



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 *DeveloperConnection* compliance testing and additional technical discussions. Testing was conducted via the *DeveloperConnection* 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.

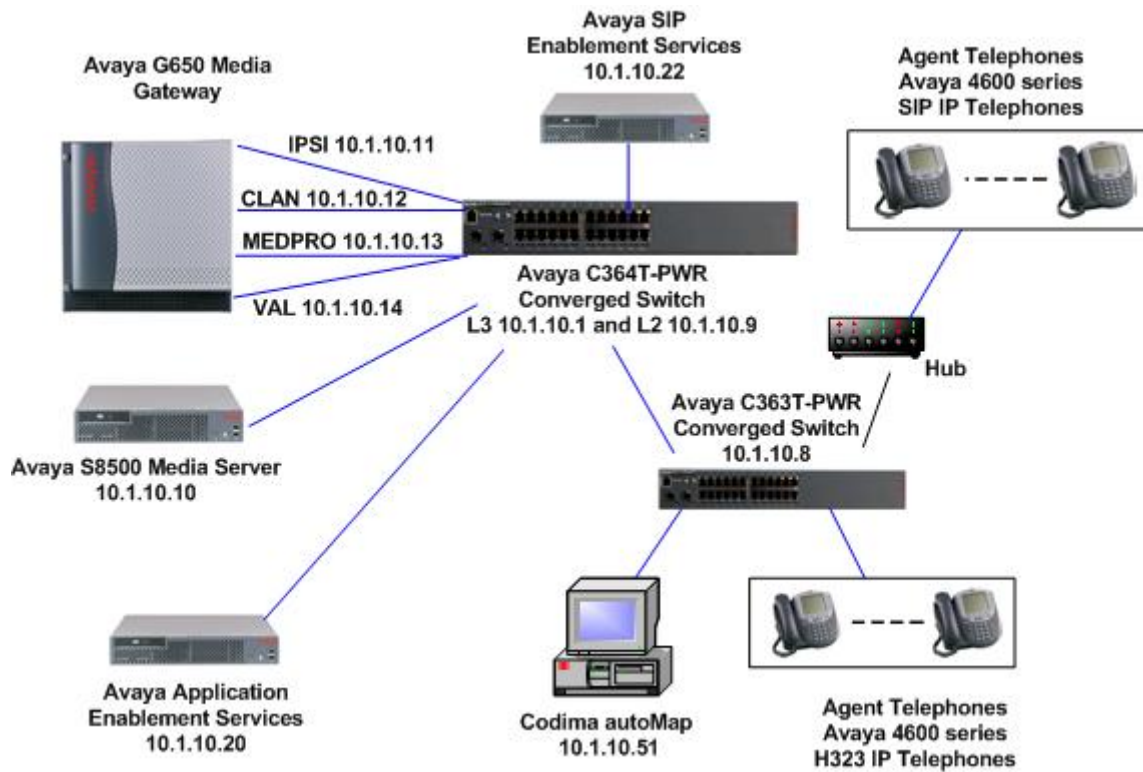


Figure 1: Avaya Test Network Infrastructure with Codima autoMap

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

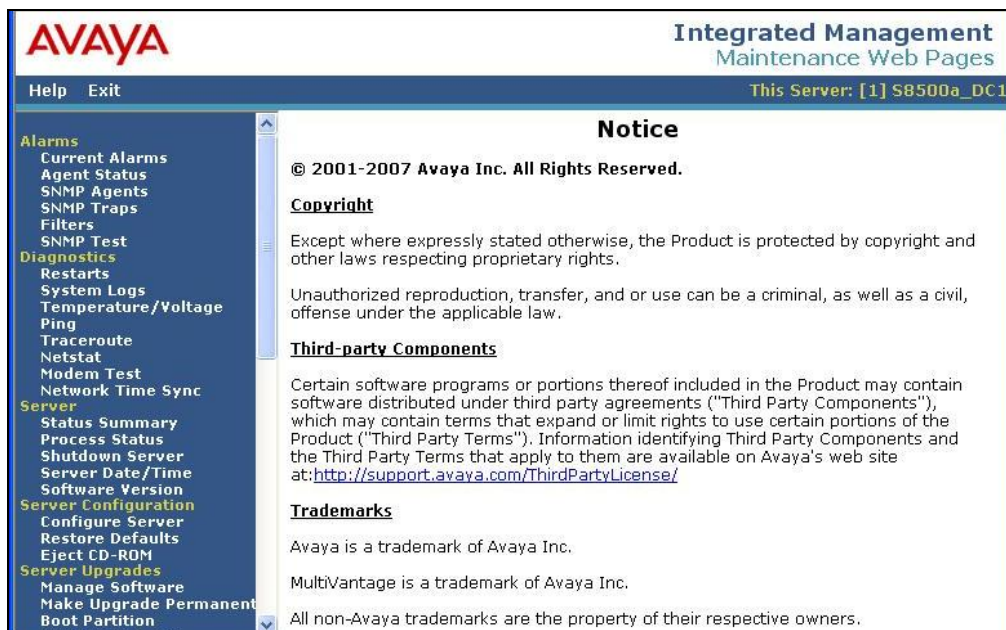
SNMP was enabled on Avaya Communication Manager, SES and Avaya IP telephones.

3.1. Configure SNMP on Avaya Communication Manager

Access the Avaya Communication Manager administration web interface, by entering `http://<ip-addr>/as` 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).

The screenshot displays the Avaya Integrated Management Maintenance Web Pages interface. The top header includes the Avaya logo, the title "Integrated Management Maintenance Web Pages", and the server identifier "This Server: [1] S8500a_DC1". A navigation menu on the left lists various system management functions under categories like Alarms, Diagnostics, Server, and Configuration. The main content area is titled "View G3-AVAYA-MIB Data" and shows the "Master Agent status: Up". Under the "IP Addresses for SNMP Access" section, the "Following IP addresses:" radio button is selected, and the "IP address1" field contains "10.1.10.51". The "SNMP Users / Communities" section has two checked options: "Enable SNMP Version 1" and "Enable SNMP Version 2c". For each, the "Community Name (read-only)" field is filled with "devconuk", while the "Community Name (read-write)" field is empty.

AVAYA Integrated Management Maintenance Web Pages
This Server: [1] S8500a_DC1

Help Exit

View G3-AVAYA-MIB Data
Master Agent status: Up

IP Addresses for SNMP Access

☐ No Access
☐ Any IP address
☒ Following IP addresses:

IP address1 : 10.1.10.51
IP address2 :
IP address3 :
IP address4 :
IP address5 :

SNMP Users / Communities

☒ Enable SNMP Version 1
Community Name (read-only) : devconuk
Community Name (read-write) :

☒ Enable SNMP Version 2c
Community Name (read-only) : devconuk
Community Name (read-write) :

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.

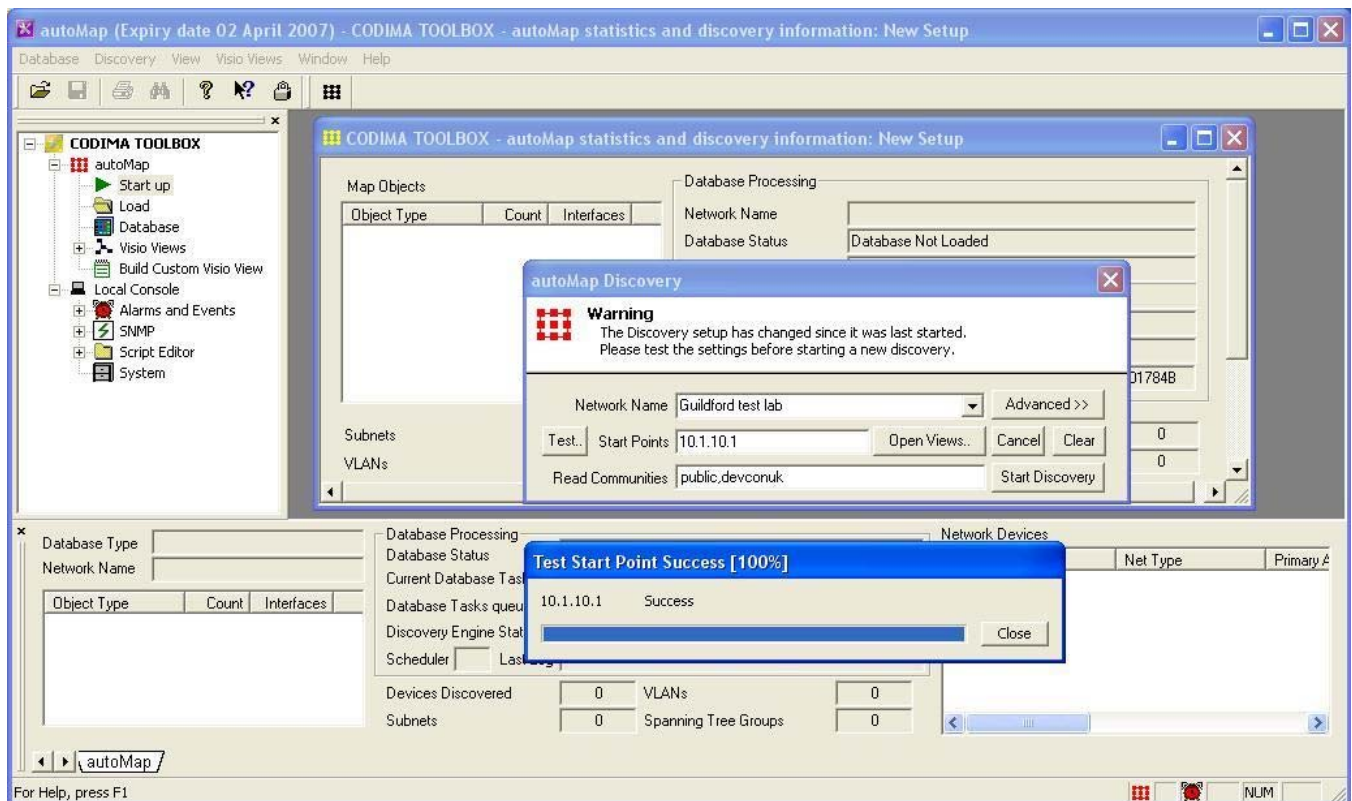
4.1. Configure autoMap Discovery

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.



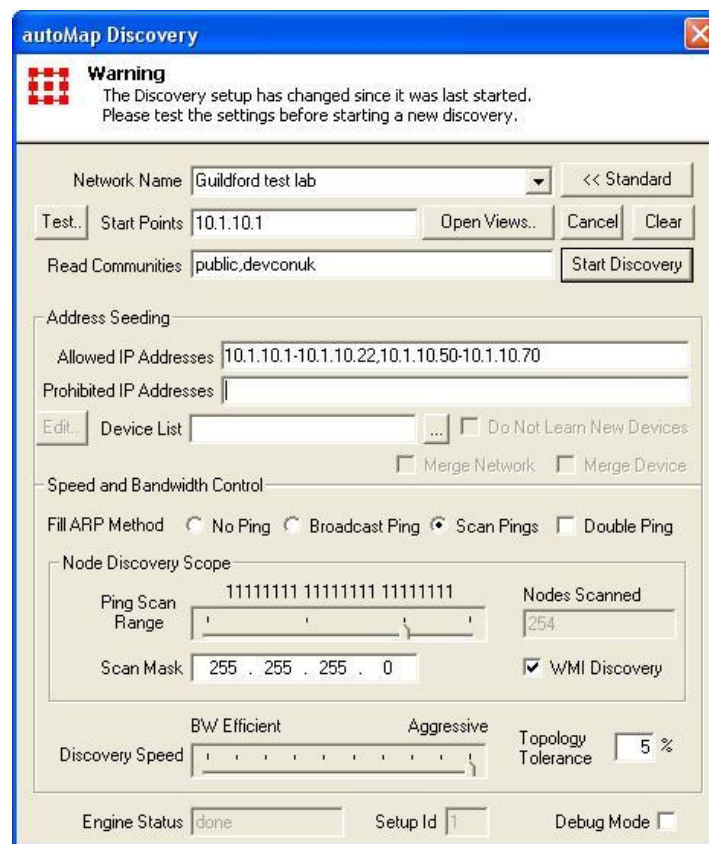
In the **autoMap View Selector** dialog box, check the boxes of the views to be displayed when the discovery of the network has finished. Click **OK**. In the **autoMap Discovery** dialog box shown above, click on the **Advanced** button.



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.

The screenshot displays the autoMap application window with the title "autoMap (Expiry date 02 April 2007) - CODIMA TOOLBOX - autoMap statistics and discovery information: Guildford test lab". The interface includes a menu bar (Database, Discovery, View, Visio Views, Window, Help), a toolbar, and a left-hand tree view under "CODIMA TOOLBOX" with options like Start up, Load, Database, and various Visio Views.

The main window is divided into several sections:

- Map Objects:** A table showing the count and interfaces for various object types.
- Database Processing:** A section showing the network name, database status, and various task and engine statistics.
- Network Devices:** A table listing discovered devices with their host names, net types, primary addresses, vendors, interfaces, and primary indices.
- Subnets and VLANs:** Summary statistics for subnets, VLANs, and spanning tree groups.
- Layer 2 Topology:** A visual diagram showing the network topology with various devices connected.

Map Objects Table:

Object Type	Count	Interfaces
L3 Switch	3	85
MAC Address	2	2
IP Address	6	11
VoIP Phone	7	14
Layer2Broadcast	4	18
Workstation	3	3
Server	1	5
VoIP Server	1	5
Subnet	8	59

Database Processing Section:

- Network Name: Guildford test lab
- Database Status: Network Discovery Complete. Database Loaded.
- Current Database Task: [Empty]
- Database Tasks Queued: 0: 0%
- Discovery Engine Status: [Empty]
- Scheduler Status: Off
- Database Type: Microsoft Access
- Id: Guildford test lab-460A5

Subnets and VLANs Summary:

Subnets	VLANs	Spanning Tree Groups
8	0	0

Network Devices Table:

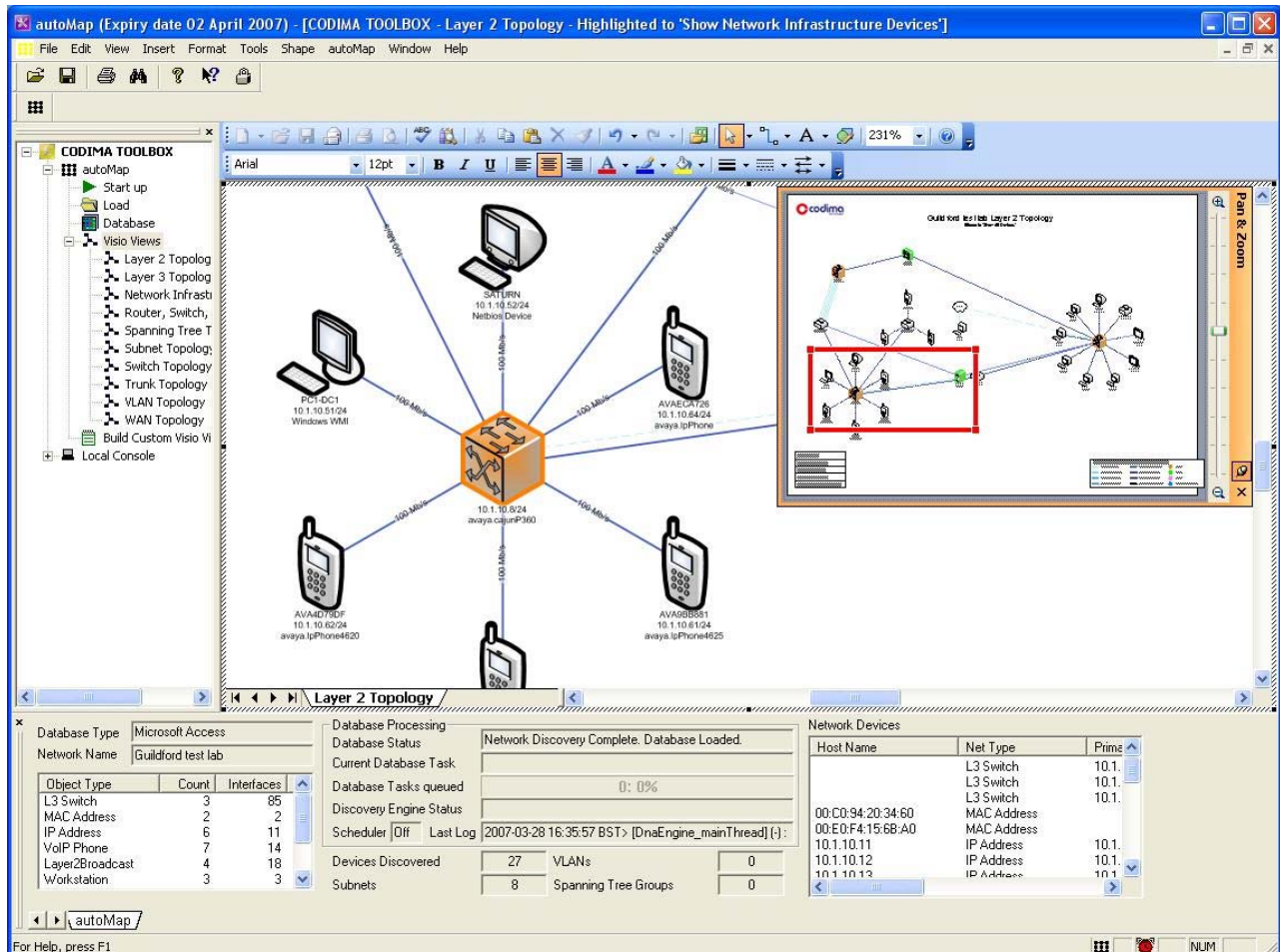
Host Name	Net Type	Primary Address	Vendor	Interfaces	Primary Index
	L3 Switch	10.1.10.8	Lucent Technologies	27	100
	L3 Switch	10.1.10.9	Lucent Technologies	51	100
	L3 Switch	10.1.10.1	Lucent Technologies	7	110
00:C0:94:20:34:60	MAC Address		VMX Inc.	1	

Bottom Panel Summary:

- Database Type: Microsoft Access
- Network Name: Guildford test lab
- Database Processing: Network Discovery Complete. Database Loaded.
- Current Database Task: [Empty]
- Database Tasks queued: 0: 0%
- Discovery Engine Status: [Empty]
- Scheduler: Off
- Last Log: 2007-03-28 16:35:57 BST> [DnaEngine_mainThread] (-):
- Devices Discovered: 27
- VLANs: 0
- Subnets: 8
- Spanning Tree Groups: 0

The bottom right corner shows a visual representation of the network topology with various devices connected.

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.



The diagram illustrates a complex network topology. At the center is a switch labeled '10.1.10.9/24 avaya.cajunP360'. It is connected to several other components:

- Left Side:** A group of desktop computers with IP addresses 10.1.10.11 through 10.1.10.14. Two servers are also connected: 'SEServer 10.1.10.22/24 avaya.SIPserver' and 'SR500a_DC1 10.1.10.14/24 Avaya.s8500'. Connections are labeled with speeds like '100 Mb/s' and '10 Mb/s'.
- Top:** A cloud representing a network segment '0.1.10.0/24'.
- Right Side:** A switch labeled '10.1.10.1/24 avaya.cajunP330' is connected to a 'Layer 2 Broadcast' device 'L2B-L3S000002-110'. Below it, another switch '10.1.10.8/24 avaya.cajunP360' is connected to another 'Layer 2 Broadcast' device 'L2B-L3S000004-1048'. This switch is also connected to various mobile phones (AV) and a PC labeled 'PC1-DC1 10.1.10.51/24 Windows WMI'.
- Bottom:** A switch labeled '10.1.10.5/24 IP Address' is connected to a 'Netbios Device' 'SRV1-DC1 10.1.10.2/24' and another 'Netbios Device' 'SATURN 10.1.10.52/24'.

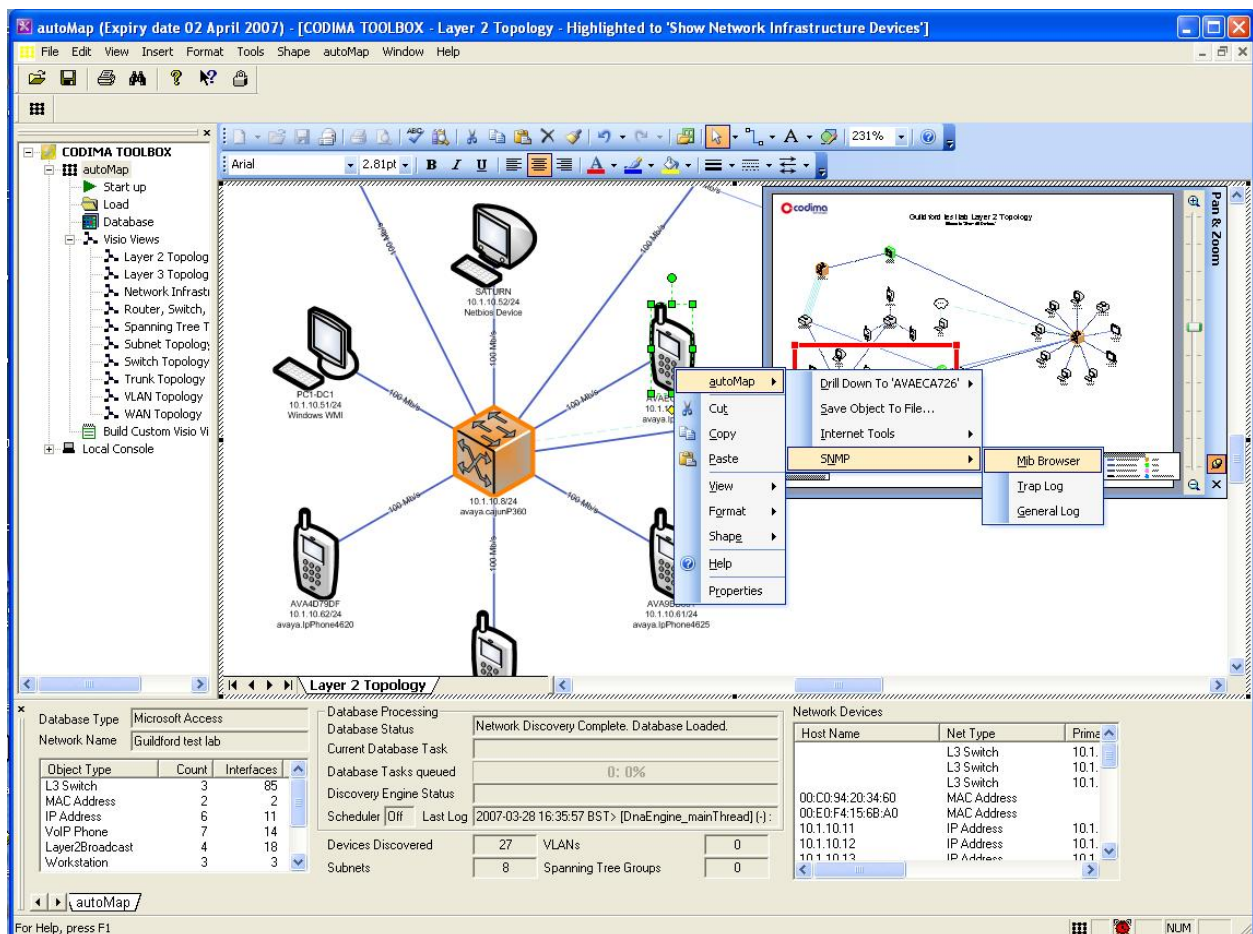
The diagram uses various icons to represent different device types: desktop monitors for PCs, server racks for servers, clouds for network segments, and mobile phone icons for AV devices. Lines with arrows indicate the direction and speed of data flow between these components.

4.3. MIB Browser

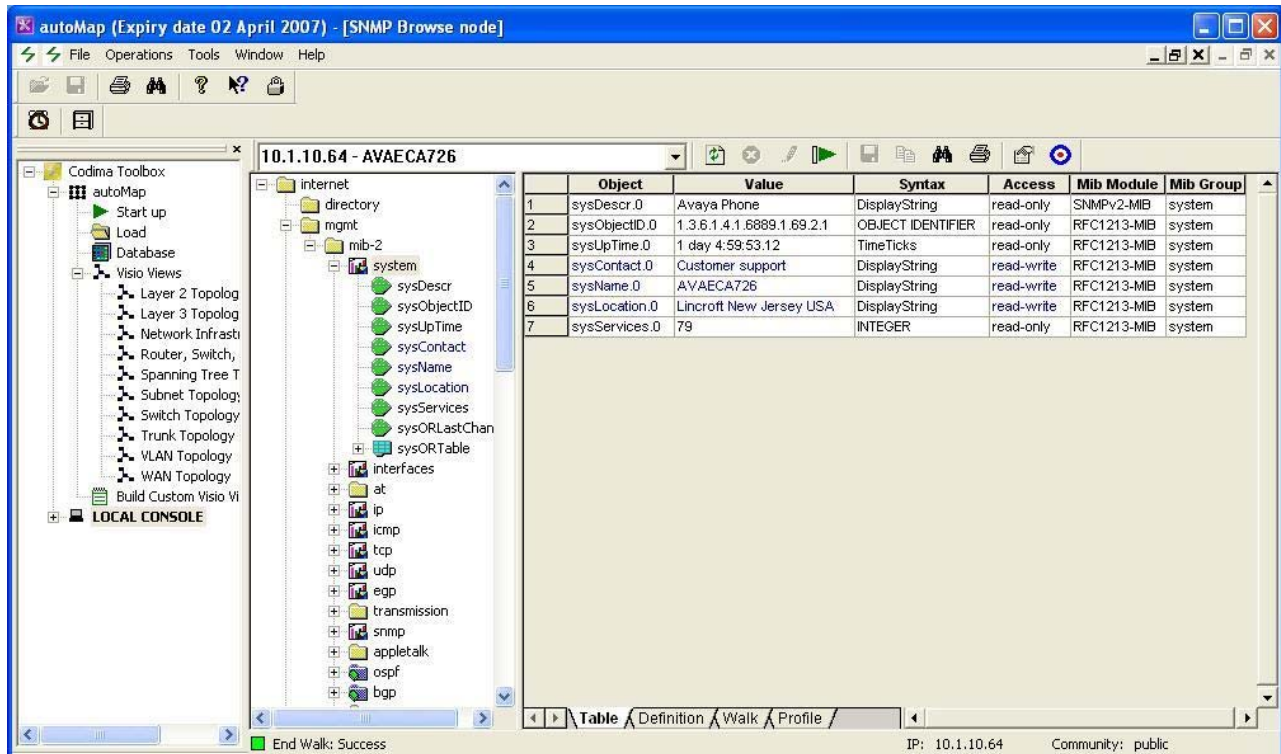
The MIB walk is used to establish what SNMP support is required on the network. Providing a MIB walk from the device itself is one way of customising the Codima discovery engine.

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.

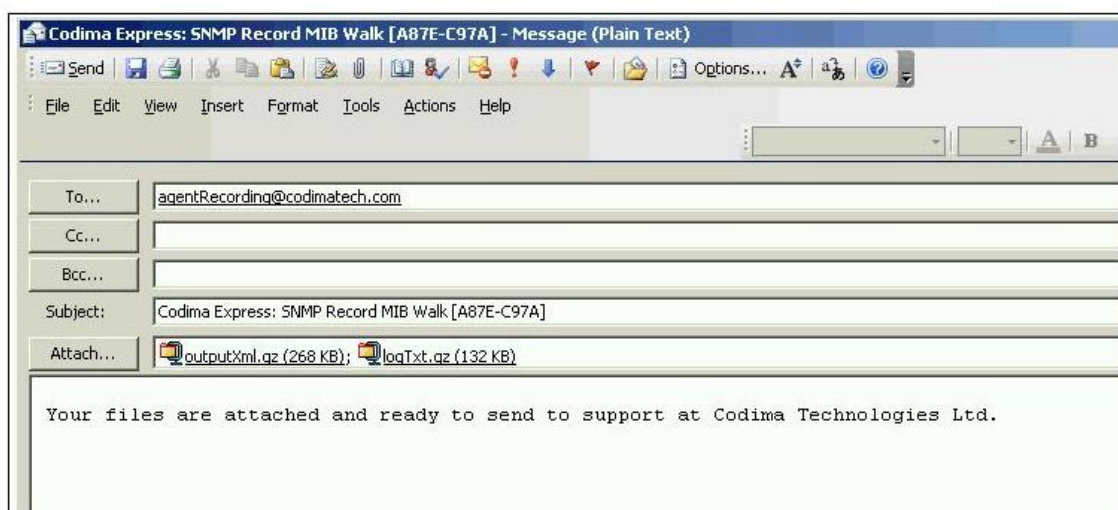
Select an autoMap Visio view that includes devices with IP addresses (e.g., layer 2 topology). Select the node to browse, right click and select **autoMap → SNMP → MIB Browser**.



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.

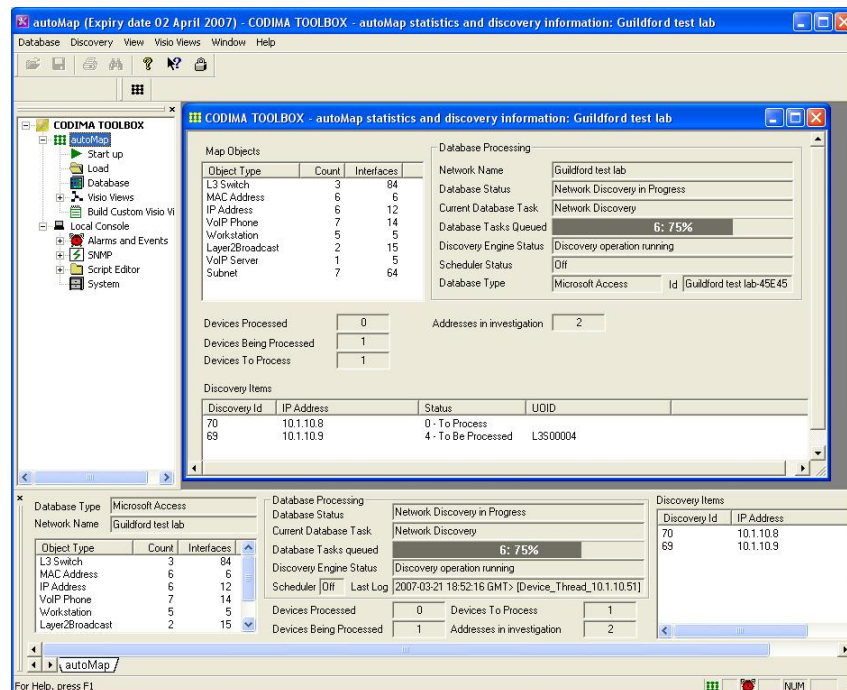


The process can take a few minutes. When the process is finished, the results are stored in a file that is automatically added to an email addressed to Codima. An example is shown below.



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>

©2007 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 DeveloperConnection Program at devconnect@avaya.com.