master for day-to-day monitoring and control activities. It’s much more convenient and much less frustrating to use an interface that automates the process of sending commands and displays alarms in a standard format. You’ll also benefit from the advanced capabilities integrated into a master (see page 16).
Using RTRV-HDR to confirm that a TL1 device is online

Unlike polled protocols, TL1 sends autonomous messages to your master. While this reduces network traffic, it also means that you do not automatically receive notification that a network element is down. If you’re not receiving autonomous alarms from a device, you don’t know for sure whether the situation is normal or your TL1 device has failed. You must send a command to act as a “ping”. If you receive a reply, you will know that your network element is online.

In TL1, The RTRV-HDR (“Retrieve Header”) command is commonly used to confirm a network element is online. Both the command and the response are simple, but they achieve the intended purpose of testing device status.

**RTRV-HDR Command Format:**

```
RTRV-HDR:TID::CTAG;
```

**Example RTRV-HDR Command:**

```
RTRV-HDR:FRESNO_NODE3::4287;
```

**Example RTRV-HDR Response:**

```
FRESNO_NODE3 07-03-27 09:47:27
M 4287 COMPLD
;
```

You must insert the TID of the device you are pinging and specify a CTAG. If you receive a response with the same TID and CTAG you used, you have confirmed that the TL1 device you pinged is online.

While manual RTRV-HDR commands can be useful in some situations, a good alarm master can be programmed to send RTRV-HDR commands to devices at regular intervals to ensure that failures will be detected within a reasonable amount of time. RTRV-HDR can also be used check the NE’s current time-of-day and to avoid being logged off due to inactivity.

Using RTRV-ALM to request a report of standing alarms

The “Retrieve Alarms” command is commonly used to review an NE’s current standing alarms. It’s also useful if you see a gap in the CTAG sequence of autonomous messages. This almost always means that you’ve missed an alarm message, so it’s important to request a full alarm listing so you can see what’s happening with your network element. One handy feature of RTRV-ALM is the availability of additional modifiers that limit the scope of your alarms (Ex. RTRV-ALM-ALL will return all standing alarms, white RTRV-ALM-T1 will return only standing T1 alarms). This is similar to a database query and has the added advantage of limiting the bandwidth consumed by the response message. You can also restrict the alarm list by adding other criteria, as shown in the example below:

**Example (Retrieve all critical alarms (“CR”) from the “FRESNO_NODE3” network element):**

```
RTRV-ALM-ALL:FRESNO_NODE3::8607::,CR;
```

**Example (Response to RTRV-ALM-ALL, critical alarms only command):**

```
FRESNO_NODE3 1998-06-20 14:30:00
M 8607 COMPLD
"AC_FAIL,EQPT:CR,,SA,,,NEND,NA:\""
"BATT_LOW,EQPT:CR,,NSA,,,NEND,NA:\""
"GENERATOR_FAIL,EQPT:CR,,SA,,,NEND,NA:\""
;
```
Mediate Your TL1 Alarms to SNMP

Before T/Mon:

Without T/Mon, you have to run a TL1 master side-by-side with your SNMP master, increasing the number of screens you have to watch.

After T/Mon:

Are you running a TL1 master side-by-side with your SNMP manager? That’s two screens to watch, which increases the chance that you’ll miss an alarm. You have to train and pay multiple operators just to achieve basic alarm visibility.

T/Mon NOC collects alarms from over 25 protocols, including TL1, and forwards them as SNMP traps to your SNMP manager. Now you can see your entire network status from just one screen.

You also get all of the other benefits of T/Mon, including paging and email notifications, derived alarms and controls, text messages, trouble logs, and more. To learn more about T/Mon NOC, visit http://www.dpstelecom.com/tmon

With T/Mon, you can mediate your TL1 and other alarms as SNMP traps to your SNMP manager, so you can see all of your alarms on one screen.
Case Study: Triple Play Provider EastLink Manages Rapid Network Growth with T/Mon NOC Network Alarm Management

A rapidly growing, technologically advanced network. A mix of diverse equipment. Remote sites spread across three provinces.

Canadian triple-play provider EastLink is successfully managing the network of the future with help of T/Mon NOC and the NetGuardian 832A.

Based in Halifax, Nova Scotia, EastLink is considered a market leader and innovator for its successful launch of telephone service over a cable network in the late 1990s. The company saw an opportunity to expand and enter a new market when the Canadian government deregulated telecom, allowing local competition.

In 1999, with a strong entrepreneurial spirit at its back, EastLink became the first Canadian cable company to successfully expand into the local residential telephone service. Service was later launched to business customers in 2001.

Since then, EastLink has been growing offering bundled telephone service, high-speed Internet access and digital cable at competitive prices in a rapidly expanding service area.

"We were the first cable company in Canada to launch residential telephone service and bring competition to the local market. That's an achievement for a company that at the time employed just over 200 employees," said Jim Bower, EastLink's telecom operations manager. "Then we were the first to introduce communications and entertainment bundles. Six years have passed and cable and telephone companies continue to follow our lead."

Leveraging the existing network
EastLink has a terrific advantage in delivering triple-play — the company leverages its existing cable TV infrastructure to deliver all three services. It provides voice telephony over a hybrid fiber-coaxial network using an Arris Cornerstone cable telephony system.

From the customers' point of view, phone service over EastLink's coax looks and feels no different than service from a traditional provider — even the standard phone jack looks the same. "The secret to our success is that we've been able to deliver a phone service that meets our customers' needs, while at the same time providing them with great value and choice. " said Bower.

Managing a growing network is an alarm monitoring challenge
Rapid growth, new customers and leveraging new use from existing network equipment are all strengths — but they also add up to a tremendous network management challenge. Besides the growing number of network sites to manage, EastLink operates a diverse mix of equipment, each of which has its own monitoring and management interface.

"We have an array of different diagnostics and notifications from our Operational Support Systems (OSS)," said Bower. "While we know there are a number of things happening on our network, visually it was often difficult to locate the exact problem.

Despite all those multiple systems, EastLink still needed an environmental monitoring system and that is why it turned to DPS Telecom. "Until we starting using the NetGuardian, we didn't have consistent environmental telemetry at our head-end sites. We have approximately 15 main sites and 25 to 30 smaller sites, and we weren't always aware of some small and larger issues like: Is the door open? Is it too hot? Is there power?" Bower said.
Getting that environmental information is crucial, because EastLink's remote sites are scattered throughout the Maritimes. Some of the sites are located six hours away from EastLink's Halifax headquarters, posing significant challenges if or when a problem arises.

That is why tackling the monitoring challenge with the NetGuardian and T/Mon NOC was so important. EastLink first came to DPS Telecom to add environmental monitoring capability and from that point started installing NetGuardian 832A remote telemetry units at their headend sites to monitor power supplies, temperature and door alarms. Working with the NetGuardian led EastLink to see the advantages of the T/Mon NOC Remote Alarm Monitoring System.

"At first we were using an SNMP manager to pick up SNMP traps from the NetGuardians," said Bower. "SNMP managers have an extensive programming background and in order to understand the information, you also needed to have this background. We needed a system that could be understood by someone with a basic telephony background."

Bower then compared the awkwardness of the SNMP manager's presentation with the ease-of-use and presentation capabilities of T/Mon NOC.

"Every year I've been to SUPERCOMM, a major telecommunication conference, I've always stopped by the DPS booth and looked at T/Mon. I've seen demos and Rick Dodd, DPS Director of Sales, demonstrated a live T/Mon demo over the Web. We were impressed with T/Mon — someone with a basic telecommunications background could use the technology," Bower said.

T/Mon presentation provides exact information about alarms
According to EastLink NOC supervisor Derrick Stennett, T/Mon NOC's specific and detailed alarm information is helping the company manage problems better and faster.

"The most important way we've been able to use T/Mon is to list specific information in the text messages for each alarm. For example, in the event of a smoke alarm, I can see a specific number to call to escalate the alarm, a contact for security company to follow up on the site and the specific location of the site in case 911 needs to be called. The information's right in front of me, resulting on overall increased efficiency and a significantly shorter repair time," Stennett said.

By consolidating alarm information in one place, T/Mon also lowers staffing costs, according to Bower. "We have a 24-hour staffed Network Operating Centre and with all we have to manage, we had to evaluate whether we add more resources or find a technology that can help us manage the network. With T/Mon, we hope to move towards a time when one employee can monitor the network and use just one screen as their first alert," Bower said.

T/Mon consolidates multiple alarm systems onto one screen
T/Mon NOC's unified presentation — displaying all alarms from the entire network on one screen — is helping EastLink manage its diverse mix of equipment. EastLink's Cornerstone equipment reports to T/Mon NOC over TL1 protocol using T/Mon's ASCII Alarm Processor Software Module. Their DMS switch reports via ASCII messages, which are also parsed by T/Mon's ASCII Processor. NetGuardian 832A remote telemetry units collect environmental alarms at remote sites and report them to T/Mon NOC.

In the future, Bower and Stennett hope to use SNMP alarm reporting to tie even more equipment to T/Mon NOC's integrated alarm presentation.

"We're trying to consolidate all alarms into T/Mon so, if I want to know what's happening on the network, I can look at one screen and, with a high degree of accuracy, know it's been a quiet day with no alarms," said Stennett.
Monitor a Complete SONET Ring with TL1 by Connecting to Just One Network Element

SONET devices are some of the most commonly deployed TL1 network elements today. The special architecture of a SONET ring offers added benefits for TL1 monitoring.

A SONET ring must be connected to the TL1 OSS through only one device on the ring (known as the “Gateway”). Whenever the gateway network element receives a TL1 message, it uses the TID to route the message to the appropriate network element.

In this way, you can reach all of the devices on a SONET ring by connecting to only one.
Mediate Over 25 Protocols to Your Existing TL1 Master

If you are primarily using a TL1 master, you understand the difficulties of monitoring devices that communicate in other protocols. To maintain adequate visibility, you have to run multiple masters simultaneously, which means more screens to watch, more interfaces to learn, and a significant risk that you’ll miss a critical alarm.

T/Mon provides the solution, offering you the capability to collect alarms in over 25 protocols and mediate them to your existing master as TL1 messages. Alternatively, since T/Mon can also interpret TL1 messages from network elements, you have the option of replacing your TL1 master with T/Mon and using it as your top-level monitoring platform. To learn more about T/Mon NOC, visit http://www.dpstelecom.com/tmon
DPS is Committed to Meeting Your Exact Needs

DPS Telecom is an industry-leading manufacturer of customized alarm management products. Our custom engineering and agile manufacturing capabilities allow us to create custom monitoring products that meet your exact needs.

“Considering the very strict AT&T OS systems compatibility requirements we placed on you, and the short project timelines we both faced on this project, we are very pleased with the remarkable end results. DPS Telecom has done a fantastic job, and your entire team has far exceeded our very high expectations.”

—Walter E. Dziama
AT&T

"We wanted to replace all the masters with one master. We also wanted to add native IP remotes and migrate as many sites as possible to IP network monitoring."

"DPS was the only one that said it could do it all, either through hardware or software. Everyone else had an exception."

—John Mullen and Daniel Jackson
Dominion

"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

"It was very important for us to find a vendor who was willing to customize the alarm system to meet our needs. Like many carriers, we have a mix of equipment — everything from microwave radio systems to high capacity dense wave division multiplexing systems. We needed an alarm system that could pull in TBOS alarms, discrete alarms, SNMP ... DPS has products that meet our needs."

—Paul Mankins
Norlight Telecommunications

For Additional Information

This guide provides an introduction to the basics of TL1 protocol. For additional information concerning TL1 please refer to the following Telcordia documents:

• GR-831-Core
• GR-835
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.

The 3 Fatal Mistakes Telecom Executives Commonly Make When They Attempt To Maintain Service Levels at Remote Sites In the Face Of Reduced Staffing ...
And How You Can Avoid Them
Your network monitoring can be an asset to your business, or it can be a threat. Here are the three fatal mistakes telecom executives make in planning their network monitoring-and how you can avoid the mistakes and gain a competitive edge. To receive this report, send an e-mail to: 3fatalmistakes@dpstelecom.com.

SNMP Tutorial: A Fast Track Introduction to SNMP and its Practical Use in Network Alarm Management
An introduction to SNMP from the perspective of network alarm management. It summarizes the history and structure of the protocol, and offers some concrete applications for using SNMP for network alarm management. To receive this report, send an e-mail to: snmpfasttrack@dpstelecom.com.

Unsupported Legacy Network Alarm Monitoring Equipment: Why It's a Problem - What You Can Do About It
Many companies are dependent on legacy network monitoring equipment that is no longer supported by the manufacturer. This guide to legacy support issues explains why legacy equipment is a dead-end-and how you can escape the legacy trap. To receive this report, send an e-mail to: legacytrap@dpstelecom.com.

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.”
“(At DPS Factory Training), ASCII and TL1 commands... [were] presented very well, making the introduction to a new language enjoyable!”

—Dewayne Hamilton
Level 3 Communications

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

—Lee Wells
Pathnet

About the Authors

Robert Berry is founder and CEO of DPS Telecom, an industry-leading developer of network alarm management solutions. Two decades' experience designing remote telemetry systems have taught Berry that technology is most powerful when it meets real-world business needs. DPS Telecom clients have grown to appreciate Berry's dedication to developing technology solutions that lower costs and raise revenue.

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