Avaya Solution & Interoperability Test Lab

Application Notes for Codima autoMap with Avaya Communication Manager, Avaya SIP Enablement Services, and Avaya Application Enablement Services - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Codima autoMap 3.10 to successfully interoperate with 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. Codima autoMap provides a quick and simple method of automatically generating graphical network topology drawings using Microsoft Office Visio.

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 autoMap to successfully interoperate with 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. Codima autoMap provides a quick and simple method of automatically generating graphical network topology drawings using Microsoft Office Visio.

Codima autoMap 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 SNMP (Simple Network Management Protocol) capable. The Codima Discovery Engine will inspect the ARP (Address Resolution Protocol) 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, it starts to see more devices, 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 MIB (Management Information Base) 2 and current vendor MIBs. WMI (Windows Management Instrumentation) is also supported. The autoMap product has a device database covering most current and many older generation equipment types. The protocols used in the process include SNMP, ICMP (Internet Control Message Protocol), NetBIOS (Network Basic Input/Output System), STP (Spanning Tree Protocol), 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.

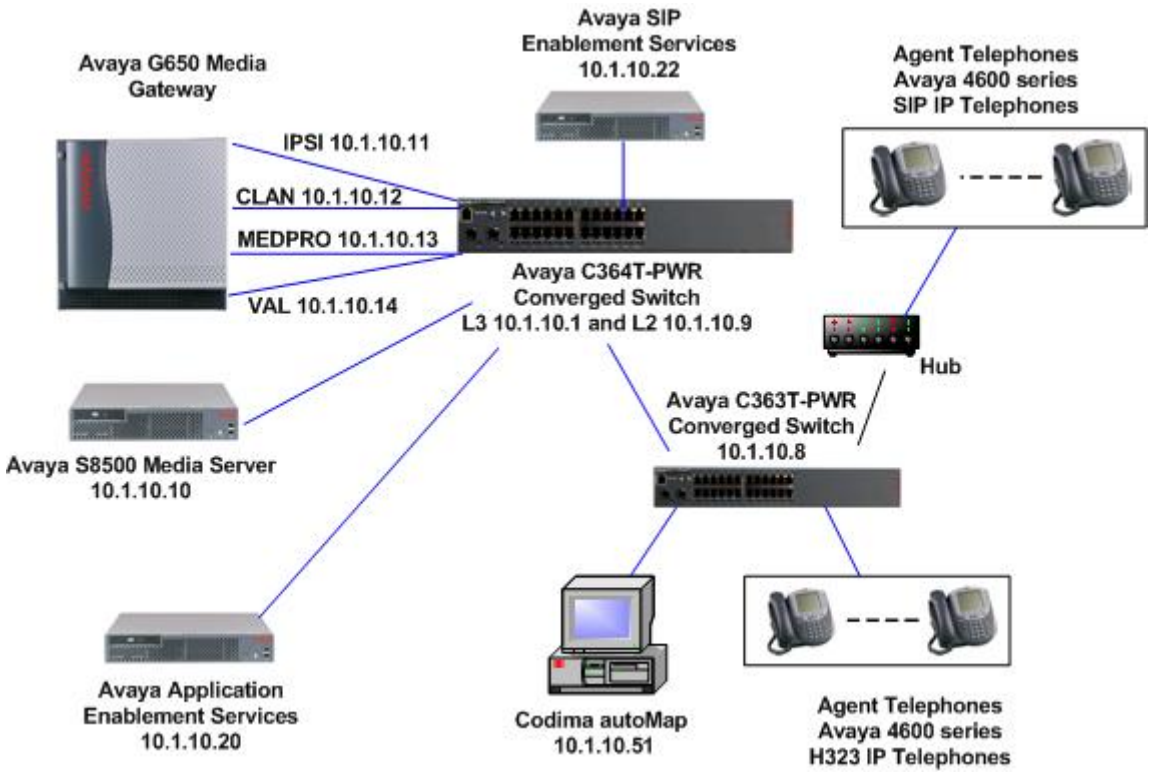


Figure 1: Avaya Test Network Infrastructure with Codima autoMap

2. Equipment and Software Validated

Figure 1 shows the equipment discovered by autoMap of the compliance-test network. The table below lists the equipment and software versions used in 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
3COM OfficeConnect Dual Speed 16 port Hub	
Codima autoMap (10.1.10.51) running on: Dell Workstation 370 Pentium 4 CPU 2.80GHz RAM 1.00GB Disk Space >4GB	3.1 0023 Windows XP SP2 Microsoft Visio 2003
Dell Workstation 370 (10.1.10.52) – not shown	Windows XP SP2
Dell Server (10.1.10.2) – not shown	Windows 2003 Server
Dell Server (10.1.10.5) – not shown	Windows 2003 Server

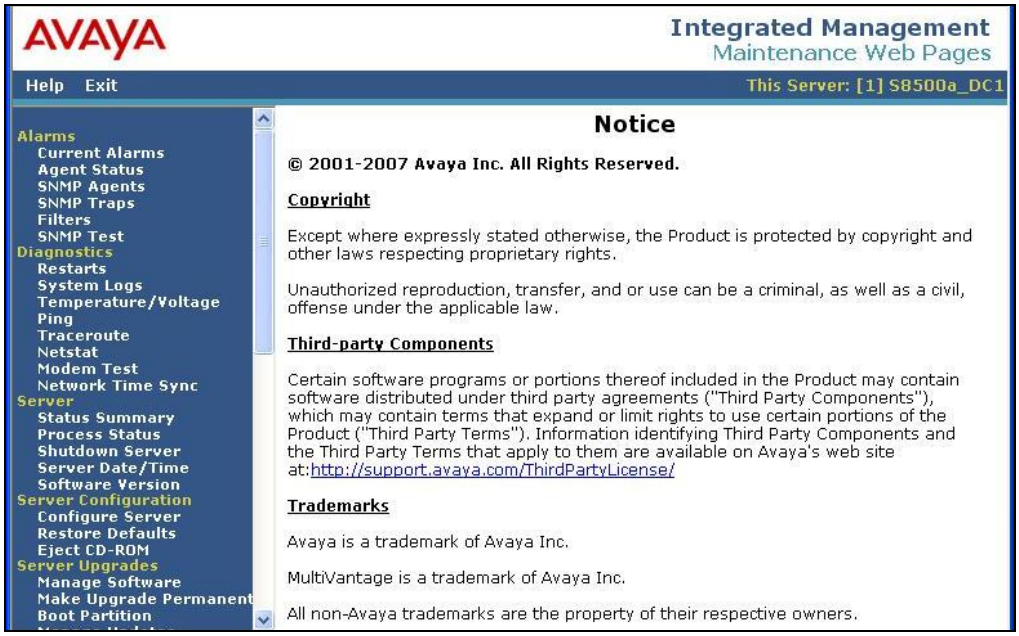
3. Configure Avaya Infrastructure

SNMP was enabled on Avaya Communication Manager, SES and Avaya 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 autoMap 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 using an Internet browser. 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** and click the **Set** button. Click **Continue** on the following screen to confirm the changes (not shown).

3.3. Configure SNMP on Avaya IP Telephones

As of 46xx Release 2.0, Avaya IP telephones allow administrators to set the SNMP community string (SNMPSTRING) and to restrict SNMP access to administered IP Addresses (SNMPADD). Avaya IP Telephones customizable system parameters can be set using the settings script file (46xxsettings.txt). This file resides on the IP Telephone's 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 and 10.1.10.55 IP addresses.

```
#####################  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 10.1.10.51,10.1.10.55
##
## 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 switch.

4. Configure autoMap

Ensure that the 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, which will be used in Section 4.1.

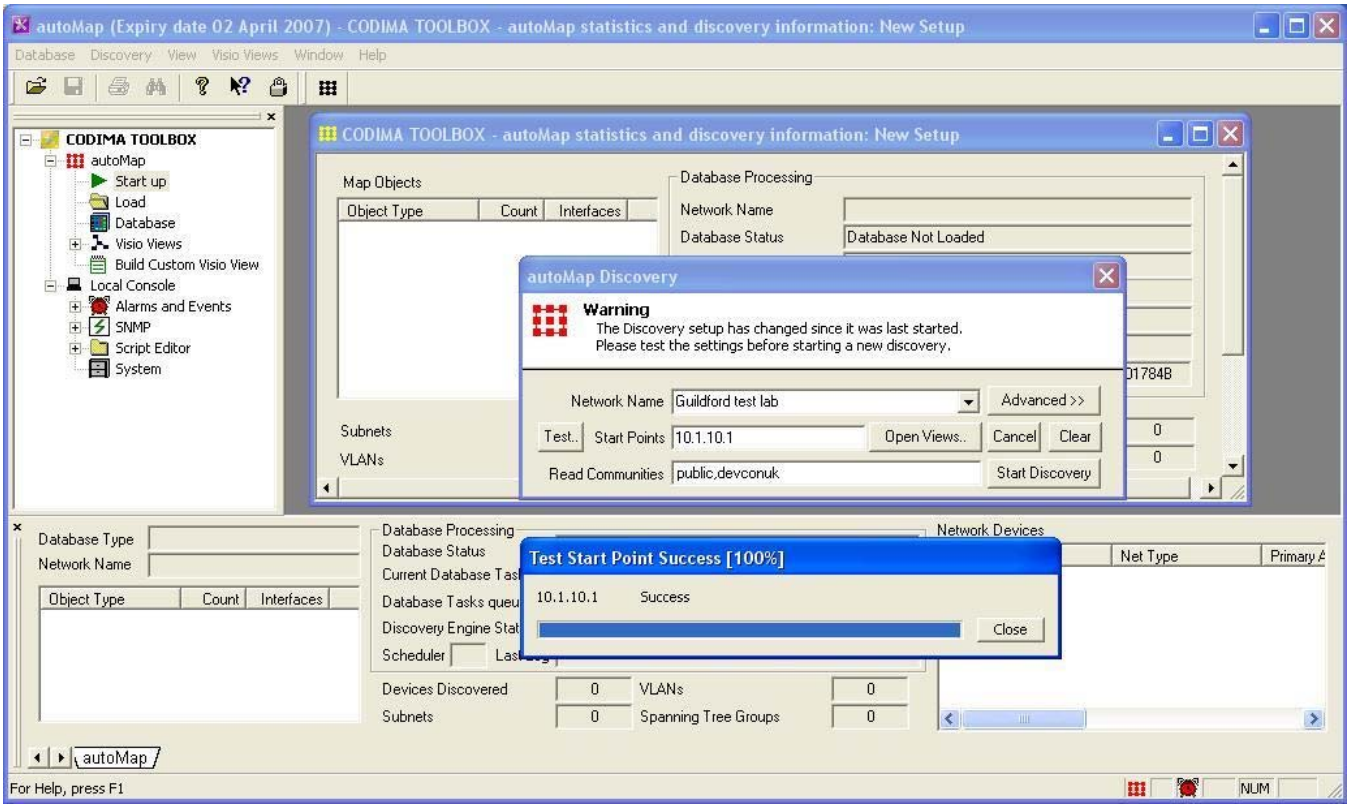
4.1. Configure autoMap Discovery

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

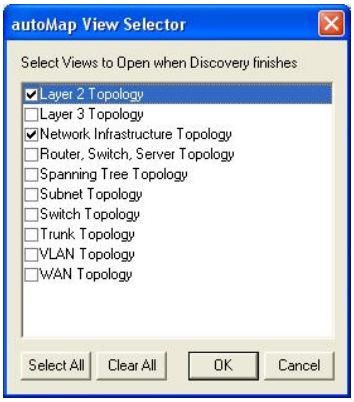
Expand the **Enterprise** tree menu by clicking on **autoMap → Start up**. In the autoMap Discovery dialog box, enter the following parameters:

- **Network Name** – enter a descriptive name for the network.
- **Start Points** – enter the IP address of the seed device "10.1.10.1".
- **Read Communities** – 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 **Open Views…** button.



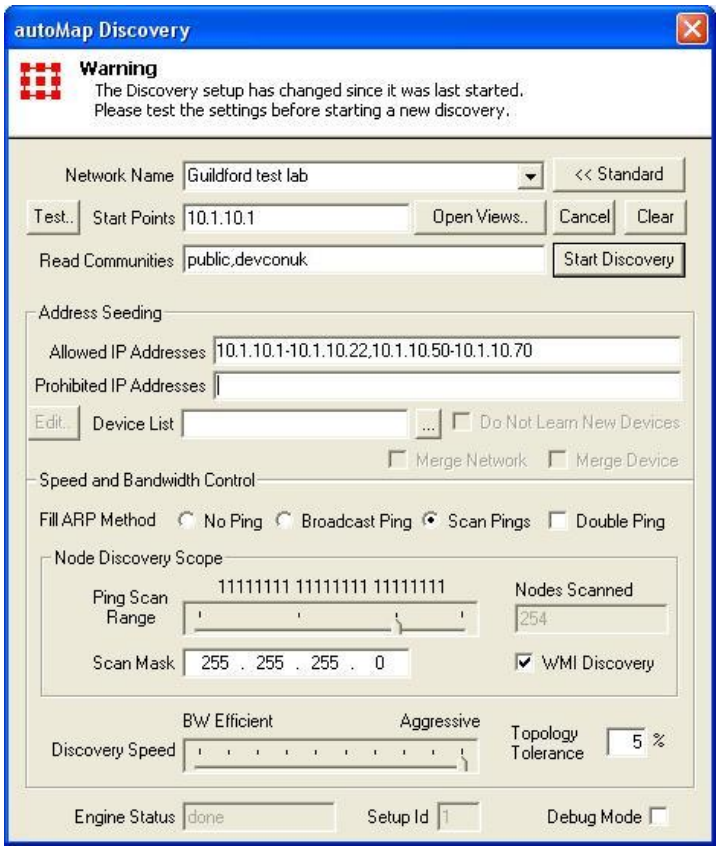
In the **autoMap View Selector** dialog box, check the boxes of the views to be displayed when the discovery of the network has finished. Click **OK**. In the **autoMap Discovery** dialog box shown above, click on the **Advanced** button.



In the Address Seeding section, enter the following parameters.

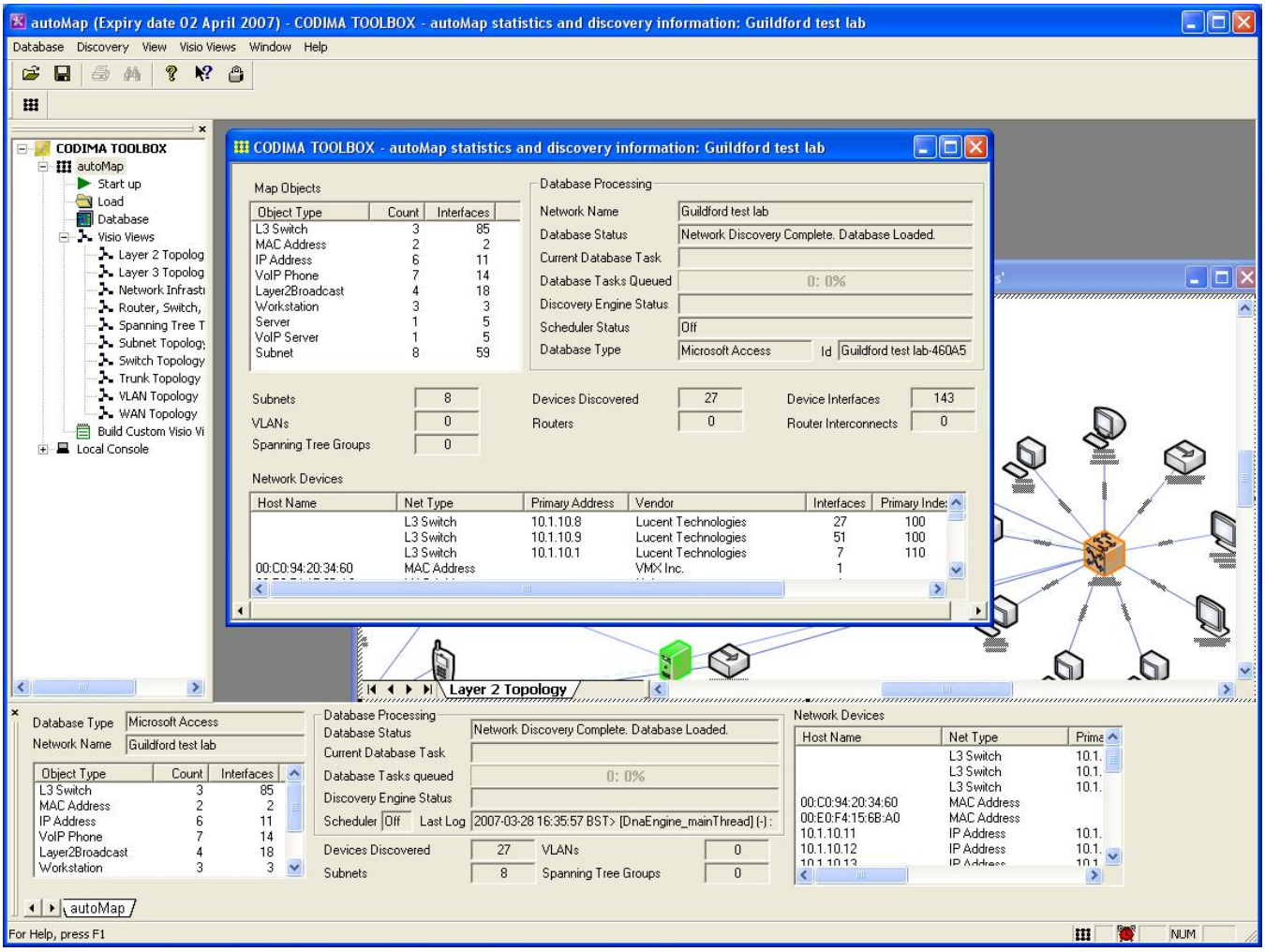
- **Allowed IP Addresses** – enter the IP subnet ranges "10.1.10.1-10.1.10.22, 10.1.10.50-10.1.10.70".
- **Scan Mask** – enter the mask "255.255.255.0".

Default values can be retained for the remaining parameters. Click the **Start Discovery** button.

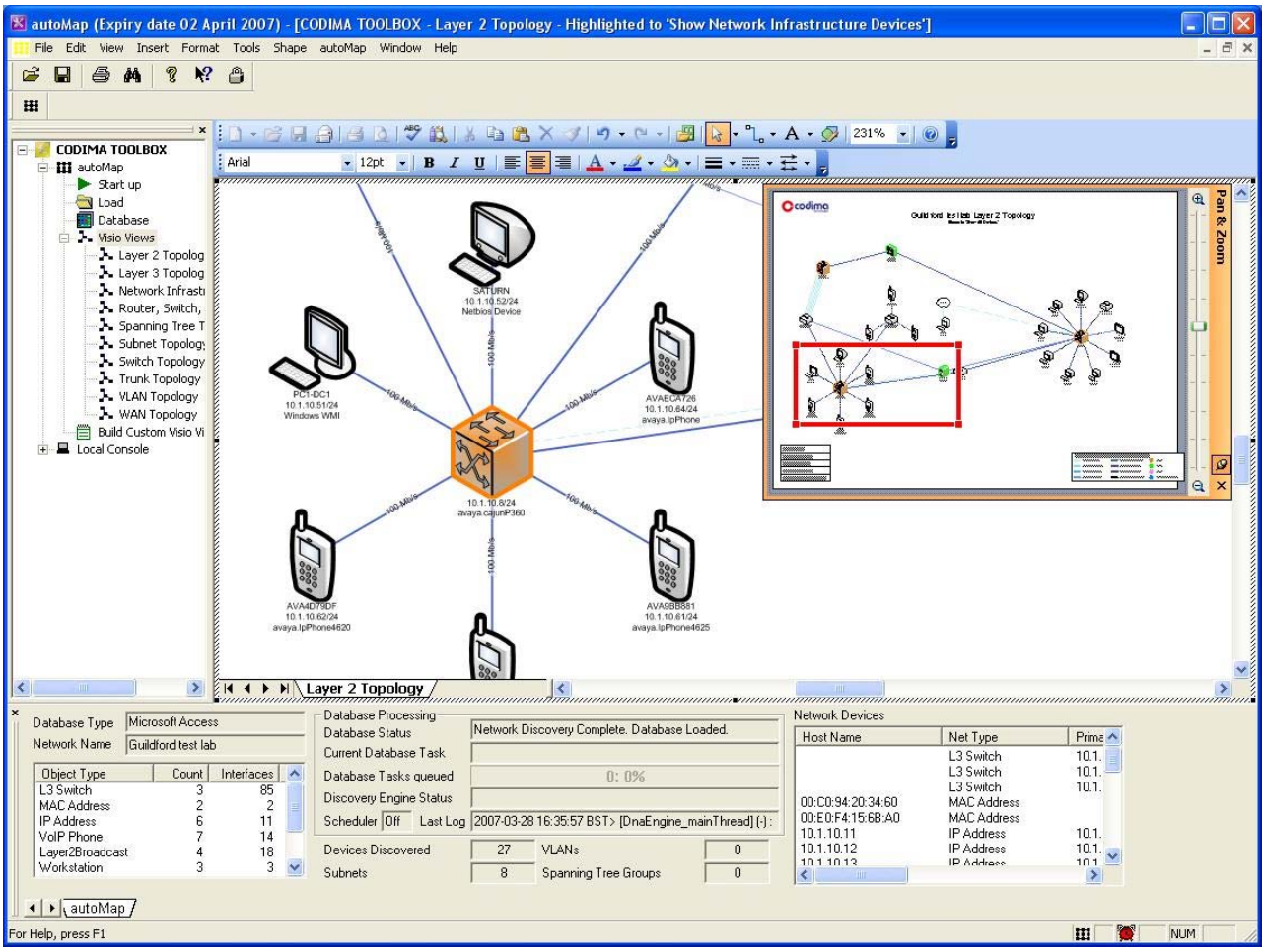


4.2. autoMap Discovery Results

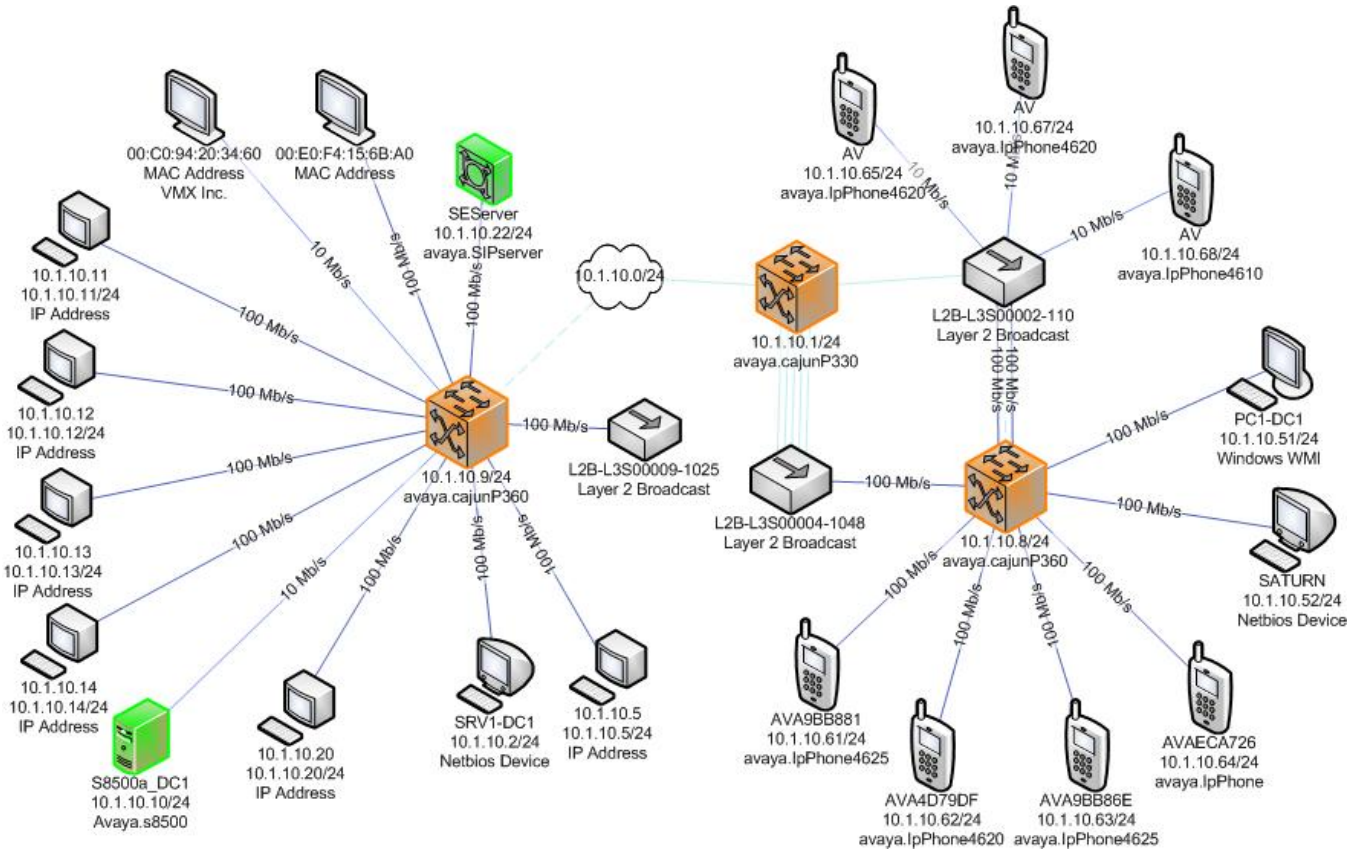
Once the discovery of the network has been completed, the **Database Status** in the **Database Processing** section will show the value “Database Loaded” and the results will be displayed in the **Network Devices** section. An example is shown below. The results include the number and types of devices found in the network, IP addresses, subnets, and MAC addresses.



Different topology views can be selected and displayed by clicking the options available under **Enterprise → autoMap → Visio Views**. Since autoMap uses Microsoft Visio to plot the network diagram, all the functionality available on Microsoft Visio can be used on the autoMap plotted network diagrams. An example is shown below.



An autoMap generated drawing is shown below and can be compared to **Figure 1**. Avaya G650 cards (IPSI, CLAN, MEDPRO, VAL) are shown as PC icons since only ping responses were received by autoMap. The MAC addresses found in the ARP table are also shown. autoMap creates a Layer 2 Broadcast object, based on a MAC address having only one connection to a switch or hub. The result is a Layer 2 Broadcast device (with a set of MAC addresses present on a trunk port that are not directly connected to any discovered managed switch).

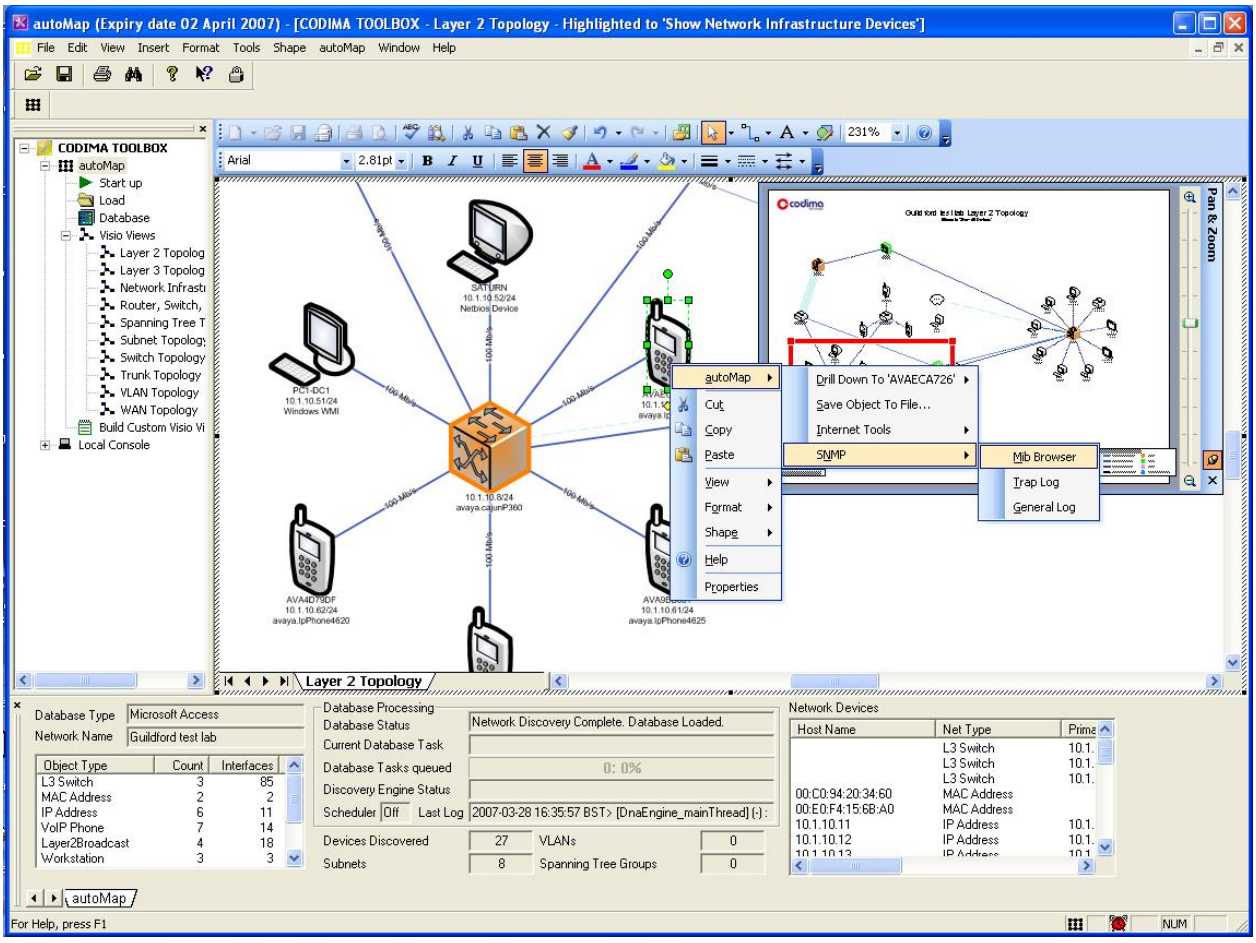


4.3. MIB Browser

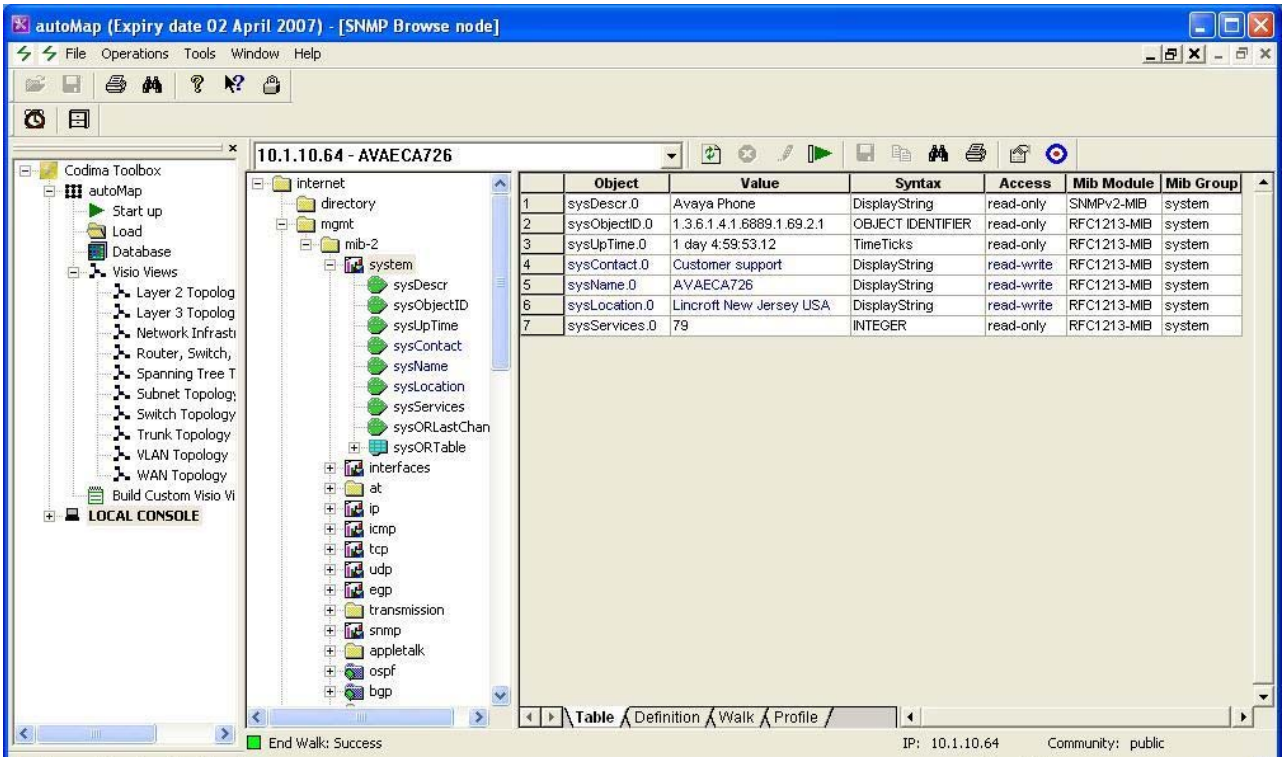
The MIB walk is used to establish what SNMP support is required on the network. Providing a MIB walk from the device itself is one way of customising the Codima discovery engine.

SNMP SIM generator is a tool to automate the MIB walk process and email results back to Codima Technologies. The tool is specifically designed to obtain information for the customisation of the Codima Discovery Engine used by the autoMap and autoAsset products.

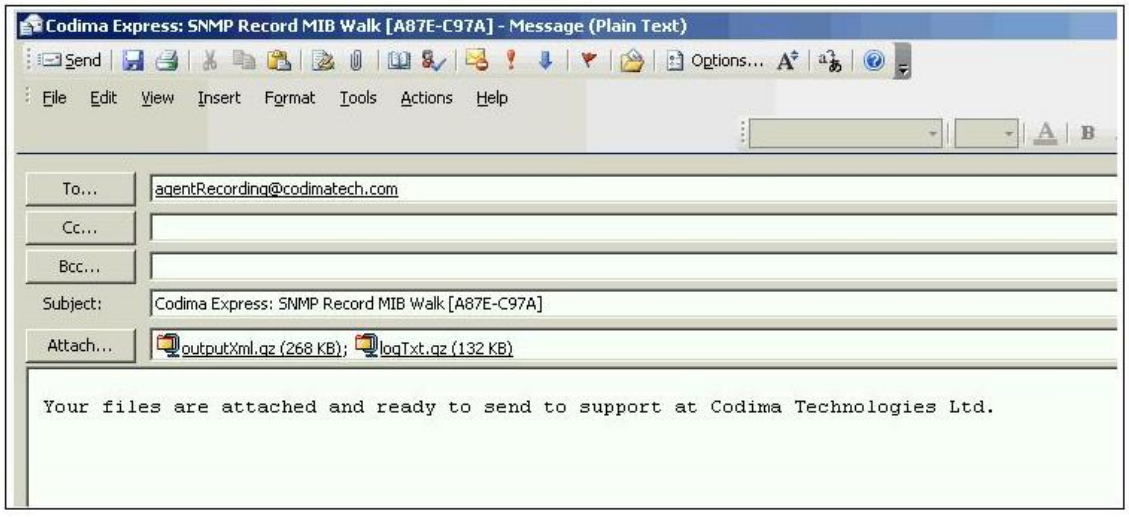
Select an autoMap Visio view that includes devices with IP addresses (e.g., layer 2 topology). Select the node to browse, right click and select **autoMap → SNMP → MIB Browser**.



Ensure the computer is connected to the internet and has email facilities installed. Click on the **green arrow** "Record and email simulation" button in the SNMP Browse Node window, or click on **Operations → Record Simulation** from the tool bar.

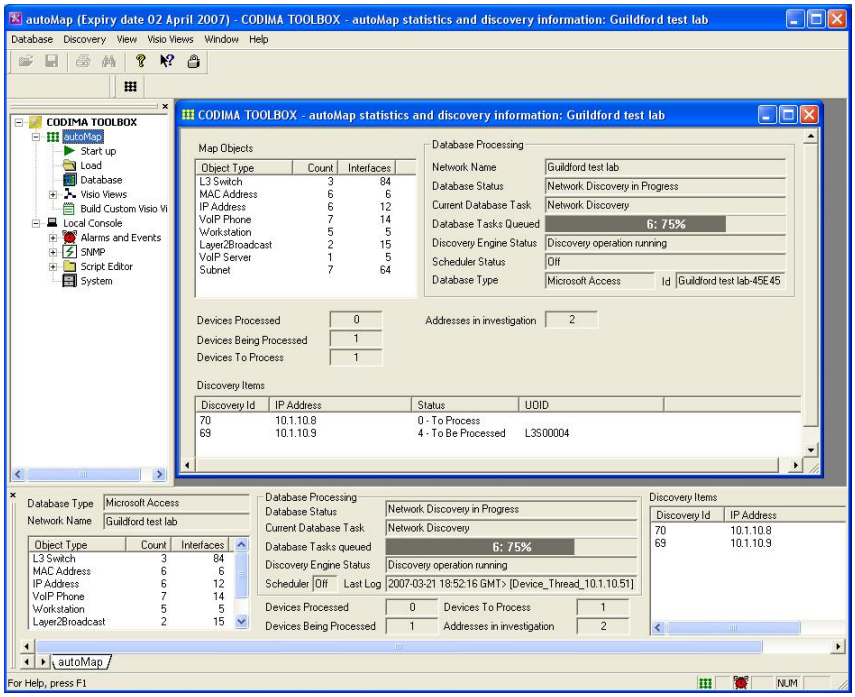


The process can take a few minutes. When the process is finished, the results are stored in a file that is automatically added to an email addressed to Codima. An example is shown below.



5. Verification Steps

When the discovery process has started successfully, the **Database Status** in the **Database Processing** section will show the value "Network Discovery in Progress" as shown below. Once the discovery process has been completed, the autoMap Visio diagram will be loaded 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 the Codima autoMap to accurately discover the compliance test network using SNMP, ICMP, NetBIOS and STP to generate a Visio diagram of the compliance-tested network. The serviceability tests included stopping and starting the discovery process.

6.1. General Test Approach

The feature test was performed by entering the seed device IP address and private SNMP community strings configured on Avaya Communication Manager, Avaya SES and Avaya IP Telephones and starting the autoMap discovery process. This tested the ability of autoMap to discover the compliance-tested network. Serviceability tests included stopping and starting the discovery process. Different topological views of the compliance-tested network generated Visio diagram were compared to the compliance test network diagram shown in **Figure 1**.

6.2. Test Results

All test cases were executed and passed. autoMap presently 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 required configuration steps for Codima autoMap 3.10 to successfully interoperate with Avaya Communication Manager, Avaya SES, Avaya C360-Series Converged Stackable Switches and Avaya IP Telephones. All test cases were completed successfully and the configuration described in these Application Notes has been successfully compliance tested.

9. Additional References

This section references the Avaya and Codima product documentation that are relevant to these Application Notes.

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.