Avaya Solution & Interoperability Test Lab

Application Notes for Codima autoAsset with an Avaya Infrastructure - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Codima autoAsset to interoperate with an Avaya infrastructure. The Avaya Infrastructure consisted of Avaya Communication Manager, Avaya SIP Enablement Services, Avaya Application Enablement Services, Avaya C360 Series Converged Stackable Switches and Avaya 4600 Series IP Telephones. autoAsset can be used to produce asset inventory HTML reports and to display the asset information associated with devices found in a network. autoAsset can be integrated into the Codima autoMap product.

Information in these Application Notes has been obtained through Developer*Connection* 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 configuration steps required for Codima autoAsset to interoperate with an Avaya infrastructure. The Avaya infrastructure consisted of Avaya Communication Manager, Avaya SIP Enablement Services (SES), Avaya Application Enablement Services, Avaya C360 Series Converged Stackable Switches and Avaya 4600 Series IP Telephones. autoAsset can be used to produce asset inventory HTML reports and display the asset information associated with devices found in a network. autoAsset can be integrated into the Codima autoMap product.

autoAsset uses the Codima Discovery Engine to scan the network. The Codima Discovery Engine begins the discovery from a starting point called a seed-device, which must be Simple Network Management Protocol (SNMP) capable. The Codima Discovery Engine will inspect the Address Resolution Protocol (ARP) table and the Routing and Forwarding tables for the seed-device and use this information to begin the interrogation. As the Discovery Engine finds the next switch or router, more devices are discovered and the discovery process works in a recursive manner to find all active devices.

The Codima Discovery Engine uses a variety of techniques to interrogate devices, such as inspection of ARP tables, Routing and Forwarding tables and controlled scanning techniques. Once discovered, devices are queried using SNMP for Management Information Base (MIB) 2 and current vendor MIBs. Windows Management Instrumentation (WMI) is also supported. autoAsset has a device database covering most current and many older generation equipment types. The protocols used in the process include SNMP, Internet Control Message Protocol (ICMP), Network Basic Input/Output System (NetBIOS), Spanning Tree Protocol (STP), and vendor-specific discovery protocols. As ARP tables get flushed, the discovery engine can force those tables to be populated by using a controlled ping scan to discover additional devices that have not been recently active.

Figure 1 illustrates the network used for compliance testing.

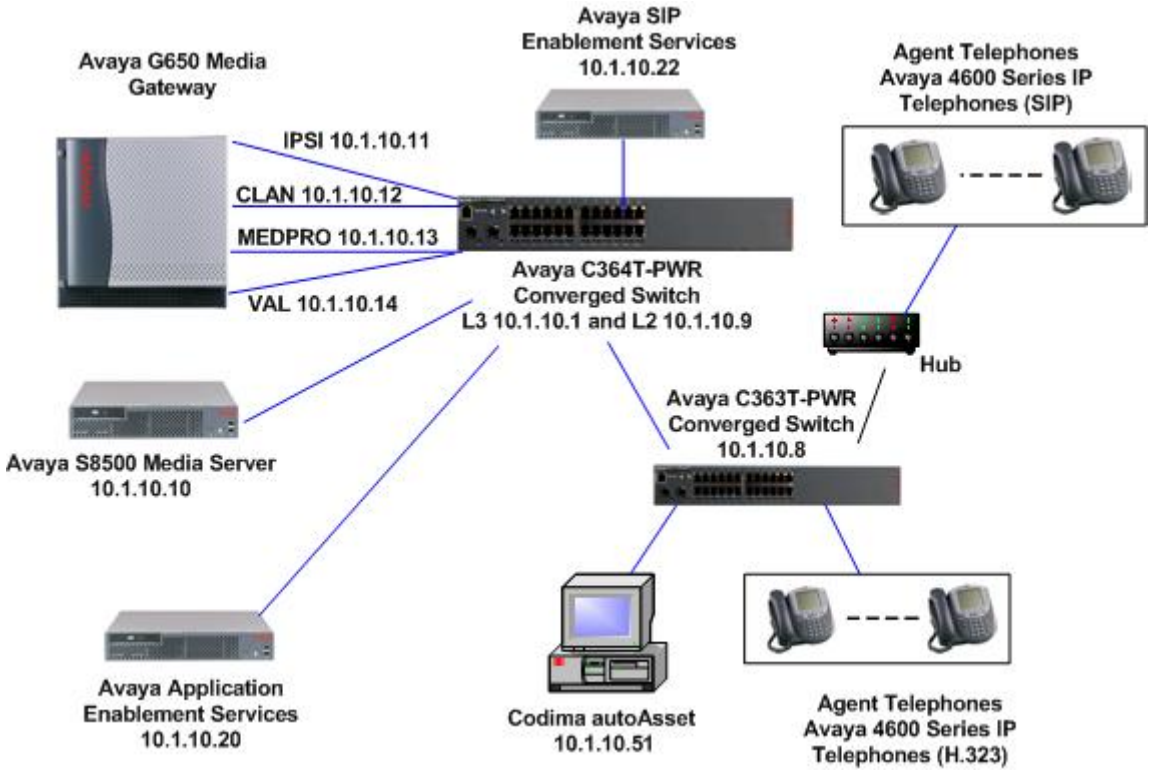


Figure 1: Avaya Test Network Infrastructure with Codima autoAsset

2. Equipment and Software Validated

Below is a list of the equipment and software versions used within the compliance-tested network.

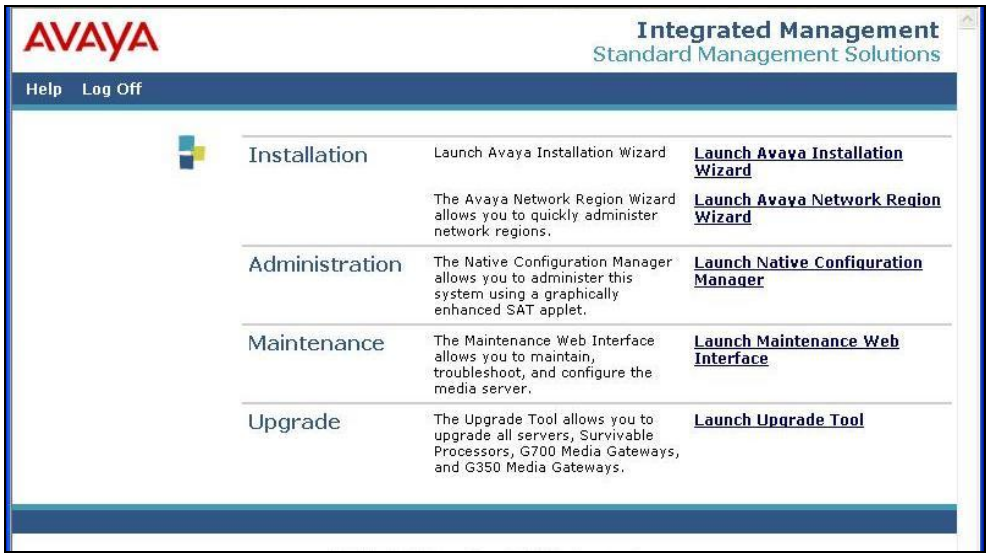
Equipment	Software
Avaya SIP Enablement Services (10.1.10.22)	3.1.2
Avaya S8500 Media Server running Avaya Communication Manager (10.1.10.10)	4.0
Avaya G650 Media Gateway IPSI - TN2312BP (10.1.10.11) CLAN - TN799DP (10.1.10.12) MEDPRO - TN2302AP (10.1.10.13) VAL - TN2501AP (10.1.10.14)	 HW07 FW036 HW01 FW017 HW20 FW115 HW02 FW007
Avaya Application Enablement Services (10.1.10.20)	4.0
Avaya 4600 Series IP Telephones (SIP)	2.2.3
Avaya 4600 Series IP Telephones (H.323)	2.7
Avaya C364T-PWR Converged Stackable Switch (10.1.10.9)	4.3.12
Avaya C363T-PWR Converged Stackable Switch (10.1.10.8)	4.3.12
Codima autoAsset (10.1.10.51) running on: Dell Workstation 370 Pentium 4 CPU 2.80GHz RAM 1.00GB Disk Space >4GB	2.30 0011 Windows XP Professional SP2
Network hub	N/A

3. Configure Avaya Infrastructure

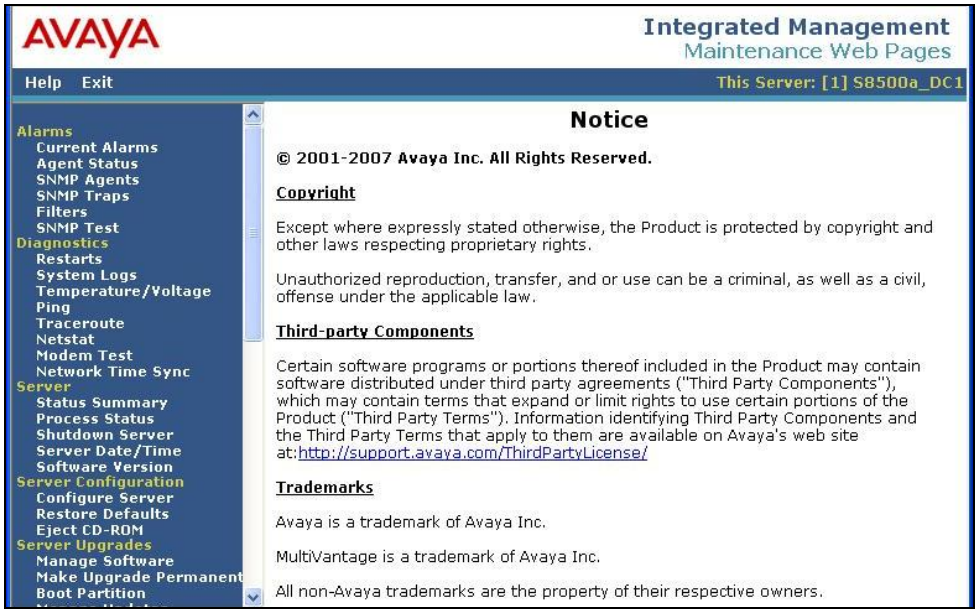
SNMP was enabled on Avaya Communication Manager, Avaya SES and Avaya 4600 Series IP telephones.

3.1. Configure SNMP on Avaya Communication Manager

Access the Avaya Communication Manager administration web interface by entering *http://<ip-addr>/* as the URL in an Internet browser, where *<ip-addr>* is the IP address of Avaya Communication Manager. Log in with the appropriate credentials to the Avaya Communication Manager web interface and click **Launch Maintenance Web Interface**.



Under the **Alarms** options, select **SNMP Agents**.



For increased security, click on the **Following IP addresses** radio button and enter the IP address of the autoAsset workstation in the **IP address1** field. Check the **Enable SNMP Version 1** and **Enable SNMP Version 2c** check boxes and enter a SNMP community string in the **Community Name (read-only)** field. Click on the **Submit** button at the bottom of the page (not shown).

3.2. Configure SNMP on Avaya SIP Enablement Services

Access the Avaya SES administration web interface by entering *http://<ip-addr>/admin* as the URL in an Internet browser, where *<ip-addr>* is the IP address of Avaya SES. Log in with the appropriate credentials to the Avaya SES web interface (not shown) and click on **Launch Administration Web Interface**.

Expand the **Server Configuration** menu and select **SNMP Configuration**. Enter a SNMP community string in the **SNMP v2c Community name** field and click the **Set** button. Click **Continue** on the following screen to confirm the changes (not shown).

3.3. Configure SNMP on Avaya 4600 Series IP Telephones

As of Release 2.0 for the Avaya 4600 Series IP Telephones, administrators can set the SNMP community string (SNMPSTRING) and restrict SNMP access to administered IP addresses (SNMPADD). The customizable system parameters for the Avaya 4600 Series IP Telephones can be set using the settings script file (46xxsettings.txt). This file resides on a TFTP, HTTP, or HTTPS administered file server.

The **SET SNMPSTRING** parameter is a text string containing the SNMP community name string. The **SET 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.

The SNMP configuration in the 46xxsettings.txt file used during compliance testing is shown below. The configuration will set the SNMP community string to "devconuk" and will restrict SNMP queries to the 10.1.10.51 IP address.

```
######################  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 10.1.10.51
##
## SNMP community name string
##   This value must be set to enable viewing of the phone's
##   MIB. This value must match the community string name
##   used in the SNMP query (up to 32 ASCII characters, no
##   spaces).
##
SET SNMPSTRING devconuk
##
```

3.4. Configure SNMP on Avaya Switches

During compliance testing, the Avaya C360 Series Converged Stackable Switches used the default community SNMP string "public". This can be verified by entering the command "show SNMP" from the command line interface of the switches.

4. Configure Codima autoAsset

Ensure that the IP address of the start point (seed-device) is SNMP-compliant. In the compliance-tested network, the seed-device was a layer 3 switch with the IP address 10.1.10.1. Note the SNMP read community strings. These strings will be used in Section 4.1.

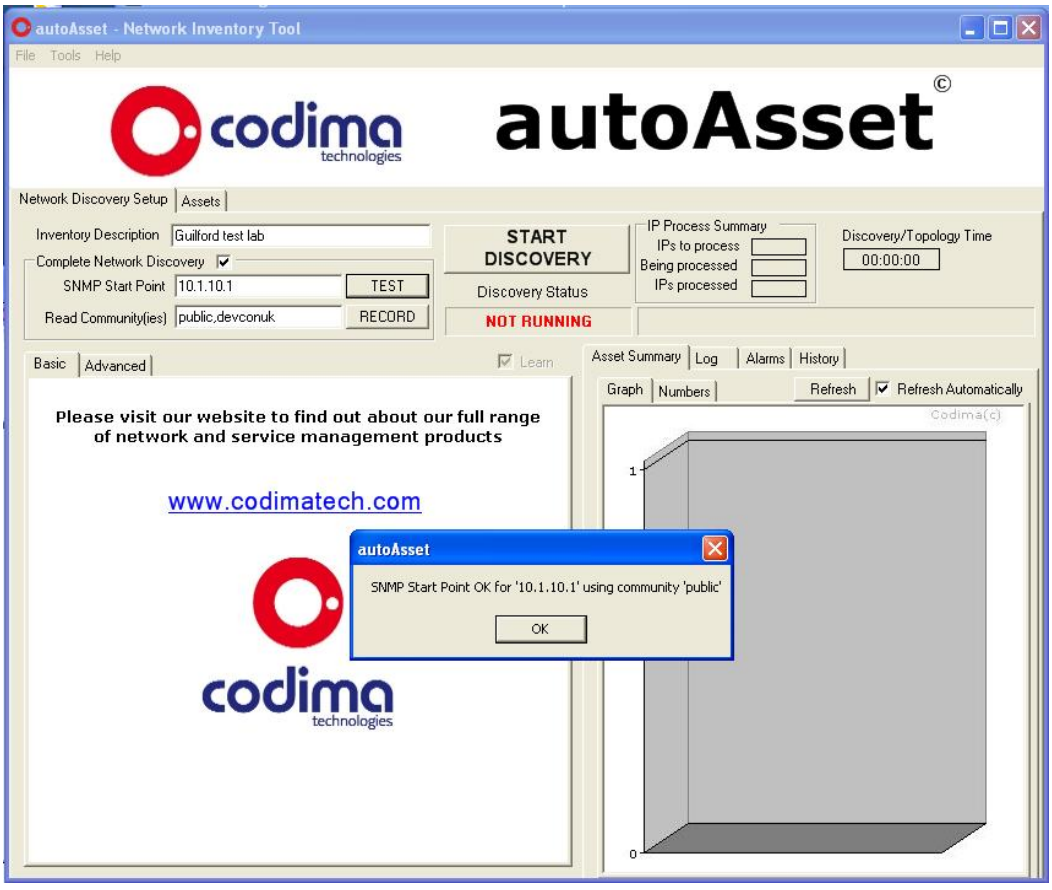
4.1. Configure Codima autoAsset Discovery

From the workstation that has autoAsset installed, launch the Codima Toolbox console by clicking **Start → Programs → Codima Technologies → Codima autoAsset** and log in with the appropriate password.

In the **autoAsset – Network Inventory Tool** screen, enter the following parameters:

- **Inventory Description** – enter a descriptive name for the network.
- **SNMP Start Point** – enter the IP address of the seed-device "10.1.10.1".
- **Read Community(ies)** – enter SNMP strings configured in Section 3.1, 3.2, 3.3 and 3.4 "public,devconk"

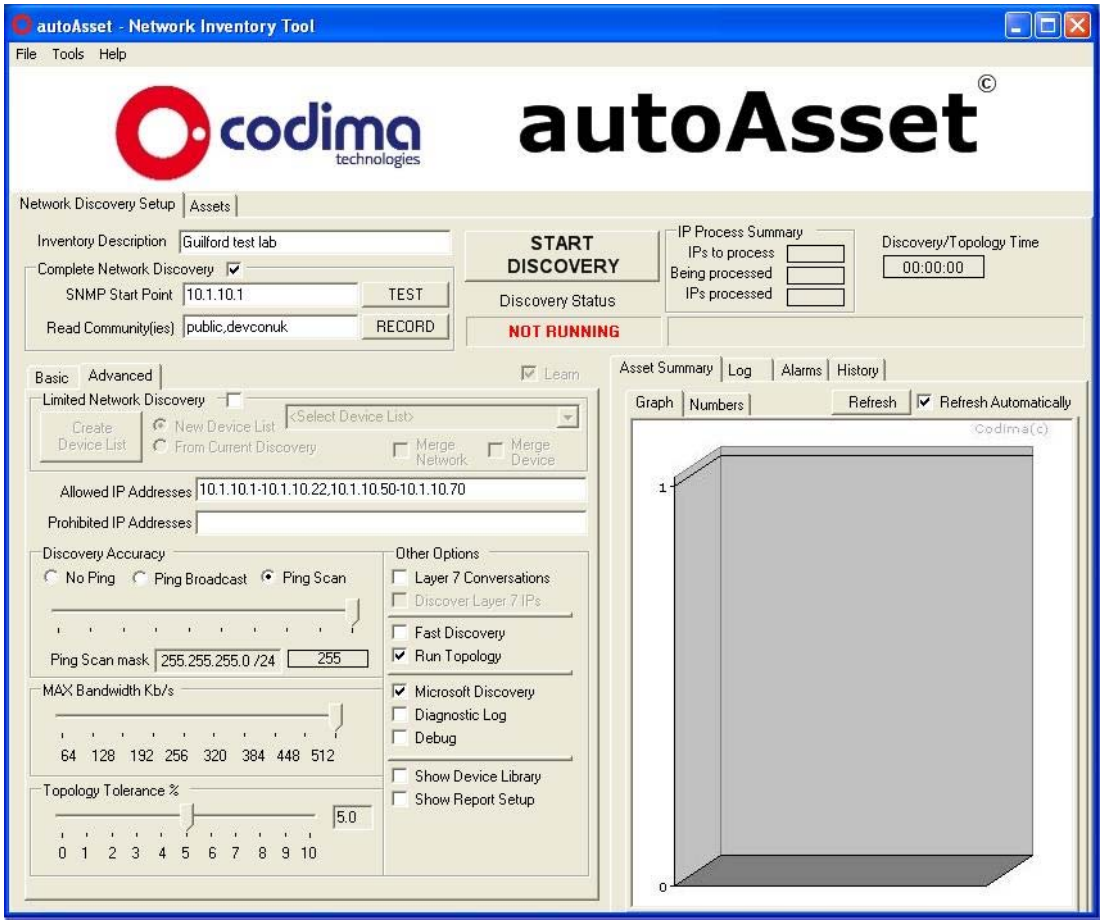
Click the **TEST** button to check that the start point is successful. Next, click the **OK** button.



In the **autoAsset – Network Inventory Tool** screen shown above, click on the **Advanced** tab and enter the following parameter.

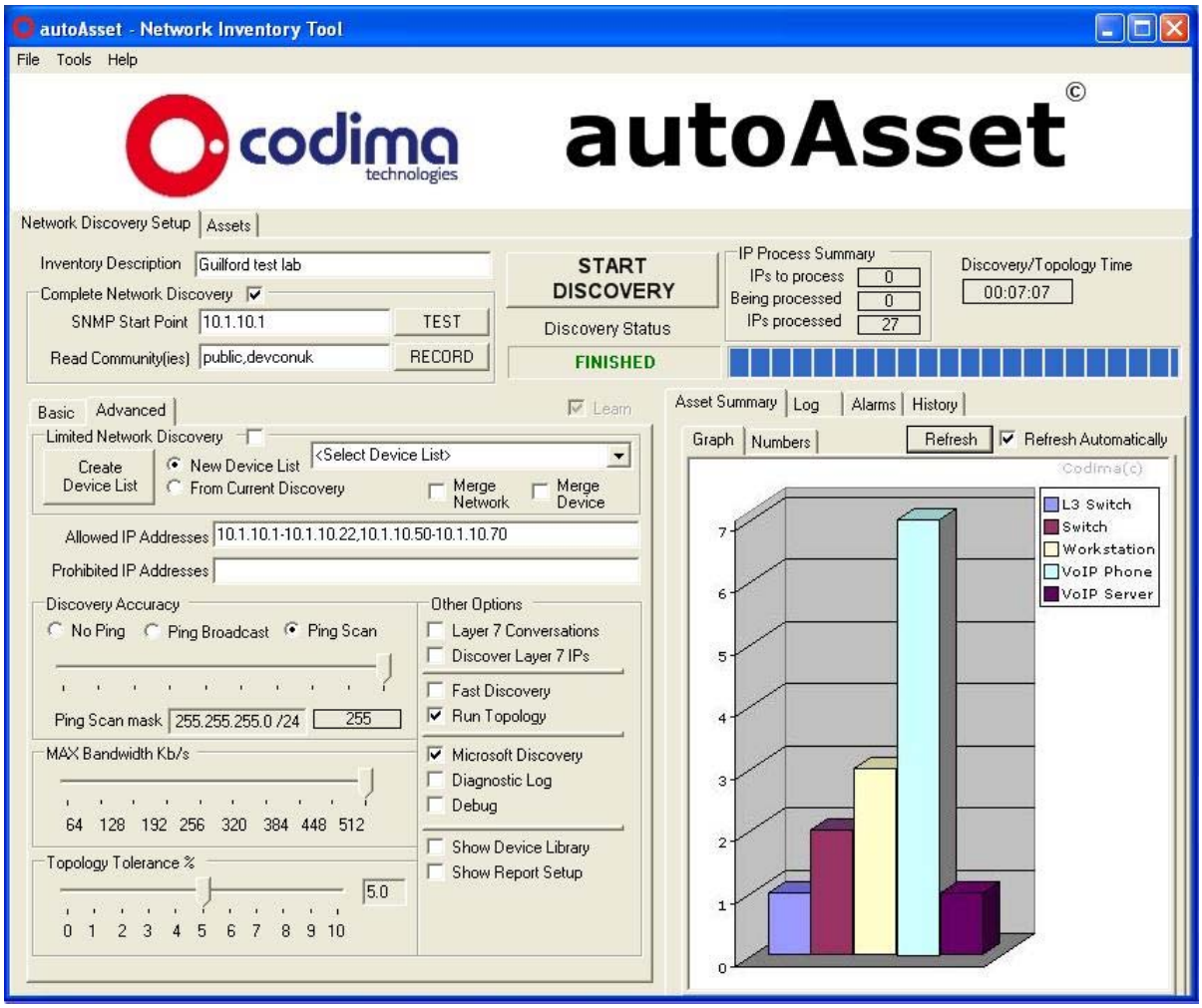
- **Allowed IP Addresses** – enter the IP subnet ranges "10.1.10.1-10.1.10.22,10.1.10.50-10.1.10.70".

Default values can be retained for the remaining parameters. Click the **START DSICOVERY** button.

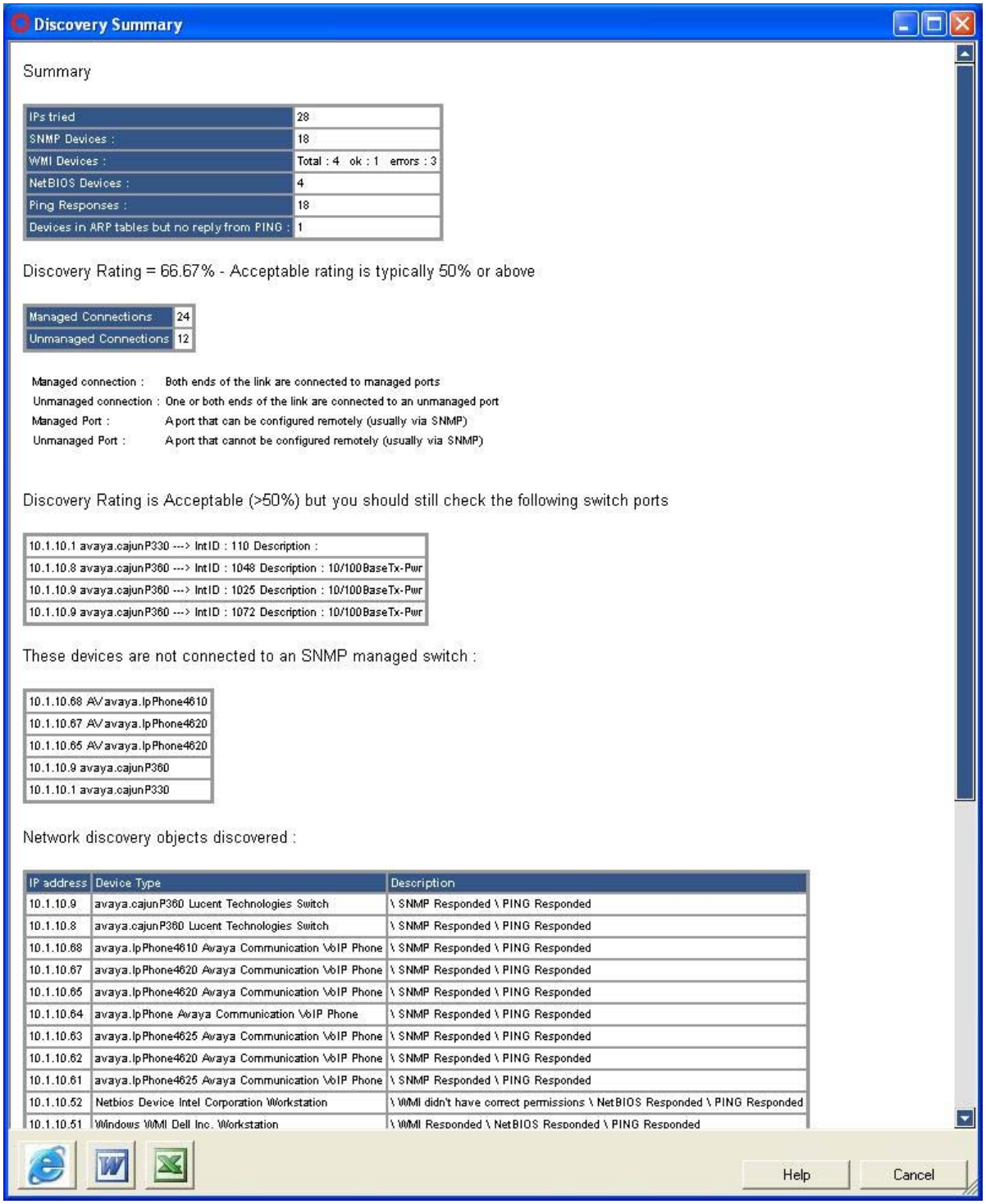


4.2. Codima autoAsset Discovery Results

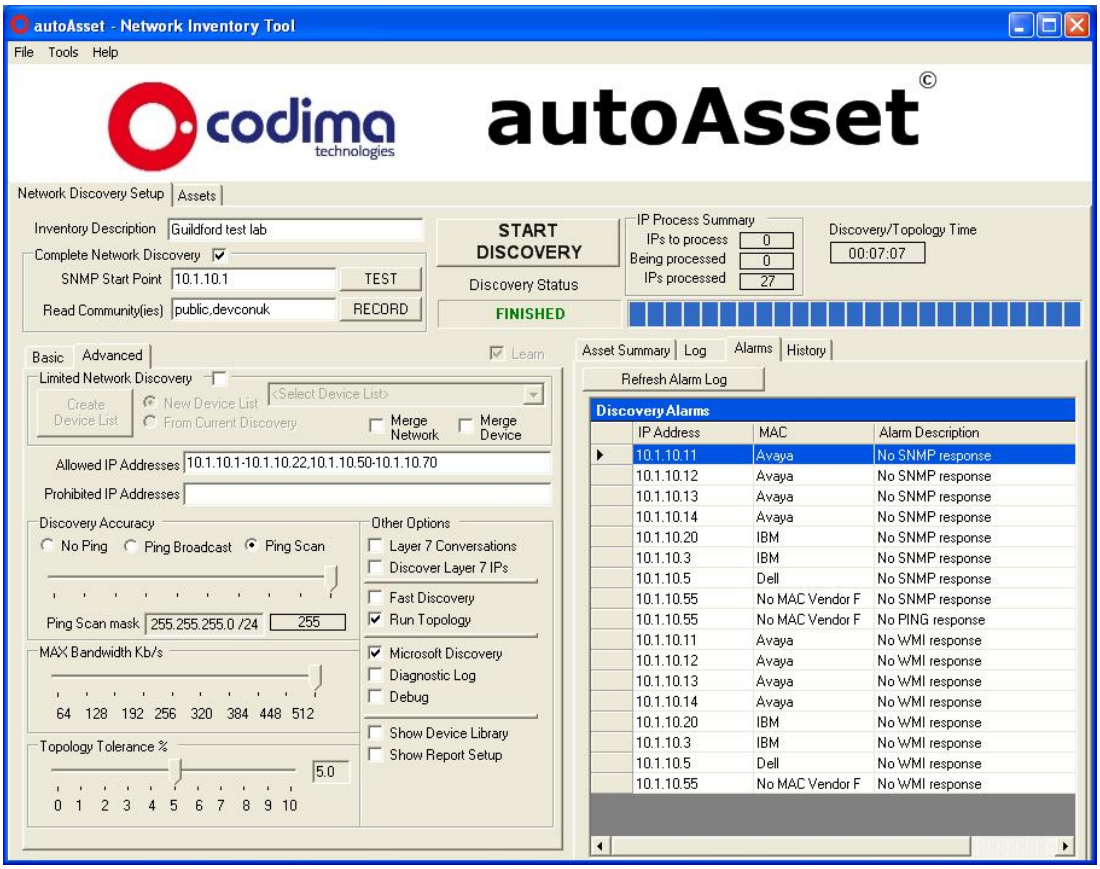
Once the discovery of the network has been completed, **Discovery Status** will show the value "FINISHED".



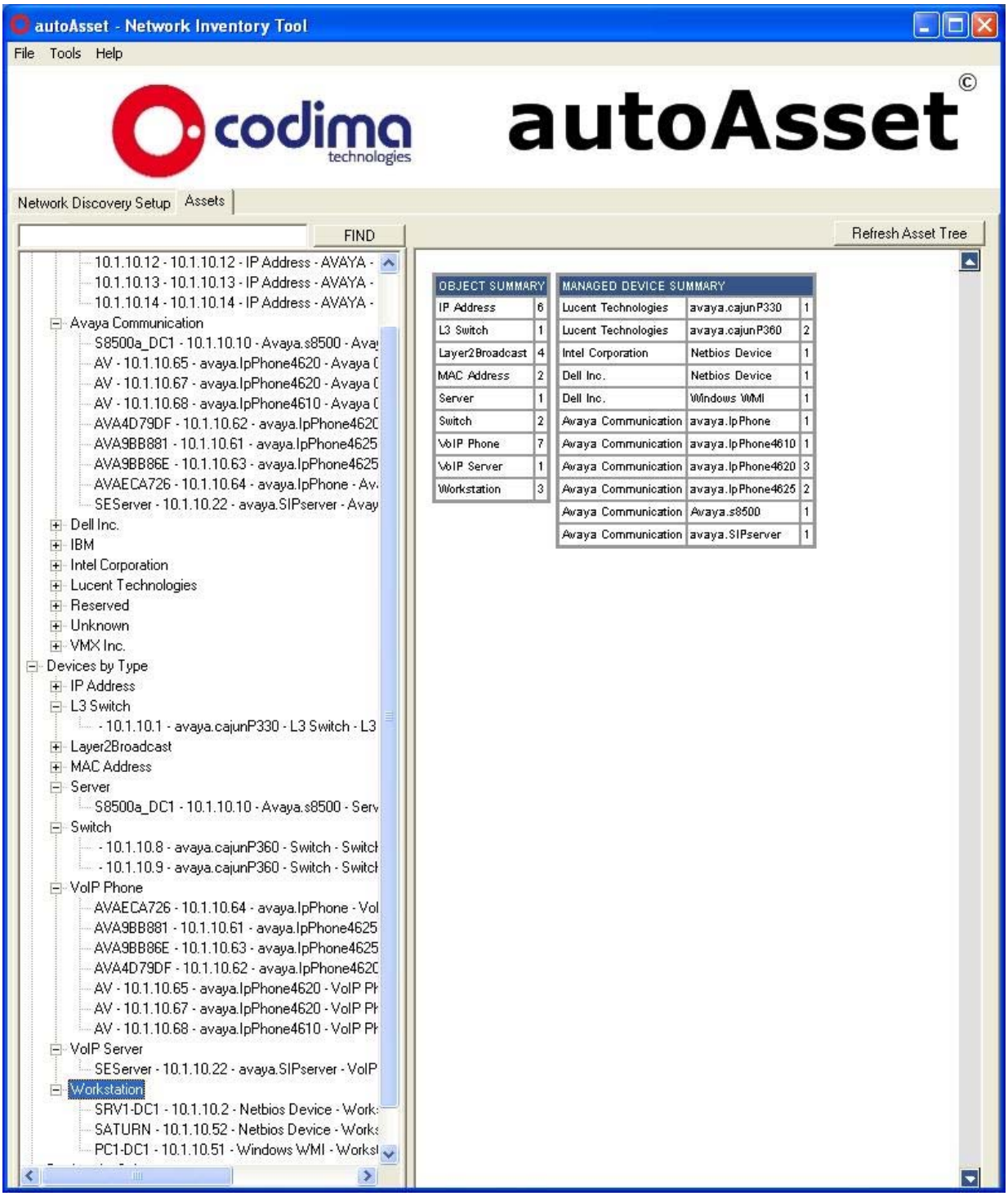
The **Discovery Summary** screen, shown below, appears when the autoAsset discovery process has completed. The results include the number and types of devices found in the network and associated IP addresses.



In the **autoAsset – Network Inventory Tool** screen, click on the **Alarms** tab to see the list of the IP addresses that did not respond to SNMP or WMI.

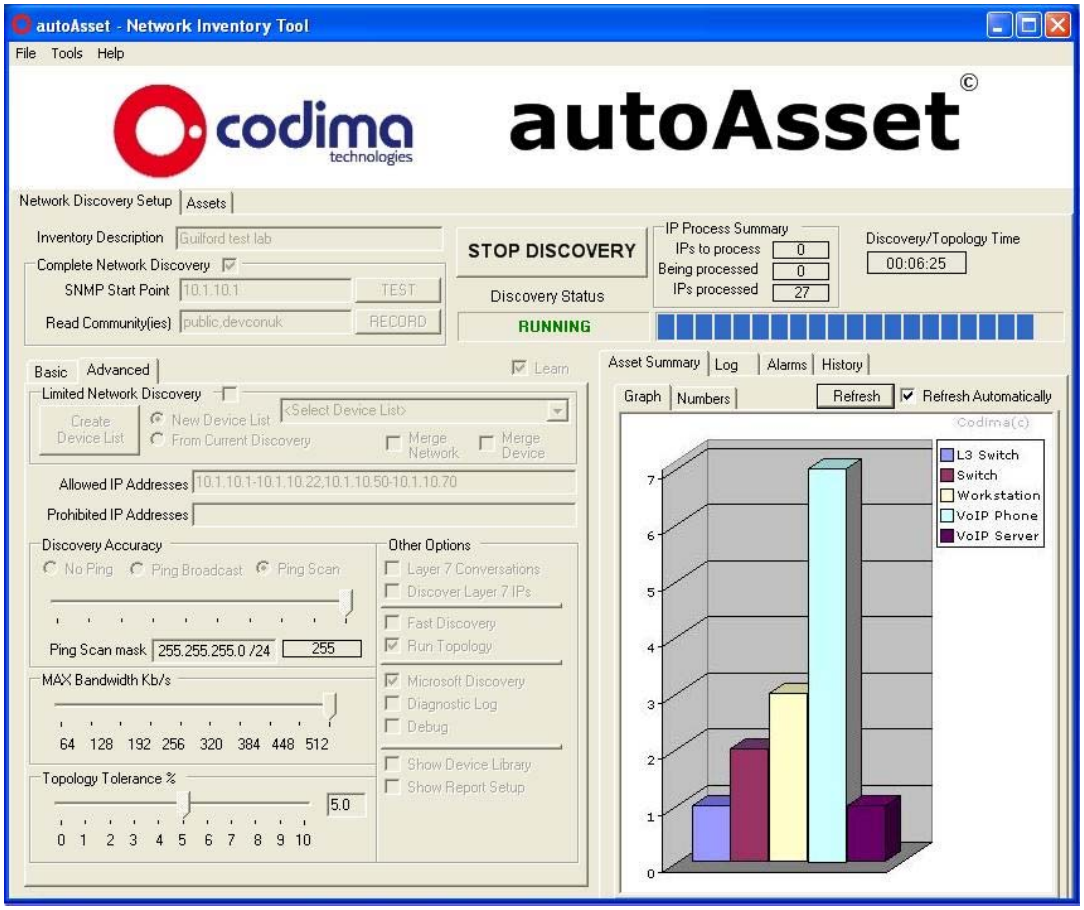


In the **autoAsset – Network Inventory Tool** screen, click on the **Assets** tab to list all the devices found during the autoAsset discovery process.



5. Verification Steps

When the discovery process has started successfully, **Discovery Status** will show the value "RUNNING" as shown below. Once the discovery process has completed, the **Discovery Summary** screen will appear as shown in Section 4.2.



6. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing focused on the ability for Codima autoAsset to accurately discover devices in the network using the following discovery protocols: SNMP, ICMP, NetBIOS and STP. These discovery protocols allowed autoAsset to create an inventory of the network. The serviceability tests included stopping and starting the discovery process.

6.1. General Test Approach

The feature test was performed by first entering the seed-device IP address and the private SNMP community strings configured on Avaya Communication Manager, Avaya SES and Avaya 4600 Series IP telephones. The test continued by starting the autoAsset discovery process testing the ability of autoAsset to discover devices in the network. Serviceability tests included stopping and starting the discovery process. The inventory created by autoAsset was compared to the network diagram shown in **Figure 1**.

6.2. Test Results

All test cases were executed and passed. autoAsset 2.30 supports SNMP versions 1 and 2c.

7. Support

For any support related enquiries, contact: tech_support@codimatech.com or
Codima Technologies.

149a Grosvenor Road London SW1V 3JY UK
Tel: +44 (0) 207 881 0700
Fax: +44 (0) 207 730 5194

8. Conclusion

These Application Notes describe the configuration steps for Codima autoAsset 2.30 to interoperate with Avaya Communication Manager, Avaya SES, Avaya C360 Series Converged Stackable Switches and Avaya 4600 Series IP telephones. All test cases were completed successfully and the configuration described in these Application Notes has been successfully compliance tested.

9. Additional References

Avaya product documentation can be found at http://support.avaya.com.

Company and product information available from Codima can be found at http://www.codimatech.com

- http://www.codimatech.com/products.php
- http://www.codimatech.com/products_datasheets.php
- http://www.codimatech.com/support.php

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.