1. AlarmTraq SNMP Configuration

This section describes the procedure for configuring the Avaya S8300 and S8700 Media Servers to report alarms to an SNMP trap destination (AlarmTraq). The required steps are:

- Activating SNMP alarm notification on the Avaya S8300 and S8700 Media Servers,
- Allowing SNMP traps to be output from the Avaya Media Server on UDP port 162, and
- Checking that Avaya alarms that should generate SNMP traps are being reported according to the alarm reporting options. The alarm reporting options are specified in the **set options** form accessible through the System Access Terminal (SAT). See reference [2], *Maintenance Command Reference*, for a description of the **set options** form.

Note: Warning alarms raised by the Avaya Communication Manager are not reported via SNMP traps. However, warning and informational level traps could be generated directly by the G700 Media Gateway for events and alarms related to the P330 stack processor and MGP.

1.1. Configuring SNMP Trap Destinations to AlarmTraq

The SNMP trap destinations for the Avaya S8300 and S8700 Media Servers are configured through the server's web interface. To access the web interface, launch a web browser and connect to the media server by specifying its IP address in the URL (e.g., type http://192.45.100.11 or http://192.45.100.12 in the URL for the Avaya S8700 Media Servers). For an S8700 Media Server pair, the SNMP trap destinations need to be configured on each media server. Supply the login and password for an account with super-user privileges. After logging in, a main menu is presented along the left hand side of the screen. In the **Alarms** section, click on **SNMP Traps** to display the **Change Trap Destination** screen shown in **Figure 2**.

In the **Change Trap Destination** screen, enter the IP address of the AlarmTraq server (i.e., 216.153.153.107) and enable this SNMP trap destination. Select **SNMP version 1** and set the community name to *public*, as shown in **Figure 2**. For SNMP v2c or v3, set the **Notification Type** field to *Trap* and set the **Community Name** or **User Name** field to a valid string. Click on the **Change** button to submit the form.

The **SNMP Traps** configuration allows the Avaya Media Server to send traps for alarms raised by Communication Manager and alarms related to the media server's operating system and support software. Certain alarms related to the Stack Processor and the Media Gateway Processor (MGP) in the G700 Media Gateway are not detected or raised by the Avaya Media Server. Therefore, the SNMP agents in those components of the G700 Media Gateway are responsible for sending those traps directly to the configured SNMP trap destination(s). See reference [1] for the SNMP traps generated by G700 Media Gateway. Avaya Communication Manager running on the S8700 Media Server detects internal failures in the G600 Media Gateway and sends all traps when it controls a G600 Media Gateway.
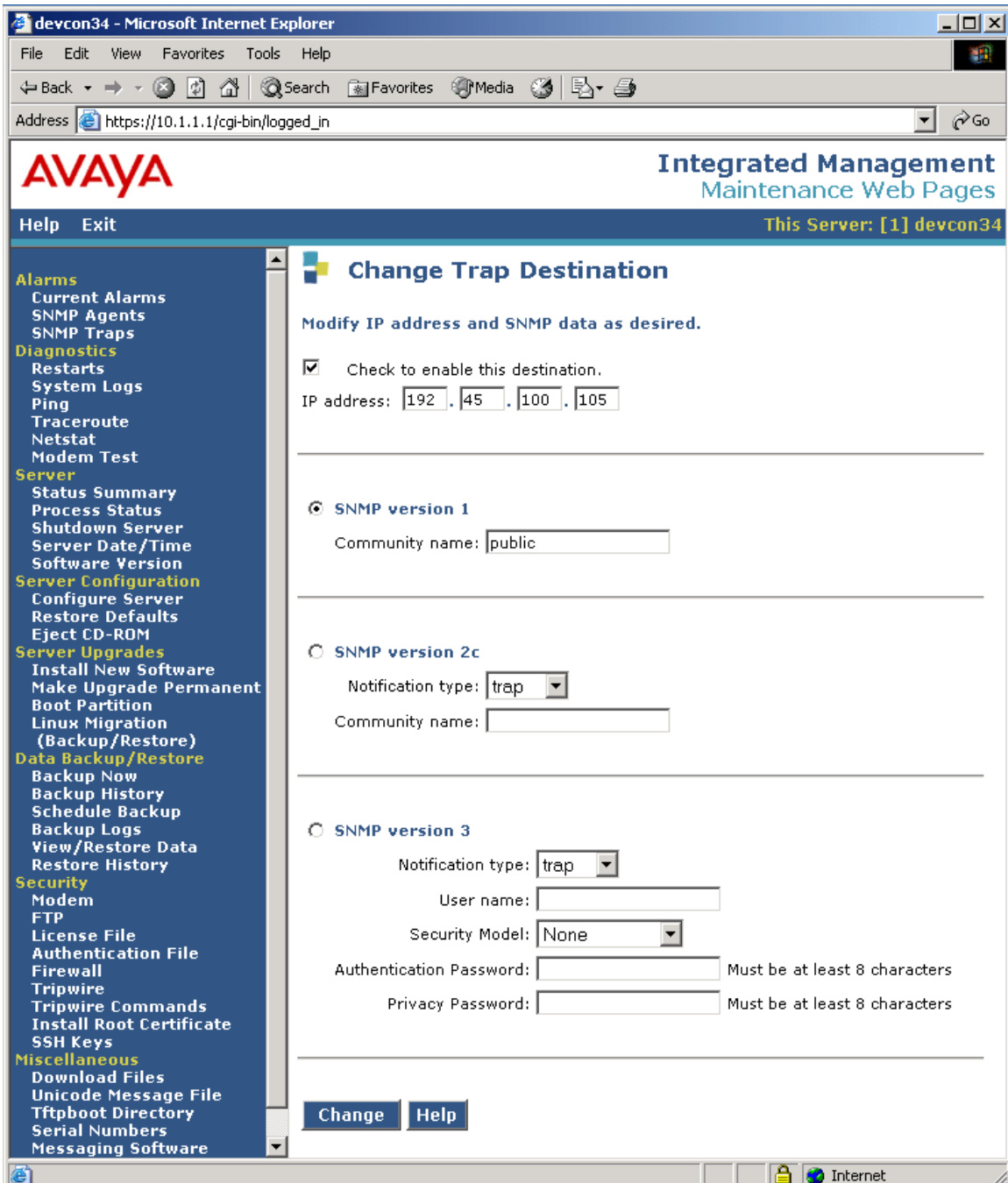
Figure 2: SNMP Traps Configuration

1.2. Firewall Configuration

The firewall in the Avaya Media Server must allow SNMP traps to be sent on UDP port 162. Click on the **Firewall** option in the **Security** section of the menu to display the **Firewall Configuration** screen. At the bottom of the screen, click on the **Advanced Settings…** button to display the screen shown in **Figure 3**. Click on the **Output from Server** checkbox (2nd column) for **snmptrap 162/udp** and submit the form. This is the only port that needs to be enabled for the media server to send SNMP traps. For an S8700 Media Server pair, the **Firewall** configuration should be performed on each media server.
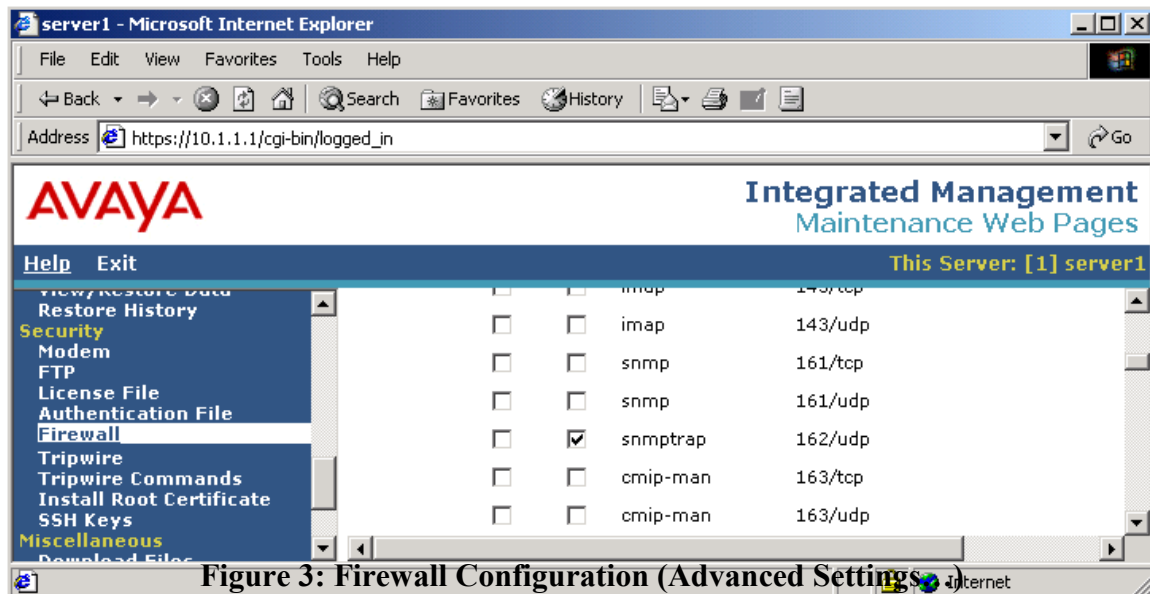
Figure 3: Firewall Configuration (Advanced Settings)

1.3. Configuring Alarm Reporting Options

Ensure that the alarms the customer would like to have reported to AlarmTraq ver 5 have not been downgraded to a warning alarm; otherwise, these alarms will not be reported via an SNMP trap. Enter the **set options** command on the media server's SAT to display the form in **Figure 4**, and check the **Major** and **Minor** columns for each alarm type. In summary, if the **Major** or **Minor** column is set to **[w]**arning, **[r]**eporting, or **[n]**o, then that alarm type has either been downgraded to warning severity or alarm reporting has been suppressed. However, if the column is set to **[y]**es or **[m]**inor, then an SNMP trap is sent. See reference [2] for more details on the **set options** form.

Note: The settings in the set options form do not affect the SNMP traps generated by the G700 Media Gateway, which always sends warning and informational level traps, if an SNMP trap destination is configured.

```
                               ALARM REPORTING OPTIONS

                                           Major   Minor
                      On-board Station Alarms: y     y
                     Off-board Station Alarms: y     y
         On-board Trunk Alarms (Alarm Group 1): y     y
        Off-board Trunk Alarms (Alarm Group 1): y     y
         On-board Trunk Alarms (Alarm Group 2): w     w
        Off-board Trunk Alarms (Alarm Group 2): w     w
         On-board Trunk Alarms (Alarm Group 3): w     w
        Off-board Trunk Alarms (Alarm Group 3): w     w
         On-board Trunk Alarms (Alarm Group 4): w     w
        Off-board Trunk Alarms (Alarm Group 4): w     w
                 On-board Adjunct Link Alarms: y     y
                Off-board Adjunct Link Alarms: y     y
                   Off-board MASI Link Alarms:       y
                        Off-board DS1 Alarms: y     y

                 Off-board TCP/IP Link Alarms: y     y
                      Off-board Alarms (Other): y     y
                 Off-board ATM Network Alarms:       y
```
Figure 4: Set Options Form (Page 1)

Page 2 of the set options form continues with the alarm reporting options for other alarm types, such as Signaling Group alarms.

```
                               ALARM REPORTING OPTIONS

                                           Major   Minor
             Off-board Firmware Download Alarms:       y
              Off-board Signaling Group Alarms:       y
                           Remote Max Alarms:       y
```
Figure 5: Set Options Form (Page 2)