



STEP – BY – STEP GUIDE

Netformx Discovery Step By Step Guide Version 6

Table of Contents

Netformx Discovery Overview	3
Additional Online Resources	3
New Features.....	3
Getting Started	4
Setting Customer’s Expectations.....	4
Customer Site Prerequisites	5
Start a Discovery.....	5
Network Tab	7
Configuring Seed Router.....	7
Configuring Addresses/Subnets	8
Excluding Addresses/Subnets.....	10
SNMP Tab.....	11
SNMP Configuration	11
Telnet/SSH Tab.....	12
Configuring Protocols	12
Cisco Config Tab.....	14
Scan Options Tab	15
Scan Mode.....	15
Ping Settings.....	15
Import Tab	18
Import Options.....	18
Existing Discovery Data	18
Run Network Discovery	19
Post Discovery Operation.....	20
Discovery Reports.....	21
Two Valuable Discovery Reports	22
Network Analysis Using Cisco Discovery Service (CDS):.....	22
CDS Analysis Reports.....	26
Netformx Discovery Files and Databases.....	27
Tips Summary.....	27
Netformx Technical Support.....	28
Online Resources.....	29

Netformx Discovery Overview

Netformx Discovery (ND) is the SNMP/SSH/Telnet-based audit and multi-vendor network discovery feature of Netformx DesignXpert®. Netformx enables pre-sales engineers, SE's and design engineers to quickly and accurately audit the network, and automatically identify topology, equipment, and configuration data down to specific nodes. It can capture a baseline of existing equipment with the detailed specs for each device. DesignXpert Discovery Reports can assist during the analysis phase by identifying EoX (End of Life, End of Support, etc) devices, IOS versions, insufficient resources and gaps in the discovered network.

Additional Online Resources

We encourage you to take advantage of the additional online resources listed on page 27 including the Netformx [ND Web Page](#), the Netformx [Resource Center](#) and the Netformx [Learning and Certification Center](#). There you will find information including:

- Netformx Discovery: Netformx Technical Support
- Self-Paced Video on Demand Training modules
- Information on how to become a certified DesignXpert® engineer
- Archive of recorded Monthly Users' Forums
- Archive of Monthly Newsletter
- ... and much more

New Features

The following enhancements were added to Netformx Discovery through several DesignXpert upgrades over several quarters:

1. DesignXpert version 11.3
 - a. Discovery of Cisco IP phones
 - b. Enhanced discovery results grid and filtering/sorting options
 - c. Improved warning and errors mechanism for early identification of incorrect discovery settings
2. DesignXpert version 11.4
 - a. Cisco Discovery Service (CDS 1.0) Integration which provides
 - i. hardware and software lifecycle milestone (end-of-sale-announcement, end-of-sale, last-date-of-support) analysis and
 - ii. product security incident response team (PSIRT) notices for IOS/CATOS
 - b. Ability to query devices configured only for SNMP v2
 - c. Leverage bulk extensions of SNMP v2 (also with v3) to accelerate the device querying process
 - d. Save all Cisco-device configuration files to a selected directory
 - e. Discover HP Procurve devices and their serial numbers
 - f. Support wild cards for subnet range definitions
 - g. Hide passwords and security phrases
3. DesignXpert version 12.0

Netformx Discovery Step-by-Step Guide

- a. CDS 1.1 Integration along with Service Coverage Reports
 - b. Support multiple discovery seeds
 - c. Support multiple Telnet / SSH login credentials
 - d. Improved Discovery Juniper equipment
 - e. Discovery of Cisco WLAN controllers
 - f. Improved device configuration discovery for equipment supporting Entity MIB
 - g. Improved detailed results grid with ability to export the data.
 - h. Ability to import entire Network Discovery into a single drawing page, recommended for simple networks
4. DesignXpert version 12.3
 - a. Ability to edit multiple seeds including copy & paste
 - b. SNMP v3 encryption standards support for AES 128, 192, 256 & 3-DES
 - c. Ability to export Cisco configuration files for a discovered project, using "Tools Menu --> Export Configuration Files".
 - d. Added new CDS report to review the data to be uploaded to Cisco before transaction is submitted
 5. DesignXpert Version 12.7
 - a. Users can now continue with other DesignXpert work instead of being blocked while the network discovery data continues to be uploaded to CDS in the background.
 - b. Search the exact customer name in Cisco database to ensure consistency in reports while uploading network discovery data to CDS
 - c. Submit a selected scope of the project (Device, subdrawing) rather than selecting the entire project while uploading network discovery data to CDS.
 - d. Ability to simultaneously download the profiling analysis while KTN analysis is running.
 - e. Ability to add additional device(s) to an existing CDS transaction.

Getting Started

It is strongly recommend that before conducting a discovery of a customer's network, users follow these three important steps. Users who followed these steps reported that it significantly increased not only their comfort level with Netformx Discovery, but increased their success when conducting their first customer discovery.

1. Take advantage of the training Videos on Demand (VoD) located in the [Learning and Certification Center](#) where users can review a selection of short videos in five feature categories as well as information about the Netformx certification program.

Once there, click on "Log On" and Register to access the VoD catalog.

2. Conduct a test discovery before contacting the customer.

Setting Customer's Expectations

1. Depending on the size of the customer's network, it may take anywhere from 30 minutes to overnight to complete a discovery.
 - a. Average time for 1000 – 2000 network devices is approximately two to three hours.

- b. Even though Netformx Discovery only creates a negligible impact on the network's performance, Netformx recommends conducting the assessment during non-peak business hours.
2. *SNMP* will need to be enabled on the customer's networking equipment before conducting the discovery.
3. In addition, either the user or the customer must have the *SNMP (Read only) passwords / Community Names* that are required to enter into the discovery parameters used to collect the device information.
Note: Conducting a discovery does not expose the customer's network or create any security risks.
4. Schedule an appointment with the customer to conduct a network assessment. Inform the customer that the assessment is an important first step in the design process as it provides an up to date baseline for the design discussions.

Customer Site Prerequisites

Before initiating a discovery, please make sure to take the following steps:

1. Enable *SNMP* on the customer's devices.
2. Have the *SNMP read-only password(s)* readily available to collect *SNMP* information.
3. Have the *SNMP read-write password(s)* readily available if you wish to collect Cisco Config Files.
4. If using Telnet to capture the Cisco Config Files, be sure to have the *Telnet User name(s), Password(s) & Enable Password(s)* available.

Tips:

- ***Start with a limited discovery of routers and subnets only.*** Then analyze the project to decide the limits and requirements of the desired outcome. (Note: a router/subnets only discovery should complete in just a few minutes.)
- ***Start with low limits*** (e.g., hops, retries, and timeouts). Gradually expand the discovery by changing one parameter at a time.

Start a Discovery

1. **Open DesignXpert** and **select Project menu/Open**

Netformx Discovery Step-by-Step Guide

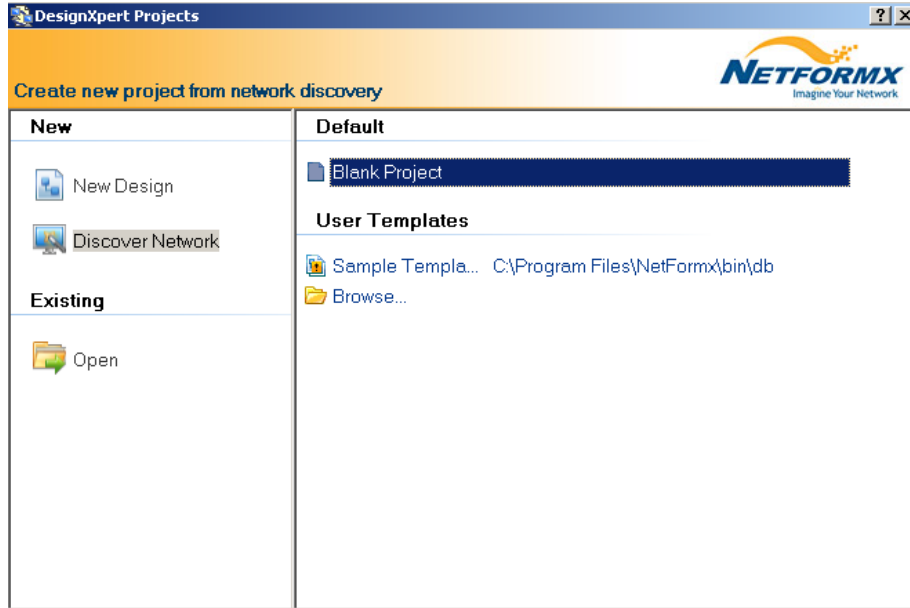


Figure 1

2. Under "Create a new network using", **select Discover Network**.
3. **Select "Blank Project"**.
4. **Type File name and select the path** where the file should be saved. Then click **Save**.

The user should now see the Netformx Discovery Dashboard dialog box (Figure 2). Click the **Configure** button to open the Discovery Configuration window (Figure3).

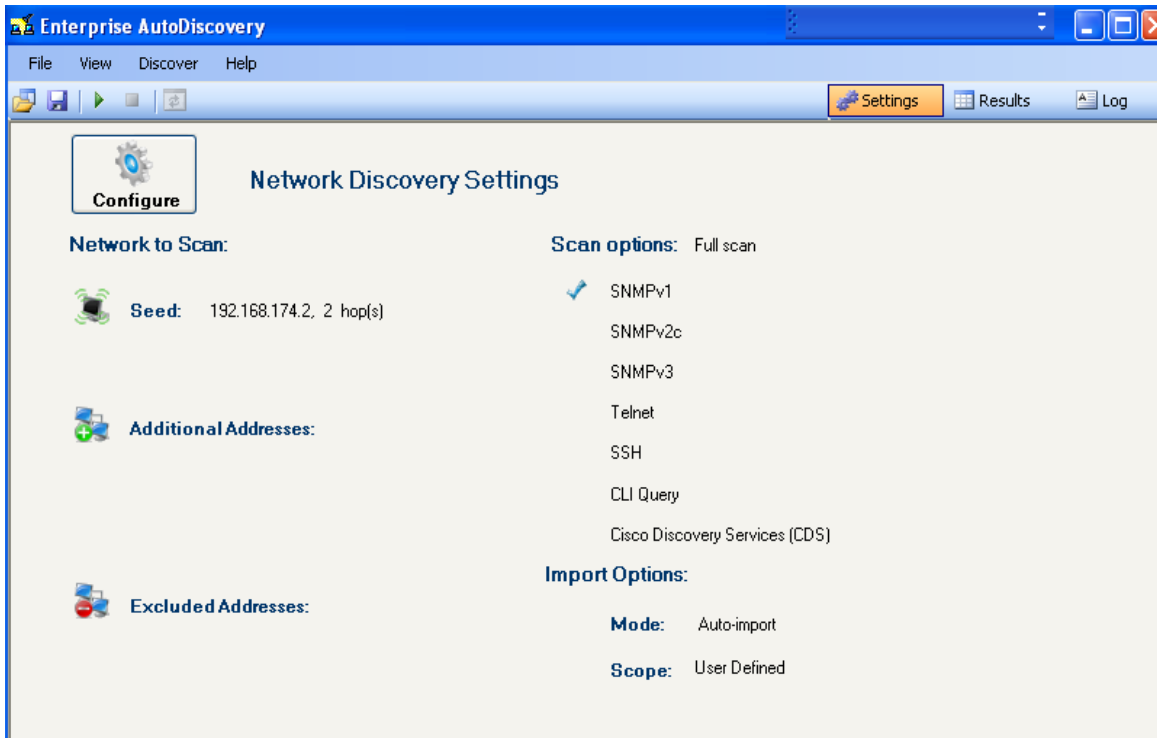


Figure 2

Network Tab

Configuring Seed Router

1. **To discover an entire network**, check the **Seed Router box**. This is the starting point to launch a full network discovery.

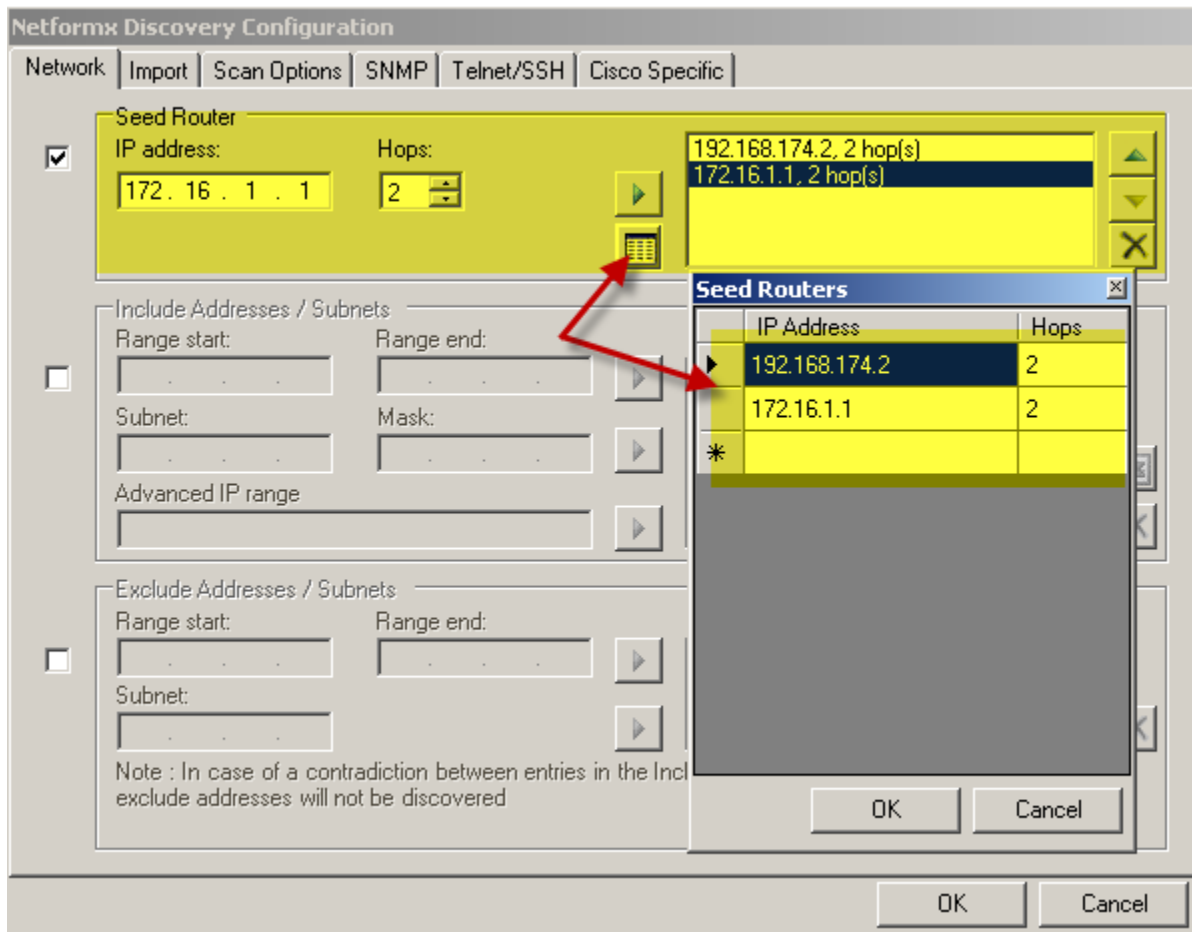


Figure 3

2. **Confirm that the IP address** displayed in the seed router pane is accurate.
3. **Numbers of hops – In the Hops field, enter** the maximum number of hops from the seed router that the discovery should include.
4. Click on the **mover** arrow to include the seed router IP address and the number of hops in the right-hand pane.
5. If required, add multiple Discovery Seeds (*Limitation: Each seed should belong to an isolated network. Overlapping between seed hop count may produce the wrong results.*)

Example:

Hop count 0 – discovers the seed router and devices immediately adjacent to this router (in other words, they share a subnet with the seed router).

Hop count 2 - discovers everything up to two routers away from the seed router.

6. If required, copy & paste multiple seed router IP addresses and hop count from other sources

Configuring Addresses/Subnets

A Full Discovery may be expanded to include additional addresses/subnets outside of the seed router hop count by also selecting the Include Addresses/Subnets box.

Alternatively, only addresses/subnets can be discovered without a Full Discovery by un-checking the seed router box.

1. To **include specific subnets and devices**, check the **Include Addresses/Subnets** box.

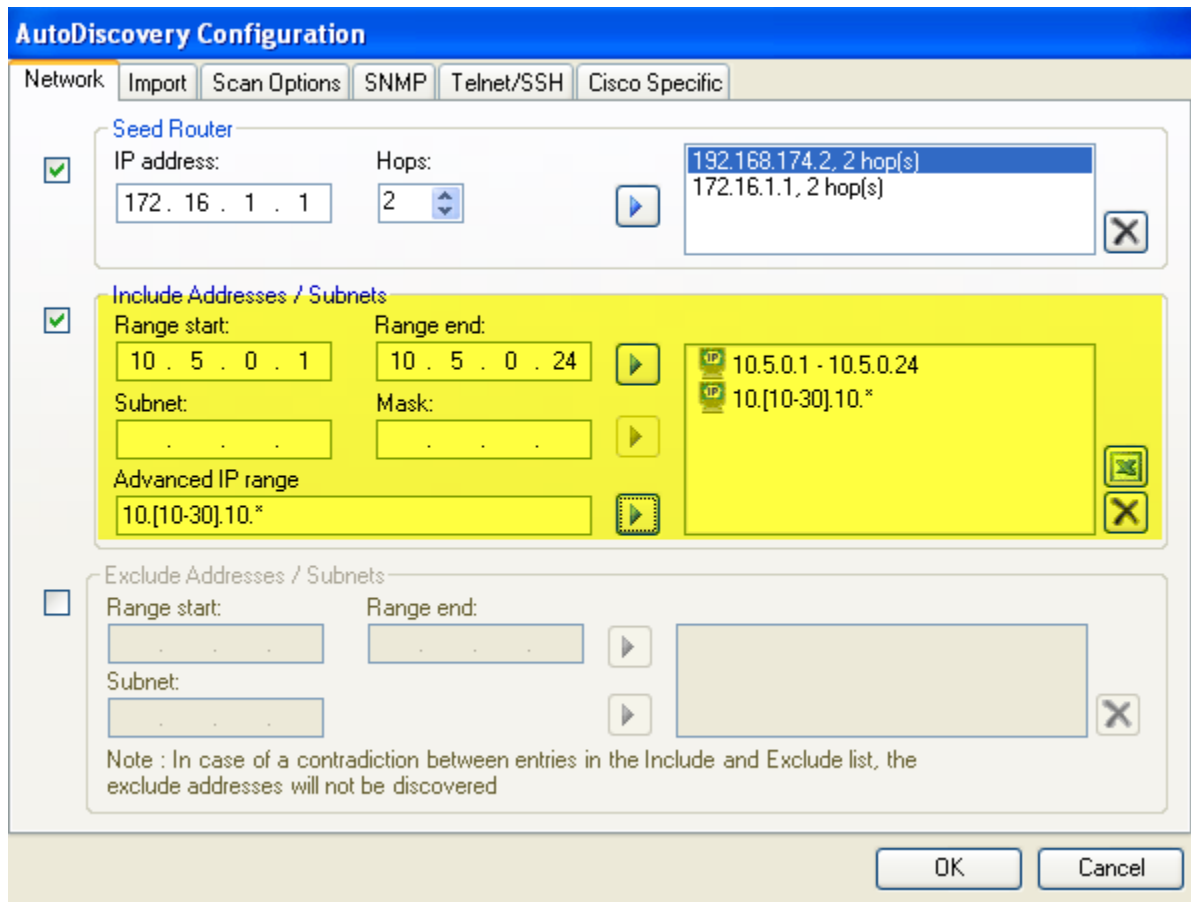





Figure 4

2. Enter a **range of device addresses** using the **Range Start** and **Range End** fields.

Note: If there are multiple ranges, repeat this step for each. For single addresses, only complete the Range Start field. An alternative is to use the Excel icon to the right and enter the information into the spreadsheet. This can also be used for entering multiple Telnet/SSH Username and passwords

3. Click the **include arrow button** .
Enter the **subnet address and mask address** in the corresponding fields.
4. Click the **include arrow button** .
Note: Enter the subnet address only without including a mask address. The entered addresses may be outside the seed router's hop count boundaries.
5. **To remove a subnet** from the list, **select the listed item** and **click the remove button** .
6. **Advanced IP Range:** This feature enables the user to define an Advanced IP range. The Advanced IP Range can be used for splitting a large address space or addressing smaller portions of the range

This option allows multiple subnet entries to be defined using one range definition. For example, the user can enter 10.10. [1-5]. [20-22] in order to define the following list of subnets:

10.10.1.20
10.10.1.21
10.10.1.22
10.10.2.20
10.10.2.21
10.10.2.22
...
10.10.5.21
10.10.5.22

Netformx Discovery will interpret the ranges and expand the expressions automatically.

Next, enter a valid IP range, which must be A.B.C.D where A, B, C and the following represent D:

- A number from 0 to 255
- {X-Y} where X and Y are from 0 to 255 and X<Y.
- (Represent range of 0 to 255).

Note: The main difference between range and subnet is:

In subnet mode, Netformx Discovery starts with Ping request to every IP address within the subnet. Then it will send SNMP request ONLY to devices that responded to Ping.

In Range mode, it will send Ping request and then SNMP request to every IP address within the range. Obviously, in this mode the discovery will take longer. In addition, in Range mode, devices that did not responded to SNMP will have an error in the dashboard.

Excluding Addresses/Subnets

The user may exclude addresses/subnets within the Seed Router hop count and/or include Addresses/Subnets lists by selecting the Exclude Addresses/Subnets box.

1. To **exclude specific subnets and devices**, check the **Exclude Addresses/Subnets** box.

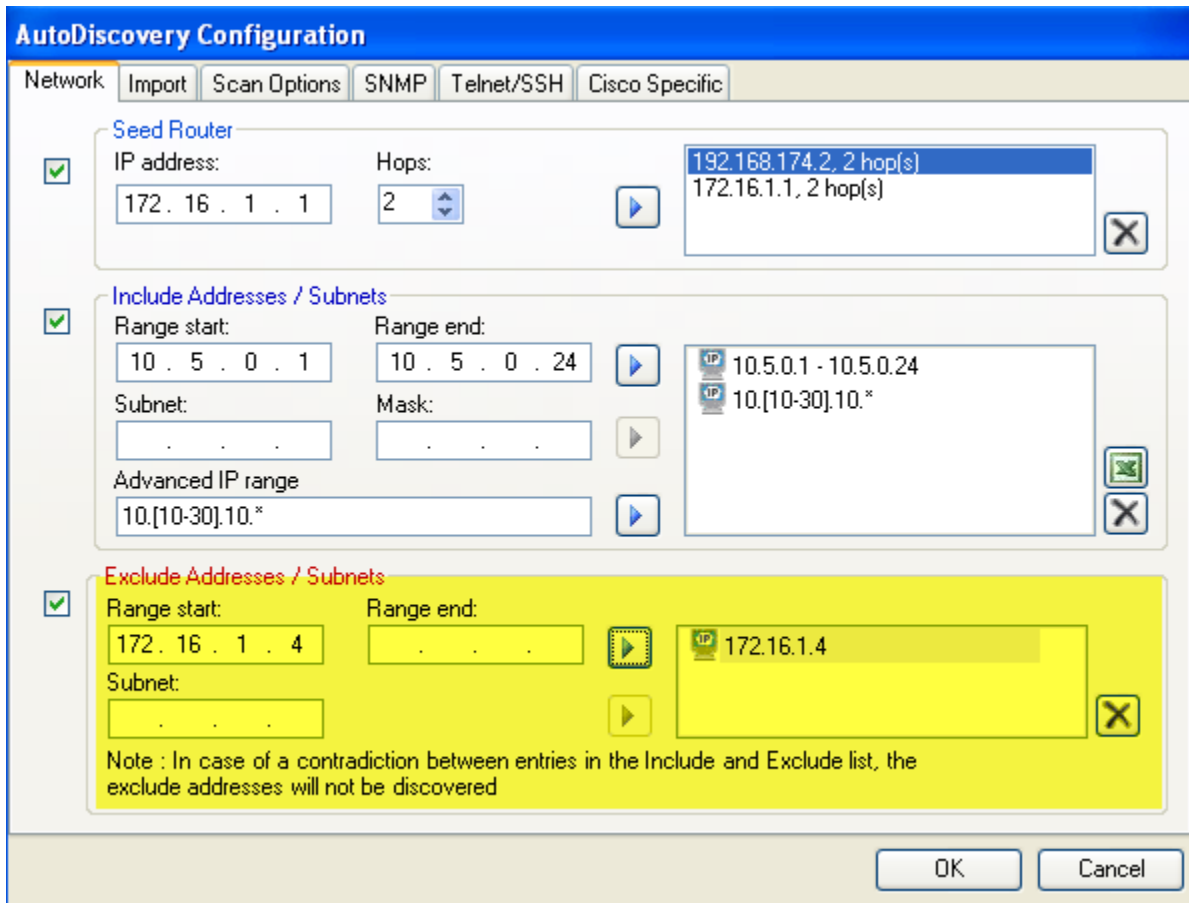




Figure 5

2. Enter a **range of device addresses** using the **Range Start** and **Range End** fields; then click the include arrow button .
- Note: If there are multiple ranges, repeat this step for each. For single addresses only, complete the Range Start field.*
3. Enter the **subnet address** in the corresponding field and **click the include arrow button**.
4. To **remove a subnet from the list**, **select the listed item** and **click the remove button** .

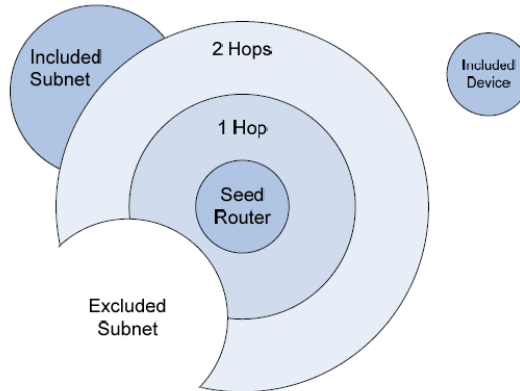


Figure 6

SNMP Tab

SNMP Configuration

1. Select **SNMP V1** and/or **SNMPv2c** and/or **SNMP V3** box to activate the corresponding pane(s) below.
Note: If all three-protocol versions are used, set the order to use the network's more commonly used protocol by clicking the Up ▲ or down ▼ arrow.

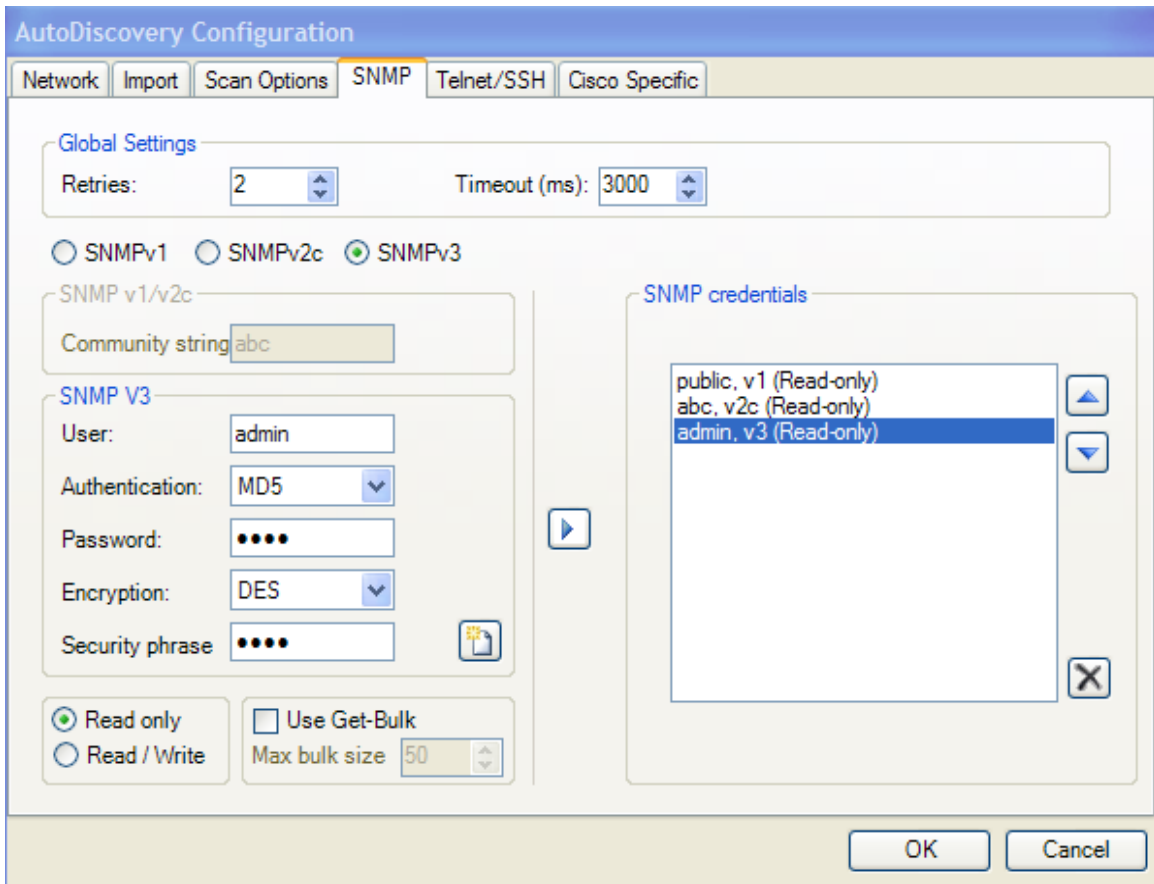


Figure 7

2. **Read Only Community String.** Enter the specific Community String; otherwise the default, "public" string will be used. Multiple strings can be entered
3. **Define the order** that to initiate SNMP transactions using the Up and down arrows.
Note: It is a best practice to order strings based on their importance (most commonly used being first on the list), to optimize the discovery process.
4. **Read/Write Community String.** This is only required to collect Cisco Config Files information. Use with the **Cisco Config Tab.**
5. **Use Get-Bulk:** For SNMPv2c and SNMPv3 define whether to Use Get-Bulk and the Max bulk size by checking the Use Get-bulk checkbox and specify the Max bulk size. The number defined represents the number of Get Next commands to link together. This allows Discovery to retrieve SNMP tables faster thus speeding up the discovery process.
6. **Adjust timeout and retries counts** based on the needs.

Telnet/SSH Tab

Configuring Protocols

1. Select **Telnet** and/or **SSH box** based on the user's requirements (Figure 8).
2. Use the **Login Settings** pane to complete the **User, Password, and Enabled password** fields.
3. It is possible to make multiple entries with Telnet/SSH credentials and then click the mover arrow to include the entry in the right-hand pane.

*Note: To import a list of addresses and their specific Telnet/SSH credential, go to the Network Tab and click on the **Excel icon** under Include Subnets/Address options. (Figure 9)*

4. **Adjust timeout and retries counts** as needed.
5. **Check the "Query all devices using Telnet/SSH"** which is mandatory for *Network Analysis using Cisco Discovery Services (CDS).*

Netformx Discovery Step-by-Step Guide

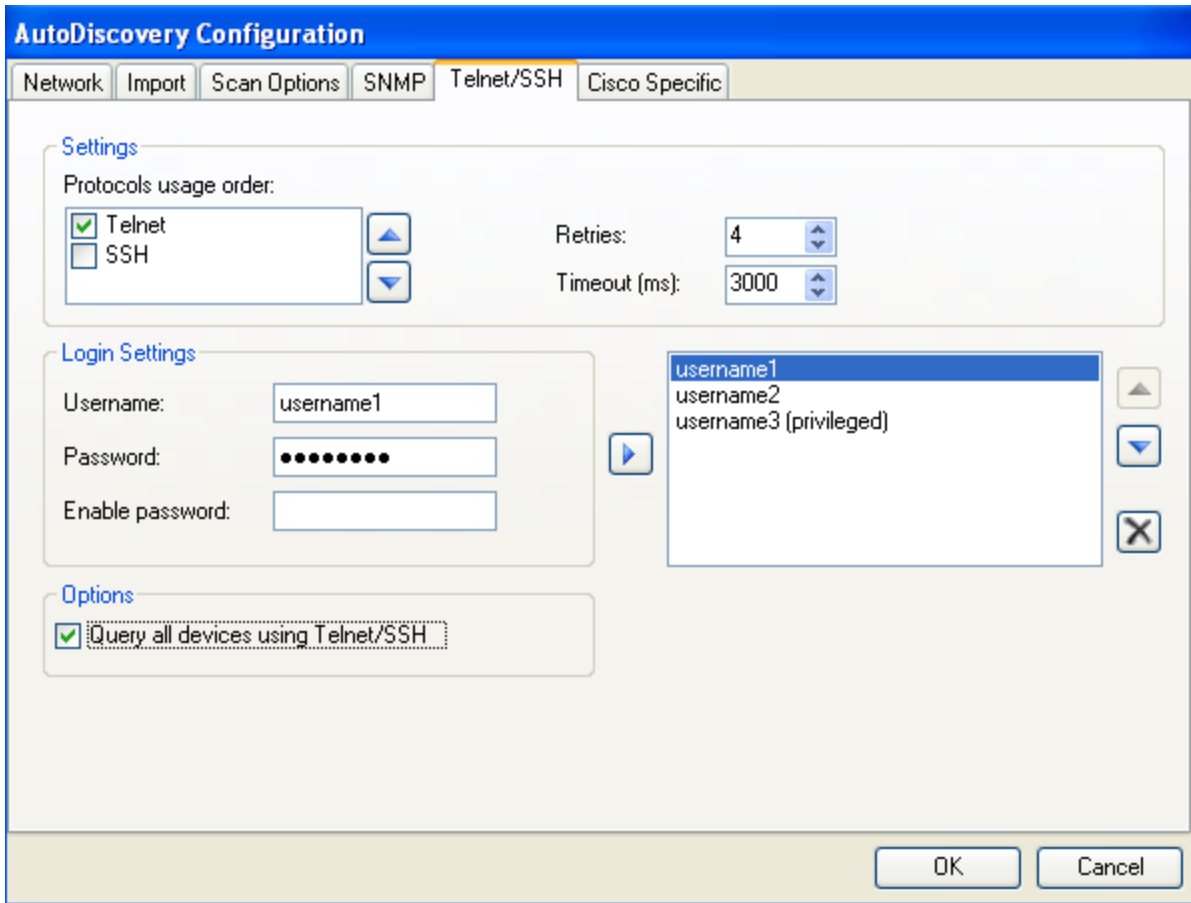


Figure 8

	A	B	C	D	E	F	G	H	I
1									
2		From Address	To Address	Host Name	Telnet/SSH Device Type	Protocol Order	Telnet/SSH Username	Telnet/SSH Password	Telnet/SSH Enabled Password
3		10.10.10.1			Cisco	Telnet Only	UserName1	password1	enPwd
4		10.10.10.2			Cisco	Telnet Only	UserName2	password2	enPwd
5		10.10.10.3			Cisco	SSH Only	UserName3	password3	enPwd
6									
7									
8									
9									
10									

Figure 9

Cisco Config Tab

The discovery process to collect Cisco Configuration files can be configured using Netformx Discovery.

1. To **download Cisco config files**, check the box **Use Cisco configuration files** (Figure 10).
2. **Select Save To** and specify a location where to save all Cisco configuration files.
3. Under **Download Settings**, select the appropriate method for downloading the configuration files
 - a. **Telnet/SSH** or **TFTP/SNMP**.
Note: Enable Password must be set to use this option.
 - b. **SNMP tab**
Note: Configure Read/Write Community Strings to use this option. See SNMP Tab instructions.
4. **Adjust Retries & Time out Count.**
5. Under **Scope**, select **All Devices** or **Selected Devices** and provide IP Addresses.
6. Check the "**Retrieve IP Phone Configuration**" to discover Cisco IP Phones and to retrieve their configurations. Checking this option enables the system to retrieve Cisco IP phones configuration via HTTP for each phone. If this option is disabled then the IP phone will be presented with a generic IP phone symbol. The query identifies the following: Model Number, MAC Address, Serial Number, Host Name, Phoned, SysDesc & Subnet Mask.
7. Check "**Enable Cisco Discovery Service (CDS)**" which is mandatory to enable data collection for Cisco Analysis Service.

Note: Devices must support both SNMP and Telnet for Netformx Discovery to use Telnet.

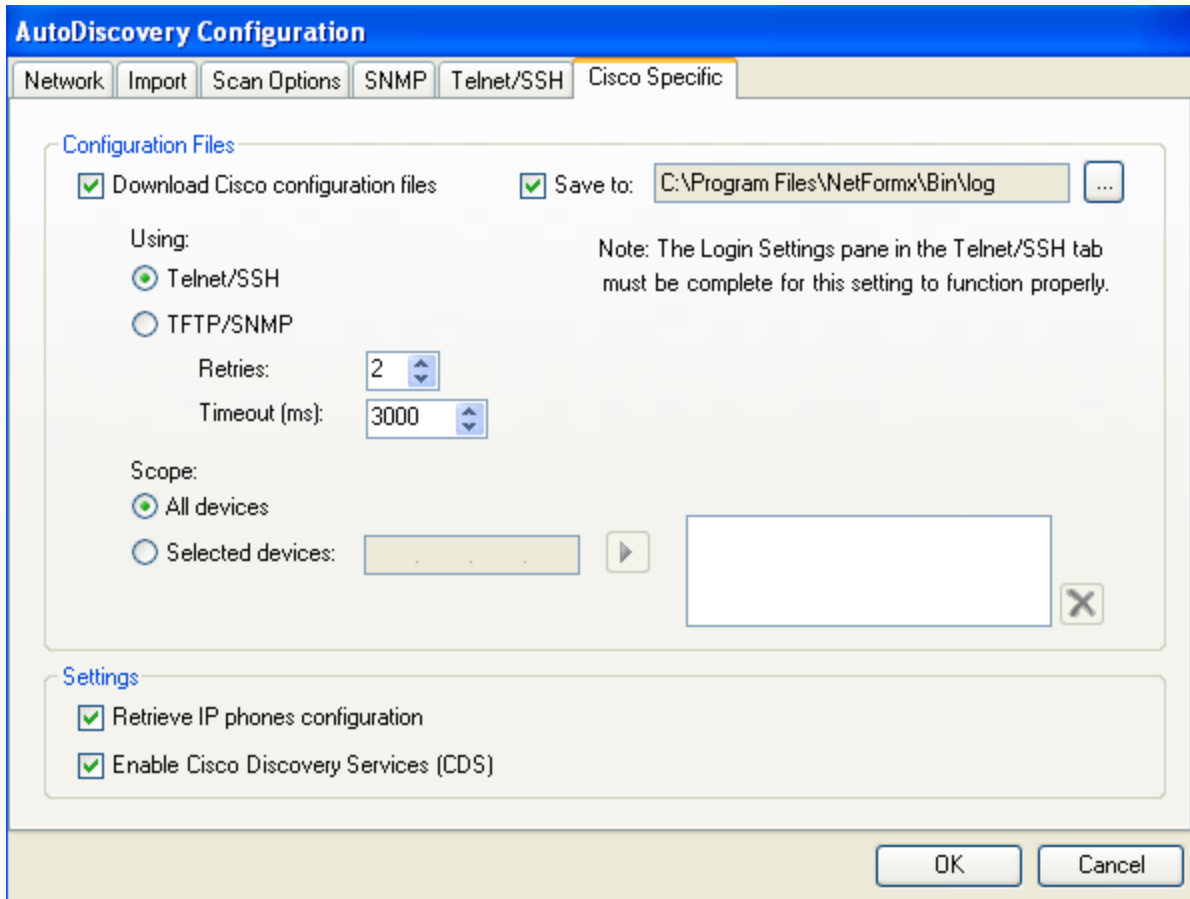


Figure 10

Scan Options Tab

Netformx Discovery enables the user to manage the scope of the discovery by defining the **Scan Mode** and **Ping Settings**.

Scan Mode

Quick scan (routers only): Generates a quick overview of the network by scanning only the routers.

Full scan: Discovers all devices in the defined network. The discovery process tries to scan beyond non-responsive routers.

Discover physical links: Discovers physical connections, i.e. Cisco Discovery Protocol (CDP) and VLAN's.

Ping Settings

Perform Ping Sweep: Discovers any unregistered SNMP and IP nodes in the network.

Note: Adjust the retries & timeout count as required.

Name Resolution: Resolves IP addresses into DNS host names.

Note: This may add time to the discovery process.

Use Windows services: Poll Microsoft Windows environment by providing domain username and password for authentication.

Note: This may add time to the discovery process.

Set the **Advanced settings**, including:

- a. **Device Discovery Profile** settings:
 - **SNMP only:** Selecting this option instructs Discovery to search for devices that communicate with SNMP protocol only. This option is useful for networks that ICMP is blocked. In this case, Discovery will attempt to query directly the device using SNMP protocol.
 - **Ping then SNMP:** Selecting this option means that Discovery will first initiate a ping request and then will initiate a query using SNMP. (*Note: This method presents devices that do not respond to SNMP*)
 - **Perform SNMP upon successful ping:** Checking this option means that only devices that respond to ping will be queried using SNMP protocol.
- b. **SNMP/ Ping sweep all addresses in discovered subnet(s):** This checkbox is dependent on the selections made in the *Device Discovery* profile above. Checking this option will initiate Ping/SNMP requests for every address in a discovered subnet.
- c. **Include non-responding devices in Results:** Check this option to include non-responsive devices in the Results tab (may decrease performance).

Max PPS: In the **Performance area**, define the maximum number of packets sent each second. A larger number of packets can accelerate the discovery process, but will load the network.

Netformx Discovery Step-by-Step Guide

The screenshot shows the 'AutoDiscovery Configuration' dialog box with the 'Scan Options' tab selected. The dialog has a blue title bar and a light beige background. At the top, there are five tabs: 'Network', 'Import', 'Scan Options', 'SNMP', 'Telnet/SSH', and 'Cisco Specific'. The 'Scan Options' tab is active. The configuration is organized into several sections:

- Scan Mode:** Contains two radio buttons: 'Quick scan (routers only)' (unselected) and 'Full scan:' (selected). Below 'Full scan:' is a checked checkbox for 'Discover physical links'.
- Name Resolution:** Contains two checked checkboxes: 'Resolve names' and 'Use Windows services'. Below these are two text input fields labeled 'Username:' and 'Password:'. A note below the fields reads: 'Note: Use of windows services might slow down discovery process'.
- Ping Settings:** Contains two spinners: 'Retries:' set to '1' and 'Timeout (ms):' set to '4000'.
- Advanced <<:** A button to expand advanced options.
- Device Discovery Profile:** Contains two radio buttons: 'SNMP only' (unselected) and 'Ping then SNMP' (selected). Below it is a checked checkbox for 'Perform SNMP upon successful ping'.
- Performance:** Contains a spinner for 'Max PPS:' set to '10'.
- Global Options:** At the bottom, there are two checkboxes: a checked one for 'Ping sweep all addresses in discovered subnet(s)' and an unchecked one for 'Include non-responding devices in Results (may decrease performance)'.

At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

Figure 11

Import Tab

Netformx Discovery enables you to define the types of devices to import into the DesignXpert project.

Import Options

All Devices: Import all devices in the network.

SNMP Devices Only: Import only SNMP devices.

Selected Types: Imports devices only from selected categories.

Import New Devices Only: Import only devices not discovered during a previous discovery activity.

Auto Import after Discovery: Uncheck this box to preview the discovery results before importing to the DesignXpert project.

Note: The default setting checks this box.

Import devices into a single drawing: When this box is checked the discovery import does not generate a sub-drawing for each subnet site rather only for a single network drawing in which all discovered devices are located.

Existing Discovery Data

Override existing data with Discovered data: Replaces devices with the newly discovered devices regardless of device type discrepancies.

Prompt in case of contradiction: Creates messages alert for any discrepancies

Locate newly discovered devices on drawing margins: Netformx Discovery will place newly discovered devices outside the drawing area.

Match Existing Devices by select matching criteria (Mac or PC) device address (Figure 12).

When rediscovering a network, Netformx Discovery may discover a new device with the same host name as a pre-discovered device. If so, it attempts to confirm the devices' equality by discovering the MAC and IP Address.

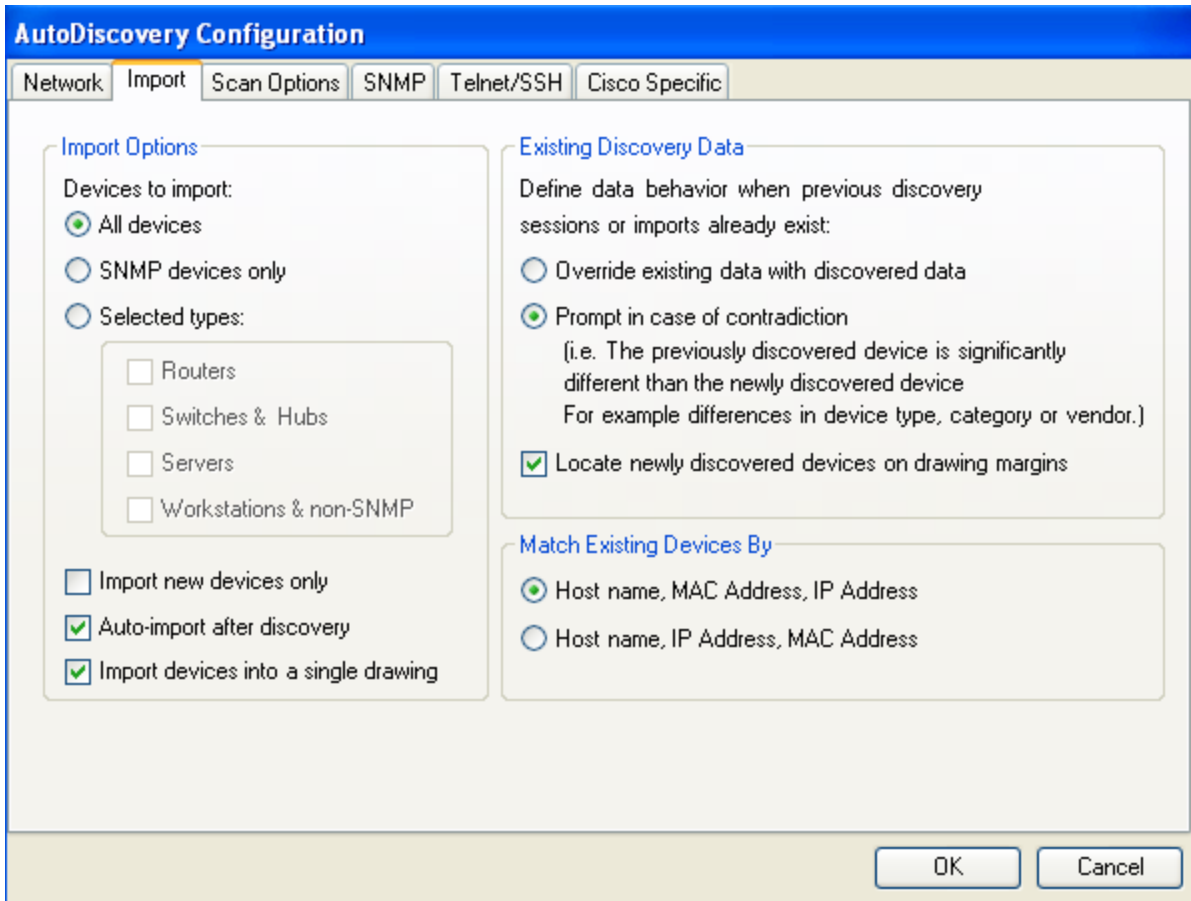



Figure 12

Run Network Discovery

After you have completed entering the Network Discovery Configuration Settings, Click OK; that will bring you to Network Discovery Dashboard where you can now click the **Start Discovery** button  (available from the toolbar).

The time to complete the discovery process is dependant to the parameters configured in the settings. A progress bar in the bottom left hand corner of the window indicates that the discovery process is in progress as well as providing an Elapsed time readout.

Discovery completed

Post Discovery Operation

Here are some of the ways to view the results of the discovery.

View device information in the drawing by right clicking on the device (Figure 13).

- View SNMP Tables (Figure 13)
- Interface table (Figure 13)
- Cisco Power supply table (Figure 13)
- Cisco IP Phone table (Figure 14)
- Open Configuration File (Figure 15)

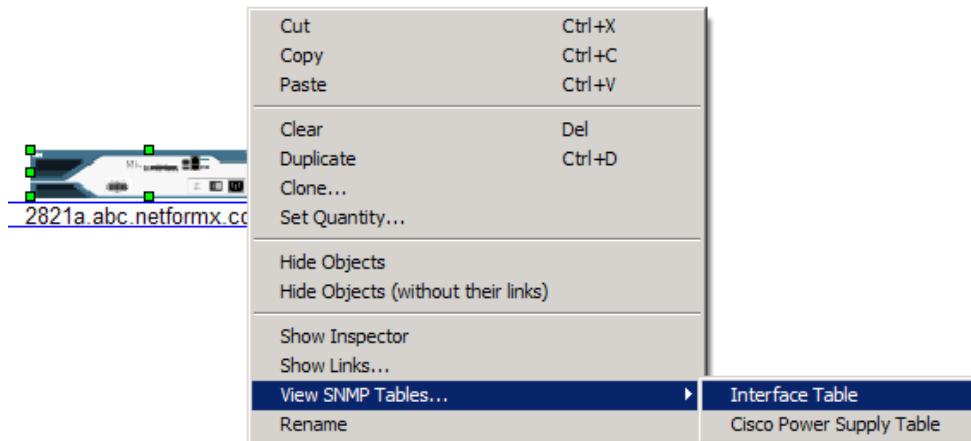


Figure 13

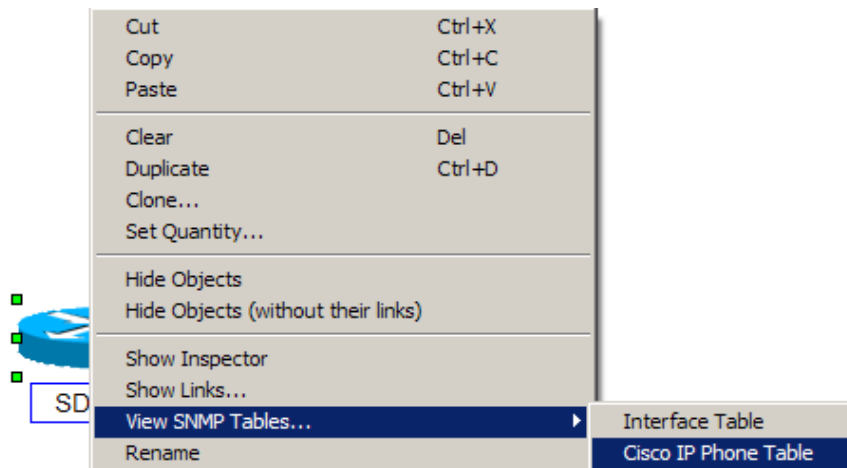


Figure 14

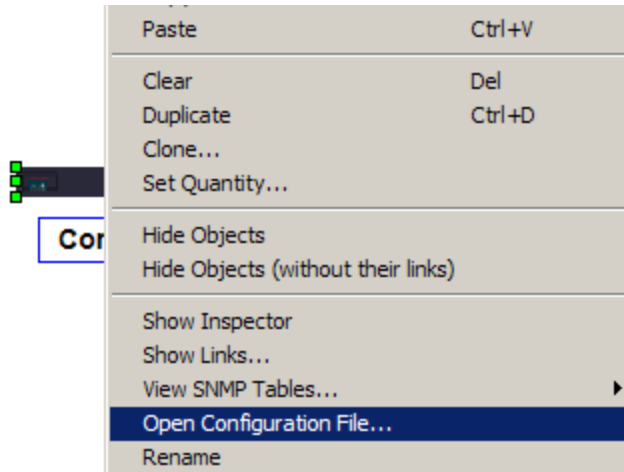


Figure 15

Tabular view (Figure 16)

View menu/ Tabular view

- Devices tab
- Address tab
- Assets tab
- Links tab

Name	Device Name	Vendor Name	Catalog Num	Verified Status	SysDesc
npv-7513b-mc-corp...	CISCO7513/8X2-MX	Cisco	CISCO7513/8X2-MX	Unverified and non-...	Cisco Internetwork ...
mexico-3640-se0-0	CISCO3640	Cisco	CISCO3640		Cisco Internetwork ...
ashburn-3640-s0-0-0	CISCO3640	Cisco	CISCO3640		Cisco Internetwork ...
saopaulo-s0-0-1	CISCO2621	Cisco	CISCO2621		Cisco Internetwork ...
bldgf-s-0-1-t1-to-npv	CISCO3640	Cisco	CISCO3640		Cisco Internetwork ...
buenos-aires	CISCO3640	Cisco	CISCO3640		Cisco Internetwork ...
sao-paulo-warehouse	CISCO1601	Cisco	CISCO1601		Cisco Internetwork ...
apacwan-in02	CISCO2621	Cisco	CISCO2621		Cisco Internetwork ...
germantown-3640-s...	CISCO3640	Cisco	CISCO3640		Cisco Internetwork ...
Hub#2	Hub	Generic Vendor			
Hub#3	Hub	Generic Vendor			

Navigation tabs: Devices / Addresses / Assets / Links

Figure 16

Discovery Reports

From the **reports menu** in DesignXpert, you can select standard reports or customize Excel reports to assist in analyzing the discovered data by using one of the following paths:

Reports menu → Discovery → select the report (See figure 17)

Report Menu → Cisco Product Availability Report (For Cisco EoX information)

Report Menu → Customize Excel Report and create desired report template.

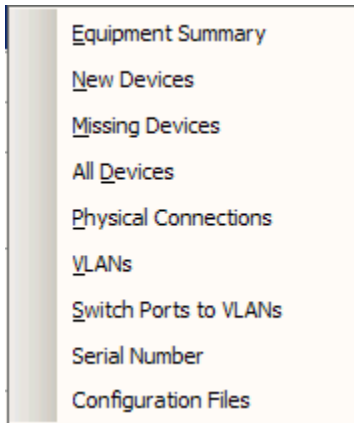


Figure 17

Two Valuable Discovery Reports

1. **Equipment Summary Report**
 - a. Use this report to assess vendor equipment, description, software version, number of switching ports, etc.
 - b. If participating in a Vendor Network Assessment program, the vendor may request the 'Equipment Summary' report.
2. **Cisco Product Availability Report**
 - a. Use this report to assess the status of Cisco equipment to decide whether to upgrade, replace or maintain devices based on the End of Life, Last Date of Sale, Last Date of Support, etc.
 - b. To see all of the discovered products in this report, go to the *Scope Tab*, select *include* from the drop-down menu and then select *All*.

Network Analysis Using Cisco Discovery Service (CDS):

- Once the network is discovered and imported to DesignXpert, a network assessment request can be submitted using Cisco Discovery Services.
- From the **Tools menu** in DesignXpert, select **Submit Network Assessment Request** and select the scope of the discovery project you want to submit to CDS for analysis (Project, Current drawing or Selection) This will bring up the CDS registration form. Fill in the complete form and **click Submit**.

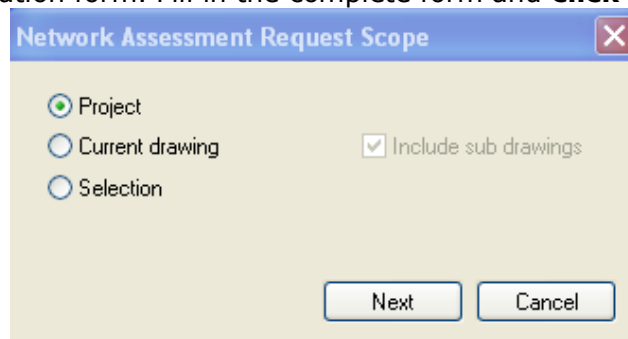


Figure 18a

Netformx Discovery Step-by-Step Guide

Submit Network Assessment Request (Cisco equipment)

Request Details
 You are about to submit Network Assessment request for project **Lab.npz**

Transaction Name:

Service Type: **Product Alert**

Enable CDS Services: Service Coverage Report [KTN] Field Notices
 Show IP addresses Enhanced PSIRT Reporting

Note: The IP address will be sent to Cisco discovery service (CDS)

Customer Details

* Company name:

* Vertical market: * Market segment:

* Theater:

User Contact Details

* First name: * Last name:

* Country: State/Province:

* Email: Enable email notification

* User type: Cisco SE Cisco partner

Partner details

Contact type	CCId	First name	Last name	E-mail
Primary Cisco Sales Engineer	DYOSHASP			
Alternate Cisco Sales Engineer				
Cisco Sales Engineer Manager				
Cisco Sales Engineer Director				
Cisco Account Manager				

* Mandatory fields Note: When re-submitting the project any data that was previously analyzed will be over-written.

Figure 18b

Product Alert

- Device Level Query
- KTN Only ANSR Transaction
- Network Inventory
- Product Alert**
- Repeat Inventory Transaction
- Supplemental Transaction
- Test/Lab Inventory Transaction

Figure 18c

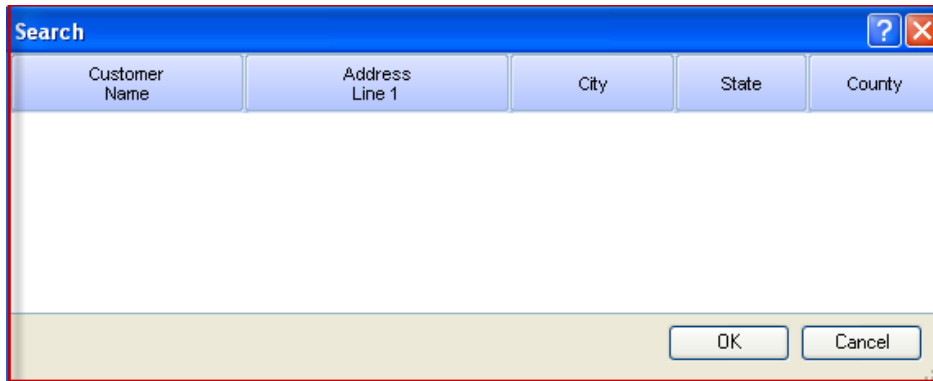


Figure 18d

Submit Network Assessment Request- Service Types

Service Type: From the dropdown list, select the relevant CDS Service Type:

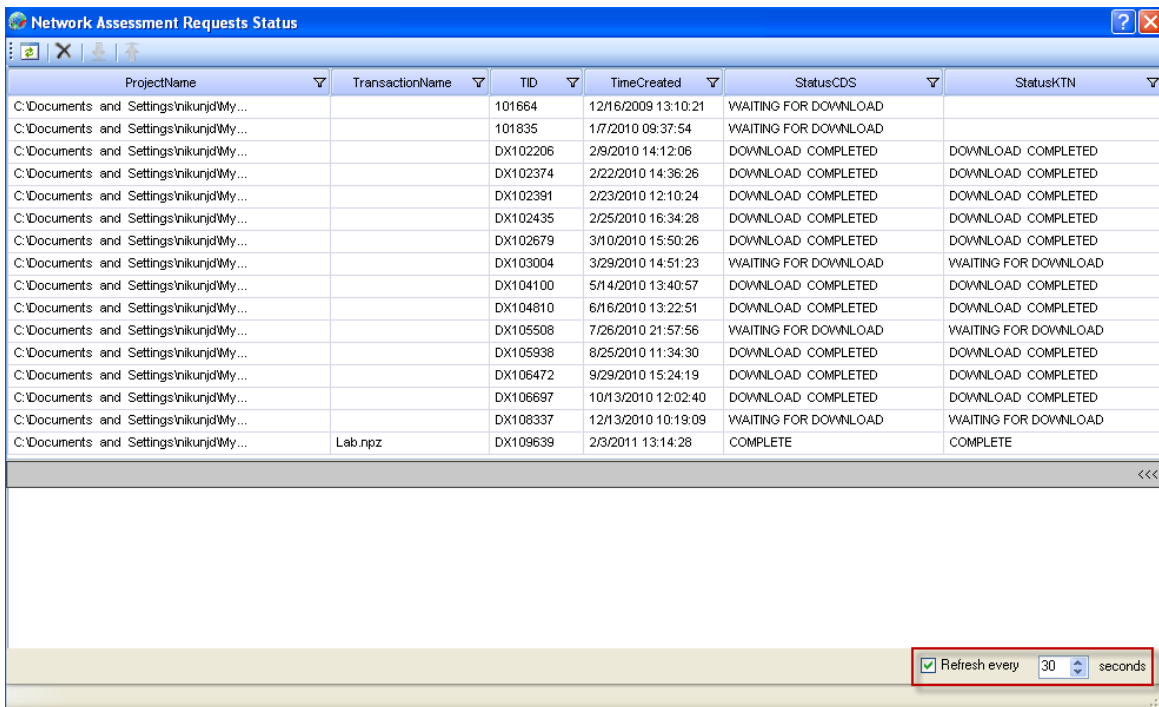
- a. **KTN Only ANSR Transaction:** This transaction is intended for users who require a KTN analysis and ANSR report. This report is produced by Cisco and does not contain device profiling. Data is submitted to the KTN system and not the CDS Profiler for the purposes of service contract reporting. The user can access the report from the KTN portal only and is not available via DesignXpert.
- b. **Device Level Query (DLQ) Definition:** Limitation of up to 5 devices. Process is fast however it does not include KTN analysis. The transaction is tracked in standard metrics as device level query.
- c. **Network Inventory Transaction:** A standard customer transaction that includes a full network assessment scan including site as well as segment assessment. This service type:
 - Creates a regular CID
 - Works with KTN
 - Tracks in metrics as a regular transaction.
 - Allows NL Database Classification & Storage: These types of transaction are classified as "NI" in CDS database. The data is forwarded to the Cisco Discovery transaction system and the CA IB database.
- d. **Repeat Inventory Transaction:** Repeats the profiling of an existing transaction without the need to upload the Discovery data a second time. Analyzes the discovered network again based on up-to-date data from Cisco.
- e. **Supplemental Transaction:** This transaction is an add-on to an existing transaction for the purpose of adding additional devices. This transaction does not have a TID and can't be traced separately from the associated transaction. However, an existing TID is required in the initial registration in order to process new devices, resulting in them being added to the same TID record.
- f. **Test/Lab Inventory Transaction:** Profiling transaction that is not tracked in metrics and does not include KTN analysis.

Netformx Discovery Step-by-Step Guide

Customer Details: Enter the relevant customer details and then click **Search**. The application now conducts a search for "CCOID" based on the search criteria. The results will display in a pop up window.

- DesignXpert will begin uploading the discovered information to the CDS server in the background (non-blocking).
 - To check the status of the transaction From the **Tools menu**, select "**Network Assessment Queries Status**". User can now refresh the screen automatically with the ability to identify how often the refresh should occur.

Note: Processing time depends on the size of the transaction (number of devices and cards loaded) and the number of pending transactions ahead in the queue. The approximate processing time is eight seconds for each piece of equipment.



The screenshot shows a window titled "Network Assessment Requests Status" with a table of transaction data. The table has columns for ProjectName, TransactionName, TID, TimeCreated, StatusCDS, and StatusKTN. The data rows show various transactions with their respective IDs and creation times, and their current status (e.g., WAITING FOR DOWNLOAD, DOWNLOAD COMPLETED, COMPLETE). At the bottom right of the window, there is a refresh control with a checked box, the text "Refresh every", a spin box set to "30", and the text "seconds".

ProjectName	TransactionName	TID	TimeCreated	StatusCDS	StatusKTN
C:\Documents and Settings\nikunjid\My...		101664	12/16/2009 13:10:21	WAITING FOR DOWNLOAD	
C:\Documents and Settings\nikunjid\My...		101835	1/7/2010 09:37:54	WAITING FOR DOWNLOAD	
C:\Documents and Settings\nikunjid\My...		DX102206	2/9/2010 14:12:06	DOWNLOAD COMPLETED	DOWNLOAD COMPLETED
C:\Documents and Settings\nikunjid\My...		DX102374	2/22/2010 14:36:26	DOWNLOAD COMPLETED	DOWNLOAD COMPLETED
C:\Documents and Settings\nikunjid\My...		DX102391	2/23/2010 12:10:24	DOWNLOAD COMPLETED	DOWNLOAD COMPLETED
C:\Documents and Settings\nikunjid\My...		DX102435	2/25/2010 16:34:28	DOWNLOAD COMPLETED	DOWNLOAD COMPLETED
C:\Documents and Settings\nikunjid\My...		DX102679	3/10/2010 15:50:26	DOWNLOAD COMPLETED	DOWNLOAD COMPLETED
C:\Documents and Settings\nikunjid\My...		DX103004	3/29/2010 14:51:23	WAITING FOR DOWNLOAD	WAITING FOR DOWNLOAD
C:\Documents and Settings\nikunjid\My...		DX104100	5/14/2010 13:40:57	DOWNLOAD COMPLETED	DOWNLOAD COMPLETED
C:\Documents and Settings\nikunjid\My...		DX104810	6/16/2010 13:22:51	DOWNLOAD COMPLETED	DOWNLOAD COMPLETED
C:\Documents and Settings\nikunjid\My...		DX105508	7/26/2010 21:57:56	WAITING FOR DOWNLOAD	WAITING FOR DOWNLOAD
C:\Documents and Settings\nikunjid\My...		DX105938	8/25/2010 11:34:30	DOWNLOAD COMPLETED	DOWNLOAD COMPLETED
C:\Documents and Settings\nikunjid\My...		DX106472	9/29/2010 15:24:19	DOWNLOAD COMPLETED	DOWNLOAD COMPLETED
C:\Documents and Settings\nikunjid\My...		DX106897	10/13/2010 12:02:40	DOWNLOAD COMPLETED	DOWNLOAD COMPLETED
C:\Documents and Settings\nikunjid\My...		DX108337	12/13/2010 10:19:09	WAITING FOR DOWNLOAD	WAITING FOR DOWNLOAD
C:\Documents and Settings\nikunjid\My...	Lab.npz	DX109639	2/3/2011 13:14:28	COMPLETE	COMPLETE

Figure 19

- DesignXpert continues to poll the server in the background (based on your timing selected), checking for a change in the transaction status. Once a submitted transaction is completed, the following messages pops up see Figure 20. Click **Download Now** (above) for the transaction status to change to "Complete". Clicking *Download Later* will set the status to "Waiting for Download"

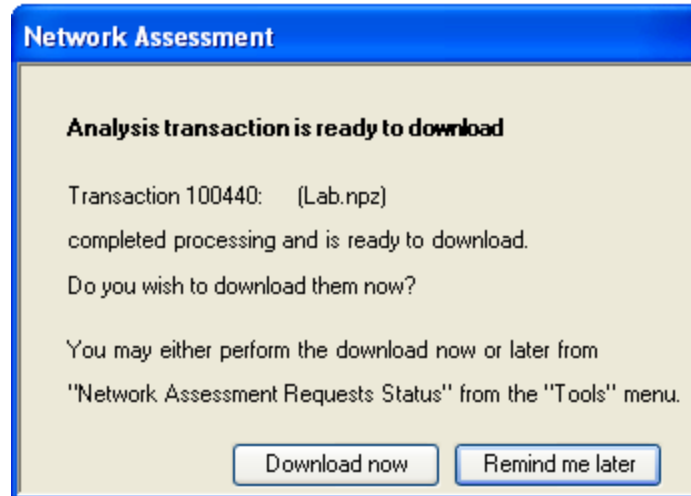



Figure 20

- Either press **Download now button** OR while in the transaction monitor (Figure 20), select the row of a completed transaction and click the **Download button**.

- *Note: that only a single row can be marked at a time*
- You will see a progress bar (Figure 21) as transaction results are being downloaded.
- Once the transaction has finished downloading, the status will change to "Download completed". There is no restriction on downloading the transaction more than once, although it will add no new information.

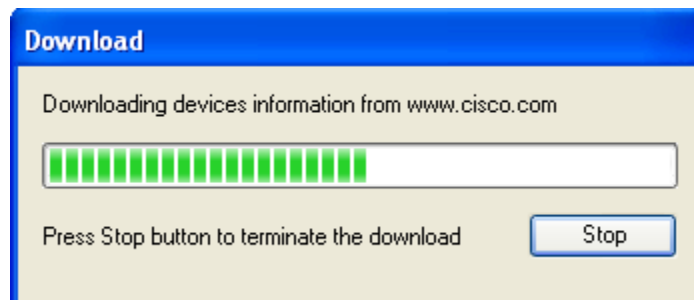


Figure 21

CDS Analysis Reports

With CDS (Cisco Discovery Service), integration into Netformx Discovery introduces three new reports: **Network Assessment Report**, **Network Assessment Executive Report** and **Network Assessment Summary Document**. These reports are located in the "Cisco" sub menu, found in "Reports" menu of DesignXpert.

Network Assessment Report

This report is a detailed analysis of the data, including information down to the level of single device (by IP address) and models (catalog numbers and OS versions) including: Detailed Equipment List, Chassis Summary, Component Summary, Contract Validation Summary, Detailed PSIRT Report, Chassis PSIRT Summary.

Network Assessment Executive Report

The executive report shows aggregated information on the analyzed data, at the product line and family levels. This report places special emphasis on showing equipment that has reached or is approaching the Last Day of Support (also called EOL). Reports include Summary, Product Series – IOS, Product Series – CatOS, Product Series, Train, and PSIRT.

Each report consists of several pages (Excel spreadsheets), each showing a different aspect of the analyzed data.

Network Assessment Summary Document

The Network Assessment Summary Document is a helpful customer-facing document with a Professional look and feel. Customize this report by applying a branding logo. This report includes useful Pie charts, Bar charts for IOS, CatOS, Train, PSIRTS, and Contracts etc.

Network Assessment Data Review

This report will allow you to view data to be uploaded to CDS before the submission.

Netformx Discovery Files and Databases

After the Netformx Discovery process is complete, DesignXpert generates the following files and database:

Log Files: Lists all network elements with their IP address and status. This file is generated automatically during a Netformx Discovery session.
Path: %appdata%/Roaming/Netformx/ND/log

Interface Table: Provides detailed information about each device's interface in a customizable table.

Netformx Discovery Database: DesignXpert creates a database with a file name consisting of the project's filename with an ".ndr" extension. By default, this file is located in the same directory as the project file. The file name can change using the Project Properties dialog box.

Tips Summary

- Start with a limited discovery of routers and subnets only, prior to analyzing the project to decide the limits and requirements of the desired outcome (a router/subnets discovery only should complete in just a few minutes).
- Start with low limits (hops, retries, and timeouts) and progress to discover more by changing one parameter at a time.
- Usually no retries and a shorter timeout limit on SNMP and Pings will suffice for a response receipt from all nodes.
- When doing a Ping Sweep, raise the rate to 50pps (The traffic generated will be around 25Kbps, considered negligible in today's networks).

Netformx Discovery Step-by-Step Guide

- Note that packets will need to travel back and forth so the Firewall should allow SNMP, Telnet in both directions.
- If the Firewall or the Networks do not allow ICMP then check that the configuration does not include ping as an SNMP filter.
- DNS Name resolution could take up to 10 seconds per node. Therefore, it may not be best to run it on first-time discovery (Example: In a 5000 node network, it could take up to 14 hours).
- If not using Windows networks and there is no significance in that type of information, do not ask to run them since these is a time consuming operation.
- It is important to pay attention to discovery errors and warnings generated in the discovery results grid. It may indicate that the discovery settings are not accurate.
- For optimum performance, the discoveries should run from workstations connected directly to the Local Area Network.
- SNMP must be enabled on a device and configured for RO (read only) or RW (read – write) in order to discover the device’s internal configuration. Enter the specific community string in DesignXpert, otherwise the default, “public”, is used.
- Note to allow SNMP access from the workstation running the discovery to the discovered addresses.
- To read multiple NT domains, enter a single user name and password that is a member of all these domains under the NOS Services tab in the Windows Service window.
- Disable local firewall software during discovery (either windows internal firewall or third party products).
- If the discovery log file is very large, it may not open properly with WordPad. In this situation, it is best to save the log as a .txt file and open manually with Microsoft Word.

Netformx Customer Support

To request Netformx Customer Support, please complete the [Online Case Submission Form](#) located in the [Customer Support](#) section of the Netformx web site. This will enable Customer Support to quickly assess and answer any discovery questions. The following information will be needed:

1. **Software and Library Version Of DesignXpert** (see Help>About Files)
2. Provide the following files:
 - a. **Discovery File** – The file name is *projectname.ndr*. To find this name, follow this path: *Project* → *Properties* → *Discovery* from the open Discovery project.
Note: The default is the directory where the saved project file is located
 - b. **Please Zip the file** to reduce the size prior to sending.
 - c. **Log File** - To find this file, follow this path: C:\Program Files\bin\log.

3. A list of **IP addresses of the incorrectly discovered chassis** from the discovery file.
4. Please confirm the following has been checked before submitting the request of improperly discovered devices:
 - a. *Right click* → *Properties* on the device in question and make sure to populate the Discovery tab with the SNMP information captured during the discovery.
 - b. Attach results of Tools Menu → Record SNMP Walk SNMP log for issues with missing SNMP information in device Netformx Discovery properties for a specific IP device.

To create an SNMP log file:

1. From the *Tools* menu, select **Record SNMP Walk**.
The *SNMP Log* window is displayed.
2. Enter the IP Address of the device you wish to log in the *IP address* field.
3. Enter the **Root OID**. The SNMP will log all entries for this SNMP sub tree level.
4. Enter the file name and path for the file you wish to generate in the *File name* field.
5. Click **Configure** to open the *SNMP* window, in order to configure the SNMP parameters.
6. Click **Start Log** to create the Excel file.

Send follow-up correspondence to support@netformx.com or call Netformx Customer Support at 1-888-314-6031 (U.S. and Canada) or 1-408-423-6650 (International).

Online Resources

VOD Training/Certification Center	http://learning.netformx.com/home/
Customer Support Center	http://www.netformx.com/home/customerservice
DesignXpert Web Page	http://www.netformx.com/home/designxpert
ND Resource Web Page	http://design.netformx.com/nnd
Resource Center	http://www.netformx.com/home/resourcecenter
Support Case Form	http://download.netformx.com/Support/Web2Case.htm

IBLM Resources Link

All IBLM Resources www.cisco.com/go/emiblm

Recorded ND/CDS Training by local Cisco Channel Team (Cisco EMEA):
<https://cisco.webex.com/ciscosales/lr.php?AT=pb&SP=EC&rID=42431632&rKey=1f469158f4dae196>