Avaya IP Telephone SNMP Security - Issue 0.1

Abstract

The purpose of this document is to discuss Simple Network Management Protocol (SNMP) security enhancements in Avaya IP Telephones. As of H.323 Release 2.6 for 46xx and Release 1.0 for 96xx Avaya IP Telephones, SNMP is disabled by default. The previous practice of using a default read community string has been discontinued, and administrators are now required to specify the read community string to enable SNMP read access. This document outlines the steps required to securely enable and restrict SNMP for the above-mentioned releases. In addition, this document also details the steps that must be taken to disable SNMP in previous 46xx IP Telephone releases.

Table of Contents

1. Introduction

Simple Network Management Protocol (SNMP) is a family of standards-based protocols and procedures to allow vendor-independent data network management. Using a simple set of protocol commands, a SNMP-compliant device stores information in standard format in one or more Management Information Bases (MIBs). In addition to supporting standards-specific MIB termed MIB-II, devices can define one or more “custom MIBs” that contain information related to device-specific features.

As of Release 2.6 for 46xx and Release 1.0 for 96xx, Avaya’s IP Telephones are fully compatible with SNMPv2c, a later version of SNMP, and with Structure of Management Information version 2 (SMIv2). The telephones will also respond to queries from entities that comply with earlier versions of SNMP, such as SNMPv1. “Fully compatible” means that the telephones respond to queries directed towards either the MIB-II or the Custom MIB[1]. The 46xx and 96xx Series IP Telephones MIBs are read-only. Read-only means that the values therein cannot be changed externally by means of network management tools.

Avaya Services and/or Avaya’s Business Partners often rely on SNMP and the IP Phone’s MIB for troubleshooting purposes, as IP Telephone configuration information, statistics, and device logs can be retrieved using the phones’ SNMP read access. Regardless of whether SNMP is disabled, troubleshooting information continues to be logged and stored in the phones MIB until power is lost. The reader should take note that SNMP must be enabled and administered on the IP Phone prior to attempting to retrieve the MIB data. If an IP telephone does not have SNMP enabled, it must be rebooted to enable SNMP, using methods described in this document.

To find more information about SNMP and MIBs, see the IETF references listed in the Additional References section of this document. The Avaya Custom MIB for the 4600 and 9600 Series IP Telephones are available for download in *.txt format on the Avaya support Web site at http://www.avaya.com/support.

2. SNMP Security

Currently, there are three major versions of SNMP. SNMP version 1 and 2 which transmit and send all information in the clear (unencrypted), and SNMP version 3, which offers secure authentication and encryption. Versions 1 and 2 use unencrypted community strings as the only authentication mechanism. As such, an attacker could eavesdrop and capture SNMP traffic as it’s transmitted across the network. Sensitive information includes, but is not limited to, phone information, call server information, and networking information and logs.

[1] Although both 46xx and 96xx telephones support SNMP v2c and have custom Management Information Bases (MIBs), the MIBs are formatted differently.

A widely known issue regarding SNMP security is that many administrators don't change the default community strings, such as "public" and "private", shipped with the vast majority of SNMP-enabled devices. An attacker, who has access to the SNMP-enabled devices and knows the community strings, can obtain sensitive information from read-only MIBs and/or modify read-write MIBs when SNMP is unrestricted. Avaya recommends that "public" and "private" community strings are not utilized.

An attacker who has captured SNMP traffic, such as a community string, brute-force guessed the community string, or finds default community strings can disclose sensitive information about the IP Telephone and other converged telephony elements if SNMP is not secured.

3. SNMP Security in Avaya IP Telephones

3.1. IP Phone SNMP Security

Avaya 46xx Release 1.1 through Release 2.4 has SNMP enabled by default. As of 46xx Release 2.0 and 96xx Release 1.0, the IP Telephones allow administrators to set the SNMP community string (SNMPSTRING) and to restrict SNMP access to administered IP Addresses (SNMPADD).

In response to customer feedback, beginning with Avaya 46xx H.323 Release 2.6 and 96xx Release 1.0 IP Telephones, SNMP is disabled by default.

The following table further defines the above mentioned SNMP settings and release dependencies:

IP Phone Models and Releases	**SNMP Default**	**SNMPSTRING Administrable?**	**SNMPADD Administrable?**
46xx Release 1.1 through Release 2.4	Enabled	R2.0 (and later)	R2.0 (and later)
46xx H.323 Release 2.6 (and later) 4601+,4602+,4610SW,4620SW,4621SW,4622SW	Disabled	R2.0 (and later)	R2.0 (and later)
96xx Release 1.0 (and later)	Disabled	R1.0 (and later)	R1.0 (and later)

Table 1 – SNMP Settings and Release Dependencies

On Avaya IP Telephones SNMP security is controlled by setting SNMP-specific Customizable System Parameters in the phone to desired values. The Customizable System Parameters are controlled by means of the DHCP or TFTP/HTTP/HTTPS servers. The following sections will discuss how to change Customizable System Parameters which affect SNMP security.

3.2. Customizable System Parameters

Avaya IP Telephones Customizable System Parameters are set using the Avaya-provided settings script (**46xxsettings.txt**) and/or DHCP Site-Specific Option Number (SSON). The relevant SNMP-specific parameters include SNMPSTRING and SNMPADD.

The SNMPSTRING parameter is a text string containing the SNMP community name string (up to 32 ASCII characters, no spaces). If SNMPSTRING is set to " " (Null), then SNMP is disabled on Avaya IP Telephones.

The SNMPADD parameter is a text string containing zero or more allowable source IP addresses for SNMP queries, in dotted decimal or DNS format, separated by commas, with up to 255 total ASCII characters including commas.

3.2.1. DHCP SSON

Customizing the SSON affects all telephones, on a specific Dynamic Host Control Protocol (DHCP) subnet scope, associated with the DHCP server. Avaya 4600 Series IP Telephones utilize DHCP Option-176 while 9600 Series IP Telephones utilize DHCP Option-242 for SSON. For each SNMP-specific system parameter included, append the SSON string with a comma followed by *name=value* where *name* is a parameter name and *value* is its associated value[2]. Invalid values cause the data to be ignored for that name.

The following is an example SNMP-specific SSON setting utilizing Option-176:

Option 176: "**SNMPSTRING="*mystring***", "**SNMPADD=192.168.0.22,192.168.0.23"**

This option will set the SNMP community string to **mystring** and will restrict SNMP queries to the **192.168.0.22** and **192.168.0.23** IP addresses.

Note:

The above is intended only as an example. Your settings will vary from the settings shown.

For more information on DHCP and Customizing the Site-Specific Option Number (SSON) see the 4600 or 9600 Series LAN Administrator Guides.

3.2.2. Settings File

As an alternative to setting Customizable System Parameters via DHCP SSON, the Avaya-provided settings script (**46xxsettings.txt)** can also be utilized to change SNMP-specific values from the default settings. This file resides on the IP Telephone's TFTP, HTTP, or HTTPS administered file server.

What follows is an example of SNMP-specific settings utilizing the 46xxsettings.txt file:

[2] The total length of the DHCP packet cannot exceed 576 bytes and some DHCP applications limit the length of Option 176 and 242 to 247 characters.

Note:

The following is intended only as an example. Your settings will vary from the settings shown.

```
####################  SNMP SETTINGS  #####################
##
## SNMP addresses
##   If this parameter is set, an SNMP query will only be
##   accepted if the source IP address of the query matches
##   one of these values. This parameter may contain one or
##   more IP addresses in dotted-decimal or DNS name format,
##   separated by commas without any intervening spaces
##   (0 to 255 ASCII characters, including commas).
SET SNMPADD 192.168.0.22,192.168.0.23

## SNMP community name string
##   This value must match the community string name used in
##   the SNMP query (up to 32 ASCII characters, no spaces).
SET SNMPSTRING mystring
```

This option will set the SNMP community string to **mystring** and will restrict SNMP queries to the **192.168.0.22** and **192.168.0.23** IP addresses.

For more information on TFTP/HTTP/HTTPS file servers and the settings file see the 4600 or 9600 Series LAN Administrator Guides.

The following sections explain how to change SNMP-specific parameters, which affect whether SNMP is enabled, the administered community string, and access controls, by means of the DHCP or TFTP/HTTP/HTTPS servers. In all cases, these steps are setting Customizable System Parameters in the telephone to a desired value.

3.3. Disabling SNMP

To disable SNMP read access in Avaya 4600 Series Telephones, prior to Release 2.6, the Customizable System Parameter SNMPSTRING value should be set to “ “ (Null)[3]. The following steps will disable SNMP in 4600 Series phones prior to R2.6:

1) Set the IP Telephone SNMPSTRING to “ “ (Null) by either of the following methods:
    a) If DHCP addressing is utilized, edit Site-Specific Option Numbers (SSON), Option-176 on 4600 phones and Option-242 on 9600 phones, add the following value:

        SNMPSTRING=“ “

[3] Release 2.6 (and later) for 4600 and Release 1.0 (and later) for 9600 Series IP Telephones ship with SNMP disabled by default.

Note: A space must exist in between the quotes.

OR

b) Editing the 46xxsettings.txt file and add the following line:

SET SNMPSTRING " "

Note: A space must exist in between the quotes.

2) Restart the IP Telephone using one of the following methods:
   a) Using Local Procedure:

   Note:
   If **PROCPSWD** is administered as indicated in the *4600 and 9600 Series IP Telephone LAN Administrator Guide*, you must type the **Local Procedure password** after pressing **Mute** and before pressing the code for your given local programming option.

   i) While the telephone is on-hook and idle, press the following sequence of keys on the faceplate of the telephone: **Mute 7 3 7 3 8 # (Mute R E S E T #)**
   ii) Press the star (*) to continue without resetting the values to their defaults.
   iii) Pressing the pound sign (#) to restart the phone.

   OR

   b) Using the Station Administration Terminal (SAT) command **reset ip-stations:**
      i) On the media server where the IP endpoint(s) are registered enter:

      reset ip-stations [ip-phones | all | tti] [ip-network-region *n* |all-regions]

   Use the **reset ip-stations** command to simultaneously unregister and reset all IP phones on a system, or a certain group of IP phones.

3.4. Setting SNMP Community String and Enabling SNMP

Avaya recommends that "public" and "private" community strings are not used, as these are well-known default values which could be exploited by a potential attacker. To set a SNMP community string and enable SNMP read access, the Customizable System Parameter SNMPSTRING value should be set to a new value:

1) Set the IP Telephone SNMPSTRING to a new value by either of the following methods:
   a) If DHCP addressing is utilized, edit Site-Specific Option Numbers (SSON), Option-176 on 4600 phones and Option-242 on 9600 phones, add the following value:

SNMPSTRING=”myexample“

OR

b) Editing the 46xxsettings.txt file and add the following line:

SET SNMPSTRING “myexample“

2) Restart the IP Telephone using one of the following methods:
   a) Using Local Procedure:

   Note:
   If **PROCPSWD** is administered as indicated in the *4600 and 9600 Series IP Telephone LAN Administrator Guide*, you must type the **Local Procedure password** after pressing **Mute** and before pressing the code for your given local programming option.

   i) While the telephone is on-hook and idle, press the following sequence of keys on the faceplate of the telephone: **Mute 7 3 7 3 8 # (Mute R E S E T #)**
   ii) Press the star (*) to continue without resetting the values to their defaults.
   iii) Pressing the pound sign (#) to restart the phone.

   OR

   b) Using the Station Administration Terminal (SAT) command **reset ip-stations.**
   i) On the media server where the IP endpoint(s) are registered enter:

   reset ip-stations [ip-phones | all | tti] [ip-network-region *n* |all-regions]

   Use the **reset ip-stations** command to simultaneously unregister and reset all IP phones on a system, or a certain group of IP phones.

Note:
Access to the IP telephone configurations, statistics, and device logs is often required for troubleshooting. Regardless of whether SNMP is disabled, troubleshooting information continues to be logged and stored in the phones MIB until power is lost. However, in order to access the SNMP MIB information, SNMP must be enabled. If an IP telephone does not have SNMP enabled, it must be rebooted to enable SNMP, using methods 1 or 2 above, and optionally SNMP restricted read access, outlined in the next section. The device logs that are particularly important for troubleshooting are Recent and Reset Logs found in Avaya’s custom MIB. Rebooting the IP telephone to enable SNMP means that the “Recent” logs will be transferred to the “Reset” logs upon reboot, and the “Reset” logs will be lost.

When SNMP is enabled, it's recommended that the community string is changed periodically to prevent disclosure of information from the SNMP MIBs. Restricting SNMP read access can also prevent authorized SNMP information disclosure.

3.5. Restricting SNMP Access

To restrict SNMP read access to administered IP addresses, the Customizable System Parameter SNMPADD should be set to the allowable source IP addresses or DNS hostname for SNMP queries. The follow steps will restrict SNMP access on 4600 and 9600 IP Telephones:

1) Set the IP Telephone SNMPADD to a list of allowable addresses by either of the following methods:
   a) If DHCP addressing is utilized, edit Site-Specific Option Numbers (SSON), Option-176 on 4600 phones and Option-242 on 9600 phones, add the following value:

      SNMPADD="192.168.0.22,192.168.0.23"

   OR

   b) Editing the 46xxsettings.txt file and add the following line:

      SET SNMPADD 192.168.0.22,192.168.0.23

Note:

As Avaya support engineers will typically launch SNMP queries to the IP telephones from the call server platform (S8700, S8500, S8300, etc.), the call server address(es) should be permitted SNMP access to the phones.

2) Restart the IP Telephone using one of the following methods:
   a) Using Local Procedure:

   Note:
   If **PROCPSWD** is administered as indicated in the *4600 and 9600 Series IP Telephone LAN Administrator Guide*, you must type the **Local Procedure password** after pressing **Mute** and before pressing the code for your given local programming option.

      i) While the telephone is on-hook and idle, press the following sequence of keys on the faceplate of the telephone: **Mute 7 3 7 3 8 # (Mute R E S E T #)**
      ii) Press the star (*) to continue without resetting the values to their defaults.
      iii) Pressing the pound sign (#) to restart the phone.

   OR

b) Using the Station Administration Terminal (SAT) command **reset ip-stations.**
   i) On the media server where the IP endpoint(s) are registered enter:

   reset ip-stations [ip-phones | all | tti] [ip-network-region *n* |all-regions]

Use the **reset ip-stations** command to simultaneously unregister and reset all IP phones on a system, or a certain group of IP phones.

4. Additional References

- *4600 Series IP Telephone LAN Administrator Guide, April 2006.*
- *9600 Series IP Telephone LAN Administrator Guide, TBD 2006.*
- *Management Information Base for Network Management of TCP/IP Internets: MIB-II,* March 1991, edited by K. McCloghrie and M. Rose (RFC 1213)
- *SNMPv2 Management Information Base for the Internet Protocol using SMIv2,* November 1996, edited by K. McCloghrie (RFC 2011)
- *Structure of Management Information Version 2 (SMIv2),* April 1999, edited by K. McCloghrie, D. Perkins, and J. Schoenwaelder (RFC 2578)