Realtime publishers

The Essentials Series: Solving Network Problems Before They Occur

How to Use SNMP in Network Problem Resolution

sponsored by

IPSWITCH WhatsUpGold
KNOW YOUR NETWORK

by Greg Shields

Copyright Statement

How to Use SNMP in Network Problem Resolution

I've spent almost 15 years of my life as an IT professional. In that time I've been a phone support operator, field technician, systems administrator, consultant, and now an independent technology author and presenter. Through those experiences, I've seen a wide range of very different environments in very different businesses. Those IT environments range from the exceptionally simple, installed into actual closets within small business offices, all the way to multi-enterprise, multi-national collaborative networks.

What's interesting about all of them is their similarity. Some networks have more applications than others. Some have faster connections between sites. Some use more remote applications. Yet there's a common thread in all of them: *from time to time, they all have problems.*

There's also something remarkably strange about those networks I've seen. Even though we can all agree that every network occasionally has its problems, relatively few have the tools in place to find and fix them. For reasons of cost, or time, or lack of subject knowledge, many IT organizations haven't implemented unified and comprehensive network monitoring solutions.

It is my goal in this Essentials Series to explain why you should. With the right platform in place, you'll experience less downtime, more customer satisfaction, and fewer late nights tracking down the network problems of the day. Using a series of examples from my own experience, I want to show you how effective network monitoring can help to solve network problems *before they occur*.

SNMP, the Solution

Let's start by looking at actual solutions to your network's visibility problem. Networks are by nature very opaque. You can't simply peer through cables or into routers to see the behaviors going on during their operation. To see what's going on in your network, you need tools that do the peering for you.

Those tools start with the individual devices themselves. For example, if you queried the interface statistics on a Cisco router, you would be greeted with information about that interface's traffic:

```
router1#show int
Ethernet0 is up, line protocol is up
[…snip…]
37592 packets input, 2859273 bytes, 0 no buffer
Received 15938 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
15288 packets output, 1395393 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets, 0 restarts
0 output buffer failures, 0 output buffers swapped out
```

That information is descriptive of the individual device you've logged into, but stops there. Today's network devices natively include all the necessary capabilities to gather and report on their network traffic statistics. You can today request this information from each device and manually build a picture of how your network is operating. However, the complexity of doing so rises dramatically as your network's count of interconnected devices goes much past one.

To combat these complexities, the Simple Network Management Protocol (SNMP) was ratified in the early 1990s. This protocol enables a request-response framework between individual devices and a central Network Management Solution (NMS). Individual devices can be polled for their information through a GET request by the NMS. Device information is stored and can be addressed via its globally-unique Management Information Base (MIB) Object Identifier (OID). An OID's long string of digits represents the "address" for the unit of information being stored on that device. Information being stored can relate to network statistics, details about that device's configuration, performance and throughput metrics, or really any information that the device's manufacturer has enabled.

This part of SNMP's poll-based nature means that information must be requested if it is to be sent back to the NMS. For this reason, SNMP also has a unidirectional alert component. An SNMP "trap" represents a preconfigured alert from a device back to its NMS, reporting on conditions that the NMS should know about. This setup enables SNMP clients to rapidly notify the NMS when problems exist.

SNMP also comes in many versions, with later versions including additional and desired features over those in the previous. SNMP v3 is today's version commonly used by most environments because it adds a suite of critical security features that protect its data in transit and authenticates servers prior to communication. This encryption ensures that the clear text data transfers of earlier versions are protected from prying eyes, while servers must prove their identity before they're communicated with.

You'll probably recognize that this information on SNMP is neither new nor revolutionary in the way it works. With SNMP rapidly approaching its 20th birthday, its protocol is mature and its capabilities are well known. Yet in making this statement, why are so many IT organizations still not using it? Perhaps they don't understand its true power in solving network problems before they occur. Consider a few examples…

SNMP, Total Network Awareness

Recognizing how SNMP does its job is far less exciting than realizing how it can spot and solve network problems. The information gained through SNMP connections and stored in a central NMS enables a situational awareness of your network. This awareness illuminates the behaviors on all devices through a single console, providing you a single heads-up display of your network's health.

As an example of this, I used to work for a company that built satellite ground stations. This company's complex development activity required the cooperation of multiple business units and even multiple companies, all in different locations. To ensure that everyone was working on the same page, we architected a centralized collaboration environment that brought all parties together to the same set of applications. This remote application infrastructure was a perfect solution for its users, enabling them to share documents and work together whether they were in Colorado, California, Massachusetts, or anywhere.

Perfect, that is, until the network began experiencing problems. Remote application infrastructures, such as Microsoft Terminal Services or Citrix XenApp, by nature perform well over low-bandwidth connections. They enable users to work on remote applications as if they were installed locally, even over the slowest of network lines. Yet although they do well in low-bandwidth situations, the streaming nature of their protocols means they do not do well across those that are highly latent.

In this environment, it was well known that certain WAN connections to certain sites would experience latency from time to time. This project's network traffic was only a portion of the traffic sourcing from each site. Rather than waiting for administrators to get phone calls when users' experience degraded, this environment elected instead to configure SNMP across each remote device. Each device was configured to report to a central NMS. That NMS queried each device for its interface utilization and ping latency statistics on a regular basis. Traps and subsequent administrator alerts were additionally set up to alert the central NMS when metrics went below acceptable thresholds.

Device	Monitor	Up	Maintenance	Unknown	Down	Availability
10.0.0.10	Ping	39.651%	0.000%	0.000%	60.349%	
10.0.0.2	Ping	35.025%	0.000%	0.000%	64.975%	
10.0.0.1	Ping	34.627%	0.000%	0.000%	65.373%	
10.0.12.10	Interface (...	34.384%	0.000%	0.000%	65.616%	
10.0.12.10	Interface (...	34.334%	0.000%	0.000%	65.666%	
10.0.12.10	Ping	34.262%	0.000%	0.000%	65.738%	
10.0.11.10	Interface (...	32.587%	0.000%	0.000%	67.413%	

Figure 1: SNMP enables the creation of ping latency graphs across multiple devices.

The result was the creation of a real-time graph similar to that shown in Figure 1. There, you can see where ping latency information across devices was graphed, giving administrators information about the health of each connection. Because the right people were also alerted as conditions went below thresholds, they were able to compensate as necessary to maintain their users' experience.

SNMP, Disaster Protection

Although SNMP is most commonly associated with gathering network statistics and configurations, it is extensible to even non-network devices as well. SNMP was originally developed as a communications framework between all kinds of networked devices. Thus, any device with a network connection can potentially receive and respond to SNMP requests or send its own traps.

Nowhere is this more valuable than with the environmental sensors used in many data centers today. These environmental sensors regularly check the temperature, humidity, and (in the case of accidental flooding) water level present in the data center room. The installation and use of these sensors is critical to ensuring that your expensive IT investment doesn't melt down if your data center air conditioning stops functioning.

That exact situation happened to me at another former client. That day, I had the lucky privilege of stepping into their data center on the very day their air conditioning unit experienced a massive, yet unnoticed, failure. Walking into that data center, the massive outpouring of heat made me immediately recognize that something was terribly wrong. I looked over to the room's temperature sensor—a cheap model more often found attached to the outside of your bedroom window—to discover that the temperature had crossed the 80° threshold and was increasing at a rate of 1° every 10 minutes. Humidity was similarly affected.

Although the problem was quickly resolved through the forced shutdown of non-essential equipment and the introduction of backup air conditioning, the problem could have been dramatically worse had my timing been different. The network-enabling of data center sensors using protocols such as SNMP illuminates another of this protocol's key value propositions.

With the right tools in place, an alert could have notified administrators immediately when temperature conditions in the data center started their deviation. Consolidating SNMP's data into a unified network management solution enables the real-time alerting of problems directly to network administrators.

SNMP, Easy Implementation

As I travel across IT environments, I find that a common hurdle in implementing comprehensive monitoring relates to its perceived difficulty in implementation. Although numerous enterprise-scale monitoring solutions are available today, their implementation often installs little more than an empty shell to be later populated by dedicated monitoring administrators.

Needed for environments that aren't necessarily "enterprise" are cost-effective solutions that implement quickly and without the need for specialized knowledge. The right solutions for your environment will immediately begin gathering useful data with a minimum of daily maintenance. As you'll discover in the next article of this series, such solutions integrate with servers and applications as well as networking devices to provide a complete view into your network.