



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring SNMP Connectivity with Avaya Communication Manager, Avaya Application Enablement Services and ION Networks SA5600 - Issue 1.0

Abstract

These Application Notes detail the configuration process that enables SNMP connectivity with Avaya Communication Manager, Avaya Application Enablement Services, and ION Networks SA5600.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

As IP telephony continues to grow and evolve, managing the infrastructure that provides telephony services becomes an important issue that network administrators need to address. ION Networks SA5600 is a dedicated network management platform which provides network administrators SNMP monitoring of devices, including the IP telephony infrastructure.

1.1. Network Diagram

The network diagram in **Figure 1** illustrates the sample environment used for compliance testing. The network consists of multiple IP networks routed together to provide an operations and administration environment. Within each IP network, the default gateway for that network is assigned an IP address with the last octet being 254. For example, the default gateway on the 10.1.1.0/24 network is 10.1.1.254. The network is made up of Avaya Communication Manager, Avaya Application Enablement Services and ION Networks SA5600. The ION Networks SA5600 is connected to the PSTN via an analog modem which provides dial out access to an external Network Management System (NMS).

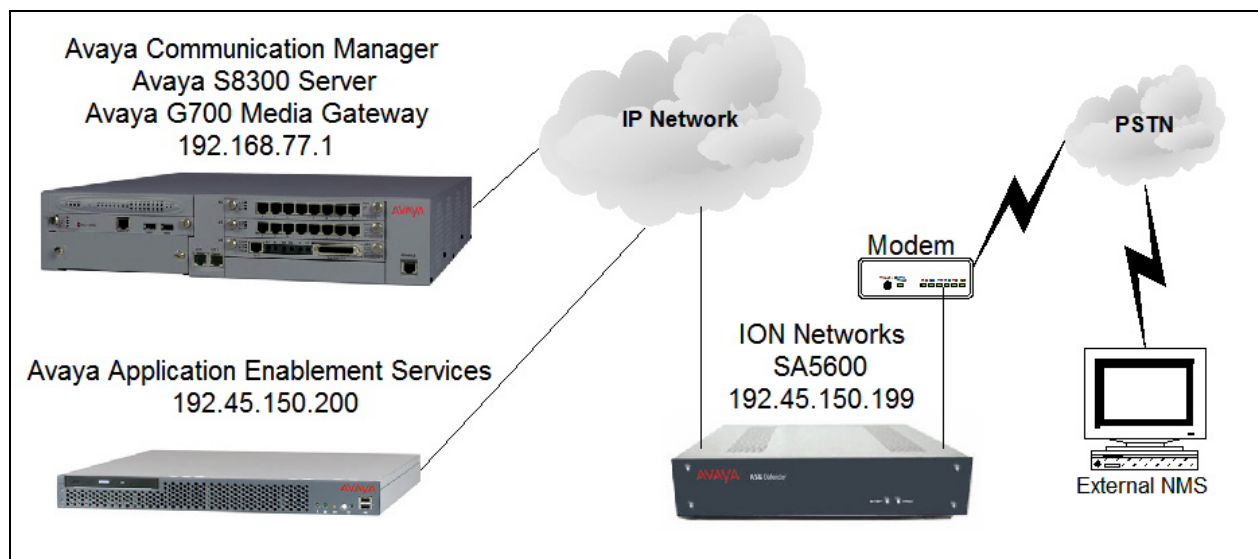


Figure 1: Sample Network Environment

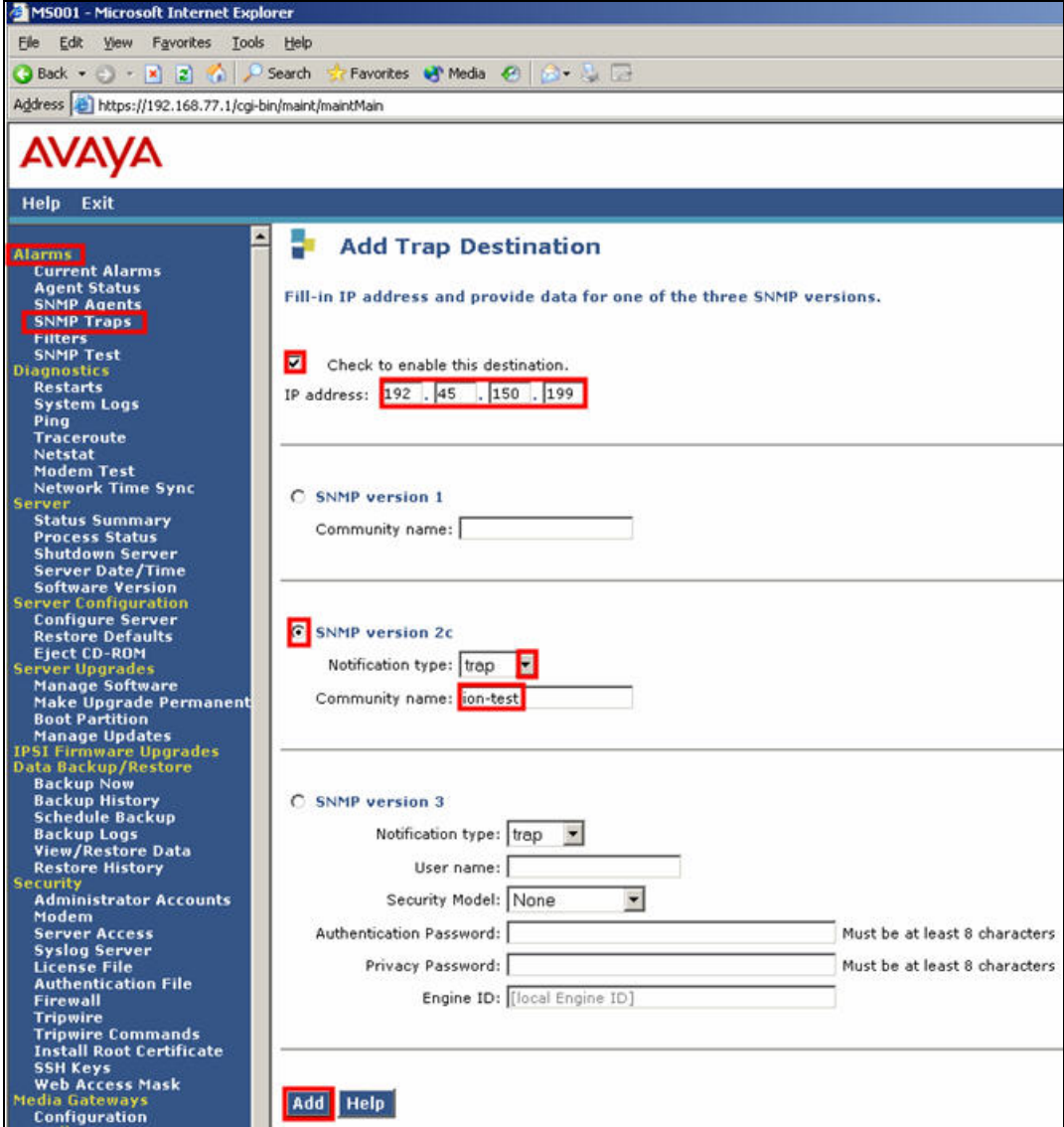
2. Equipment and Software Validated

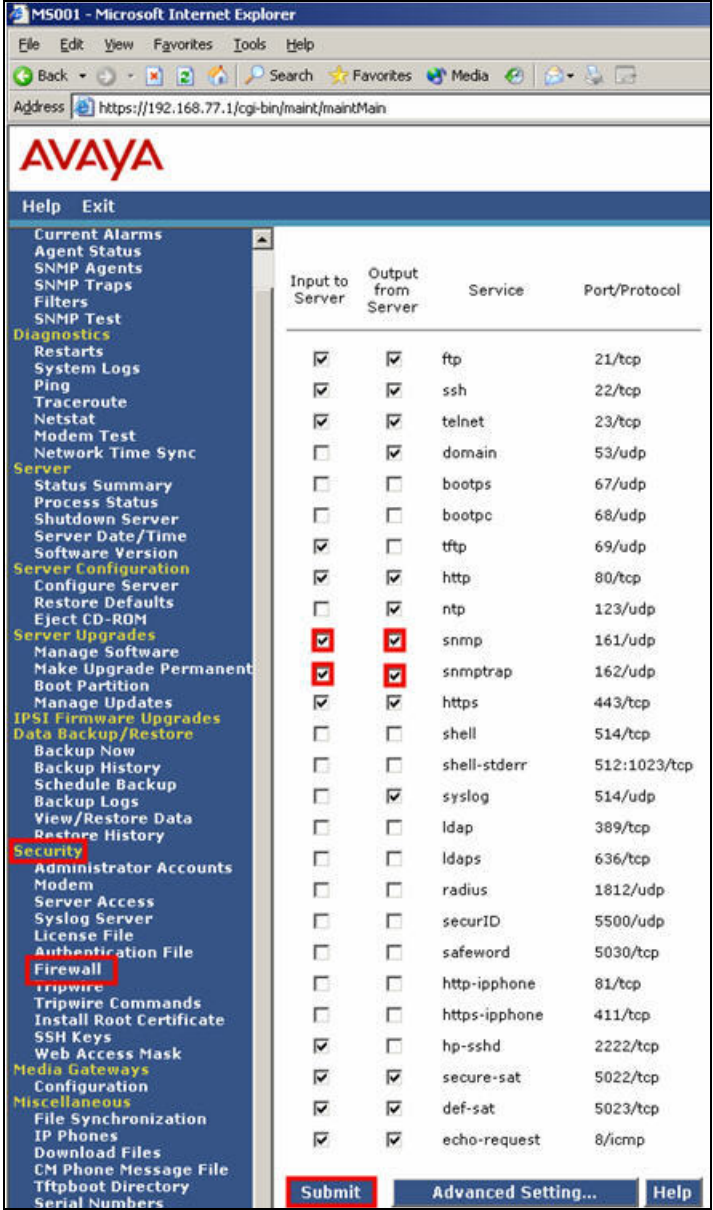
The following equipment and software were used for the sample configuration provided:

Equipment	Software
Avaya S8300 Server	Avaya Communication Manager 4.0 (R014x.00.0.730.5)
Avaya G700 Media Gateway <ul style="list-style-type: none">MM711 Analog Media ModuleMM712 DCP Media Module	26.31.0 HW04 / FW87 HW05 / FW08
Avaya Application Enablement Services	3.1.2
ION Networks SA5600	1.0.5

3. Avaya Communication Manager Configuration

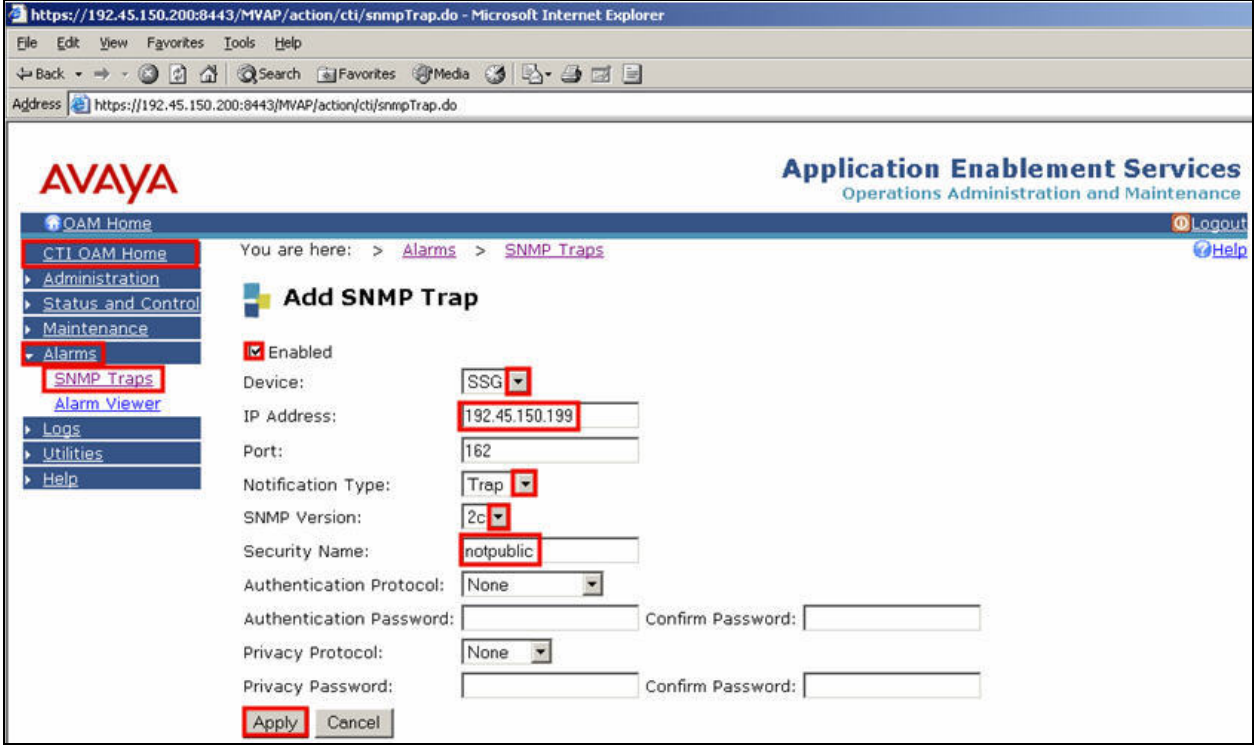
Avaya Communication Manager SNMP configuration is administered using the web interface. In the sample network Avaya Communication Manager was assigned the IP address 192.168.77.1 and the URL <http://192.168.77.1> was used to access the web interface. Login credentials are required to access web interface. For information on how to access the web interface on Avaya Communication Manager refer to [1]. Once logged in, all configuration is performed by selecting the **Launch Maintenance Web Interface** link (not shown).

Step	Description
1.	<p>Navigate to the Add Trap Destination web page by clicking SNMP Traps under Alarms within the left-side navigation panel. Enter the information displayed below and then click Add. Check the Check to enable this destination check box. IP address is the IP address assigned to the ION Networks SA5600, see Figure 1. Click the SNMP version 2c radio button and use the drop-down list for Notification type to select “trap”. Community name can be any descriptive text and in the sample network “ion-test” was used.</p> 

Step	Description
2.	<p>Navigate to the Firewall web page by clicking Firewall under Security within the left-side navigation panel. Check the snmp and snmptrap check boxes for both Input to Server and Output from Server. Click Submit.</p> 

4. Avaya Application Enablement Services Configuration

Avaya Application Enablement Services SNMP configuration is administered using the web interface. In the sample network Avaya Application Enablement Services was assigned the IP address 192.45.150.200 and the URL <http://192.45.150.200:8080> was used to access the web interface. Login credentials are required to access web interface. For information on how to access the Avaya Application Enablement Services web interface refer to [2]. Once logged in, all configuration is performed from the **CTI OAM Home** web page.

Step	Description
1.	<p>Navigate to the ADD SNMP Trap web page by clicking Alarms and then SNMP Traps. Enter the information displayed below and then click Apply. Check the Enabled check box. Use the drop-down list for Device to select “SSG”. IP Address is the IP address assigned to the ION Networks SA5600, see Figure 1. Use the drop-down list for SNMP Version to select “2c”. Security Name can be any descriptive text, which is used as the SNMP community string, and in the sample network “notpublic” was used. Port was left at the default value of “162”.</p> 

5. ION Networks SA5600 Configuration

The ION Networks SA5600 configuration is performed via a console cable connection directly to the ION Networks SA5600 serial port. For complete information on how to setup and access an ION Networks SA5600 see **Section 10 [3]**. All configuration of the ION Networks SA5600 is performed via a command line interface.

Step	Description
1.	<p>Issue the snp command to configure the IP address information. After issuing the snp command, a sub-menu is displayed. Use “1” to access the Network Initialization Params. External Address is the IP address assigned to the ION Networks SA5600, see Figure 1. Mask is the IP subnet mask associated with the External Address IP address and in the sample network “255.255.255.0” was used. Default Gateway is the IP address of the default gateway. The values used here are applicable to the sample configuration.</p> <pre>5010000000>snp --- Set Network Params --- 1 = Network Initialization Params 2 = SNMP Manager Params 3 = FTP Params 4 = PPP Params 5 = Telnet Params Select Group -->1 External Address 192.45.150.199 Mask 255.255.255.0 Default Gateway 192.45.150.254</pre>

Step	Description
2.	<p>Issue the SSP 3 command to administer system parameters. Home Phone Number 1 (Default) is the telephone number of the external NMS. Report Multiple Alarms is set to “Yes”. Default Action Routine Modem is set to “Modem #1”.</p> <pre> 5010000000>SSP 3 --- Set System Parameters --- -- Action Routine Parameters -- Home Phone Number 1 (Default) 18005551212 Home Phone Number 2 Home Phone Number 3 Home IP Address Delay Before Transmit (sec) 5 Report Multiple Alarms ? Yes Default Pager Number Default Pin Number Default Pager Message Default Action Routine Modem Modem #1 10/05/07 14:26:15 CEAE {I} [T1:31] Set System Parameters </pre>
3.	<p>Issue the aaip command to add an Avaya IP Device to the system. Device name is any descriptive text and in the sample network “Avaya-Communication-Manager” was used for the Avaya Communication Manager system. IP address and Avaya IP Address are the IP address assigned to Avaya Communication Manager, see Figure 1. Terminal Connection Type was set to “Telnet”. Ports are the actual network ports used for communication (80 for web, 443 for secure http, etc.). Host Equipment Type was set to “Intuity”. The value used for HOST Equipment Type is used to classify the type of equipment and ION Networks uses “Intuity” for VoIP equipment. Comments can be any descriptive text.</p> <pre> 5010000000>aaip --- Add Avaya IP Device --- Device name Avaya-Communication-Manager IP Address 192.168.77.1 Avaya IP Address 192.168.77.1 Terminal Connection Type Telnet Ports 80,443,22,23,5023 Host Equipment Type Intuity Comments Avaya-Communication-Manager Reinitializing rules for Avaya devices... </pre>
4.	<p>Repeat Step 3 to create an entry for Avaya Application Enablement Services using the appropriate IP address and “22” for Ports.</p>

6. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying the capability of ION Networks SA5600 to receive SNMP traps from Avaya Communication Manager and Avaya Application Enablement Services and then dialing out via a modem to an external NMS where SNMP traps are uploaded.

6.1. General Test Approach

The general test approach was to generate an IP based SNMP traps on the Avaya platforms and verify that the ION Networks SA5600 was capable of receiving, interpreting and processing those traps. SNMP traps were then uploaded via a modem to an external NMS. Additional testing verified the capability of ION Networks SA5600 to log into Avaya Communication Manager and Avaya Application Enablement Services using telnet or ssh, based on the access method supported by the specific platform.

6.2. Test Results

ION Networks SA5600 passed all test cases. ION Networks SA5600 was verified to be capable of receiving SNMP traps from Avaya Communication Manager and Avaya Application Enablement Services. ION Networks SA5600 was also verified to be capable of uploading those SNMP traps via a modem to an external NMS. ION Networks SA5600 was verified to be capable of accessing Avaya Communication Manager via a telnet or ssh connection. ION Networks SA5600 was also verified to be capable of accessing Avaya Application Enablement Services via an ssh connection.

7. Verification Steps

- Verify that the ION Networks SA5600 has IP connectivity by issuing ping commands to the configured systems. Note: The ability to successfully use ping commands may depend on how the customer's network is configured to support ICMP traffic.
- Verify that the Avaya platforms have the correct IP address configured for the ION Networks SA5600. Refer to **Section 3 Step 1** and **Section 4 Step 1**.
- Generate diagnostic test traps and verify they are received, interpreted and processed by the ION Networks SA5600. Test traps for Avaya Communication Manager can be generated via the web interface. A trap for Avaya Application Enablement Services can be created by removing and then restoring a network connection.
- Verify that the firewall setting for Avaya Communication Manager allows **snmp** and **snmptraps** to pass through the firewall. Refer to **Section 3 Step2**.
- Verify the **Device** type for Avaya Application Enablement Services is set to "SSG". Refer to **Section 4 Step 1**.

8. Support

Support information for ION Networks SA5600 can be obtained through the following:

- **Phone:** 1-800-722-8986
- **Email:** info@ion-networks.com
- **Web:** <http://www.ion-networks.com/support.html>

9. Conclusion

These Application Notes detail the configuration steps that enable SNMP connectivity with Avaya Communication Manager, Avaya Application Enablement Services and ION Networks SA5600. These Application Notes demonstrate the configuration process that enables ION Networks SA5600 to access Avaya Communication Manager using telnet or ssh and Avaya Application Enablement Services using ssh. These Application Notes also detail the configuration process that allows the ION Networks SA5600 to dial out via a PSTN connection to an external NMS.

10. Additional References

The following references are available at <http://support.avaya.com>:

- [1] *Administrator Guide for Avaya Communication Manager*, February 2007, Issue 3.1, Document Number 03-300509
- [2] *Avaya MultiVantage Application Enablement Services Administration and Maintenance Guide Release 3.1.2*, September 2006, Issue 4, Document Number 02-300357

The following reference is available upon request at <http://www.ion-networks.com/support.html>:

- [3] *ION Network's SA5600 Administration Guide*, February 2007, Issue 1, Document Number 01-13524

©2008 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.