Avaya Solution & Interoperability Test Lab

Configuring Avaya Call Management System and Avaya Communication Manager for Remote INADS Alarming using ION Networks Access Security Gateway Guard II - Issue 1.0

Abstract

These Application Notes describe the steps required for configuring the Avaya Call Management System (CMS) and the Avaya Communication Manager to support Initialization and Administration System (INADS) alarm origination and forward SNMP traps in INADS format to the ION Networks Access Security Gateway (ASG) Guard II.

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

1. Introduction

These Application Notes describe the steps required for configuring the Avaya Call Management System (CMS) and the Avaya Communication Manager to support Initialization and Administration System (INADS) alarm origination and forward SNMP traps in INADS format to the ION Networks Access Security Gateway (ASG) Guard II. INADS parses system logs specific to Avaya SNMP sub-agents that provide the ProductID and Machine Type in addition to standard SNMP information of Avaya devices enabled for INADS.

The ION Networks ASG Guard II dials out to the PSTN and establishes a PPP session in order to forward SNMP-INADS notifications to Avaya Services. Also, remote maintenance and administration of Avaya devices that are protected by ION Networks ASG Guard II can be performed through the PPP session.

In the network configuration shown below in **Figure 1**, the ION Networks ASG Guard II has a serial connection to the Avaya Call Management System and has IP connectivity to the Avaya Communication Manager. The ION Networks ASG Guard II also has IP connectivity to a local SNMP trap receiver for notification of dial-out alarming to Avaya Services.

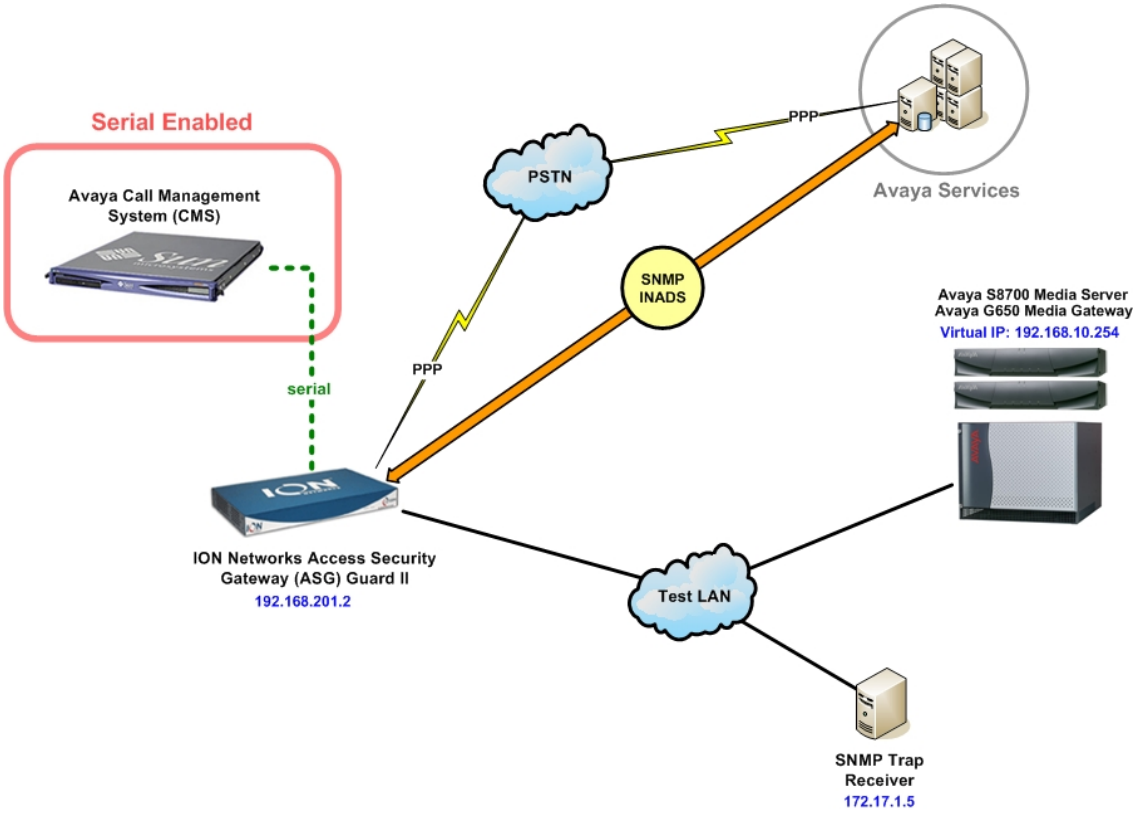


Figure 1: Network Configuration

These Application Notes will not cover details for remote administration operations of the Avaya Call Management System (CMS) or Avaya Communication Manager by Avaya Services using the dial-in capability of ION Networks ASG Guard II.

See the **References** section of this document for further information regarding serviceability and maintenance procedures that are related to Avaya Services.

2. Equipment and Software Validated

Table 2 lists the equipment and software version used in the network configuration:

Equipment	Software
Avaya Call Management System (CMS)	13.1
Avaya Communication Manager	3.1 (Build 628.6)
ION Networks Access Security Gateway (ASG) Guard II	5.2.6

Table 2: Equipment and Software Validated

3. Avaya Call Management System (CMS) Configuration

This section describes the steps necessary to configure the Avaya Call Management System for remote INADS alarming. The CMS Supplemental Services packages must be installed and the associated processes must be running for alarm origination:

- `LUahl`
- `LUaot`
- `LUim`
- `Luorbutil`

1. Log into the Avaya CMS using the proper access privileges. Verify that the Avaya CMS is monitoring an enabled serial port by entering the following command:

```
/cms/install/bin/abcadm –k

console set to local
/etc/ttydefs remote console baud rate set to 9600
ttya is set to incoming at 9600 baud
```

2. If CMS is not configured for port monitoring, enter the following command to enable monitoring for the serial ports on the Avaya CMS. Use `ttya` for serial port 1 or `ttyb` for serial port 2 to assign the serial port that will be connected to the ION Networks ASG Guard II.

```
/cms/install/bin/abcadm -i -b 9600 tty <a / b>
```

3. Change to the `/opt/cc/aot/data/admin` directory and open the `prodSetup.cfg` configuration file using vi. Edit the **Enabled** field to activate alarm origination, if necessary (0 for disabled, 1 for enabled).

4. Save any changes to the `prodSetup.cfg` configuration file and exit vi.

```
Product¦NumberInstances¦ServiceVehicle¦Enabled¦
TEST    ¦1              ¦r1v0          ¦1      ¦
CMS     ¦1              ¦r13.1ca.i     ¦1      ¦
~
~
~
```

5. Open the `sysSetup.cfg` configuration file using vi and edit the following fields:

`ProductID`	The unique system identifier specific to an Avaya product
`ModemPort`	Designate the modem port used by the ASG Guard II (1 for ttya, 2 for ttyb).
`Enabled`	External alarming (0 for disable, 1 for enable)

6. Save any changes to the `sysSetup.cfg` configuration file and exit vi.

```
ProductID¦ModemType¦DialString  ¦Exp1¦TelephoneNum  ¦Exp2   ¦ReturnStr  ¦ModemPo
rt¦BaudRate¦Enabled¦
1234567891¦HayesXXXX¦AT¦OK¦ATDT918005351234¦CONNECT¦XXXXXXXXXX¦1¦9600¦1¦
~
~
~
~
```

7. Enter the following command to start the Alarm Origination Manager (AOM) process.

```
aom start
```

8. Enter the following command to verify that the AOM has started.

```
ps -ef | grep aom
```

```
root 668 1 0 Apr 15 ? 0:13 aomSrv
```

9. Enter the following commands to set the AOM environment in Avaya CMS for INADS alarming. This command will read the parameters set in the configuration files `prodSetup.cfg` and `sysSetup.cfg` for alarm origination. Be sure to leave a space between the beginning two dots in the first command.

```
. ./opt/cc/aot/bin/aom_env
```

10. Enter the following commands to set and export the directory path to the AOM daemon.

```
AOM_SH=/usr/bin/aom
export AOM_SH
```

11. Enter the following command to execute a test alarm using the INADS format.

```
/opt/cc/aot/bin/log_error –e 30001
```

The following display shows an example of a successful generation of an INADS test alarm.

```
[16506: New Connection (cvue,IT_daemon,*,root,pid=382,optimised) ]
[16506: New IIOP Connection (cvue:4001) ]
[16506: New IIOP Connection (192.168.101.200:4002) ]
```

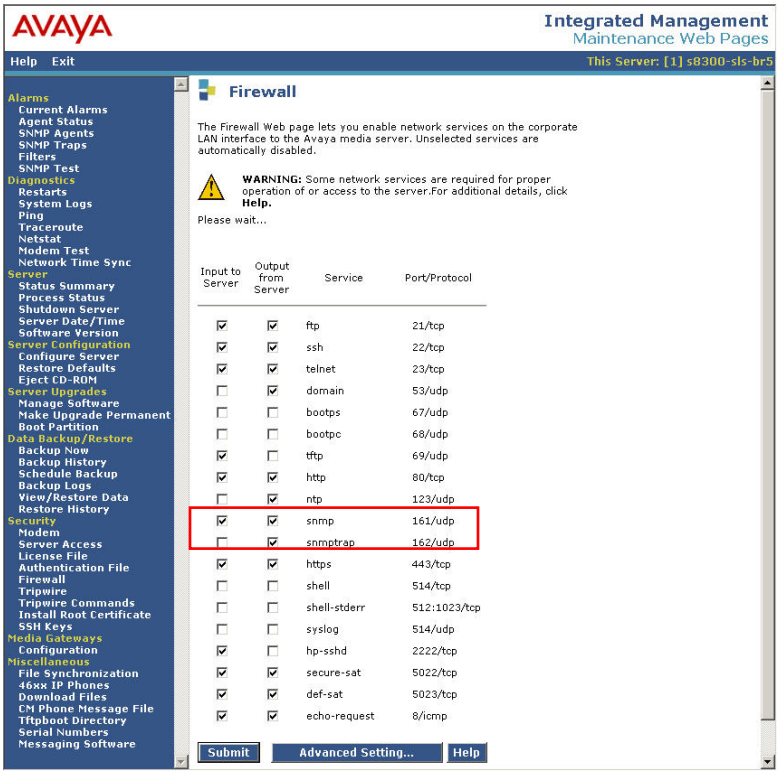
4. Avaya Communication Manager Configuration

This section describes the steps necessary to configure the Avaya Communication Manager for remote INADS alarming. These steps are applicable to the Avaya S8xxx Media Server product line that supports Avaya Communication Manager.

1. Using a browser, access the web interface of the Avaya Communication Manager and log in using `craft` permissions. Click **No** for 'Suppress alarm origination' when prompted.

2. Select **Firewall** from the left menu under **Security**. Select both the Input from Server and Output from Server check boxes for SNMP (161/UDP) to enable SNMP access. Select only the Output from Server check box for generating SNMP traps (162/UDP).

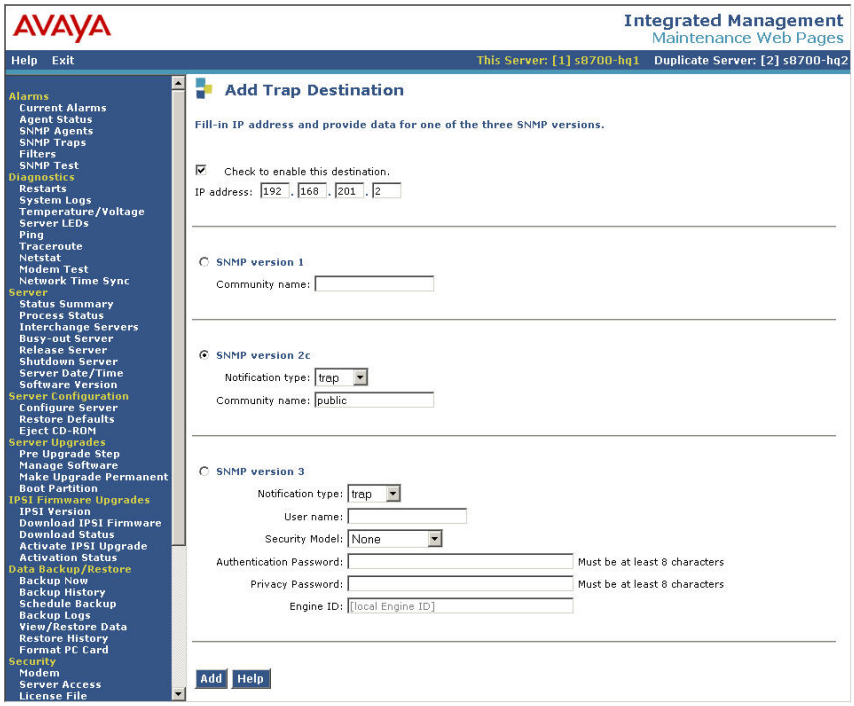
3. Click **Submit** to save changes to the Avaya Communication Manager firewall.



4. Select **SNMP Traps** from the left menu under **Alarms** and click **Add** to configure an SNMP trap destination.

5. Enter the IP address of the ION Networks ASG Guard II and mark the check box to enable the trap destination. Select an SNMP version and community string for management of traps and notifications.

6. Click **Add** to enable the configured trap destination and SNMP version.



7. Log in to the Avaya S8xxx Media Server at the Linux interface with `craft` permission and decline to suppress alarm origination when prompted.

```
Suppress alarm origination? (y/n) [y] n
Alarm is not suppressed.
Alarm origination allowed
```

8. Enter the following command to enable Avaya Communication Manager for alarm origination using the INADS format.

```
almenable -d n -s y
```

`-d` enable / disable SNMP alarm origination (y for disable, n for enable)
`-s` enable / disable SNMP alarming and traps in INADS format

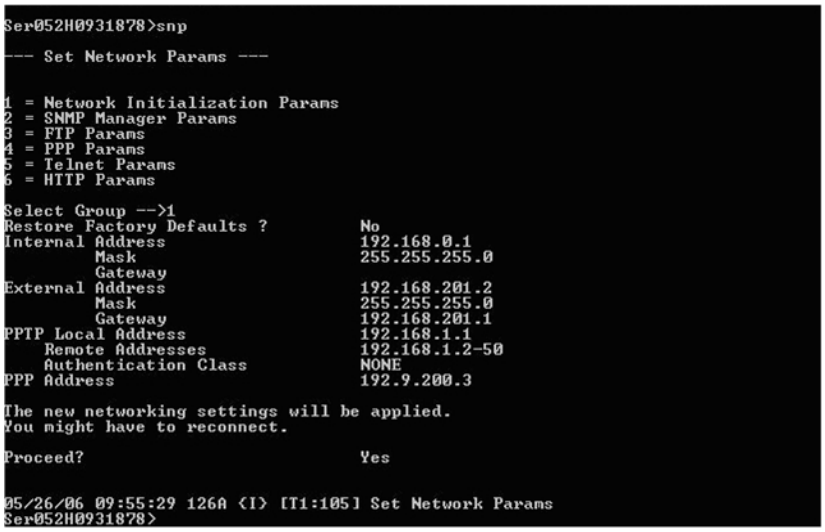
5. ION Networks Access Security Gateway (ASG) Guard II Configuration

This section describes the steps necessary to configure the ION Networks ASG Guard II for serial and IP connectivity to Avaya devices and enable forwarding of SNMP-INADS traps and notifications.

1. Access the ION Networks ASG Guard II through the AUX port using the proper login credentials. Enter the command `snp` to access the **Set Network Params** menu and select '`1`' for the **Network Initialization Params** menu.

2. Answer "`No`" when prompted to **Restore Factory Defaults** and leave the **Internal Address** at default. Enter the External Address, Subnet Mask and Gateway when prompted. This is the actual LAN address of the ION Networks ASG Guard II.

3. Leave the remaining parameters at default and answer Yes at the next prompt to submit the configuration.



4. Enter the command `snp` to access the **Set Network Params** menu and select '`2`' for **SNMP Manager Params** to configure SNMP parameters.

5. Answer "`No`" when prompted to **Restore Factory Defaults**. Configure the SNMP community strings and the IP address of the local NMS that will receive SNMP traps when the ION Networks ASG Guard II dials outbound to forward INADS alarms.

6. Leave the remaining parameters at default and press <Enter> to submit the configuration.

```
Ser052H0931878>snp

--- Set Network Params ---


1 = Network Initialization Params
2 = SNMP Manager Params
3 = FTP Params
4 = PPP Params
5 = Telnet Params
6 = HTTP Params

Select Group -->2
Restore Factory Defaults ?          No

-- SNMP Manager Parameters --
PPP link needed for trap?           No
Trap format                         Standard
SNMP Trap Community Name            public
SNMP Set Community Name             private
SNMP Get Community Name             public
Enable reboot via SNMP              No
-- IP Addresses for SNMP Managers (nnn.nnn.nnn.nnn) --
  Manager 1                         172.17.1.5
  Manager 2
  Manager 3
  Manager 4
  Manager 5
```

7. Enter the command `aaip` for **Add Avaya IP Device** to configure the Avaya S8xxx Media Server using IP connectivity to ION Networks ASG Guard II. Enter a unique alphanumeric string for the device name and enter the Corporate LAN IP address of the Avaya S8xxx Media Server.

8. (Optional) Enter the translated Avaya IP address. This translated IP address is assigned by Avaya Managed Services and is specific to serviceability by Avaya technicians accessing the ION Networks ASG Guard II remotely. Entering the translated IP address will not be necessary for non-serviceable Avaya devices.

9. Leave the remaining parameters at default and press <Enter> to submit the configuration.

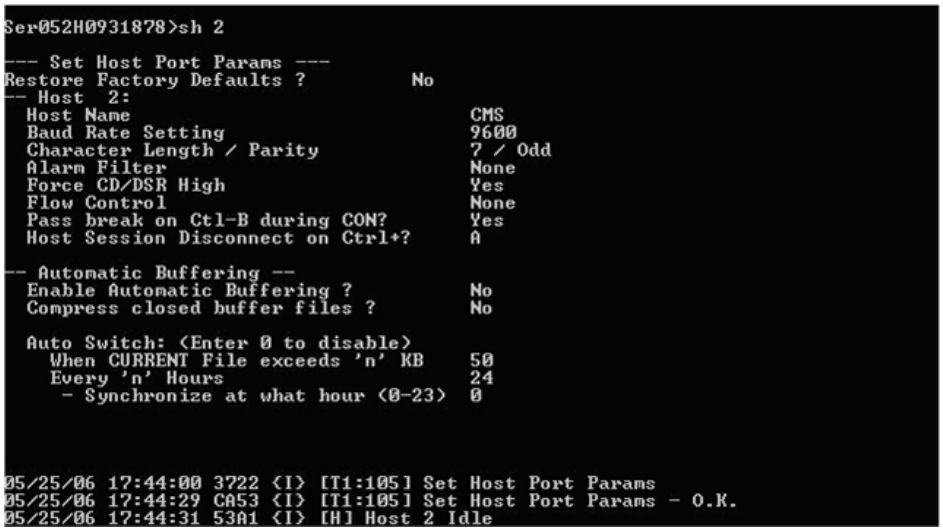
```
Ser052H0931878>aaip

--- Add Avaya IP Device ---
Device name                         S8700-dup
IP Address                          192.168.10.254
Avaya IP Address                    10.0.0.254
Terminal Connection Type            Telnet
Ports                               80,443,21,23,5023
Host Equipment Type                 Avaya
Comments
```

10. Enter the command sh for **Set Host** to configure the corresponding serial port hosting the Avaya Call Management System. Enter a unique alphanumeric string for the host port and enter the Baud Rate Setting, Character Length and Parity of the Avaya Call Management System.

11. (Optional) Enter the translated Avaya IP address. This step is specific to serviceability by Avaya technicians accessing the ION Networks ASG Guard II remotely and will not be necessary for non-serviceable devices.

12. Leave the remaining parameters at default and press <Enter> to submit the configuration.

Note: CMS is designed to send data through a serial port at 9600 baud with 7 bit data, odd parity and 1 stop bit.



13. Enter the command `ssp` to access the **Set System Parameters** menu and select '`3`' for **Action Routine Params** to enable alarm delivery from the ION Networks ASG Guard II using the PSTN for outbound dialing.

14. Enter the phone number(s) for the site(s) hosting the remote SNMP trap receiver. Be sure to add any digits for telephone numbers that require special characters or a prefix.

15. Enter **Yes** when prompted for the ION Networks ASG Guard II to send multiple SNMP traps when connected through PPP. At the **Default Action Routine Modem** prompt, select the correct internal modem designated for outbound dialing.

16. Leave the remaining parameters at default and press <Enter> to submit the configuration.

```
Ser052H0931878>ssp

--- Set System Parameters ---


1 = Site Information
2 = Scheduling Params
3 = Action Routine Params

Select Group -->3

-- Action Routine Parameters --

Home Phone Number 1 (Default)          918005351234
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

05/24/06 16:26:50 4C2B (I) [T1:105] Set System Parameters
```

6. Interoperability Compliance Testing

The following sections below will describe the compliance testing approach and results for the ION Networks ASG Guard II.

6.1. Test Approach

Using the network illustrated in Figure 1, the ION Networks ASG Guard II was configured to receive SNMP INADS alarms from the Avaya Call Management System and the Avaya S8700 Media Server. The Avaya Call Management System was configured to send test alarms through its serial port and the Avaya S8700 Media Server was configured to send test alarms through IP. Each test alarm that is received by the ION Networks ASG Guard II is processed and designated for forwarding through the PSTN.

The ION Networks ASG Guard II begins a modem connection to Avaya Services in Denver and sends an SNMP alarm to the local trap receiver for outbound dialing notification. Once the modem connection is functional, the ION Networks ASG Guard II establishes a PPP session and forwards the SNMP INADS alarms from the Avaya Call Management System and the Avaya S8700 Media Server. The ION Networks ASG Guard II receives an acknowledgement

(**ACK**) or non-acknowledgement (**NACK**) from Avaya Services. The ION Networks ASG Guard II forwards the acknowledgement (**ACK**) or non-acknowledgement (**NACK**) of the test alarms to the respective system.

The PPP session between the ION Networks ASG Guard II and Avaya Services enabled connectivity to the Avaya Call Management System and the Avaya S8700 Media Server for Avaya technicians to also test serviceability.

6.2. Test Results

The following features for the ION Networks ASG Guard II were successfully verified during the compliance testing:

- Local access to test equipment behind ASG Guard II via Avaya Site Administrator and SSH.
- Avaya Services access to test equipment via dial-up PPP session through PSTN
- Alarming forwarding and generation from ASG Guard II to Avaya Services
- Notification of trap receipt status to the respective test equipment

The following Avaya products were verified during the interoperability compliance testing of the ION Networks ASG Guard II:

- Call Management System (CMS)
- Definity
- Avaya Communication Manager
- Avaya Intuity LX
- Avaya IR

7. Verification Steps

The following verification steps were used to verify correct device operation for remote INADS alarming. Upon successful delivery and confirmation of the SNMP-INADS trap, the ION Networks ASG Guard II sends the acknowledgement back to the alarm originating device.

7.1. Avaya Call Management System (CMS) Verification

1. Log into the Avaya CMS using the proper access privileges and change to the **/opt/cc/aot/data/log** directory.

2. Observe the **alarm_log** log file to view INADS alarm responses from alarm delivery through the ION Networks ASG Guard II. The highlighted ASCII text identifies the status of the modem signal to the ASG Guard II created by the alarm origination.

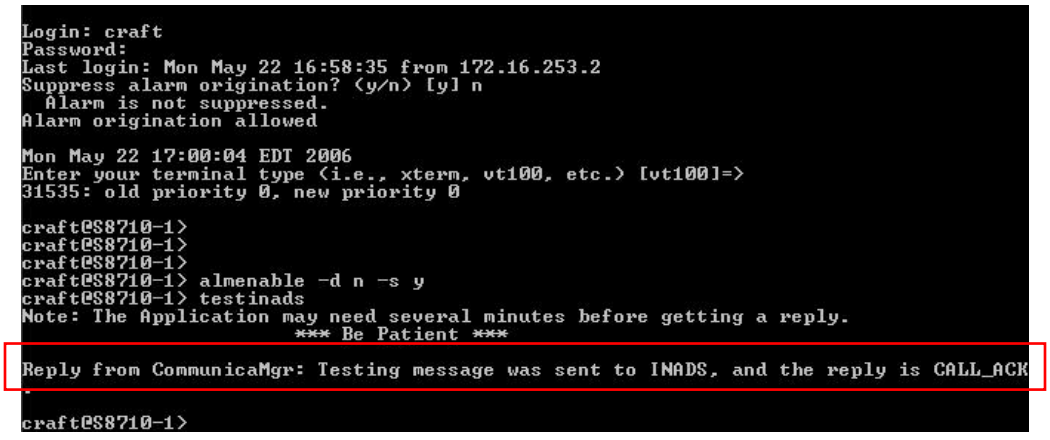
```
+71143867-5:b0x2:
DialStr = "" \dAT\r OK\r ATDT18005351234\r CONNECT\r
+71143868-5:b0x2:
```

```
ModemCall::parseDialStr
+71143868-5:b0x2:
expStr = ""
+71143868-5:b0x2:
ModemCall::sendDialStr
+71145870-5:b0x2:
Writing char: A
+71145870-5:b0x2:
Writing char: T
+71145871-5:b0x2:
Writing char: ^M
+71145871-5:b0x2:
Expecting OK
+71145872-5:b0x2:
ModemCall::getResponse
+71147880-5:b0x2:
3 bytes read
+71147880-5:b0x2:

--- Output omitted ---

+71151900-5:b0x2:
Characters: [OK]
+71151901-5:b0x2:
Response = OK
```

7.2. Avaya S8xxx Media Server Verification

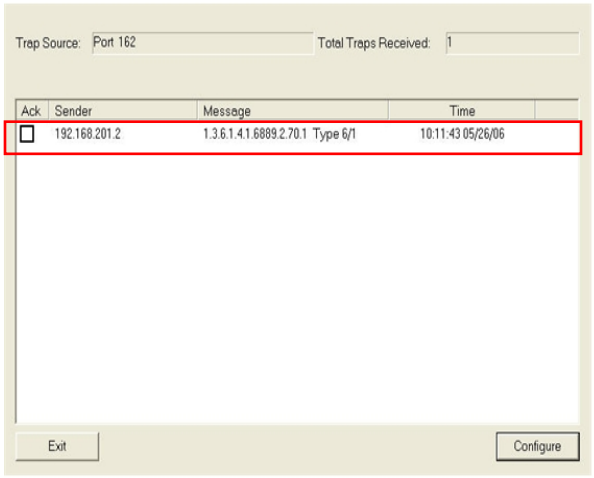
Enter the command `testinads` to execute an INADS test alarm and observe the results of alarm delivery through the ION Networks ASG Guard II.

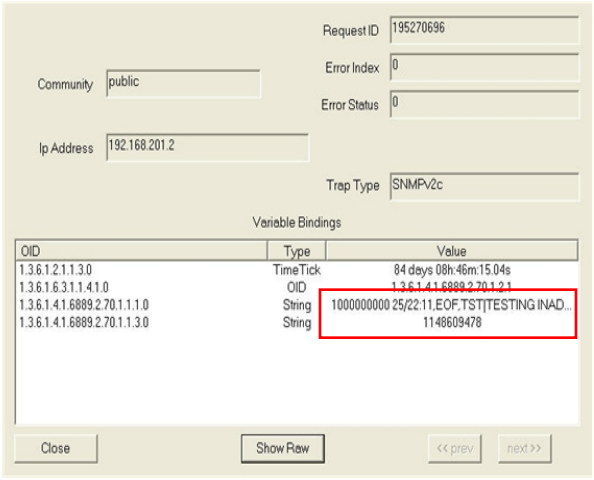
- A successful alarm delivery - `CALL_ACK`.
- A successful alarm delivery with an incorrect or no product ID - `CALL_NACK`.
- An alarm delivery failure - `ALARM FAILURE`.



7.3. ION Networks ASG Guard II Alarm Verification

Verify that the ION Networks ASG Guard II provides notification of outbound calls and sends an SNMP trap to the local trap receiver. Below is output from the local trap receiver showing the reception of the SNMP trap sent by the ION Networks ASG Guard II.





8. Conclusion

These Application Notes have illustrated the procedures necessary to configure the Avaya Call Management System and the Avaya Communication Manager to support remote INADS alarming using the ION Networks Access Security Gateway (ASG) Guard II.

9. References

1. Avaya S8xxx Media Server Administration for SAC Offer Support, Doc. No. 19-300247, Issue 1.0, February 2004
2. Configuring CMS for SAC Offer Support, COMPAS ID 107225, Issue 1.0, August 2005
3. ION Networks Access Security Gateway (ASG) Guard II Administrator Guide, Version 5.2, December 2005
4. ION Networks Access Security Gateway (ASG) Guard II Connectivity Guide, Version 1.2, April 2004

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 Developer*Connection* Program at devconnect@avaya.com