OPTIMIZE

MERCURY APPLICATION MAPPING™

Discovery Process Tutorial

MERCURY™

BUSINESS TECHNOLOGY OPTIMIZATION

Mercury Application Mapping

Discovery Process Tutorial

Version 6.2

Document Release Date: August 1, 2006

MERCURY™

Mercury Application Mapping Discovery Process Tutorial, Version 6.2

Mercury Interactive Corporation
379 North Whisman Road
Mountain View, CA 94043
Tel: (650) 603-5200
Toll Free: (800) TEST-911
Customer Support: (877) TEST-HLP
Fax: (650) 603-5300

If you have any comments or suggestions regarding this document, please send them by e-mail to documentation@mercury.com.

MAMDPT6.2/02

Table of Contents

Welcome to this Tutorial

Welcome to the Mercury Application Mapping Discovery Process Tutorial, a self-paced guide that teaches you how to run the discovery process.

This tutorial instructs you on how to discover the IT resources in your system. It takes you through a gradual discovery process, from the most basic network discovery to more in-depth discoveries such as applications, databases and servers.

Before You Begin

To do this tutorial, you must have Mercury Application Mapping operational. The Mercury Application Mapping server and Discovery Probe must be preconfigured and running. You must also have access to the Mercury Application Mapping user interface to activate the discovery patterns.

Using This Tutorial

This tutorial contains the following lessons:

Lesson 1 Introducing the Discovery Process

Introduces you to the discovery process, discovery patterns and the Configuration Item Type Model.

Lesson 2 Defining the Seed Network

Shows you how to define the seed network from which to start the discovery process.

Lesson 3 Discovering Network CIs

Shows you how to activate the discovery pattern **ICMP_NET_Dis_IpC**, which is designed to discover the networks that fall within the defined IP address range.

Lesson 4 Creating a TQL Query

Shows you how to define a TQL query that retrieves specified network CIs from the Mercury Universal CMDB.

Lesson 5 Performing an Advanced Network Discovery

Shows you how to activate a task whose job it is to discover SNMP connection data of the new IPs discovered in your IT infrastructure.

Lesson 6 Expanding the Network Discovery

Shows you how to expand the network discovery to include the discovery of other network resources such as ARP tables and TCP connections.

Lesson 7 Discovering Database Instances and Oracle Resources

Shows you how to discover the database instances and Oracle resources in your IT infrastructure.

Lesson 8 Discovering WebLogic Instances and Components

Shows you how to uncover WebLogic instances and WebLogic components in your IT infrastructure.

Lesson 9 Discovering Host Resources

Shows you how to activate a number of patterns that discover WMI-based resources, such as disks, CPU, memory, or files.

1

Introducing the Discovery Process

The Mercury Application Mapping discovery process is the mechanism that enables you to collect data about your system by discovering the IT infrastructure resources and their interdependencies. It can discover such resources as applications, databases, network devices, different types of servers, and so forth. Each discovered IT resource is then delivered and stored in the Mercury Universal CMDB where it is represented as a managed CI.

The Mercury Application Mapping discovery process is run by activating discovery patterns.

In this lesson, you will learn about the following:

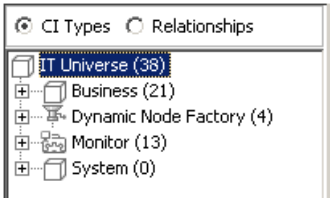
What Is a Discovery Pattern?

A discovery pattern is an XML file that defines a discovery task. The discovery pattern contains a description of the CIs and relationships that are created when the discovery pattern is run. The definitions of the CIs and relationships are taken from the Configuration Item Type Model, which contains the definitions of all CIT and relationship types. When the discovery pattern is activated, it discovers instances of CIs and relationships of the types that are described in each pattern, and places them in the CMDB.

What Is the Configuration Item Type Model?

By default, the Configuration Item Type Model (as seen in the CI Type Manager tab in Mercury Application Mapping) is divided into two logical groups.

- CI Types
- Relationships



The Configuration Item Type Model contains the definitions of all the CITs defined in the system and the relationships that define the connection between them. Each CIT has its own attributes, as well as the attributes inherited from its parent CIT. The discovery process uncovers CIs and relationships according to the attributes defined in the Configuration Item Type Model. For information on the Configuration Item Type Model, see the *Mercury Application Mapping User's Guide*.

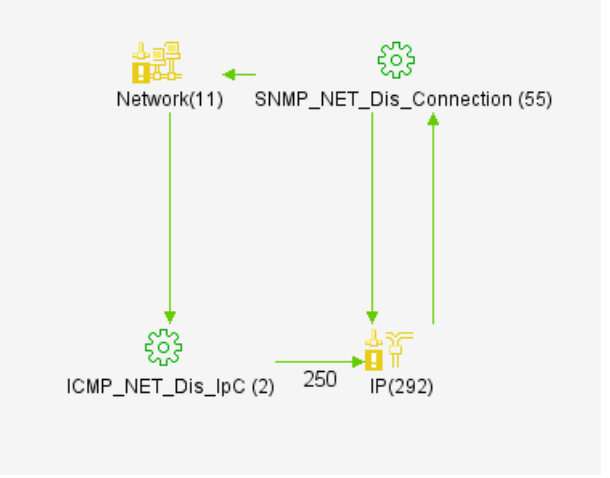
Note: The CIT definitions that appear in the Configuration Item Type Model depend on which packages were deployed. For information on packages, refer to "Package Administration Overview" in the *Mercury Application Mapping Administration Guide*.

Running the Discovery Process

The discovery process is a gradual uncovering of the elements in your system. Discovery is first done at the most basic level, and then at more in-depth ones.

After you have installed all the Mercury Application Mapping components (see "Launching Mercury Application Mapping Components" on page 6), the network in which the Discovery Probe is located, the Host on which the Discovery Probe resides, and the Host's IP address are automatically discovered. These discovered CIs are then placed in the CMDB. They act as triggers that activate a discovery pattern. Every time a discovery pattern is activated, it discovers more CIs, which in turn are used as triggers for other discovery patterns. This process continues until your entire IT infrastructure is discovered and mapped.

In the following example, the CI **Network** is a trigger that activates the **ICMP_NET_Dis_Ipc** pattern. The **ICMP_NET_Dis_Ipc** pattern then discovers 292 instances of IP addresses. These discovered IP addresses act as a trigger that activates the **SNMP_NET_Dis_Connection** pattern, which in turn discovers more IP addresses and **Network** CIs. The discovery process ends when all the IP address included in the range defined for the Discovery Probe are discovered.

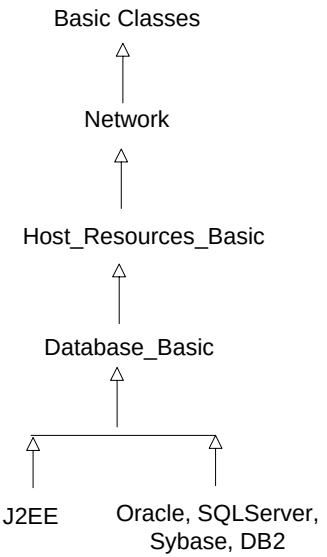


Packages That Need Deploying for This Tutorial

The following table lists all the packages you need to deploy for this tutorial. The packages are located in:
<Mercury Application Mapping root directory>\root\lib\packages.

Package	Description
Network.zip	Includes all the resources needed for discovering the network structure and components.
Database_Basic.zip	Includes all the basic resources needed for discovering databases.
Oracle.zip	Includes all the resources needed for discovering an Oracle database.
SQL_Server.zip	Includes all the resources related to a Microsoft SQL database.
J2EE.zip	Includes all the resources needed for discovering application servers using the J2EE platform.

The following diagram displays the dependency among the deployed packages.



Launching Mercury Application Mapping Components

To successfully use Mercury Application Mapping's discovery system, run the following Mercury Application Mapping components:

- The Mercury Application Mapping Server
- The Discovery Probe
- The Mercury Application Mapping main window

Note: You must launch the Mercury Application Mapping Server first

---

This section contains the following topics:

Launching the Mercury Application Mapping server

This section describes how to launch the Mercury Application Mapping server.

To launch the Mercury Application Mapping server:

Select **Start** > **Programs** > **MAM** > **Start J2F**. This **Start J2F** icon appears in the bottom, right-hand corner of your screen.

The **Start J2F**icon turns into this icon when the following appears in the **jboss_boot.log** file located in **<Mercury Application Mapping root directory> J2F\log**:

- The words **server is up** to indicate that the server has been successfully launched.
- The text that indicates that packages have been successfully loaded. For example:

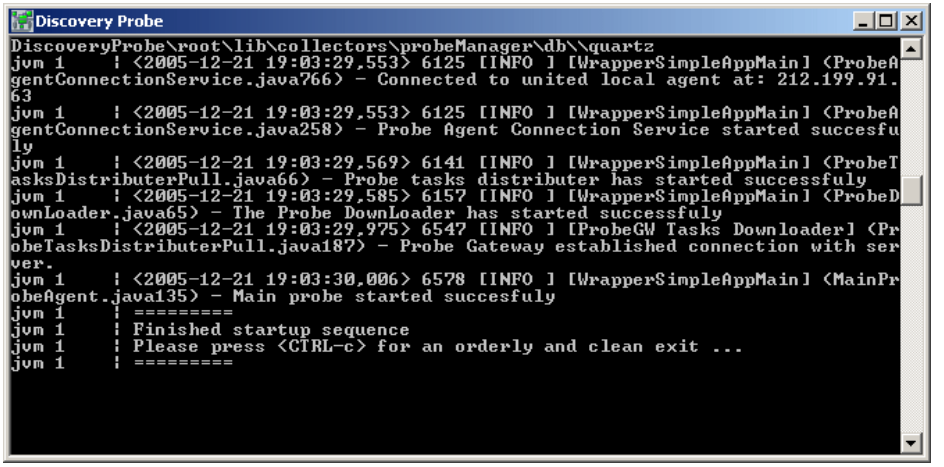
  JBoss_3_2_6 date=200410140106)] Started in 4m:18s:47ms

Launching the Discovery Probe

This section explains how to launch the Discovery Probe.

To launch the Discovery Probe:

Select **Start** > **Programs** > **MAM** > **Discovery Probe** to open the Discovery Probe window.



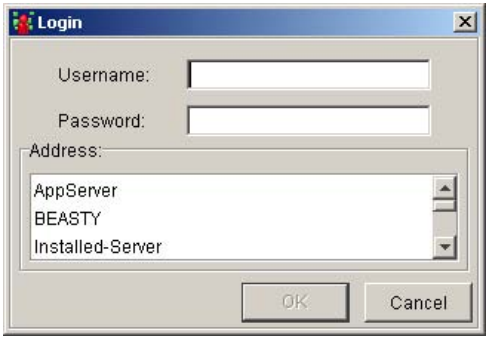
The appearance of the words **Main probe started successfully** indicates that the Discovery Probe has been launched successfully.

Launching the Mercury Application Mapping User Interface

This section explains how to launch the Mercury Application Mapping user interface.

To launch the Mercury Application Mapping user interface:

1 Select **Start** > **Programs** > **MAM** > **MAM** to open the Login dialog box.

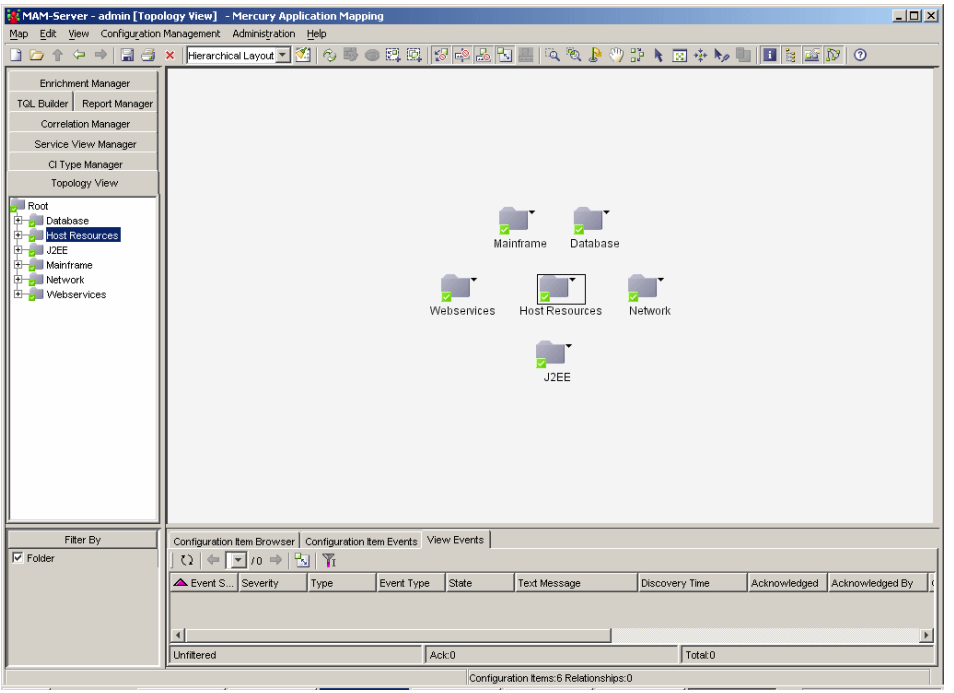


2 In the **Username** box, enter your assigned username.

3 In the **Password** box, enter your password.

4 In the **Address** box, select the server to which you want to connect.

5 Click **OK** to open the Mercury Application Mapping main window.



2

Defining the Seed Network

Once the Mercury Application Mapping server and the Discovery Probe are connected to a new IT environment, Mercury Application Mapping automatically identifies the following CIs:

- The network in which the Discovery Probe is located
- The host on which the Discovery Probe resides
- The host's IP address

These CIs are then placed into the CMDB.

Before you can begin the discovery process, you must define the seed network from which to start the process. You can either perform the discovery process by using the seed network that is already in the CMDB by default after installing Mercury Application Mapping, or define one by manually adding a CI to the CMDB.

If you want to begin the discovery process with the network that is defined in the Discovery Probe, you can use the default seed network. If you want to begin the discovery process with another network, you can define your own seed network. For information on how to define another seed network, see "Inserting a CI Manually" on page 12.

In this lesson, you will learn about:

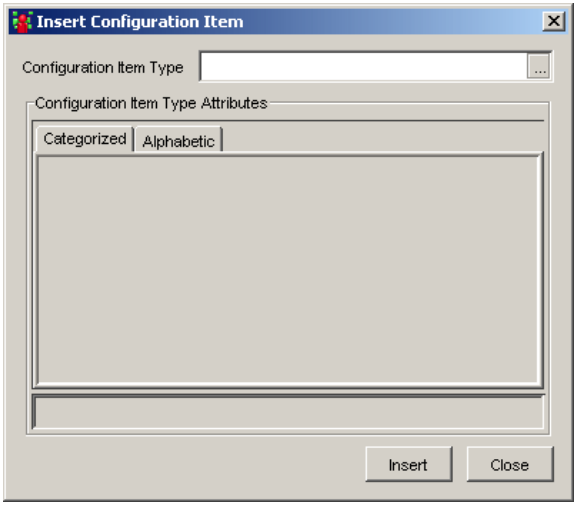
Inserting a CI Manually

To perform a discovery, you need to choose a seed network from which to perform the discovery process. You can either use the default seed network or define a new one manually.

In this exercise, you will define the seed network manually and then configure its attributes.

To define a seed network:

1 Select **Edit** > **Insert Configuration Items** to open the Insert Configuration Item dialog box.



2 Click the button at the end of the **Configuration Type** box to display the CIT Model tree.

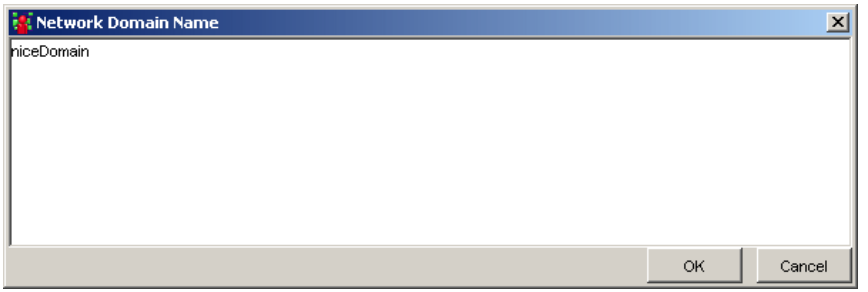
3 Select **Network** and click **OK** to display the CIT attributes.

Note: To find **network** within the CI Type Model tree, press **n** on your keyboard until **network** is selected.

---

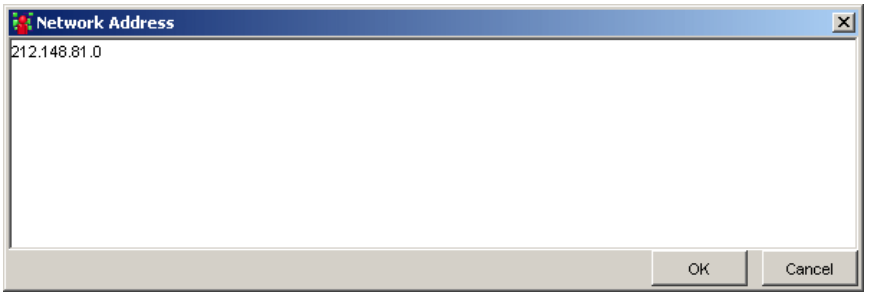
4 In the **Categorized** tab, click the **Expand** button to view all the attributes in the **network** CIT.

5 Click the button to the right of the **Network Domain Name** field and type the name of the domain as you defined it during installation. For this exercise, type niceDomain.



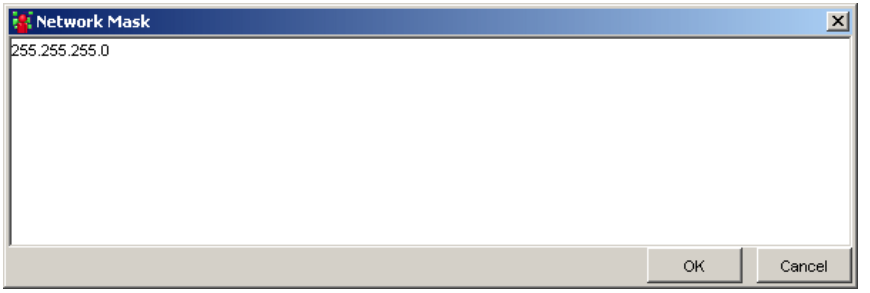
6 Click **OK** to save your changes.

7 Click the button to the right of the **Network Address** field and type the IP address of the seed network from which you want to start the discovery. For example, 212.148.81.0.



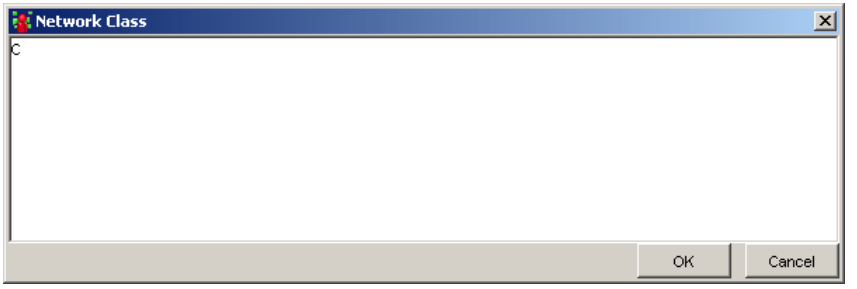
8 Click **OK** to save your changes.

9 Click the button to the right to the **Network Mask** field and type the net mask of the network for which you want to do the discovery. For example, 255.255.255.0



10 Click **OK**.

11 Click the button to the right to the **Network Class** field and enter the following network type. For example, C.



12 Click **OK**.

13 Click **Insert** in the Insert Configuration Item dialog to save the network attributes you have defined.

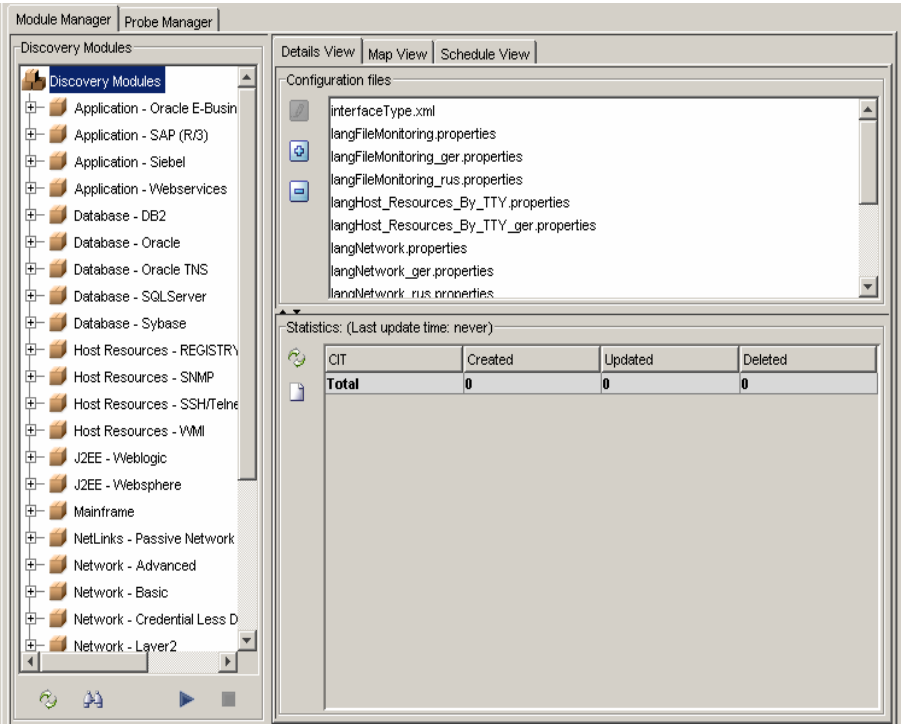
Defining the Discovery Scope

Before you activate the discovery patterns to start collecting data about your network, you need to add a Discovery Probe. For each Discovery Probe, you need to define the discovery scope that defines the range of the IP addresses to be discovered as well as configure the connection data for each protocol included in the discovery process.

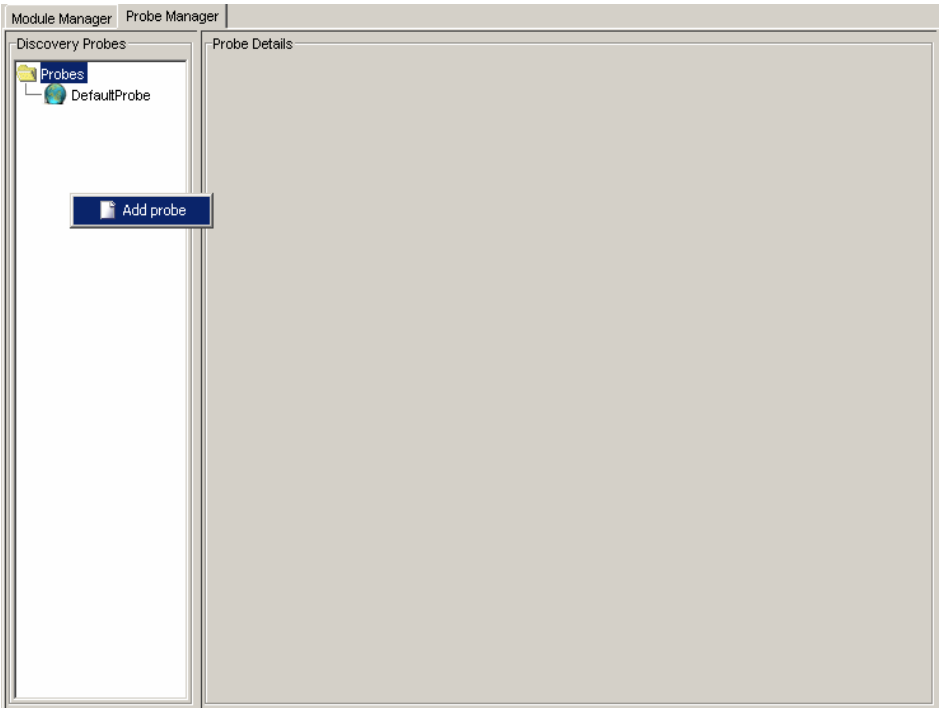
The discovery process can encompass several Discovery Probes. You need to define a separate range for each Discovery Probe. Anything discovered by the discovery patterns outside of the defined range is not included in the discovery process.

To configure the discovery scope:

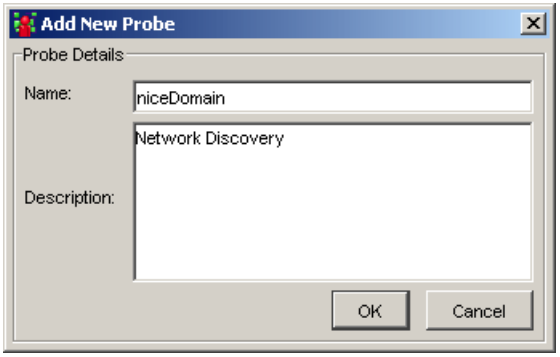
1 Select **Administration** > **Discovery Manager** to open the Discovery Manager.



2 To add a new Discovery Probe, click the **Probe Manager** tab.



3 In the Discovery Probes pane, right-click the **Probes** folder or any empty area and select **Add probe** to open the Add New Probe dialog box.

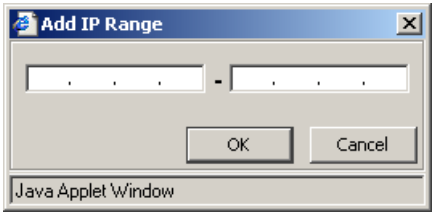


4 In the **Name** box, type the name of the Discovery Probe as defined during the installation. For example, niceDomain.

5 In the **Description** box, type description for the Discovery Probe. For this exercise, write Network discovery.

6 Click **OK** to save your changes.

7 Click the **Add IP range** button to open the Add Range dialog box.



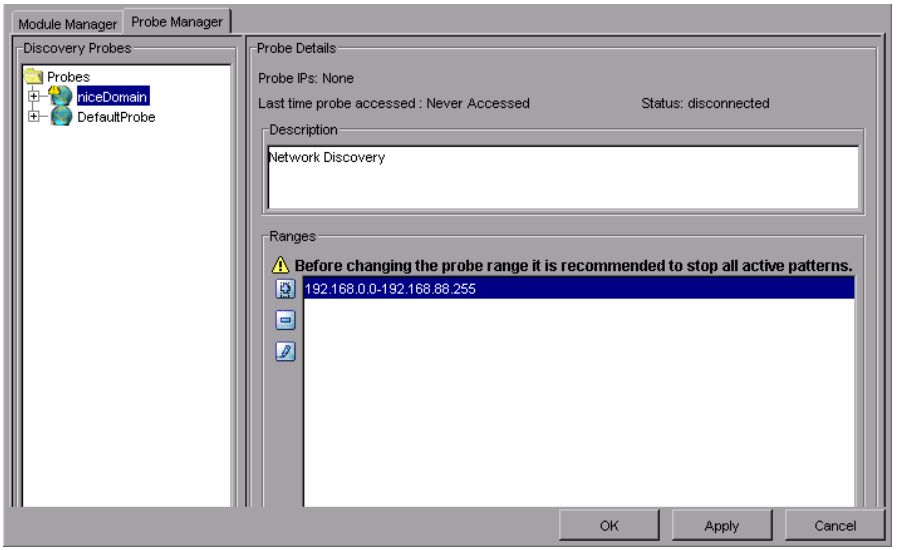
8 Enter an IP address range using the following format:

start_ip_address - end_ip_address

Note: The IP address range can include a wild card character (*) in the lower bound IP address of the IP range pattern. The asterisk represents any number in the range of 0-255. If you use an asterisk, you do not need to enter a second IP address. For example, 10.0.48.* covers the whole range from 10.0.48.0 to 10.0.48.255.

---

9 Click **OK**. The full IP address range appears in the **Ranges** pane, as seen below.

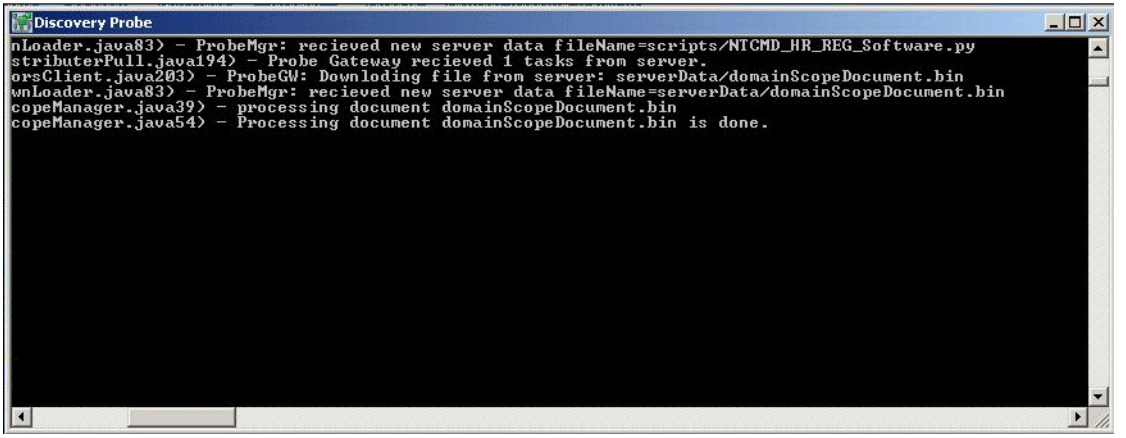


10 Click **Apply** to save the changes you made in the discovery scope configurations in the CMDB.

Verifying that the Changes Have Been Made to the Discovery Probe

The changes you made in the discovery scope configurations are delivered to and stored in the CMDB. From there, the changes are sent to the Discovery Probe. Verification that the changes have been sent to the Discovery Probe is seen in the following message displayed in the **wrapperProbe log** file, that is located in \<**Mercury Application Mapping Discovery Probe Installation directory**>**root****logs**\.

processing document domainScopeDocument.bin
Processing document domainScopeDocument.bin is done.



In the next lesson, you will activate the discovery pattern that discovers the networks contained within the range defined in this lesson.

3

Discovering Network CIs

The network CIs that were discovered in the previous lesson (see "Defining the Seed Network" on page 11) act as triggers for the continued discovery of other resources. This applies regardless of whether the default seed network was used to start the discovery or one was defined manually.

In order for the discovered network CIs in the CMDB to act as triggers for discovering other resources, the relevant discovery patterns must be activated.

In this lesson, you will activate the discovery pattern **ICMP_NET_Dis_IpC**, which is designed to discover the network IPs that fall within the IP address range as defined in the Discovery Manager dialog box in "Defining the Discovery Scope" on page 15.

In this lesson, you will learn about:

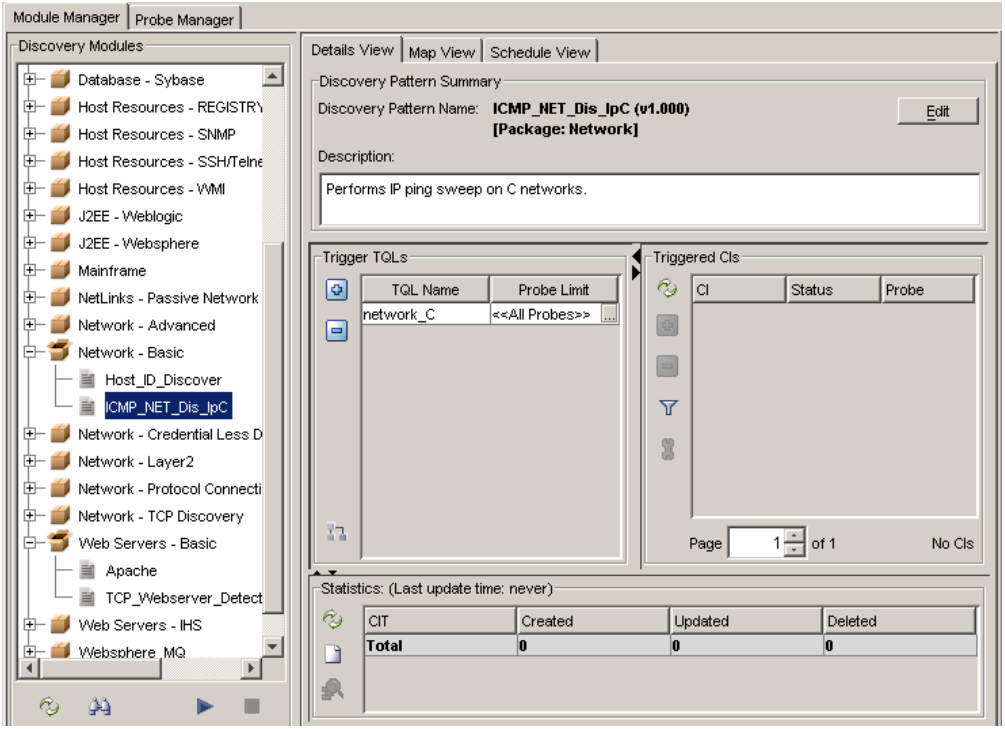
Activating the ICMP_NET_Dis_IpC Discovery Pattern

In this section, you will activate the **ICMP_NET_Dis_IpC** pattern. To activate discovery patterns, you must select the relevant patterns from the Discovery Manager.

To activate the ICMP_NET_Dis_IpC pattern:

1 Select **Administration** > **Discovery Manager** to open the Discovery Manager.

2 Click the **Expand** button to the left of the **Network - Basic** module.



3 Right-click **ICMP_NET_Dis_IpC** and select **Activate** to activate the pattern. A green dot appears on the pattern icon to indicate that is is activated.

What Happens When You Activate the ICMP_NET_Dis_IpC Pattern?

For every network in the CMDB, Mercury Application Mapping takes the network address and the network mask and calculates the range of the IP addresses you want to discover.

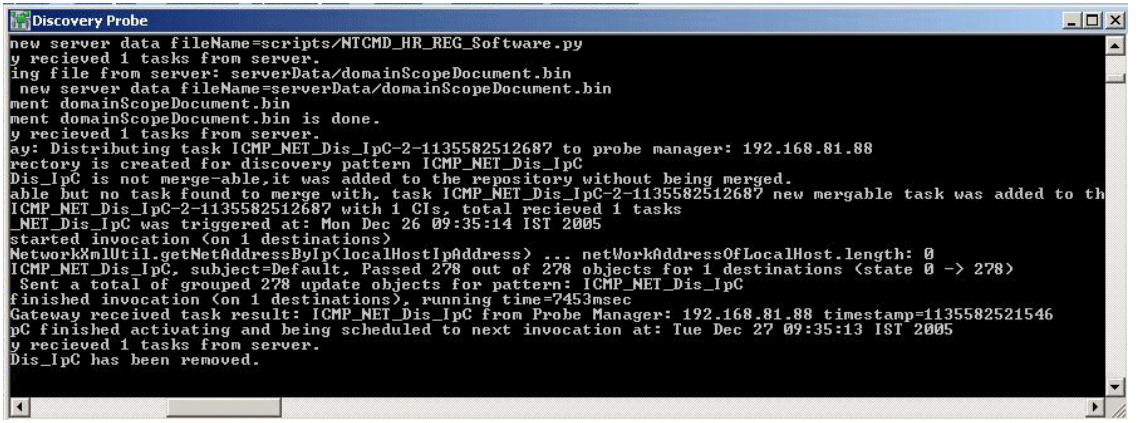
This pattern then activates a task whose job is to ping all the IP addresses that were calculated. For every IP address that answers the ping request, Mercury Application Mapping creates a CI in the CMDB.

Note: Only the IP addresses that are considered to be inside the scope defined in the Discovery Manager dialog box will be pinged.

By identifying the network's IPs, new IPs are discovered on the network. All IP addresses that respond to the ping request are the newly discovered CIs that are added to the CMDB which, in turn, act as triggers to activate other discovery patterns.

Verifying the Discovery Results

CIs that are discovered are delivered to and stored in the CMDB. Verification that the CIs have been sent to the CMDB can be seen here.



The Discovery Probe indicates that the name of the pattern that was activated and the number of network CIs discovered.

This example shows that the **ICMP_NET_Dis_IpC** discovery pattern was activated and 278 CIs were discovered.

In the next lesson, you will define a TQL that retrieves the network CIs from the CMDB so you can see the results of the discovery.

4

Creating a TQL Query

In the previous lesson, you activated the discovery pattern that discovered the networks that fell within the IP address range you defined in“Creating a TQL Query” on page 25. To see the discovered network CIs, you need to define a TQL query that retrieves the specified network CIs from the CMDB.

In this lesson, you will learn about:

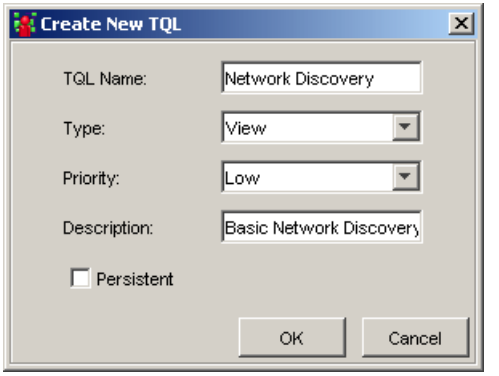
Defining a TQL Query for the Discovered Network CIs

In this section, you will create a TQL that enables you to view the discovered network CIs and define its attributes.

To create a new TQL:

1 In the TQL Builder, click the **Map** > **New** button or right-click the folder in which you want to create the new query and select **New**.

The Create New TQL dialog box opens:



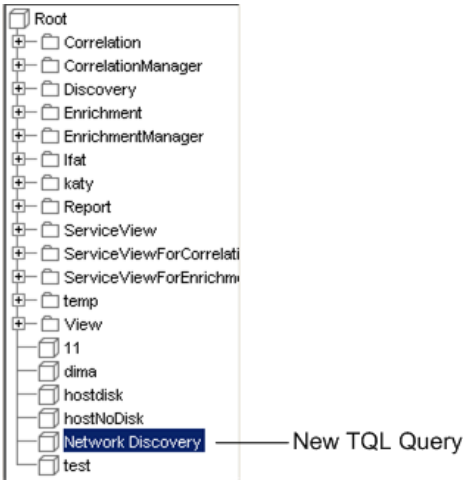
2 In the **TQL Name** box, type: Network Discovery

3 From the **Type** list, choose **View**.

4 From the **Priority** list, choose **Low.**

5 In the **Description** box, type: Basic Network Discovery

6 Click **OK**. The new TQL query is displayed in the View Explorer.



Adding TQL Nodes and Relationships to the Query

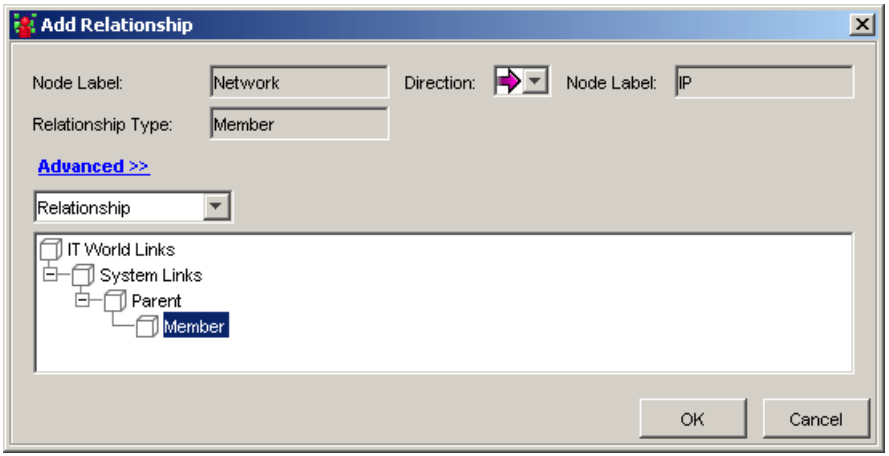
In this section, you will add the TQL nodes to the query and define the relationship between them.

1 From the tree in the View Explorer in the TQL Builder, select **Network Discovery**.

2 From the tree displayed in the Configuration Item Type Model, click and drag the following TQL nodes to the editing pane:

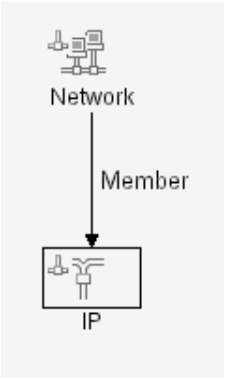
- Network
- IP

3 Select the two nodes, right-click and then click **Add Relationship** to open the Add Relationship dialog box.



4 To link the **Network** and **IP** TQL nodes, click **Advanced** and select **Member**. **Member** appears in the **Relationship Type** box.

5 Click **OK**. The TQL query you have created is displayed below.

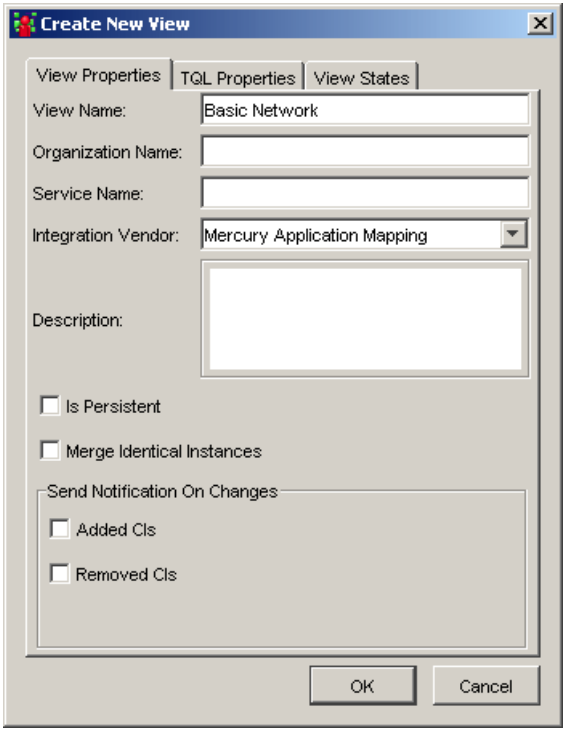


6 Click **Save** to save the TQL definitions in the CMDB.

Creating A New View

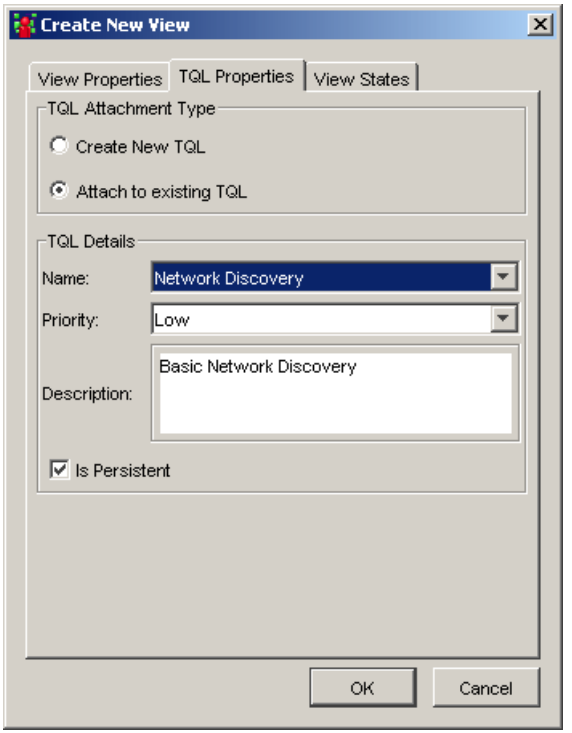
In this section, you will create a view whose map displays the results of the TQL query.

1 In the Service View Manager, click the **New** button on the toolbar or open the **Map** menu and click **New** to open the **View Properties** tab in the Create New View dialog box.



2 In the **View Name** box, enter the name of the view. For this exercise, write Basic Network.

3 Click the **TQL Properties** tab to open the following:

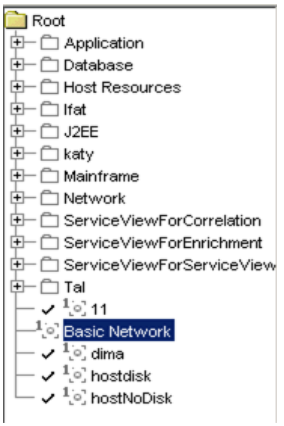


4 Select **Attach to an existing TQL**.

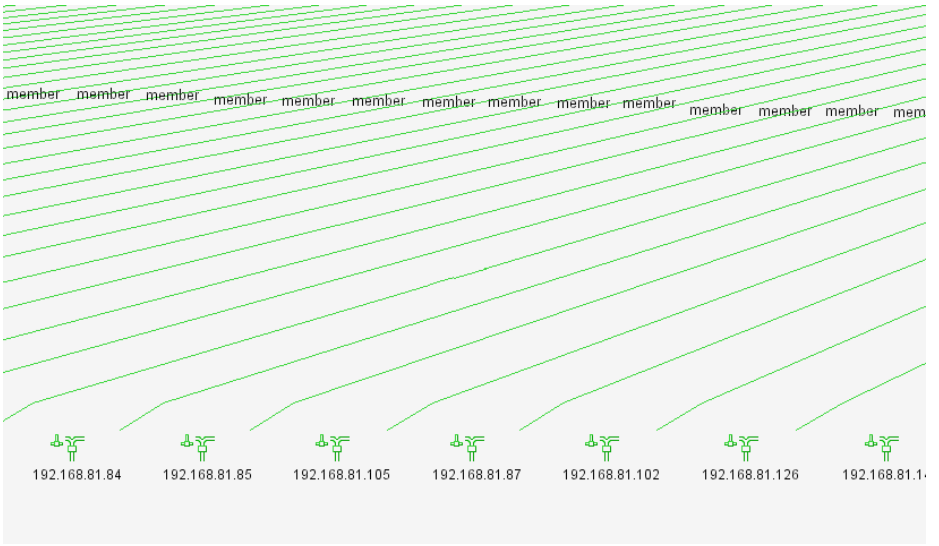
5 From the **Name** list, choose **Network Discovery**.

6 Select **Is Persistent**.

7 Click **OK**. The new view is displayed in the View Explorer.



8 Select the **Basic Network** view in the Topology Map to view the results of the query. The illustration below displays a section of the topology map.



5

Performing an Advanced Network Discovery

In“Discovering Network CIs” on page 21, you activated the **ICMP_NET_Dis_IpC** discovery pattern, which identified all the network IPs. After these IP addresses are added to the CMDB, they act as triggers for the **ICMP_NET_Dis_Connection** discovery pattern. This pattern activates a task whose job it is to discover SNMP connection data of the new IPs discovered in your IT infrastructure. The task results add a host to each IP together with its SNMP connection data to the CMDB.

In this lesson, you will define the SNMP connection data and activate the **SNMP_NET_Dis_Connection** pattern that discovers hosts that use the SNMP protocol.

In this lesson, you will learn about:

Defining the SNMP Connection Data

In this section, you will define the SNMP protocol through which the data will be collected.

To define the SNMP connection data:

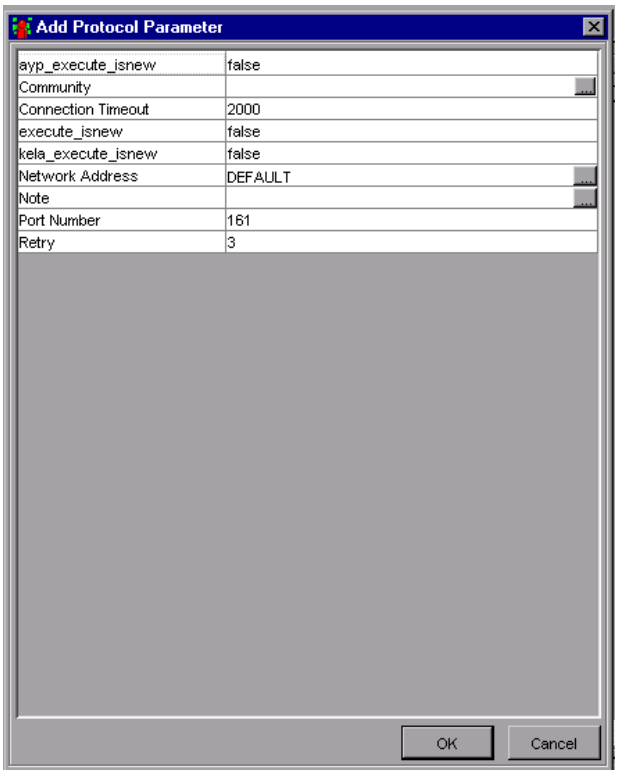
1 Select **Administration** > **Discovery Manager** to open the Discovery Manager.

2 Click the **Probe Manager** tab.

3 In the Discovery Probes pane, select **niceDomain**.

4 Click the **Expand** button to the left of **niceDomain** and then select **SNMP Protocol**.

5 Click the **Add new connection details for the selected protocol type** button in the Protocol entries pane to open the Add Protocol Parameter dialog box.



6 Click the button at the right end of the **Community** box to open the Community dialog box.

7 Ask your system administrator what the Community string is and type it in the **New Password** box.

8 Type the Community string again in the **Confirm New Password** box and click **OK**.

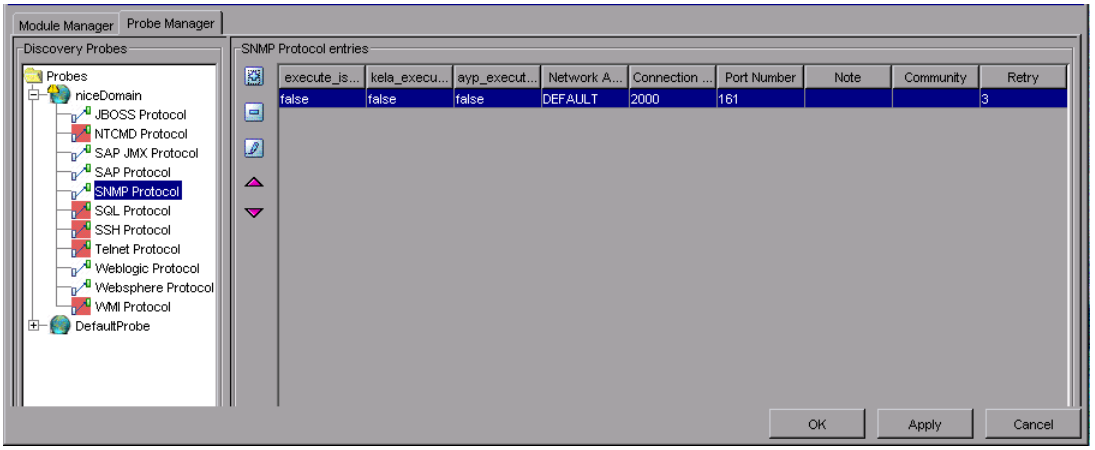
9 In the **Connection Timeout** box, leave the default value 2000.

10 In the **Network Address** box, leave the default value DEFAULT.

11 In the **Port Number** box, ask your system administrator for the required port number.

12 In the **Retry** box, leave the default value 3.

13 Click **OK**. The parameter values you have defined appear in the **Protocol Entries** section, as seen below.

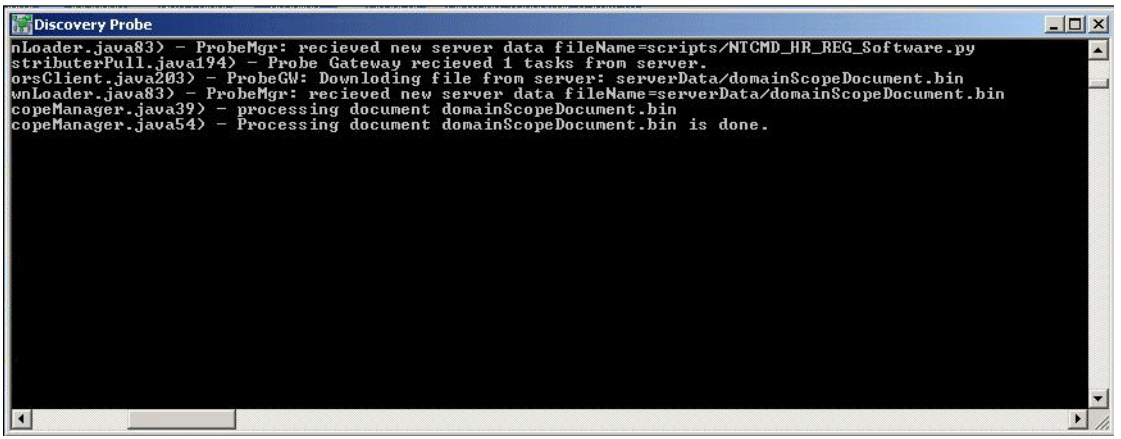


14 Click **Apply** to save the changes you have made in the CMDB.

Verifying that the Changes Have Been Made to the Discovery Probe

Each change you make in the Discovery Manager dialog box is delivered to and stored in the CMDB. From there, the changes are sent to the Discovery Probe. Verification that the changes have been sent to the Discovery Probe is seen in the following message displayed in the **wrapperProbe log** file, that is located in \< **Mercury Application Mapping Discovery Probe Installation directory**>**root****logs**\.

processing document domainScopeDocument.bin
Processing document domainScopeDocument.bin is done.



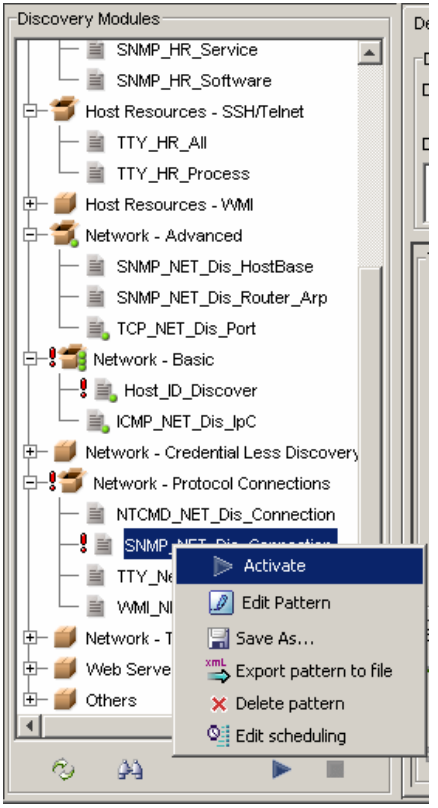
Activating the SNMP_NET_Dis_Connection Discovery Pattern

In this section, you will activate the **SNMP_NET_Dis_Connection** discovery pattern to discover hosts that use the SNMP protocol.

To activate the SNMP_NET_Dis_Connection pattern:

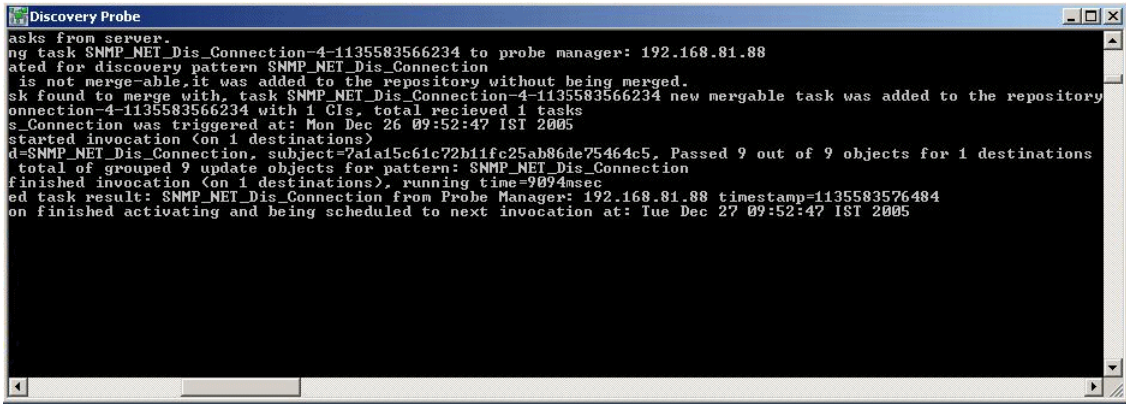
1. Select the **Module Manager** tab.
2. In the Discovery Modules pane, click the **Expand** button to the left of the **Network- Protocol Connections** module.

3 Right-click **SNMP_NET_Dis_Connection** and click the **Activate** button, or select **SNMP_NET_Dis_Connection** and click the **Activate** button in the bottom-right corner of the Discovery Modules pane.



Verifying the Discovery Results

Check the discovery results in the Discovery Probe. The following example shows that the **SNMP_NET_Dis_Connection** pattern was activated and displays the number of CIs discovered.



Defining a TQL to View the Discovered CIs

To view the discovered network CIs, you will be:

- "Defining a New TQL That Retrieves the Specified CIs From the CMDB" on page 39
- "Adding TQL Nodes and Relationships to the Query" on page 41
- "Creating A New View" on page 43

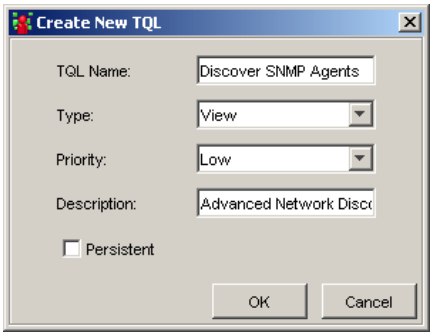
Defining a New TQL That Retrieves the Specified CIs From the CMDB

In this section, you will define the TQL that extracts hosts that use the SNMP protocol from the CMDB.

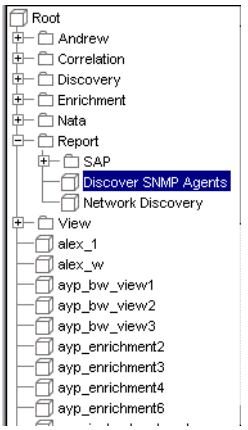
To define a new TQL:

1 In the TQL Builder, click the **New** button or right-click the folder in which you want to create the new query and select **New**.

The Create New TQL dialog box is displayed.



2. In the **TQL Name** box, enter a TQL query name. For this exercise, type: Discover SNMP Agents
3. From the **Type** list, choose **View**.
4. From the **Priority** list, choose **Low**
5. In the **Description** box, enter a TQL description. For this exercise, type: Advanced Network Discovery
6. Click **OK**. The new TQL query is displayed in the View Explorer.



Adding TQL Nodes and Relationships to the Query

After you define the TQL, you must add the required CIs and define the relationship between them.

To add nodes and relationships to the TQL:

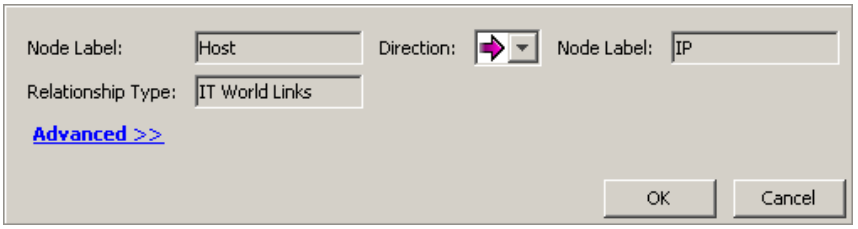
1 From the tree displayed in the Configuration Item Types, click and drag the following CITs to the topology map.

- ➤ Network
- ➤ IP
- ➤ Host
- ➤ SNMP

2 Link the nodes according to the following table.

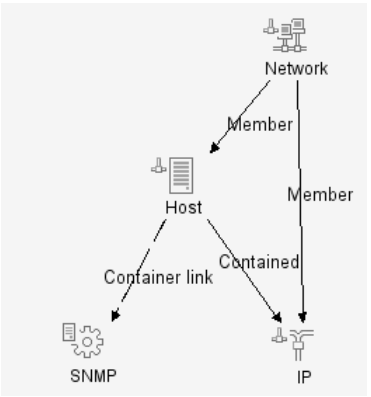
Link this node	To this node	With this relationship
IP	Network	Member
Host	Network	Member
SNMP	Host	Container Link
IP	Host	Contained

Simultaneously select the two nodes in each row, right-click and then click **Add Relationship**. The Add Relationship dialog box opens.



3 Select the relationships according to the table above, and click **OK**.

The TQL you have created is displayed below.



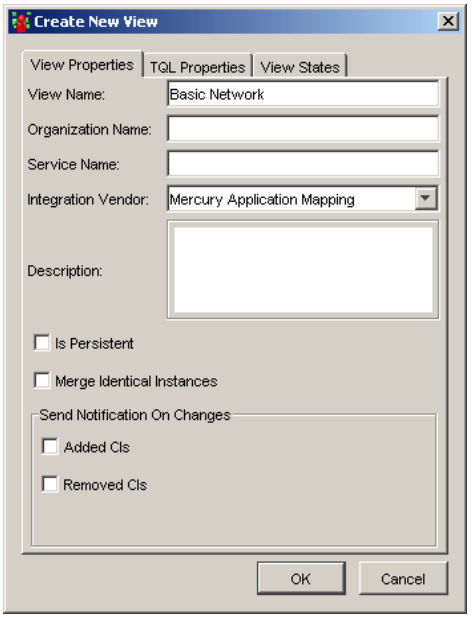
4 Click the **Save** button to save the TQL definitions in the CMDB.

Creating A New View

In this section, you will create a view whose map displays the results of the TQL query.

To create a new view:

1 In the Service View Manager, click **New** on the toolbar or open the **Map** menu and click **New** to open the **View Properties** tab in the Create New View dialog box.

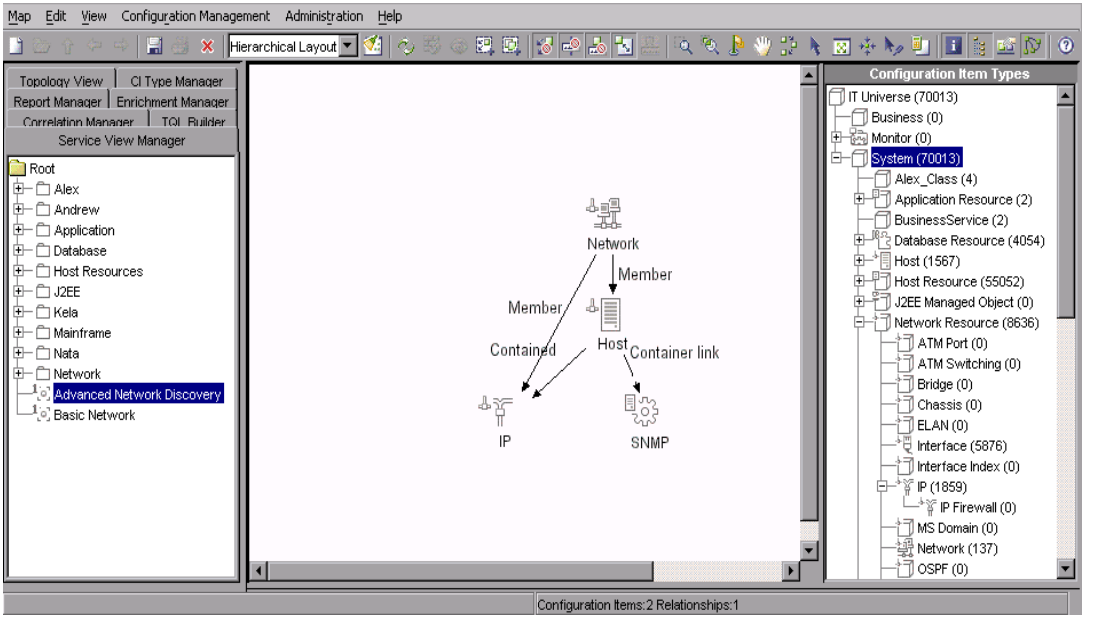


2 In the **View Name** box, enter a view name. For this exercise, type Advanced Network Discovery.

3 Click the **TQL Properties** tab and select **Attach to an existing TQL**.

4 From the **Name** list, choose **Discover SNMP Agents**.

5 Click **OK**. The new view is displayed in the View Explorer.



In the following lesson, you will expand the discovery to include other network resources.

6

Expanding the Network Discovery

In this lesson, you will expand the network discovery to include the discovery of other network resources.

In this lesson, you will learn about:

Activating Patterns That Expand the Network Discovery

The following table contains a list of discovery patterns that activate tasks whose job is to discover other network components needed for building the network infrastructure, such as relationships, ARP tables and port numbers.

Discovery Pattern	Definition
SNMP_NET_Dis_HostBase	Activates a task whose job is to discover all the routing relationships between the hosts in your system.
SNMP_NET_Dis_Router_Arp	Activates a task whose job is to discover the ARP tables containing the IP addresses of the machines with whom the server is communicating.
SNMP_NET_Dis_TCP	Activates a task whose job is to discover all the TCP connections between the different machines in your system.
TCP_NET_Dis_Port	Activates a task whose job is to discover all the port numbers in the **portNumberToPortName.xml** file, which is located in the Configuration Files pane. **Note**: This file is provided with your Mercury Application Mapping package. You can edit the file if required. The results of this discovery become the trigger CIs for discovering applications.

To activate the discovery patterns:

1 Select **Administration** > **Discovery Manager** to open the Discovery Manager.

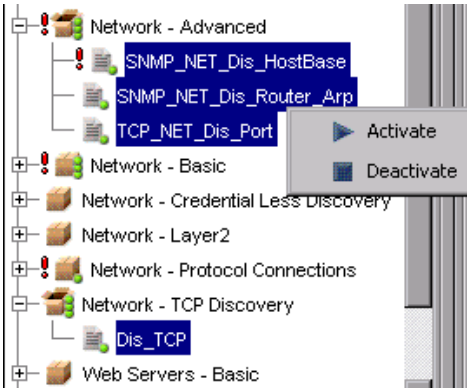
2 Select the **Module Manager** tab.

3 Click the **Expand** button to the left of the **Network - Advanced** module.

4 Select the following patterns:

- **SNMP_NET_Dis_HostBase**
- **SNMP_NET_Dis_Router_Arp**
- **TCP_NET_Dis_Port**

5 Right-click and select **Activate**.



6 Click the **Expand** button to the left of the **Network - TCP Discovery** module.

7 Select **Dis_TCP**.

8 Right-click and select **Activate**.

9 An activated pattern is marked with a green dot.

Viewing the Discovered CIs

Mercury Application Mapping provides predefined views for certain discovery results. You can view the following discovered CIs in the following predefined views:

View these CIs	In this predefined view
All the TCP connections between the different machines in your system.	Client_Server_Connections
All the routing relationships between the hosts in the network.	Route
All the ARP tables containing the IP addresses of the machines with whom your computer is communicating.	Network

---

Note: Mercury Application Mapping does not provide a predefined view for the port numbers in the **portNumberToPortName.xml** file.

7

Discovering Database Instances and Oracle Resources

The CMDB now contains networks, host CIs with SNMP connection data and other network resources. In this lesson, you will uncover the database instances and Oracle resources in your IT infrastructure.

The **SQL_NET_Dis_Connection** pattern discovers the following database types:

- Oracle
- DB2
- Sybase
- SQLServer

The CIs discovered in the **TCP_NET_Dis_Port** pattern (see "TCP_NET_Dis_Port" on page 46) act as a trigger for the **SQL_NET_Dis_Connection** pattern, which activates a task whose job is to discover database instances.

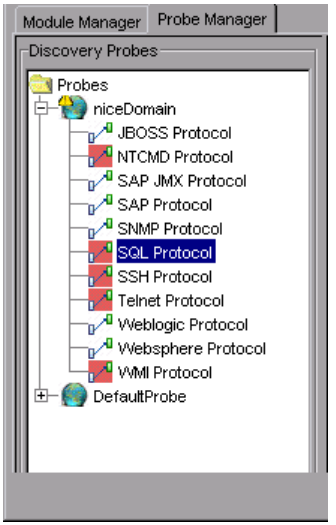
In this lesson, you will learn about:

Adding the SQL Protocol

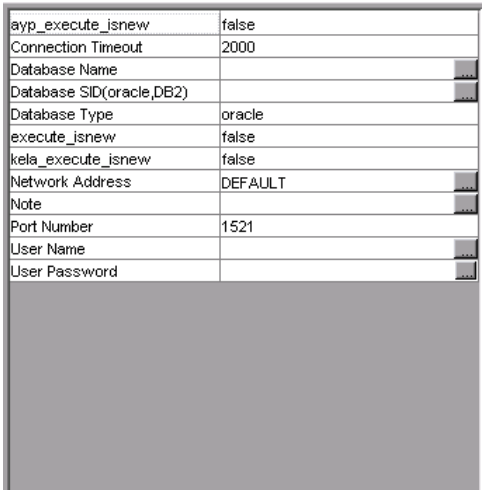
You need to add the Oracle protocol to discover all the Oracle resources.

To add the Oracle protocol:

1. Select **Administration** > **Discovery Manager** to open the Discovery Manager.
2. Click the **Probe Manager** tab.
3. In the Discovery Probes pane, select **niceDomain**.
4. Click the **Expand** button to the left of **niceDomain** and then select **SQL Protocol**.

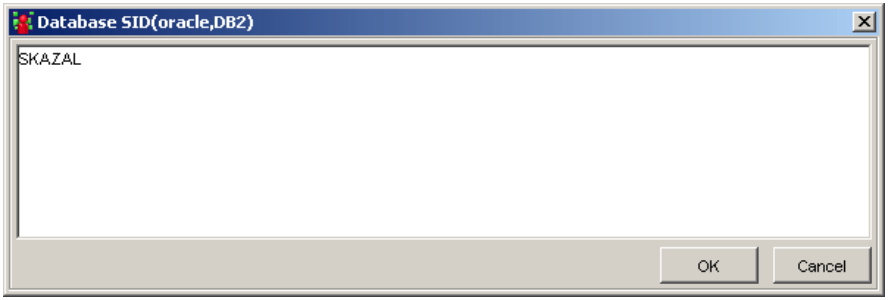


5 Click the **Add new connection details for the selected protocol type** button in the Protocol entries pane to open the Add Protocol Parameter dialog box.



6 In the **Connection Timeout** box, leave the default as 2000.

7 Click the button at the right of the **Database SID(oracle, DB2)** box. In the dialog box that opens, type the name of your database SID. For example, SKAZAL.



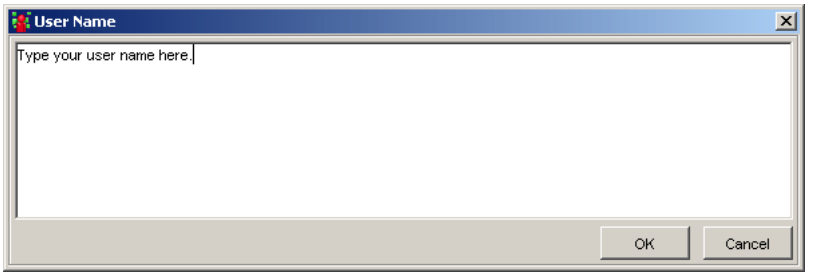
8 Click **OK** to save your changes.

9 In the **Database Type** box, leave the default value oracle

10 In the **Network Address** box, leave the default value DEFAULT.

11 In the **Port Number** box, type the port number on which the database listens.

12 Click the button at the right end of the **User Name** box. In the dialog box that opens, type your username.



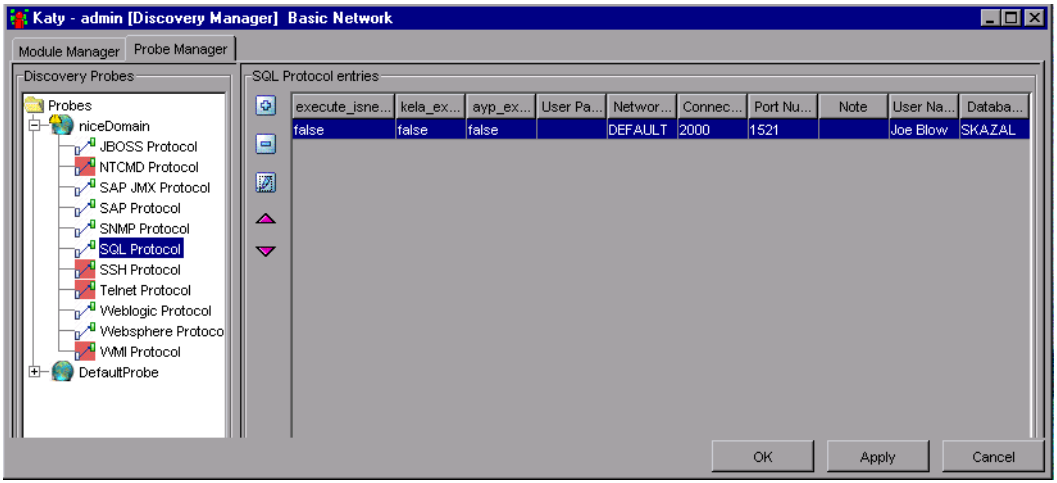
13 Click **OK** to save your changes.

14 Click the button at the right end of the **User Password** box to open the User Password dialog box.

15 In the **New Password** box, type your password.

16 Type your password again in the **Confirm New Password** box and click **OK** to save the password information and close the User Password dialog box.

17 Click **OK** to save the protocol definitions you have set. The protocol definitions appear in the **SQL Protocol entries** section.



18 Click **Apply** again to save the changes in the CMDB.

To verify that the CMDB has been updated with the changes you made in the network protocol configurations, check that the following notification appears in the Discovery Probe:
Processing document domainScopeDocument.bin is done

Activating the SQL_NET_Dis_Connection Pattern

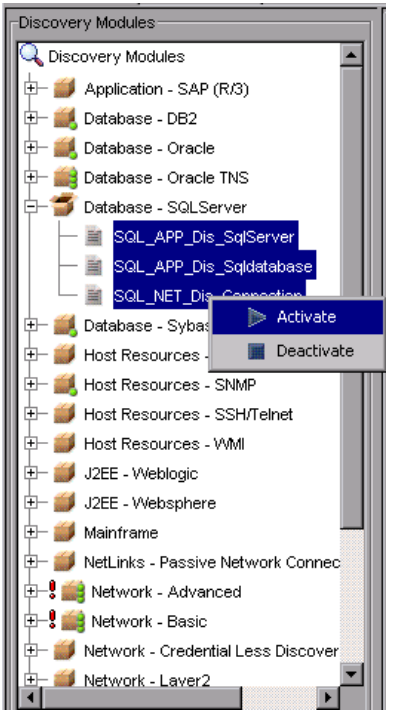
In this section, you will activate the pattern that discovers database instances in your IT infrastructure.

To activate the SQL_NET_Dis_Connection pattern:

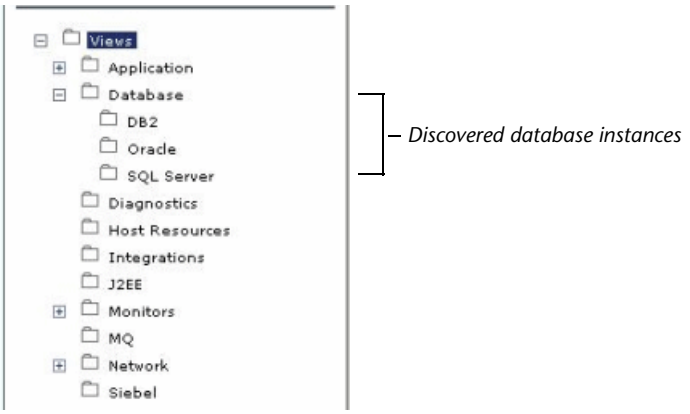
1 Select the **Module Manager** tab.

2 In the Discovery Modules pane, click the **Expand** button to the left of the **Database - SQLServer** module.

3 Right-click **SQL_NET_Dis_Connection** and click the **Activate** button, or select **SQL_NET_Dis_Connection** and click the **Activate** button in the bottom- right corner of the Discovery Modules pane.



The pattern finds all Oracle, DB2, Sybase, and SQLServer database instances that exist in your IT infrastructure. They appear in the **Database** folder in the Service View Manager.



Activating the SQL_APP_Dis_Oracle Discovery Pattern

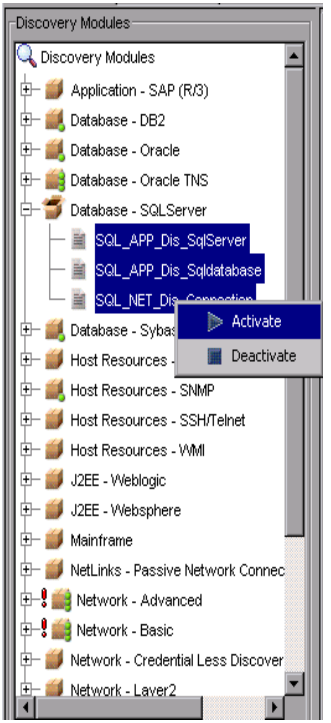
Now that you have discovered all the instances of Oracle, DB2, Sybase and SQLServer databases, you will perform a more in-depth discovery that uncovers all the existing Oracle resources. To do this, you need to activate the **SQL_APP_Dis_Oracle** pattern.

In this section, you will activate the discovery pattern **SQL_APP_Dis_Oracle** whose task is to discover Oracle resources.

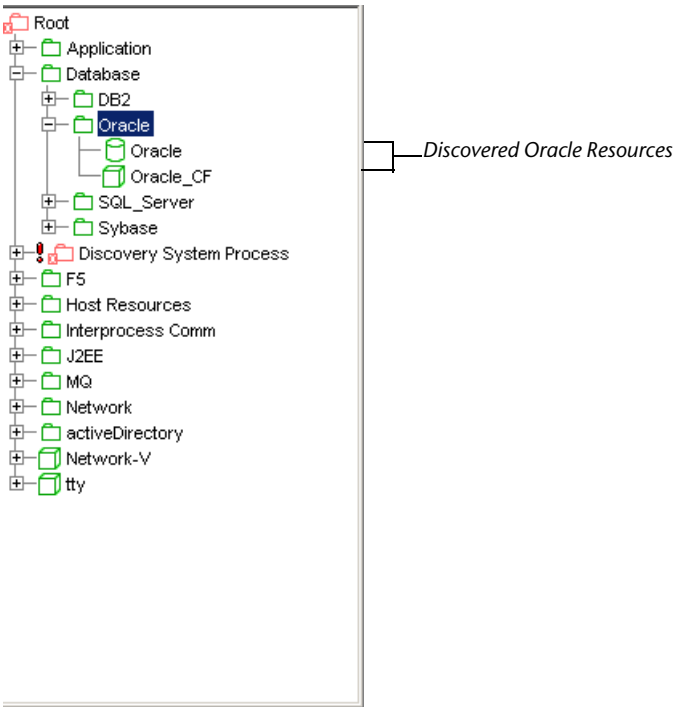
To discover Oracle resources:

1. Select the **Module Manager** tab.
2. Select the **Advanced View** check box.
3. Click the **Expand** button to the left of the **Database - Oracle** module.

4 Right-click **SQL_APP_Dis_Oracle** and click the **Activate** button, or select **SQL_APP_Dis_Oracle** and click the **Activate** button in the bottom- right corner of the Discovery Modules pane.



The pattern uncovers all the Oracle resources, such as users, tables and tablespaces for each database instance. The discovered resources appear in a predefined view called **Oracle**.



8

Discovering WebLogic Instances and Components

In the previous lesson, you discovered database instances and the Oracle resources in your IT infrastructure. In this lesson, you will uncover WebLogic instances and WebLogic components in your IT infrastructure.

- You activate the **J2EE_JMX_Weblogic_Connection** pattern to discover the WebLogic instances.

  The CIs discovered in the **TCP_NET_Dis_Port** pattern (see "Activating Patterns That Expand the Network Discovery" on page 46), act as a trigger for the **J2EE_JMX_Weblogic_Connection** pattern, which activates the task whose job is to discover all instances of WebLogic.

- You activate the **J2EE_JMX_Weblogic** pattern to discover the WebLogic components.

  The CIs discovered in the **J2EE_JMX_Weblogic_Connection** pattern act as a trigger for the **J2EE_JMX_Weblogic** pattern, which activates the task whose job is to discover all WebLogic components.

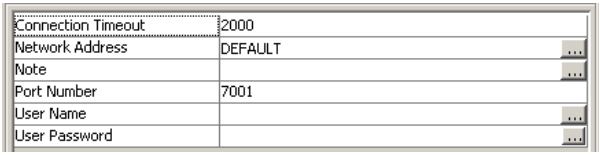
In this lesson, you will learn about:

Defining the WebLogic Protocol

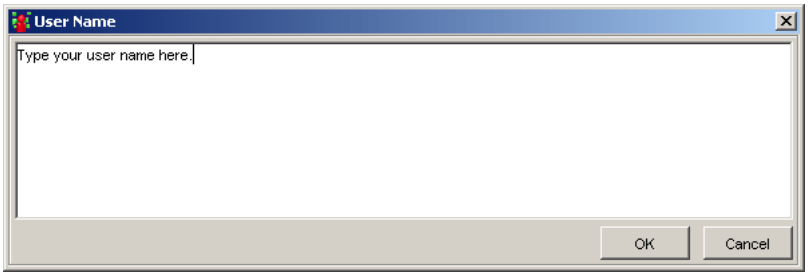
In this section, you will add the WebLogic protocol and define its connection data.

To define the WebLogic Protocol:

1. Select **Administration** > **Discovery Manager** to open the Discovery Manager.
2. Click the **Probe Manager** tab.
3. In the Discovery Probes pane, select **niceDomain**.
4. Click the **Expand** button to the left of **niceDomain** and then select **Weblogic Protocol**.
5. Click the **Add new connection details for the selected protocol type** button in the Protocol entries pane to open the Add Protocol Parameter dialog box.



6. In the **Connection Timeout** box, leave the default value as 2000.
7. In the **Network Address** box, leave the default value as DEFAULT.
8. In the **Port Number** box, type the port number on which the Weblogic server listens.
9. Click the button at the right end of the **User Name** box. In the dialog box that opens, type your user name and click **OK**.

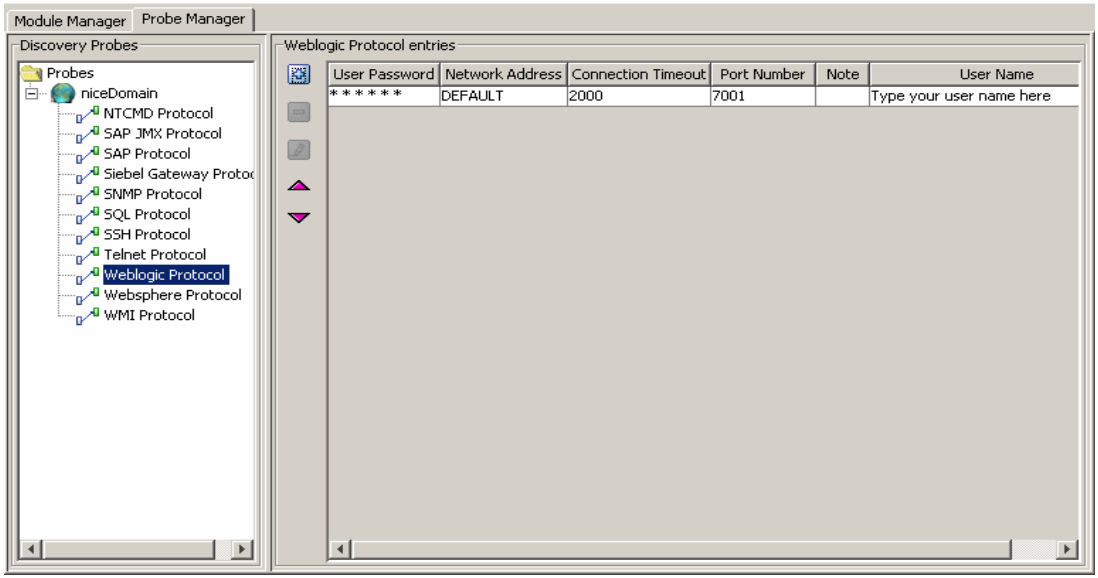


10 Click the button at the right end of the **User Password** box to open the User Password dialog box.

11 In the **New Password** box, type your password.

12 Type your password again in the **Confirm New Password** box and click **OK** to save your changes and close the User Password dialog box.

13 Click **OK** to save the protocol definitions you have set. The protocol definitions appear in the Weblogic Protocol entries pane, as seen below.



14 Click **Apply** to save the changes in the CMDB.

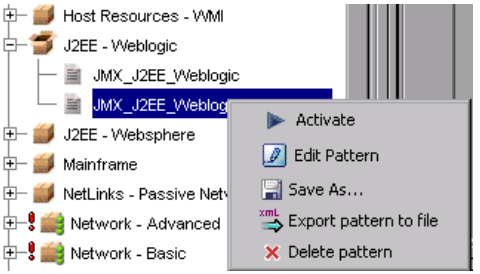
To verify that the CMDB has been updated with the changes you made in the Discovery Probe configurations, check that the following notification appears in the Discovery Probe:
Processing document domainScopeDocument.bin is done

Discovering WebLogic Instances

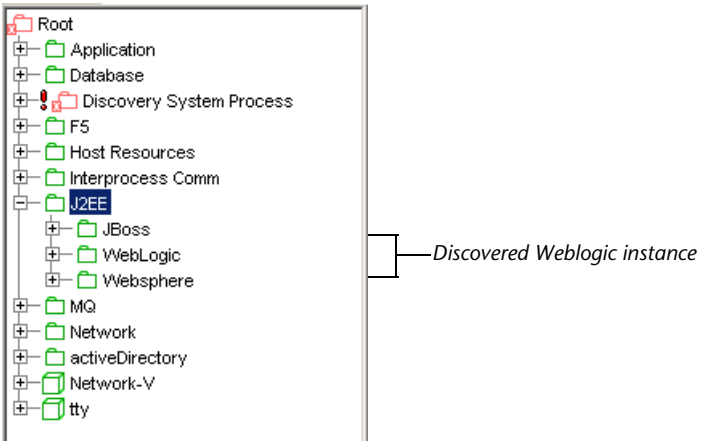
You need to activate the **JMX_J2EE_Weblogic_Connection** pattern in order to discover all the instances of WebLogic.

To discover all instances of WebLogic:

1. Select **Administration** > **Discovery Manager** to open the Discovery Manager.
2. Click the **Module Manager** tab.
3. In the Discovery Modules pane, click the **Expand** button to the left of the **J2EE - Weblogic** module.
4. Right-click **JMX_J2EE_Weblogic_Connection** and click the **Activate** button, or select **JMX_J2EE_Weblogic_Connection** and click the **Activate** button in the bottom- right corner of the Discovery Modules pane.



The pattern discovers all the WebLogic instances in your system. The discovered CIs appear in a predefined view called **Weblogic** that is located under **J2EE** in the Service View Manager tab.



The illustration above shows the **J2EE_JMX_Weblogic_Connection** discovery pattern has discovered WebLogic instances called **JBoss**, **WebLogic,** and **Websphere**.

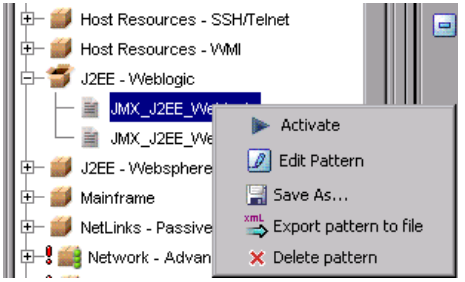
Discovering WebLogic Components

In this section, you are going to activate the pattern that discovers Weblogic components.

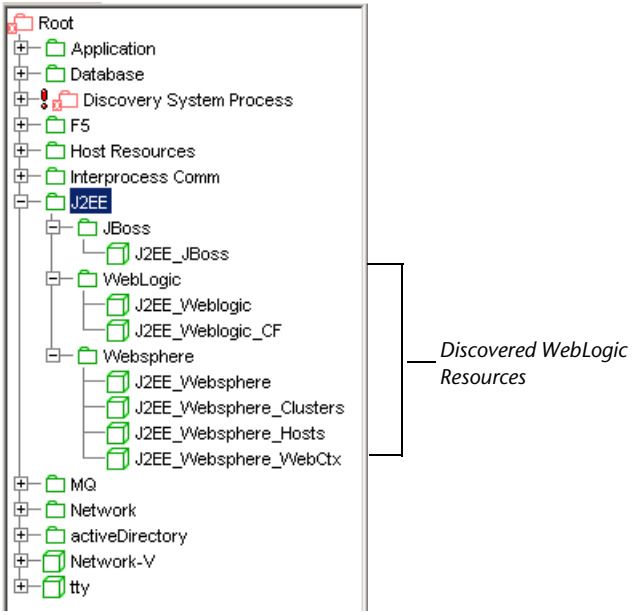
To discover WebLogic components:

1. Click the **Module Manager** tab.
2. Click the **Expand** button to the left of the **J2EE-Weblogic** module.

3 Right-click **JMX_J2EE_Weblogic** and click the **Activate** button, or select **JMX_J2EE_Weblogic** and click the **Activate** button in the bottom- right corner of the Discovery Modules pane.



The pattern uncovers all the WebLogic resources in your system.



The illustration above shows that the **J2EE_JMX_Weblogic** discovery pattern has uncovered WebLogic resources such as connection pools, JMS and EJB.

9

Discovering Host Resources

In the previous lesson, you discovered the WebLogic instances and WebLogic components in your system.

In this lesson, you will activate a number of patterns that discover WMI-based resources, such as disks, CPU, memory, or files.

- WMI_HR_CPU_Dynamic
- WMI_HR_Disk_Dynamic
- WMI_HR_Process_Dynamic
- WMI_HR_Service_Dynamic

In this lesson you will learn about:

Defining the WMI Protocol

In this section, you will add the WMI protocol and define its connection data.

To define the WMI protocol:

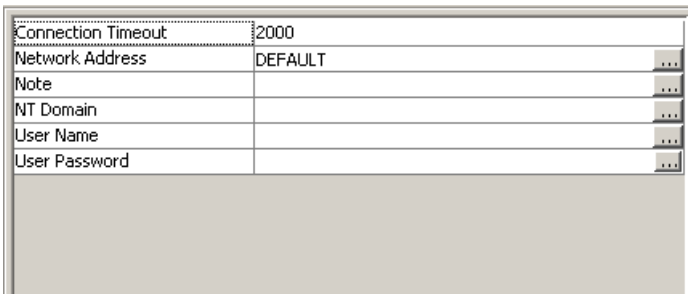
1 Select **Administration** > **Discovery Manager** to open the Discovery Manager.

2 Click the **Probe Manager** tab.

3 In the Discovery Probes pane, select **niceDomain**.

4 Click the **Expand** button to the left of **niceDomain** and then select **WMI Protocol**.

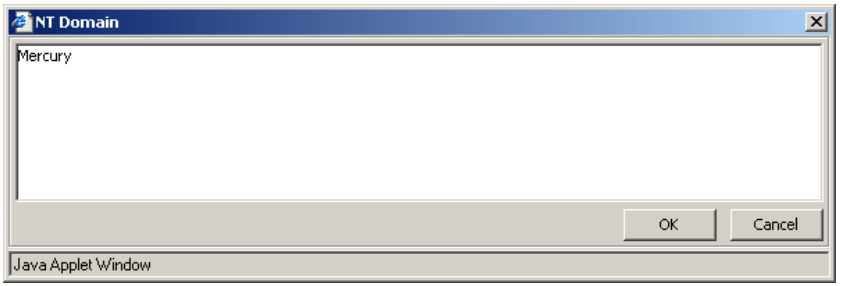
5 Click the **Add new connection details for the selected protocol type** button in the Protocol entries pane to open the Add Protocol Parameter dialog box.



6 In the **Connection Timeout** box, leave the default as 2000.

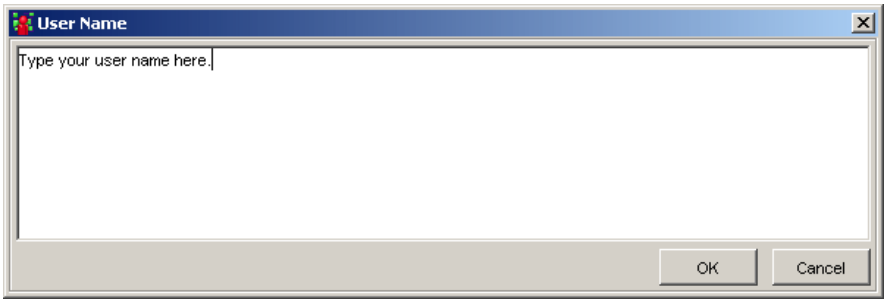
7 In the **Network Address** box, leave the default as DEFAULT.

8 Click the button at the right end of the **NT Domain** box. In the dialog box that opens, type your domain. For example, Mercury.



9 Click **OK**.

10 Click the button at the right end of the **User Name** box. In the dialog box that opens, type your user name and click **OK**.

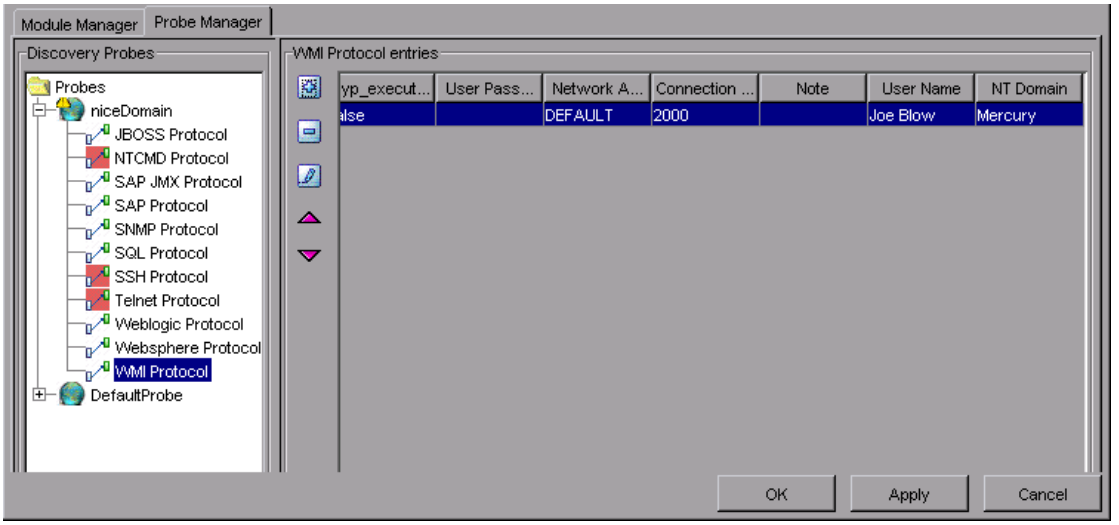


11 Click the button at the right end of the **User Password** box to open the User Password dialog box.

12 In the **New Password** box, type your password.

13 Type your password again in the **Confirm New Password** box and click **OK** to save your changes and close the User Password dialog box.

14 Click **OK** to save the protocol definitions you have set. The protocol definitions appear, as seen below.



15 Click **Apply** again to save the changes in the CMDB.

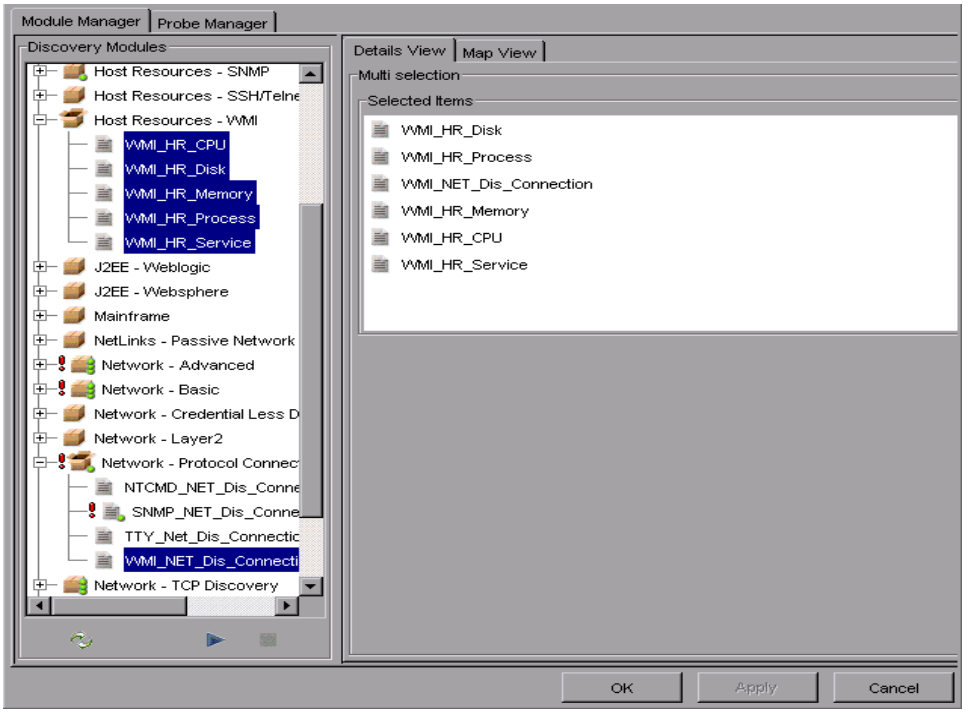
Discovering WMI Components

In this section, you are going to activate the pattern that discovers WMI-based resources.

To discover WMI components:

1. Select **Administration** > **Discovery Manager** to open the Discovery Manager.
2. Click the **Module Manager** tab.
3. Click the **Expand** button to the left of the **Host_Resources - WMI** module and select the following:
   - **WMI_HR_Memory**
   - **WMI_HR_CPU**
   - **WMI_HR_Disk**
   - **WMI_HR_Process**
   - **WMI_HR_Service**

4 Click the **Expand** button to the left of the **Network - Protocol Connections** module and select **WMI_NET_Dis_Connection**.



Note: You can connect several patterns simultaneously by holding down the CTRL key and selecting the required patterns, as seen above.

---

5 Click the **Activate** button in the bottom-right corner of the Discovery Modules pane.

The patterns uncover all the WMI-based resources, which are located under **Host Resources** in the Service View Manager.