

Securing an SNMP Environment

Simple Network Management Protocol (SNMP) is widely used for managing network activity. Although many networks employ this protocol, it can create security vulnerabilities. To secure the SNMP service, network administrators can take certain actions, including using tools such as Dell™ OpenManage™ Server Administrator. This article provides an overview of SNMP, its security vulnerabilities, and the measures administrators can take to secure an SNMP environment.

BY STEPHAN MAAHS

The Simple Network Management Protocol (SNMP) emerged in its first version, SNMPv1, in 1988 as a combination of the Simple Gateway Monitoring Protocol (SGMP) and the High-level Entity Management System (HEMS). Figure 1 shows the evolution of this protocol.

In 1990, the proposal for SNMPv1 (RFC 1157) became a standard and was then integrated into the Management Information Base (MIB) II in 1991 (RFC 1213). Together, SNMP and MIB II soon became widely used for network management applications in TCP/IP-based networks.

In 1993 and 1996, respectively, SNMPv2p and SNMPv2c were introduced as new versions of the SNMP protocol. However, these new versions were partly incompatible with SNMPv1, and because the first version had been widely adopted, the newer versions were not popular in the IT industry. Not many implementations were developed, and adoption of SNMPv2 was unsuccessful.

In 1998, the first proposal for SNMPv3 appeared. This proposal included, among other things, a model for access

control and security as well as for a new architecture. SNMPv3 has yet to attain wide acceptance, and SNMPv1 still dominates the IT industry.

Identifying the strengths and weaknesses of SNMPv1

SNMPv1 offers several advantages: It requires the agent to perform only a few functions, which do not consume substantial processor and memory resources; and it is simple to install and maintain. The additional load on the network is minimal, because SNMP normally transmits only simple values. Another advantage of this protocol is that it has been widely adopted in the IT industry and thus is supported by several systems management applications.

The most significant disadvantage of SNMPv1 is its security weakness. The protocol provides no authentication or encryption. Figure 2 shows how SNMPv1 works. To monitor, configure, and manage a network responsibly, IT administrators should address these SNMP security problems.

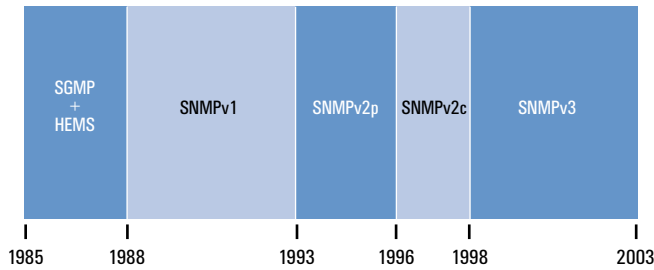


Figure 1. The evolution of SNMP

Four questions should be answered before performing the SNMP operations shown in Figure 2 (GetRequest, GetNextRequest, SetRequest, GetResponse, and Trap):

1. Is the received message authentic?
2. Who requested that this operation be performed?
3. Which objects are affected by this operation?
4. What rights does the party who requested the operation have concerning the affected objects?

Answers to the first two questions are required to secure the message, which means authentication and encryption are necessary. Answers to the third and fourth questions will provide the model for access control.

The access mechanism in SNMPv1

SNMPv1 uses only a community string for authentication. This community string is ambivalent: it is both a user ID and a password and controls access to information about the managed devices.

Standard SNMP uses two types of community strings: read-only and read-write. The read-only community string allows administrators to query the device and only read values, while the read-write community string allows administrators not only to read values but also to change those values. However, the community string names are transmitted in clear text, and a cracker who is packet sniffing the network can determine the community name from passing traffic. Once this community name is known, the attacker can then read the values of the managed device, make configuration changes, and even shut down or reboot the system.

SNMP has been widely adopted in the IT industry and thus is supported by several systems management applications.

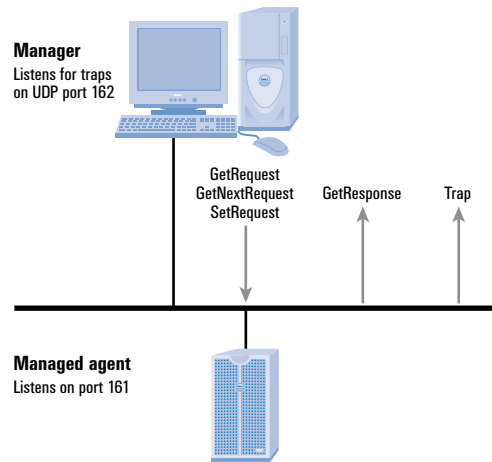


Figure 2. How SNMPv1 works

In many cases, attackers do not even need to sniff the network traffic to obtain a community name, because they can guess them relatively easily. In the past, many network administrators used easy-to-guess or well-known community names, such as “public,” “admin,” or “private,” and sometimes did not even use a password.

Attackers also can exploit the characteristics of the User Data Protocol (UDP), which SNMP uses. As a connectionless transport protocol, UDP allows the delay, replay, and reordering of packets. Consequently, attackers also can delay, replay, and change packets and also may be able to influence the managed device’s behavior.

Securing SNMP

Although SNMP presents serious security concerns, administrators can protect their networks by following the recommendations of the CERT® CA-2002-03 advisory or by using tools such as Dell™ OpenManage™ software.

Recommendations from CERT

In 2002, the CERT Coordination Center—the organization that monitors and advises users on Internet security issues—released an advisory notice describing security vulnerabilities in SNMPv1. The CERT CA-2002-03 advisory¹ provides the following recommendations for those using SNMP in a network:

Apply a vendor-supplied patch. Appendix A of CERT CA-2002-03 provides further information from vendors about their patches.

Disable the SNMP service. Administrators should disable any unnecessary services or functions, including SNMP. However, when

¹CERT Coordination Center, “CERT Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP),” <http://www.cert.org/advisories/CA-2002-03.html>.

snmp	161/tcp	# Simple Network Management Protocol (SNMP)
snmp	162/tcp	# SNMP system management messages
smux	199/tcp	# SNMP Unix Multiplexer
smux	199/udp	# SNMP Unix Multiplexer
synoptics-relay	391/tcp	# SynOptics SNMP Relay Port
synoptics-relay	391/udp	# SynOptics SNMP Relay Port
agentx	705/tcp	# AgentX
snmp-tcp-port	1993/tcp	# cisco SNMP TCP port
snmp-tcp-port	1993/udp	# cisco SNMP TCP port

Figure 3. Less common SNMP services that may benefit from ingress filtering

disabling SNMP, administrators also should implement filtering practices for additional security.

Employ ingress and egress filtering at the network perimeter.

As a temporary solution, administrators can block access to SNMP services at the network perimeter. This action may help limit the scope of security vulnerabilities.

Ingress filtering controls incoming traffic as it enters the network. Normally, the only devices that must accept inbound traffic from the public Internet are servers. External hosts do not often initiate inbound traffic to servers that do not provide public services. Therefore, administrators can perform ingress filtering at the network perimeter to help prevent unauthorized services from receiving externally initiated inbound traffic.

Administrators can employ ingress filtering on the following ports to protect those devices in the local network that are not authorized to provide public SNMP services:

```
snmp 161/udp # Simple Network Management Protocol (SNMP)
snmp 162/udp # SNMP system management messages
```

In addition, administrators may use ingress filtering for the less common services shown in Figure 3. Blocking certain services may affect other services, and administrators should carefully consider these ramifications.

Egress filtering controls outgoing network traffic. Devices providing public services usually do not need to initiate outbound traffic to the Internet. By employing egress filtering at the network perimeter, administrators can help prevent attackers from using the network to attack other sites.

Filter SNMP traffic from unauthorized internal hosts.

Only a few network management systems need to initiate SNMP request messages. Thus, administrators can configure SNMP agent systems to prohibit request messages from unauthorized

systems. This action can help reduce—although not completely eliminate—the threat of internal attacks.

Change default community strings.

Products enabled with SNMP usually feature default community strings: “public” denotes read-only access and “private” denotes read-write access. Because these default access-control mechanisms are commonly known, network administrators should change community strings to make them more difficult to guess. Nonetheless, community strings—regardless of whether they have been changed from the default setting—are passed in plain text and thus vulnerable to packet-sniffing attacks.

When configuring SNMP community strings, administrators should follow these guidelines:

- Do not use the default “public” or “private” string.
- Do not use a string that would be easy to guess, such as the company’s name or phone number.
- Do not use a text-only string; use an alphanumeric string (both text and numerals).
- Use both uppercase and lowercase letters (community strings are case-sensitive).
- Use a community string that is at least six characters long.

Server Administrator can perform almost every “set” action that IT Assistant can, without SNMP and its vulnerabilities.

Figure 4 lists examples of effective and ineffective community strings.

Segregate SNMP traffic onto separate management networks.

In some environments, blocking or disabling SNMP is not possible. Administrators can limit SNMP security threats in these environments by confining SNMP access to isolated, privately accessible management networks.

Ideally, this segregation would require physically separate networks, but that type of infrastructure is usually impractical. Instead, administrators can use techniques such as virtual LANs (VLANs) to help segregate network traffic. VLANs may not completely prevent attackers from exploiting SNMP vulnerabilities, but they can hinder an attacker’s ability to initiate an attack.

In addition, administrators can implement virtual private networks (VPNs) to segregate SNMP traffic. VPNs use cryptography to provide strong authentication. However, administrators should be aware that implementing solutions such as VLANs and VPNs may require substantial alteration of the network architecture.

Dell OpenManage Server Administrator and read-write deactivation

Dell OpenManage Server Administrator is a reliable and robust tool for managing an individual server. It also can help make the use of SNMP more secure by allowing administrators to disable SNMP read-write access and community strings completely and to use read-only access and community strings exclusively.

In such a scenario, Dell OpenManage IT Assistant is used only as a collector of SNMP traps (possibly combined with actions such as e-mail alerting), and as a console for the status overview. Every “set” action, such as setting a temperature threshold, shutting down a system, or rebooting—the SetRequest operations in SNMP—is then executed through the secure Server Administrator interface. Server Administrator can perform almost every “set” action that IT Assistant can, without SNMP and its vulnerabilities.

In addition, Server Administrator offers the following security features:

- Data encryption
- Operating system (OS) integrated authentication
- Secure Web server
- Configurable security policies

To determine whether the provided user ID and password are valid, Server Administrator queries the OS authentication mechanisms. Server Administrator is firmly integrated with native


Ineffective community strings	Effective community strings
Public	4Gomer
Hugo	0815Schröder
Dell	Ö1Ü2..212
Matahari	MVemjSunP

Figure 4. Effective community strings to enhance network security

Although SNMP presents serious security concerns, administrators can secure their networks by following the recommendations of the CERT CA-2002-03 advisory or by using tools such as Dell OpenManage software.

OS authentication schemes to perform user authentication. On Microsoft® Windows® platforms, it uses NT LAN Manager (NTLM) and domain authentication. On Linux® platforms, it uses Pluggable Authentication Module (PAM), and on Novell® NetWare® platforms, it uses Novell Directory Services® (NDS®).²

Striving toward better network security

SNMP often plays an integral part in network management, and the security issues that arise from its use can be pervasive. As future releases of SNMP enhance its capabilities, the security vulnerabilities of this protocol may diminish. In the meantime, network administrators should take action—whether following the CERT recommendations or using tools such as Dell OpenManage Server Administrator or both—to help ensure the security of their computing environments. 

Stephan Maahs (stephan_maahs@dell.com) is a system consultant for the Global Segment and Large Corporate Accounts divisions of Dell Computer Corporation and serves as a subject-matter expert in systems management. Previously, he worked at IBM as a system consultant for IBM® Netfinity® servers. Stephan has a degree in industrial engineering from the University of Applied Sciences in Giessen-Friedberg, Germany.

FOR MORE INFORMATION

CERT Advisory CA-2002-03:
<http://www.cert.org/advisories/CA-2002-03.html>

Microsoft Security Bulletin MS02-006:
<http://www.microsoft.com/technet/security/bulletin/MS02-006.asp>

Novell SNMP vulnerability fix for NetWare 4.x, 5.x, 6.x:
<http://support.novell.com/servlet/tidfinder/2961546>

Red Hat® updated SNMP packages:
<http://rhn.redhat.com/errata/RHSA-2001-163.html>

² For more information about Server Administrator security, see the Dell white paper, “OpenManage Server Administrator Security,” at http://www.dell.com/downloads/global/topics/openmanage/omsa_security.doc.