D-VIEW™ 6 Standard / Professional

NETWORK MANAGEMENT SYSTEM

User Manual

VER.1.04

D-Link®
Building Networks for People

D-Link Corporation
D-View 6.0 User Manual
Published: October 2009

PROPRIETARY NOTICE
This document supports D-Link Network Management System software.
D-View 6.0 is confidential and proprietary information of D-Link Corporation.

D-Link may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from D-Link, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2009 D-Link Corporation. All rights reserved.

Table of Contents

About this Guide 5
Scope 5
Audience 5
Reader Alert Conventions 5
Style Conventions 6

1. Introducing D-View

Overview 8
What's Included 8
Product Line 9
Hardware and Software Requirements 9
Client-Server Architecture (Professional Edition) 10
Upgrade 11
Technical Specifications 11

2. Installing D-View

Installation Steps 15
Creating a Database (for Professional Edition) 23
D-View 6.0 Licensing 27
Trial Version 27
Obtaining the Activation Code 27

3. Understanding the Architecture

Modular Architecture 30
Features 31
Functions 32

4. Understanding the Interface

Introduction 34
Context-sensitive Menus 35
Main Menu 37
File 37
View 38
Application 39
System 39
NetTools 40
Advanced 41
Help 41

5. Using D-View

Getting Started 43
Login D-View 43
Managed IP Feature 43
System Configuration 47

Domain Manager 48
Startup Wizard 48

6. Working with Topologies

Creating a Topology 53
Creating Administrator-specific Topologies.....56
Using Topo Export/Import 59
Topology Generator Principle 60
Using Topology Generator 61
Rearranging the Topology 64
Using Rearrange Totally 64
Using Rearrange by step..... 64
Rolling Back a Topology 65

7. Managing and Monitoring Devices

Identifying Devices 68
Multi-vendor Support 69
Customizing Devices 70
How to Configure Devices not in Supported List 71
Discover Devices 72
Third Party Devices: Cisco Catalyst 2960 93
Managing Devices with Device Panel Simulation 106
Managing Devices with MIB Compiler 109
Retrieving OID of the device 113
Batch Configuration 115
Backup and Update the Devices' Configuration.....117
Using Device Type Check 119
Using Safeguard Check.....120
Labeling Devices 122
Editing Device Information.....123
Managing Events 126
Setting Poll Parameters 126
Setting the Devices to Poll 127
Viewing the Poll Device List.....128
Grouping Devices using Device Manager 128
Configuring Device Events 130
Retrieving Device Event Logs 133
Defining Trap Information 135
Locating the Switch Port 136
Monitoring the Link Status 138
Locating Devices 140
Locating Users 142

8. Basic Operations

View Options 146
Copy/Paste 146

Zoom In / Out / Fit 147
Set Background.....147
Upper Layer.....147
System Log 150
Administrator Manager 150
Restoring and Backing Up D-View 154
NetTools.....155
TFTP.....157
Retrieving ARP information 157
Net Toolbox 158
Port Packet Monitor.....159
Performance Monitor.....161

9. Index

Index.....167

About this Guide

Scope

Use this document to learn, use, and configure the different features of D-View.

Audience

This document is written for network managers, system administrators, and IT personnel who needs to work with D-View.

Reader Alert Conventions

Reader alerts are used throughout this document to notify you of essential information. The following table explains the meaning of each alert.

Reader Alert	Meaning
Tip	Alerts you about supplementary information that is not essential to the completion of the task at hand.
Note	Alerts you about supplementary information.

Style Conventions

The following style conventions are used in this guide.

ELEMENT	MEANING
Bold font	Use for describing user interface elements and characters that you type into the interface. For example, Hierarchy Topology Workplace and type http://192.168.1.1.
Italic font	Variables for which you supply a specific value. For example: *Filename.ext* can refer to any valid file name.
Courier New font	Samples of code and file paths and names.
Command	A command that is typed at the command prompt. For example, **ipconfig**.

Introducing D-View

OVERVIEW

D-Link strives to provide easy-to-use devices and software for users. Networking is a core technology for data communication. Based on abundant experience and profound understanding on end-user network management requirements, D-Link introduces D-View 6.0.

Network administrators can now efficiently manage and monitor

- device configuration,
- fault tolerance,
- performance,
- and security

of multiple networks and management switches with D-View, a Simple Network Management Protocol (**SNMP**) Network Management System. This is a comprehensive standards-based management tool designed to centrally manage critical network characteristics such as availability, reliability and resilience in a consistent manner. D-View accommodates a wide range of devices including:

- Wireless bridges
- Access points
- SNMP capable Smart/Managed switches
- SNMP capable routers
- OLT/ONU devices
- Broadband CO devices
- Windows Server

This guide does not discuss network design, management concepts or provide detailed explanations of SNMP, MIB, RMON and associated concepts. We assume the reader is familiar with these networking concepts; hence variables defined in D-View menus are self-explanatory.

D-View is designed for SMB, Enterprise, and Telecom administrators to efficiently manage their networks.

What's Included

D-View 6.0 comes with:

- D-View 6.0 and User Manual on CD-ROM
- User Manual

PRODUCT LINE

There are two editions of D-View:

- **D-View 6.0 Standard Edition:** D-View standard edition targets novice-intermediate users that have a small/mid-scale network of less than 1000 devices with basic requirements.
  DBMS: Access 2000
  Operating System: Windows XP, Windows 2000 Server or Advanced Server (English Version), Windows 2003 (English Version)
- **D-View 6.0 Professional Edition**: D-View professional edition targets advanced users that have a small/mid-scale network of more than 1000 devices with higher requirements.
  Operating System: Windows Server 2000 or 2003 (English Version)
  DBMS: SQL Server 2000/2005

Hardware and Software Requirements

Hardware Requirements

- CPU: 1.4GHz or above
- DRAM: 1GB or above
- Hard Drive Space: at least 200 MB
- Ethernet Adapter
- D-View supports the following:
  D-Link Switches:
  DES-3200-10, DES-3200-18, DES-3200-28, DES-3200-28F, DES-3526, DES-3528, DES-3528P, DES-3528DC, DES-3550, DES-3552, DES-3552P, DES-3828, DES-3828DC, DES-3828P, DES-3852, DES-6500, DGS-3100-24, DGS-3100-24P, DGS-3100-24TG, DGS-3100-48, DGS-3100-48P, DGS-3200-10, DGS-3200-16, DGS-3200-24, DGS-3308FG, DGS-3324SR, DGS-3426, DGS-3427, DGS-3450, DGS-3612, DGS-3612G, DGS-3627, DGS-3627G, DGS-3650, DGS-3700-12, DGS-3700-12G, DXS-3326GSR, DXS-3350SR
  D-Link Wireless APs:
  DAP-1353, DAP-2553, DAP-2590, DAP-3220, DAP-3520, DWL-2100 AP, DWL-2200AP, DWL-2700AP, DWL-3200AP, DWL-3260AP, DWL-7700AP, DWL- 8200AP

Software Requirements

D-View 6.0 Standard Edition
Software Requirements
• Microsoft Internet Explorer 6 with Service Pack 1 or later
• Microsoft XML Parser and SDK

Operating System	Service Pack Version
Microsoft Windows 2000 Server (English Version)	Service Pack 4
Microsoft Windows 2000 Advanced Server (English Version)	Service Pack 4
Microsoft Windows Server 2003 (English Version)	Service Pack 2
Microsoft Windows XP/Home/Professional	Service Pack 2

D-View 6.0 Professional Edition
Software Requirements
• Microsoft Internet Explorer 6 with Service Pack 1 or above
• Microsoft XML Parser and SDK

Operating System	Service Pack Version
Microsoft Windows 2000 Server (English Version)	Service Pack 4
Microsoft Windows 2000 Advanced Server (English Version)	Service Pack 4
Microsoft Windows Server 2003 (English Version)	Service Pack 2

• Database Management System

Database Management System	Service Pack Version
Microsoft SQL Server 2000 English version	Service Pack 2
Microsoft SQL Server 2005 English version	N/A

The differences between the two editions are described in the following table:

STANDARD EDITION	PROFESSIONAL EDITION
Standalone architecture	**Client-Server architecture**
Single user login	**Multiple user login**
Supports ~ 1000 nodes	**Supports ~ 5000 nodes**
Supports Microsoft Access*	**Supports Microsoft SQL**

*A separate installation of Microsoft Access is not required.

Both editions use **COM** (Component Object Model) technology.

D-Link recommends using a display with 1024 x 768 resolution.

Client-Server Architecture (Professional Edition)

By using the remote access feature of SQL Server, **D-View 6.0 Professional Edition** implements Client-Server architecture allowing workstations to share

database information. Given below is an illustration of the SQL Server Remote Access chart.

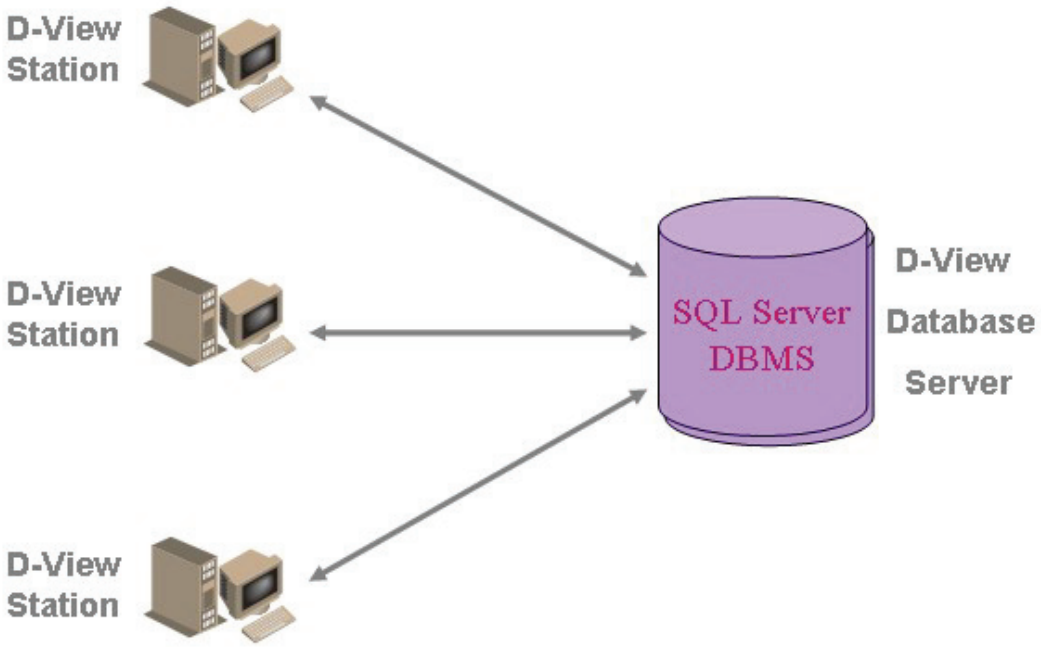


Figure 1: SQL Server Remote Access

To configure and connect to the SQL Server database, refer to Installation Steps and To Create a Database (for Professional Edition).

Upgrade

To upgrade from D-View 5.1 or earlier versions to 6.0, uninstall all the programs related to the old version and then re-install the new version.

Download the latest version of the User Manual from http://dview.dlink.com.tw for the added new features.

Technical Specifications

MIB Utilities	Security Management Functions
• Device SNMP Configuration • MIB II Information and Statistics • IF Information Tables • Spanning Tree Information and Port Configuration • Bridge 802.1d Information	• SNMP v3 covering security functions such as packet encryption/decryption, user levels for different classes of access right, MPD (RFC 2572), TARGET (RFC 2573), USM (RFC 2574) and VACM

<table>
<tr>
<td>and Port Configuration
• RMON Statistic, History and Event Group
• Transparent Bridge Forwarding and Static Filter Tables and Port
• Counter
• 802.1p Priority Configuration
• L3 Utilities
• MIB Browser
• MIB Complier</td>
<td>(RFC 2575)
• SNMP v3 Configuration
• Device Module Access Right Control
• NMS System Access Control
• NMS System Function Module Access Right Control
• Local and Radius Authentication Modes when Login</td>
</tr>
<tr>
<td>System Management Tools
• Performance Monitor (switch should support RFC1213 Interface and RMON)
• Device Panel Simulation Module
• Batch Program
• Link Capacity Check
• Safeguard Check
• Get All ARP Information
• Device Type Check
• Topology Generator
• Topology Import / Export
• Hierarchy Topology Manager
• Device Type Extension
• Web Configuration
• Telnet Configuration
• TFTP file transport
• Trace Route
• MAC Locator
• Ping</td>
<td>Resource Management Functions
• Device Resource Manager
• User Locator
• Device Locator
• User Statistics
• Device Statistics
• Device System Information Manager (RFC 1213 System)
• Device Port Status Manager

Performance Management Tools
• Performance Monitor
• Port Packet Monitor</td>
</tr>
<tr>
<td>Fault Management Tools
• Trap Filter
• Trap Log
• Ping Poll Filter
• Ping Poll Log
• SNMP Poll Filter
• SNMP Poll Log
• Event Config Manager
• Event Viewer</td>
<td>Supported Devices
• D-Link Devices:
- SNMP capable Smart/Managed switches
- OLT/ONU devices
- Wireless bridges and access points
- SNMP capable routers
- Multi-tenant broadband CO devices
• Windows Workstation, DC</td>
</tr>
</table>

	and Server • Device Panel Simulation

2

Installing D-View

INSTALLATION STEPS

To install D-View 6.0 for both Standard and Professional Edition, follow these procedures:

For Professional Edition:

Prior to installation, ensure the environment on your designated server is compliant with the software requirements given below:

- Ensure the authentication mode on MS SQL 2000 is **Mixed Mode** (SQL Server and Windows) when installing SQL Server. Use **Enterprise Manager** for configuration settings.
- Click **Microsoft SQL Server** > **SQL Server Group** > **Local Windows NT**.
- Right-click on **Local Windows NT**, and select **Security**.
- Configure **Authentication** as **SQL Server** and **Windows**

1. Insert the CD and navigate to **D-View Standard.exe**/**D-View Professional.exe**. If the installer does not start automatically, start the installer by double clicking the D-View Standard.exe/ D-View Professional.exe.

The **InstallShield Wizard** screen displays.

Figure 2: InstallShield Wizard screen

D-View Setup initiates the **InstallShield Wizard**, which after loading, will take you through the installation process.

The **License Agreement** screen displays.

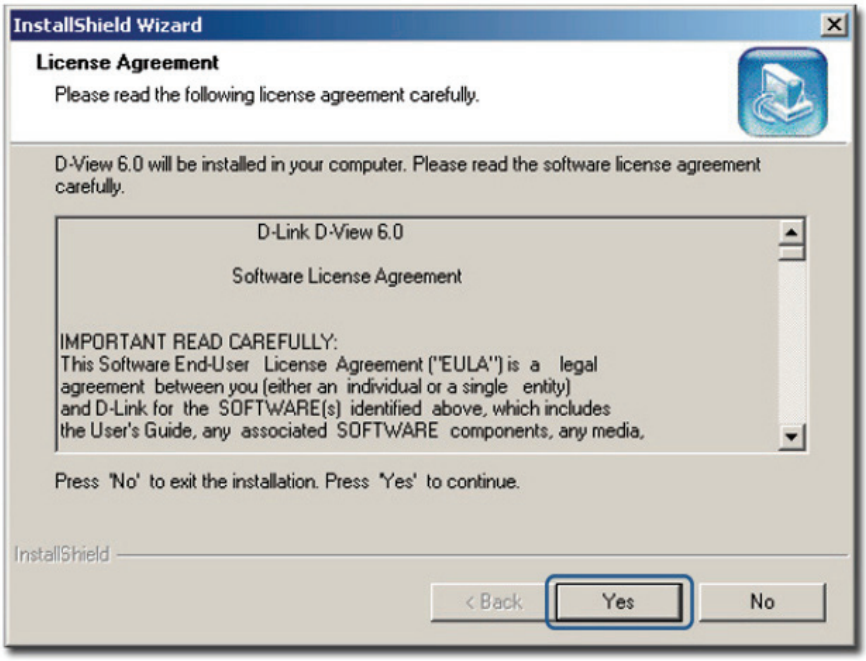


Figure 3: License Agreement screen

2. Click **Yes** to proceed.
   The **Choose Destination Location** screen displays.

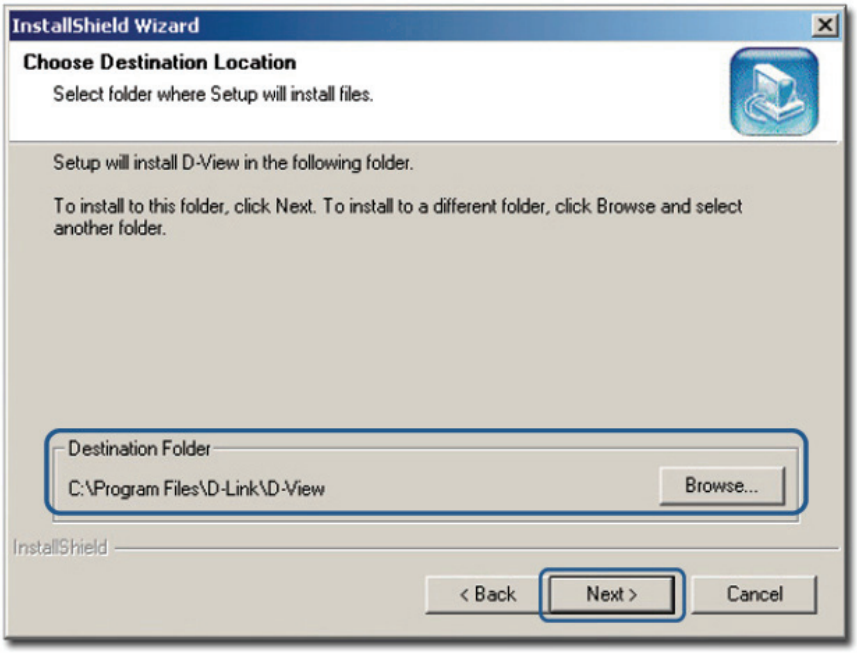


Figure 4: Choose Destination Location screen

3. By default D-View is installed in `C:\Program Files\D-Link\D-View`. Alternately, you can choose to install D-View in your preferred designated folder. Click **Browse** to select the target location and then click **Next** to continue.
   The **Select Program Folder** screen displays.

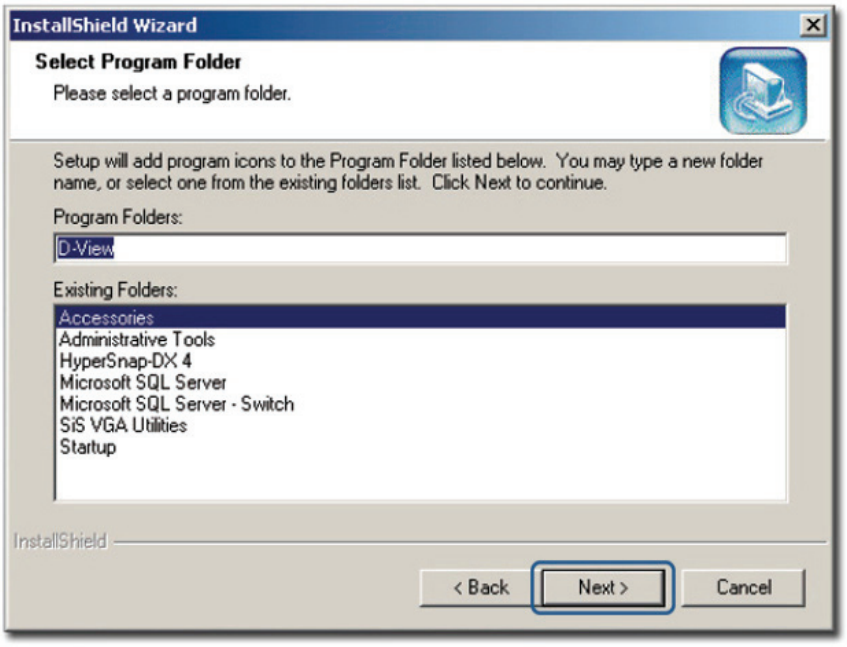


Figure 5: Select Program Folder screen

The Setup will add program icons into the Program Folder.

4. Click **Next** to continue.

The **Start Copying Files** screen displays.

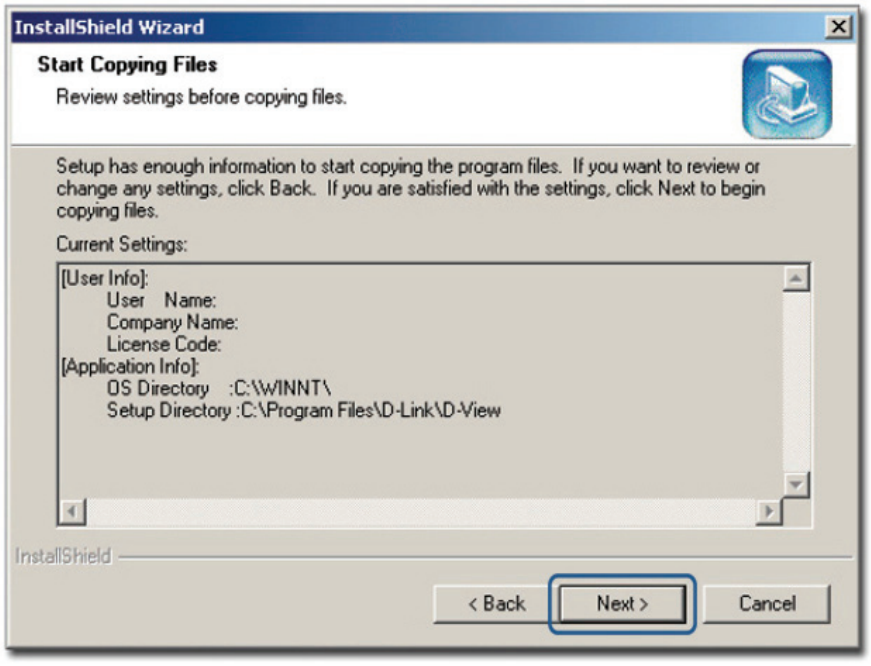


Figure 6: Start Copying Files screen

5. Verify the settings before clicking **Next**. To make changes, click **Back**.

The **Setup Status** screen displays.

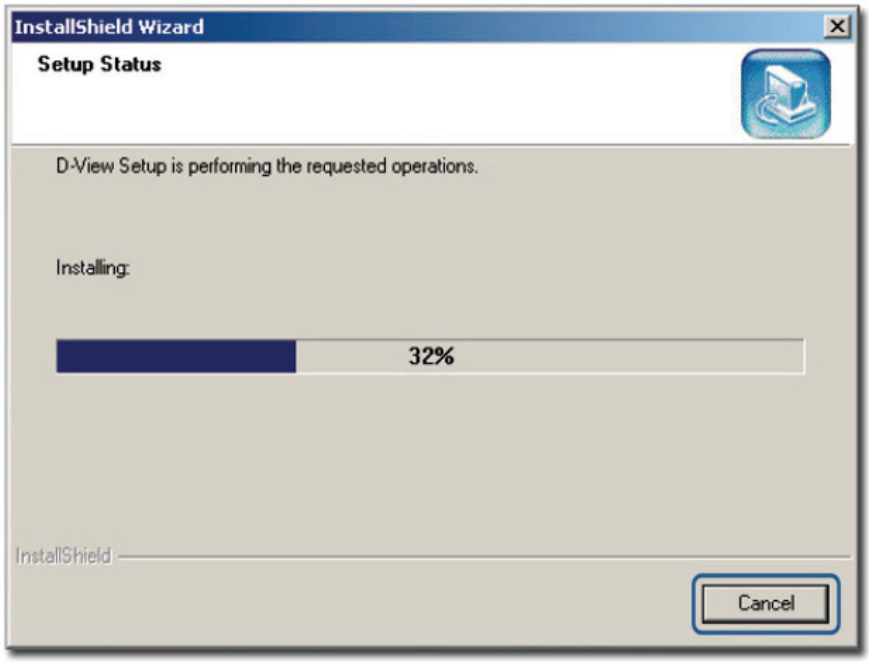


Figure 7: Setup Status screen

6. This screen indicates that D-View installation is in progress.

To stop the installation, click **Cancel**.

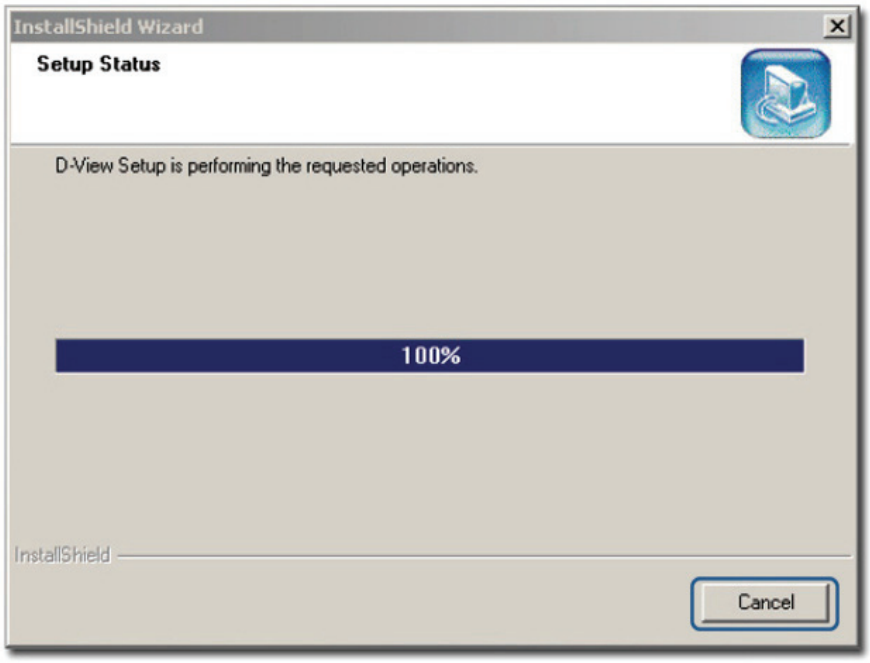


Figure 8: Setup Status screen

Once D-View installation is successfully completed the **Welcome to the Microsoft XML Parser and SDK Setup Wizard** window displays.

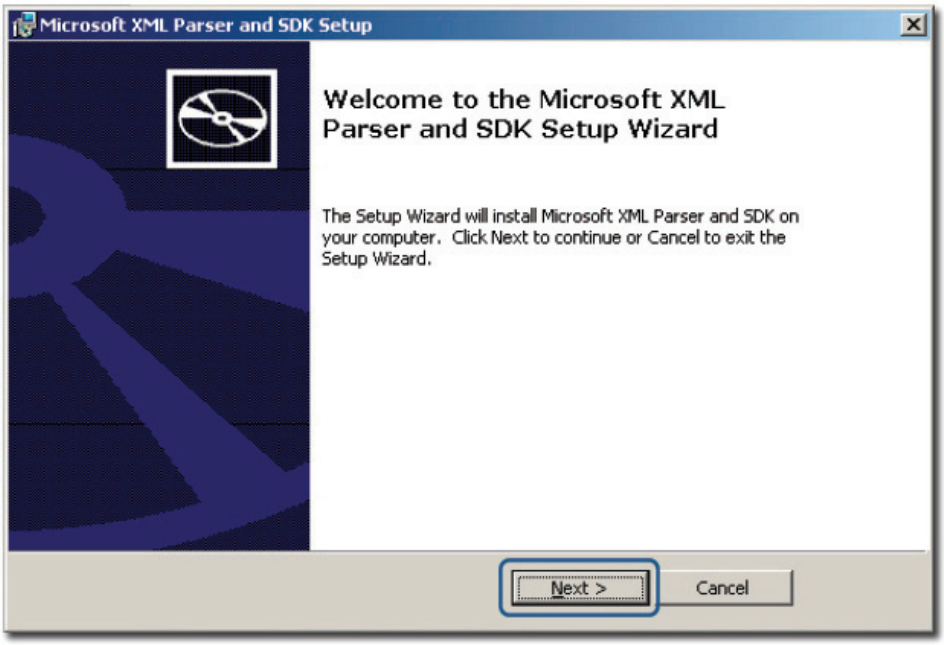


Figure 9: Welcome to the Microsoft XML Parser and SDK Setup Wizard

7. Click **Next** to continue installing Microsoft XML Parser and SDK on your server.

The **End-User License Agreement** screen displays.

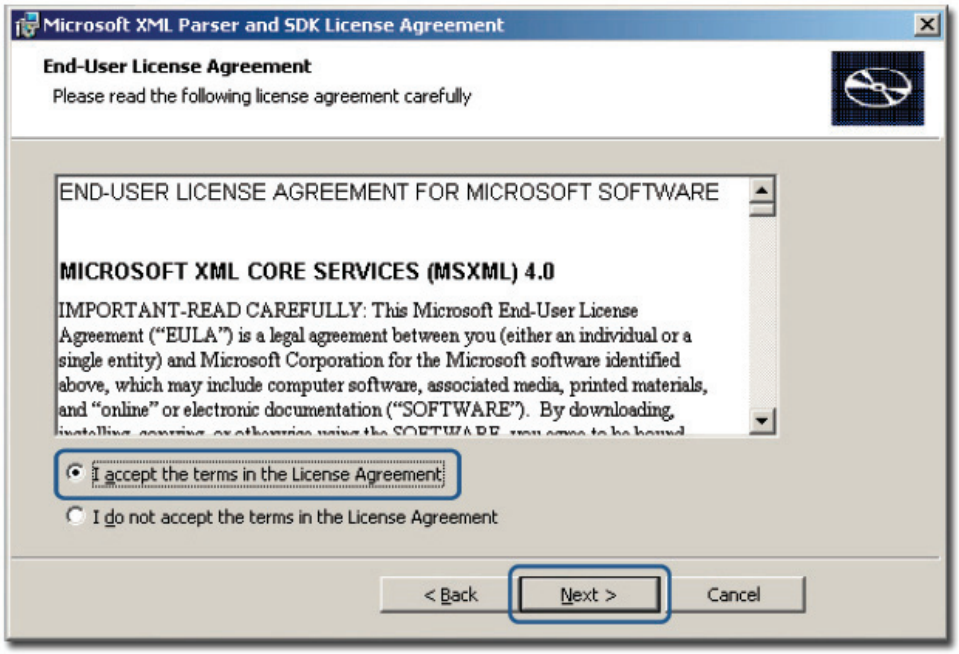


Figure 10: End-User License Agreement screen

8. Select **I accept the terms in the License Agreement** and click **Next** to continue.

The **Customer Information** screen displays.

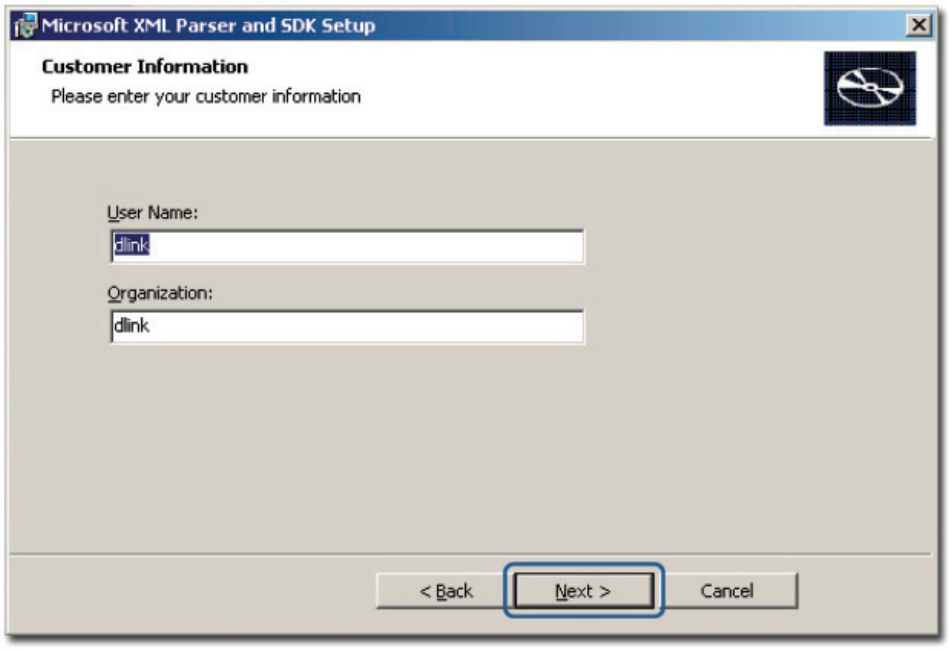


Figure 11: Customer Information screen

9. Enter the **User Name** and the name of your **Organization**. Click **Next** to continue.

   The **Choose Setup Type** screen displays.

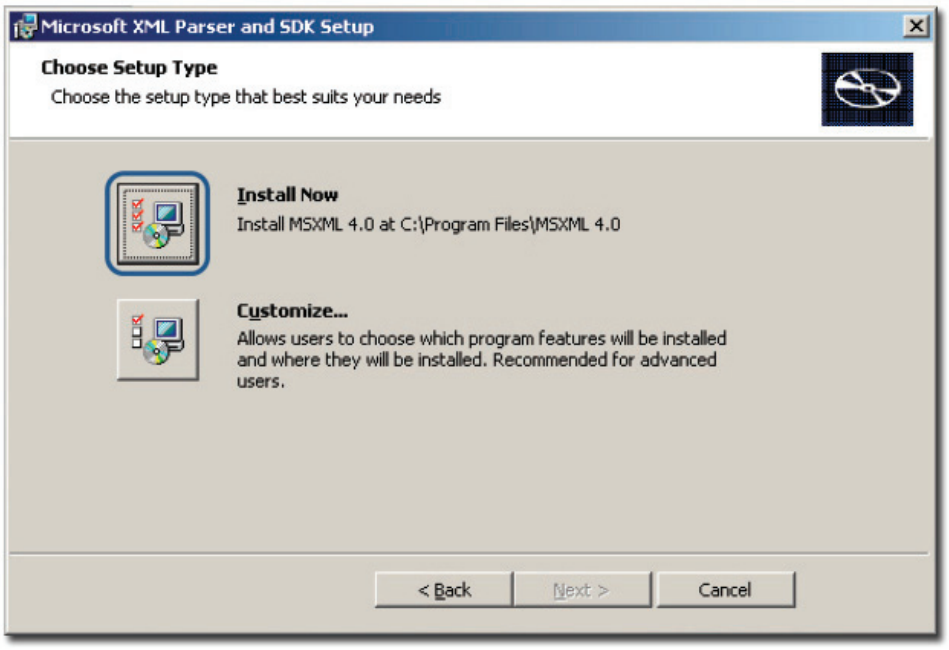


Figure 12: Choose Setup Type screen

10. Use the **Customize** option to select the program location. Click **Install Now** to continue with the installation (recommended).

The **Completing the Microsoft XML Parser and SDK Setup Wizard** screen displays.

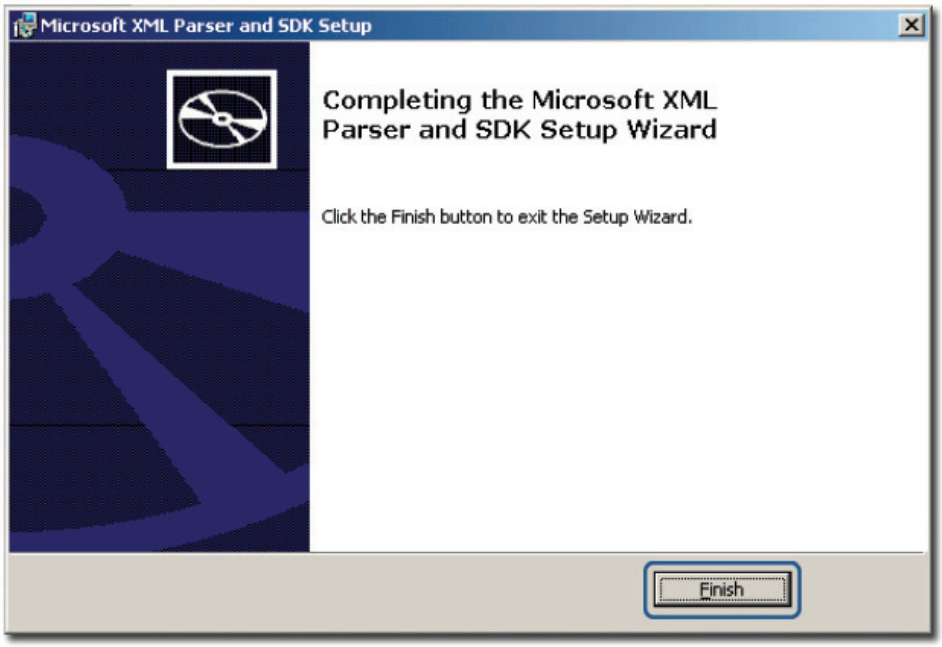


Figure 13: Completing the Microsoft XML Parser and SDK Setup Wizard screen

11. Click **Finish**.

The **Device Modules Setup** screen displays.

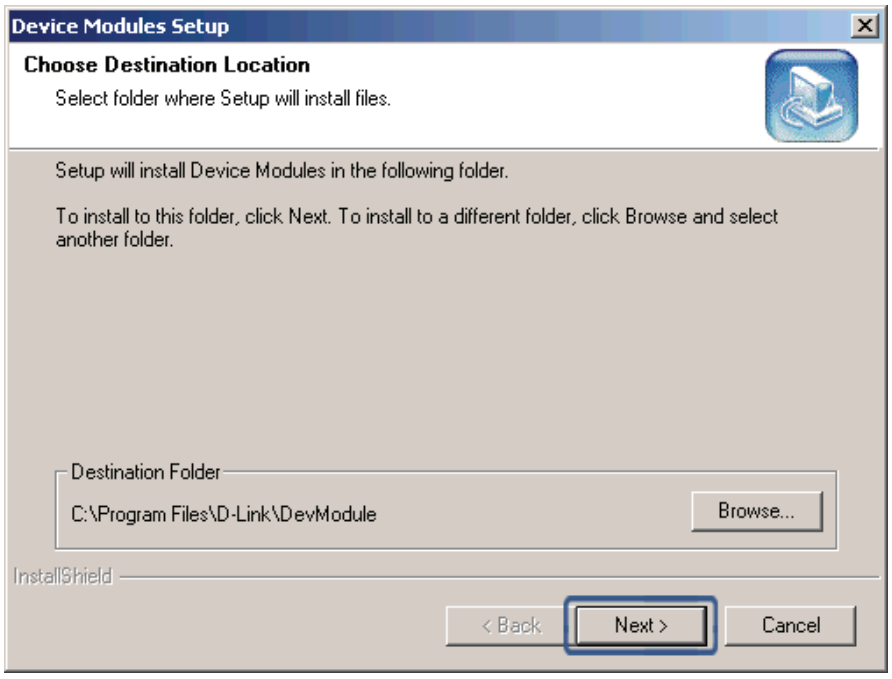


Figure 14: Device Modules Setup screen

12. To install to this folder click **Next**. To install to a different folder, click **Browse** and select another folder.

The **Setup Status** screen displays.

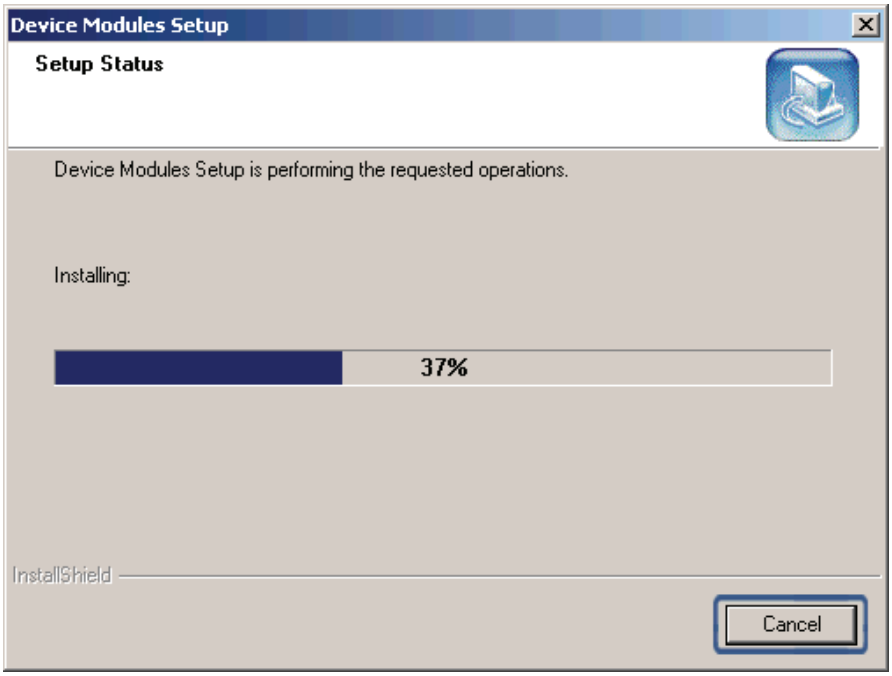


Figure 15: Setup Status screen

The Setup is installaing the required device modules. Once completed, the **Installation Completed** screen displays.

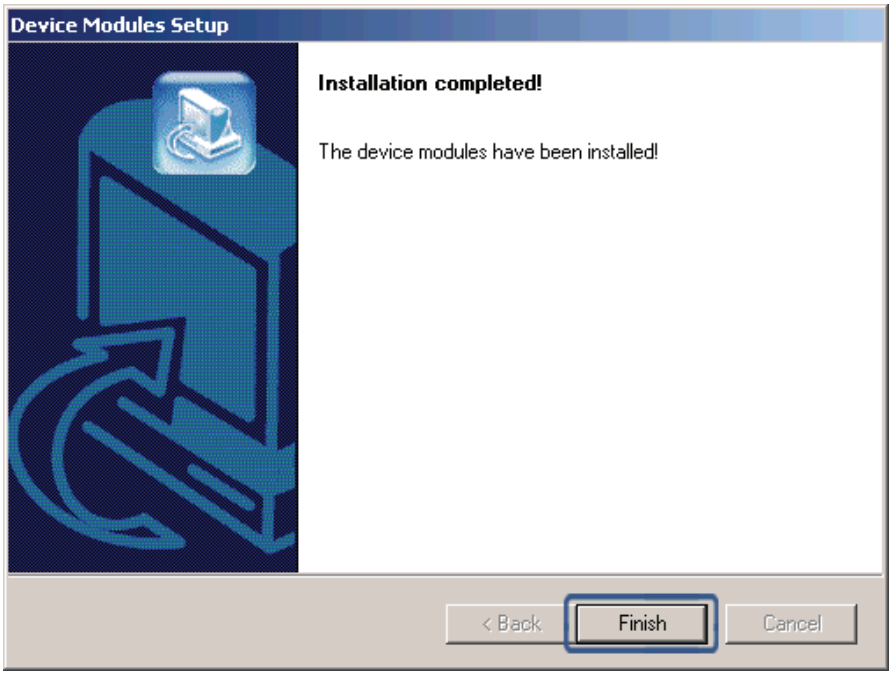


Figure 16: Installation Completed screen

13. Click **Finish** to exit and complete the installation.

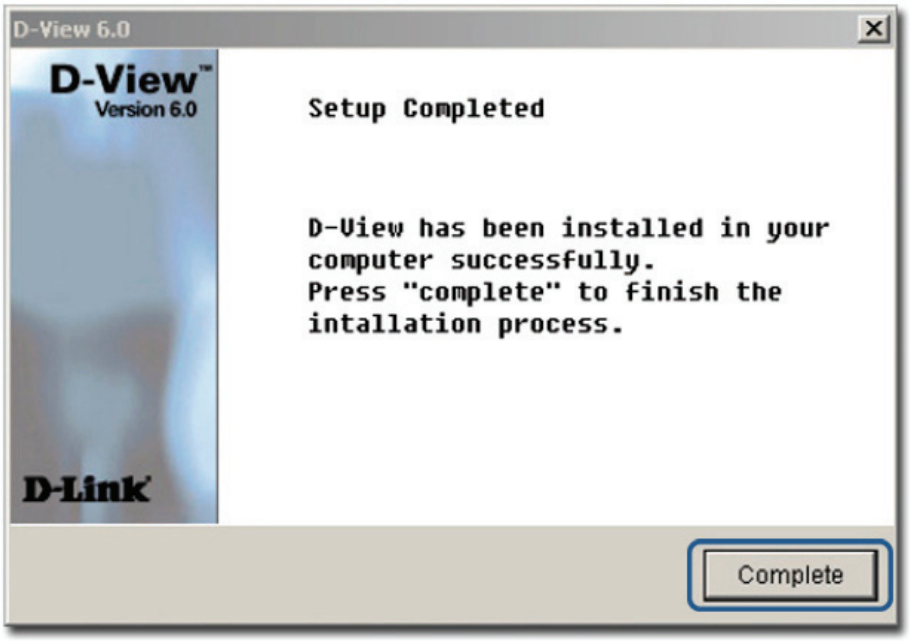


Figure 17: Setup Complete screen

The screen indicates that D-View 6.0 and Microsoft XML Parser and SDK software have been installed.

14. Click **Complete** to close this window.
15. To start D-View, double click the on the desktop.

The **Login D-View** screen displays. Refer to Getting Started to continue working with D-View and D-View 6.0 Licensing to receive the activation code.

Creating a Database (for Professional Edition)

Once D-View and Microsoft XML Parser and SDK software installation is complete, create a database for D-View.

To create a database, SQL 2000 server must be installed with SQL service running on the server.

To create a database, follow the steps below:

1. Copy the following files to a folder:
   - Make DB.exe
   - Task.SQL
   - DBCreate.SQL

   For example as seen in the following figure, the files are stored in:

   `E:\D-View 6.0\SQLDBScript\SQLDBScript`

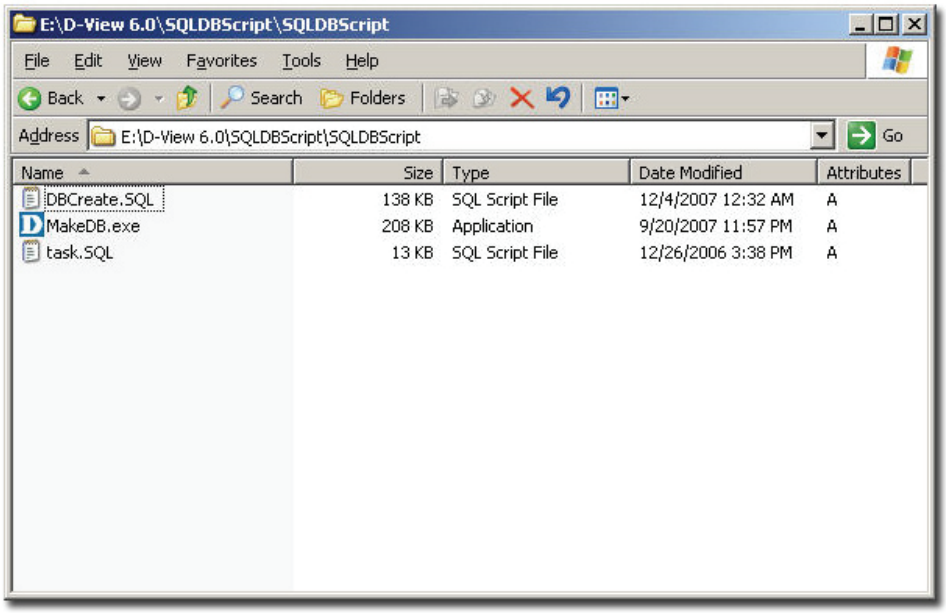


Figure 18: MakeDB screen

2. Double-click **MakeDB.exe**.

   The **D-View Database Tool** window displays.

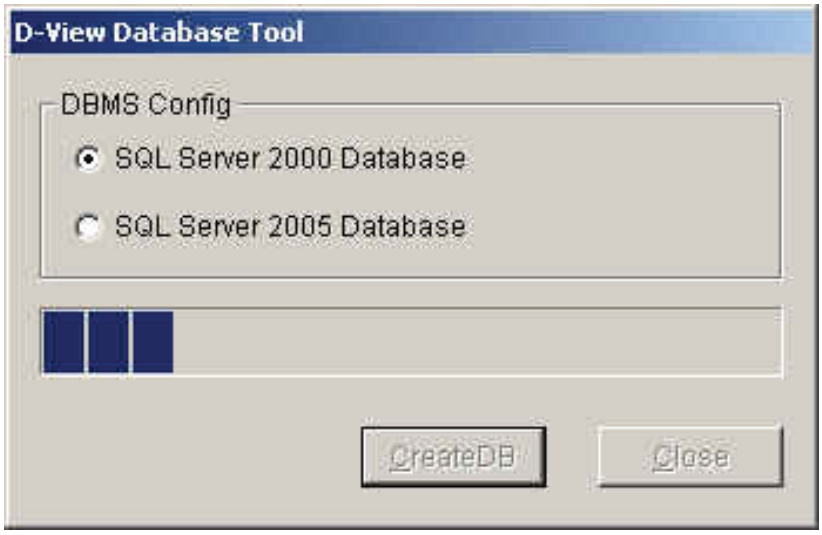


Figure 19: D-View Database Tool screen

D-View Database Tool is in the process of creating a database.

Figure 20: MakeDB screen

3. Click **OK** to close the window.
4. To edit information in the hosts file, go to:
   `C:\WINNT\system32\drivers\etc\hosts`

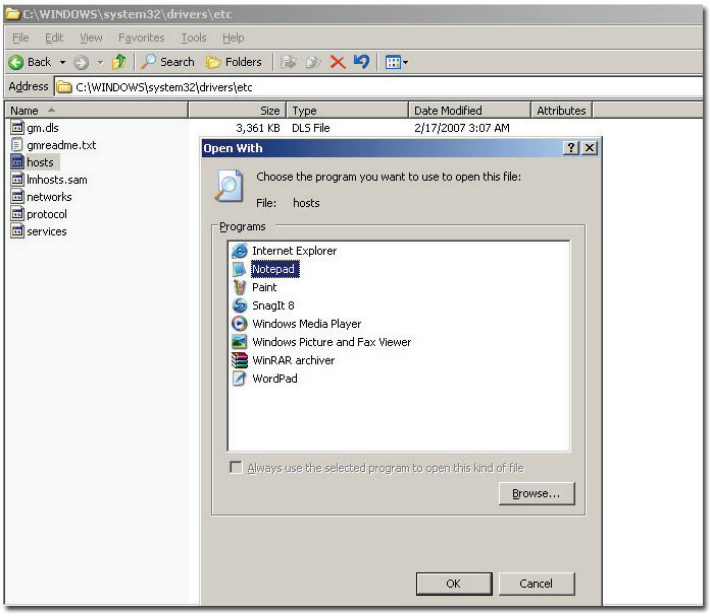


Figure 21: Etc Folder screen

5. Right-click **hosts** and select **Open With**. In the Open With window, select **Notepad**.

D-Link recommends using notepad to edit the hosts file.

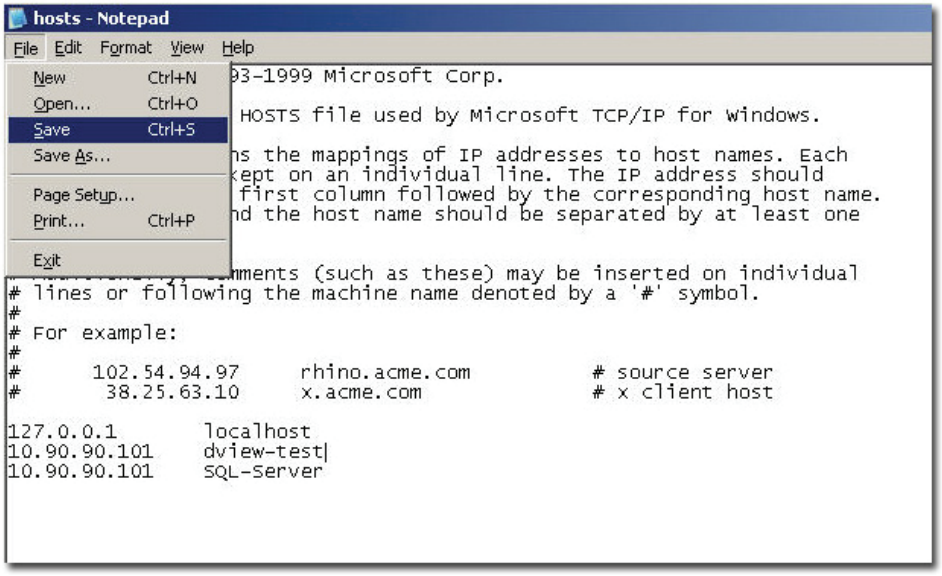


Figure 22: Hosts File screen

6. Update the host file with the following information, for example:
   - 127.0.0.1: localhost
   - dview-test : 10.90.90.101
   - 10.90.90.101: SQL-Server (Follow this format to connect to the server, i.e. "IP Address: SQL-Server").

To implement the client-server architecture, ensure to install D-View 6.0 professional edition in required servers to connect with the SQL database.

7. Click **Save** to save the file.

D-View utilizes SQL-Server alias name to query the SQL database, so therefore make sure the name entered is the same as the alias name. Ensure to add the IP address of your server in the hosts file. Check with the system administrator for the correct IP address of your server.

8. Restart your computer to complete the installation.

The **Login D-View** screen displays. Refer to Getting Started to continue working with D-View.

D-VIEW 6.0 LICENSING

Trial Version

When you install D-View, the trial version is automatically installed and allows you to evaluate the product for a period of 30 days. During this 30-day period, D-Link recommends you request a permanent license for D-View. For every single license key obtained, you can run D-View on up to five different computers.

Skip the **Activation** step as seen in Figure 23 and continue working with D-View.

During the trial period, every time D-View is started, a message is displayed indicating the time remaining before the trial version will expire.

Obtaining the Activation Code

If you opt to buy D-View, there are three ways to request for your activation code, which are as follows:

OPTION A

To register, go to http://dview.dlink.com.tw and enter user related information such as license key and MAC address of the server where D-View is to be installed. You can find the license key on the back cover of the user manual.

OPTION B

1. Start **D-View**.

The **D-View 6.0 Activation Wizard** screen displays.

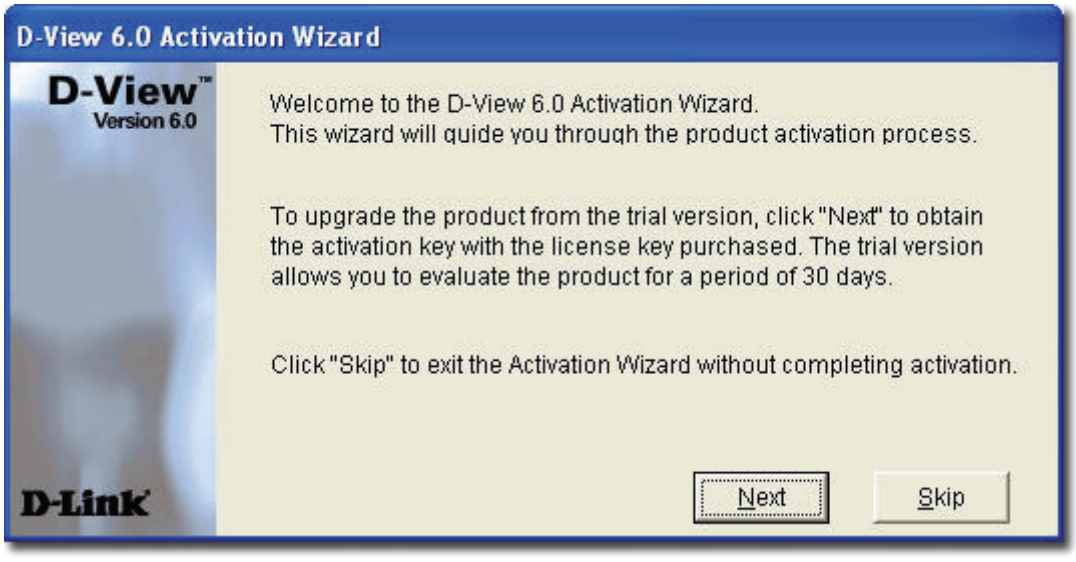


Figure 23: D-View Activation Wizard screen

2. Click **Next** to continue.
   The **Input Activation Key** screen displays.

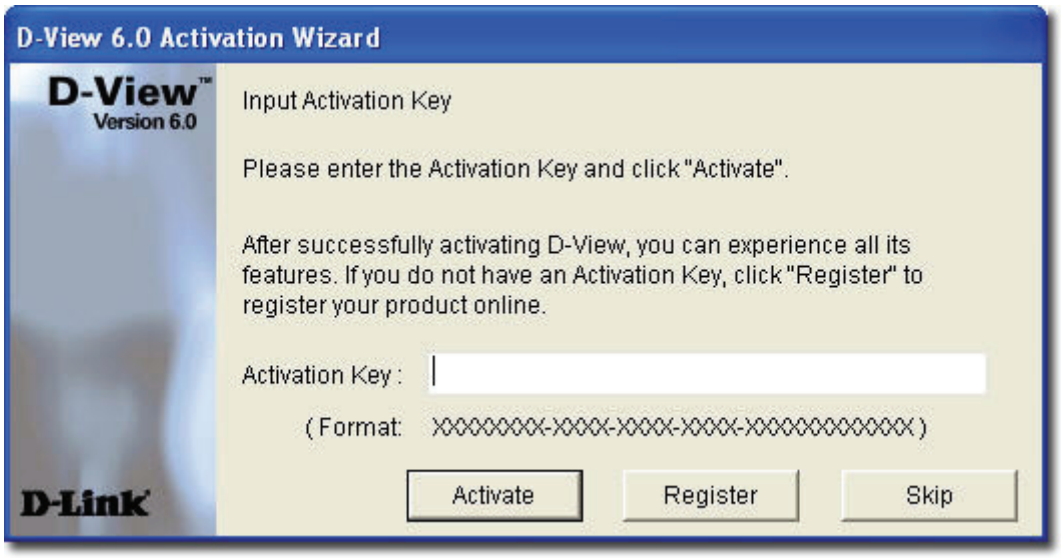


Figure 24: Input Activation Key screen

3. Click **Register** to open the registration website and update the information on-line.

OPTION C

Start **D-View**, go to **Help**>**D-View Activation Wizard**. Follow the steps accordingly to register for D-View.

Understanding the Architecture

MODULAR ARCHITECTURE

D-View 6.0 is a vendor-independent platform with user plug-in modules. This new adaptive architecture comprises multiple components such as DBMS access, basic and plug-in modules.

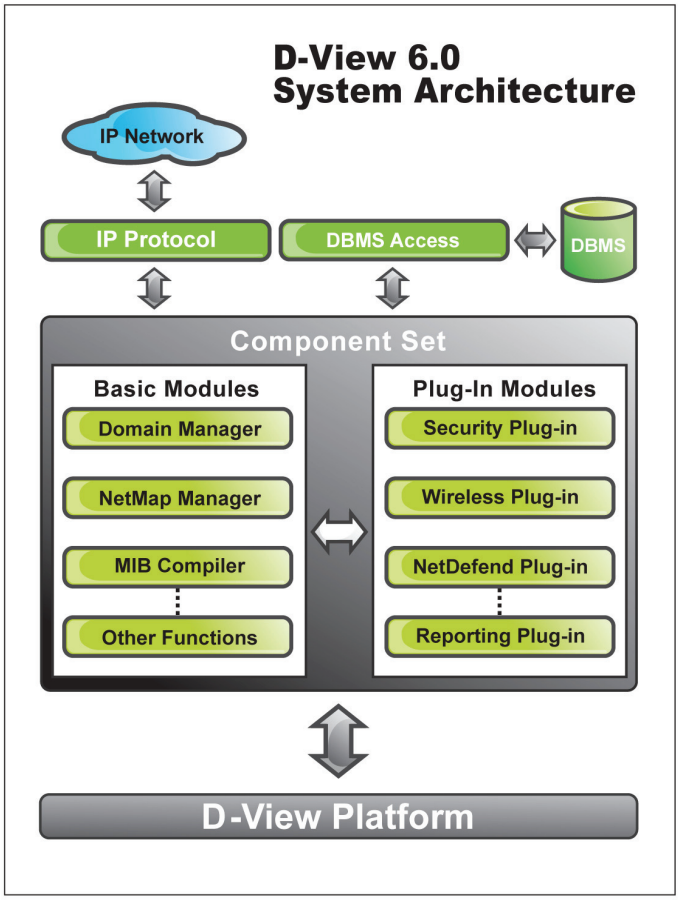


Figure 25: D-View System Architecture

D-View follows three-tier architecture that is client-server architecture in which an application is executed by more than one distinct software agent. For example, an application that uses middleware to service data requests between a user and a database employs three-tier architecture.

D-View modules are also compatible with HP's OpenView Network Node Manager (NNM v6.40, NNM v6.41, NNM v7.50, and NNM v7.51).

FEATURES

With the addition of new features to D-View, Administrators can now:

- Automatically create topology maps of device relationships.
- Graphically represent the real-time status of devices.
- Centrally manage multiple D-Link devices. Administrators can view and manage multiple devices within the LAN.
- Customize third party devices to integrate with D-View.
- Define trap events using the **Trap Editor**.
- Manage multiple identical devices at the same time using **Batch Configuration** (Firmware updates, Save config, RMON Enable and more).
- Manage third-party devices using the **MIB Compiler** and **MIB Browser.**
- Supports SNMPv3 for major MIBs.
- Monitor the status of network devices by polling network devices periodically.
- View and check the status of the **Safeguard Engine** from the topology map.
- Handle events based on severity and notify the users with email or sound alerts.

FUNCTIONS

The following section briefly describes the various functions of D-View:

- **New Device Identifier:** D-View constantly monitors the network for new devices. Once a device is plugged in, administrators can add the device into the topology.
- **Database Access Component:** Provides interface to access Microsoft Access and SQL Server 2000/2005 out of the box. If required, functional components can be changed to access other DBMS such as Oracle or Sybase.
- **Domain Management:** D-View allows administrators to categorize network devices into single or multiple domains.
- **Multiple Views:** D-View supports tree and list views for viewing devices in the domain.
- **Polling:** D-View polls network devices and displays any abnormal behavior on the Message Board. Devices are polled using **ICMP** (Internet Control Message Protocol) or **SNMP** (Simple Network Management Protocol).
- **Performance Management:** D-View provides flexible mechanism to retrieve SNMP OID information. For example, using **Performance Monitor** function, the administrator can monitor data ratio per port.
- **Syslog Management:** Maintain user action log information.
- **System Config:** Configure global parameters of the network, for example, **Local** and **Radius Authentication**.
- **SNMP v3 Support:** For major MIBs including MIB II, IF- MIB (RFC2233), Entity MIB (RFC2737), Bridge 802.1D(RFC1493), RMON, 802.1P (RFC2674) and 802.1Q (RFC2674).
- **Resource Management:** Manage, add, or remove network device resources from/to a topology.
- **Device Customization:** Include customized network devices by manually entering device type information.
- **Layer 3 Utilities:** Layer 3 utilities include IP forwarding, **RIP 2** (Routing Information Protocol), **OSPF** (Open Shortest Path First), IP MRoute, **DVMRP** (Distributed Vector Multicast Routing Protocol) and **PIM** (Protocol Independent Multicast) functions for managing switches and advanced routers in enterprise networks.
- **Topology Generator:** Create diagrams and schematics for network design and layout planning.
- **Topology Import/Export:** Import or export topology information to/from XML.

4

Understanding the Interface

INTRODUCTION

D-View's user interface provides access to all views and tools from a single location.

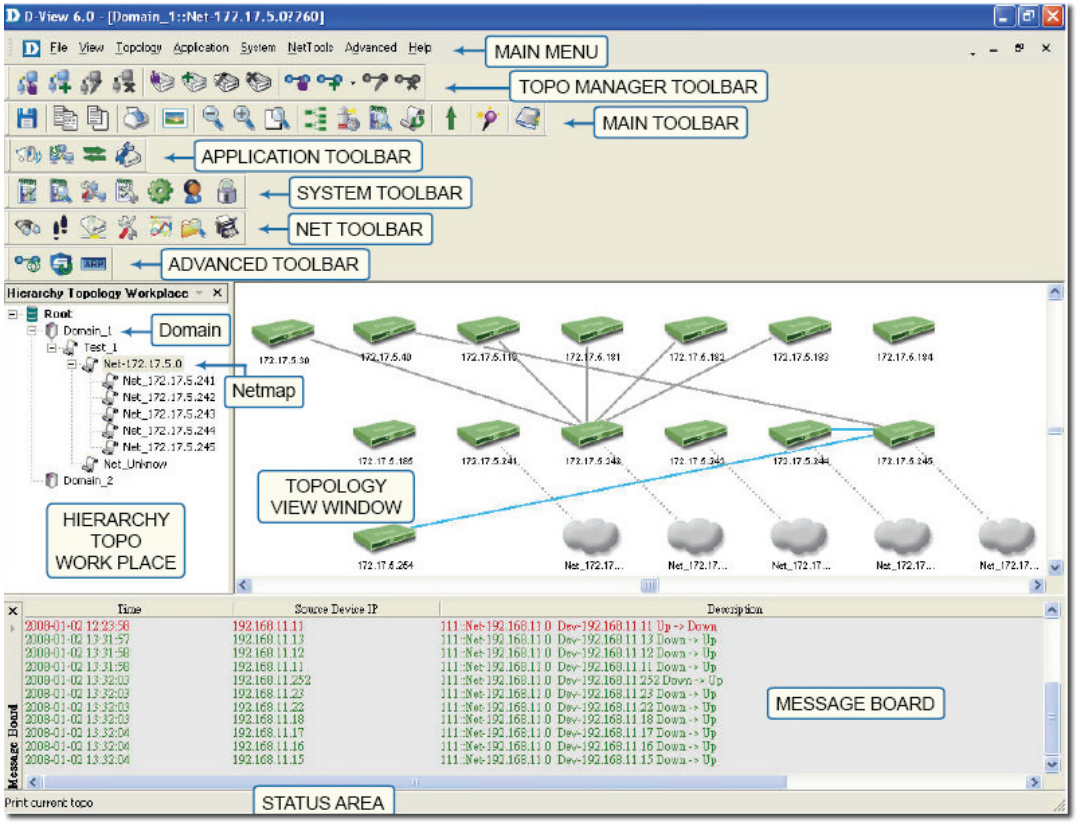


Figure 26: D-View User Interface

The key interface elements are:

- **Domain:** A subnetwork comprised of netmaps. Dividing the network into domains improves performance and security.
- **Netmap:** A netmap is a graphical representation of your domain/network. You can also refer to it as a network topology map.
- **Menu Toolbar:** Access different functional modules from the Menu toolbar.
- **Hierarchical Topology Workplace:** Displays a tree-like structure of the topology.
- **Main Toolbar:** Use the Main toolbar for quick access of the functional modules.
- **Topology View Window:** Displays the net cells that include devices, links and netmaps.
- **Message Board:** View event messages of various devices in the domain.
- **Advanced Toolbar:** Use the Advanced toolbar for quick access of the functional modules.
- **Net Toolbar:** Use the Net toolbar for quick access of the functional modules.

- **System Toolbar:** Use the System toolbar for quick access of the functional modules.
- **Application Toolbar:** Use the Application toolbar for quick access of the functional modules.
- **Topo Manager Toolbar:** Use the Topo Manager Toolbar for quick access of the functional modules.
- **Status Area:** Provides context-sensitive information about the current state of what you are viewing in the window.

Refer to Main Menu for the different functional modules.

Drag and drop the toolbar to rearrange elements around the user interface to suit your working model

Context-sensitive Menus

Most items in D-View have context-sensitive menus. Select an item and then right-click the mouse to view additional details.

Topology Workspace

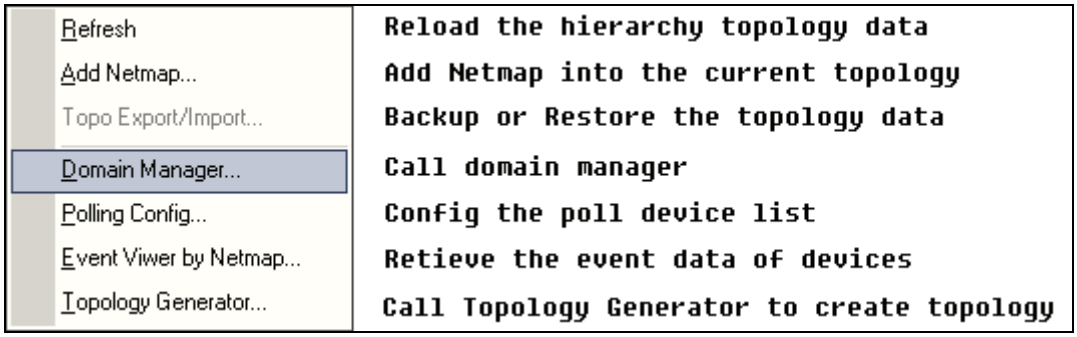


Figure 27: Context-sensitive menu accessed from the Topology Workspace

Topology View Window

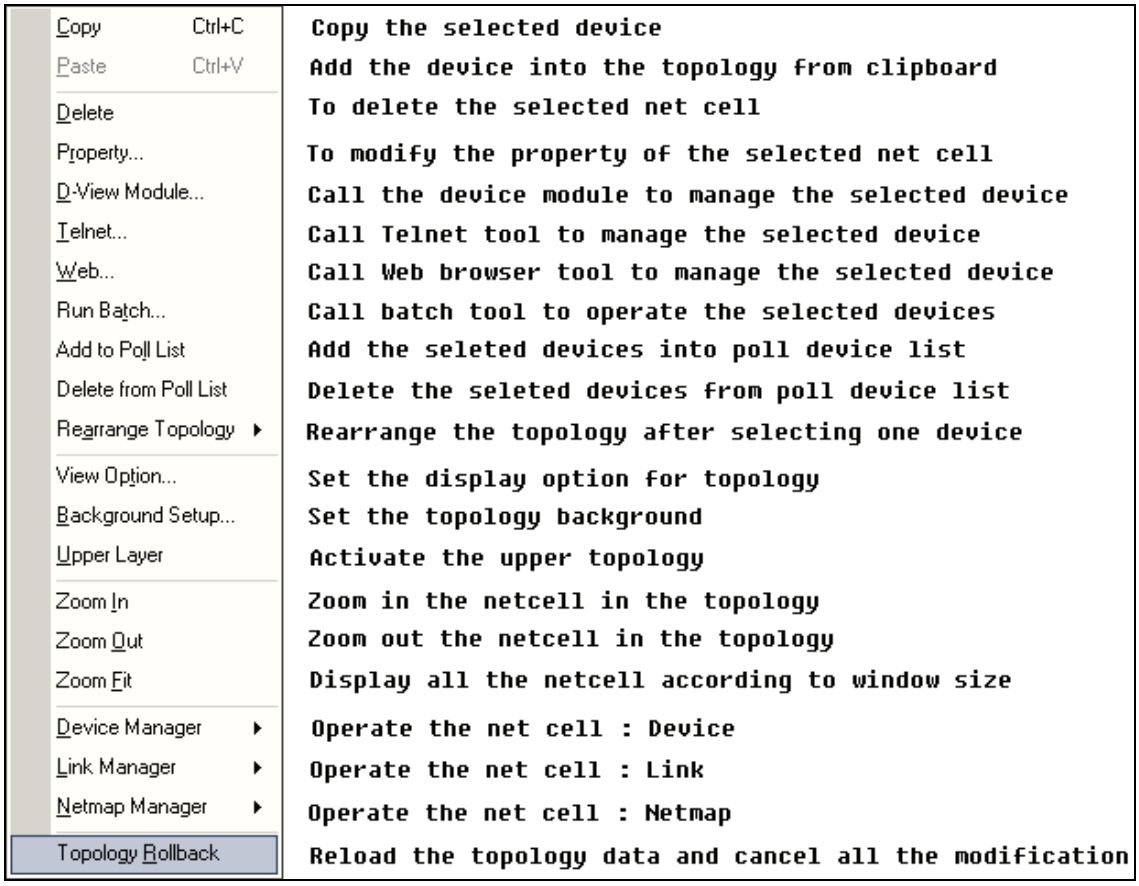


Figure 28: Context-sensitive menu accessed from the Topology View Window

Hierarchy Topology Workspace

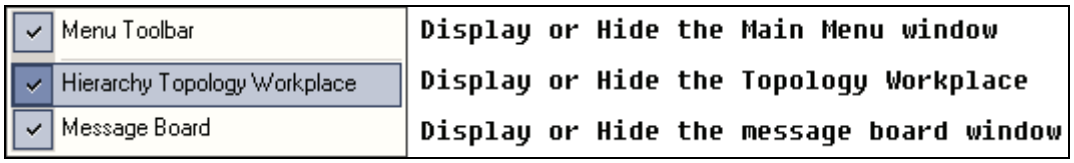


Figure 29: Context-sensitive menu accessed from the Hierarchy Topology Workspace

MAIN MENU

D-View's **Main Menu** is the entry point for accessing most of the features. It runs along the top of the screen. This section briefly describes the available menu options.

File

The following table lists the **File** menu items and their descriptions.

MENU ITEM	DESCRIPTION
Save	Save the current topology.
Startup Wizard	The wizard guides you to create a topology. Refer to Startup Wizard for more information.
Close	Close the current **Topology View** window.
Print	Print the current topology.
Preview	Preview the current topology.
Page Setup	Set printer options, properties and paper size.
Lockup	Locks D-View; only the current user or an administrator can unlock the system.
Logout admin	Logout of D-View and sign in as a different user.
Exit	Exit D-View.

View

The **View** menu enables you to view or hide various D-View Toolbars. The following table describes the different toolbars.

TOOLBAR	DESCRIPTION
Advanced Toolbar	Access Link Capacity Check, Safeguard Check and ARP info.
Net Toolbar	Access Device Discovery, Trace route, File Transport, NET Toolbox, Performance monitor, MIB browser and MIB compiler.
System Toolbar	Access System Log, Event Viewer by IP, Device Group Manager, Device Event Configure, System Config, Administrator Management, and Change Password.
Application Toolbar	Access Batch config, Run Batch Program, Topo Export Import, Device Customization.
Topo Manager Toolbar	Access Select netmap, Add netmap, Edit netmap, Delete netmap, Select device, Add device, Edit device, Delete device, Select link, Add link, Edit link, Delete link.
Main Toolbar	Access Save, Copy, Paste, Print, Background, Zoom out, Zoom in, Zoom fit, Domain Manager, Configure the devices want to be polled, Query the event log by netmap, Search the devices in the network and create

	a topology automatically, Upper Layer, Startup wizard, Help
Hierarchy Topology Workspace	Access Main Menu, Topology, and Message Board
Message Board	Access Message Board
Cascade	Cascades the different topologies one behind the others
Tile Vertically	Arranges the different topologies one below the other

Application

The following table lists the **Application** menu items and their descriptions.

MENU ITEM	DESCRIPTION
Batch Config: • **Advanced Option** • **Run Batch**	Execute a sequence of operations in D-View. For example, Save Configuration, Retrieve Port Status, and so on. Refer to Batch Configuration for more information.
Topo Export Import	Restore and backup D-View. Refer to Using Topo Export/Import for more information.
Device Customization	Add, modify and delete devices. Refer to Customizing Devices for more information.

System

The following table lists the **System** menu items and their descriptions.

MENU ITEM	DESCRIPTION
System Log	Store logged events. Refer to System Log for more information.
Domain Manager	Manage domain information. Refer to Domain Manager for more information.
Event Manager • **Event Viewer by Netmap**	Monitor and manage events. Refer to Managing Events for more information.

• **Event Viewer by IP** • **Device Group Manager** • **Polling Config** • **Device Event Config** • **Trap Editor**	
Resource Manager • **MAC Locator** • **Device Locator** • **User Locator** • **Device Collector** • **User Statistic** • **Device Statistic**	Locate devices using IP or MAC address.
System Config	Configure the root domain name, management station and authentication information. Refer to Login D-View for more information.
Administrative Manager	Create user groups and provide access rights for certain functional modules to an administrator. Refer to Administrator Manager for more information.
Change Password	Change password after login. Refer to Changing Password for more information.

NetTools

The following table lists the **NetTools** menu items and their descriptions.

MENU ITEM	DESCRIPTION
Device Discovery	Search devices using IP address. Refer to Device Discovery for more information.
Trace Route	Lists all the intermediate routers a connection must pass through to get to reach its destination. Refer to Trace Route for more information.
TFTP (Trivial File Transfer Protocol)	Upload/Download/Update configuration files to and from devices. Refer to TFTP for more information.
NetToolbox	Manage devices through Telnet, Web and Ping using the IP address. Refer to Net Toolbox for more information.

Port Packet Monitor	Monitor the port packet performance. Refer to Port Packet Monitor for more information.
Performance Monitor	Monitor the RMON performance of a device. Refer to Performance Monitor for more information.
MIB Tools • **MIB Compiler** • **MIB Browser**	Manage and configure non D-Link devices. Refer to Managing Devices with MIB Compiler for more information.
Topology Generator	Tool to generate a Topology. Refer to Using Topology Generator for more information.

Advanced

The following table lists the **Advanced** menu items and their descriptions.

MENU ITEM	DESCRIPTION
Link Capacity Check	Monitor and modify the link status. Refer to Monitoring the Link Status for more information.
Device type Check	Check the network for new and updated devices. Refer to Using Device Type Check for more information.
Safeguard Check	Check the safeguard status of devices. Refer to Using Safeguard Check for more information.
All of ARP info	Retrieve ARP information from devices in the topology. Refer to Retrieving ARP information for more details.

Help

The following table lists the **Help** menu items and their descriptions.

MENU ITEM	DESCRIPTION
D-View Help	Opens D-View online help.
Module supported	Displays a list of devices supported by D-Link.
D-View Activation Wizard	Helps you obtain the activation code.
About D-View	Displays the About D-View window.

5

Using D-View

GETTING STARTED

Before proceeding with this section, D-Link recommends you familiarize yourself with the User Interface. Refer to Introduction section.

Login D-View

After successfully installing D-View, type the default Account and Password for D-View. The default **Account** is `Admin` and the default **Password** is `111111`.

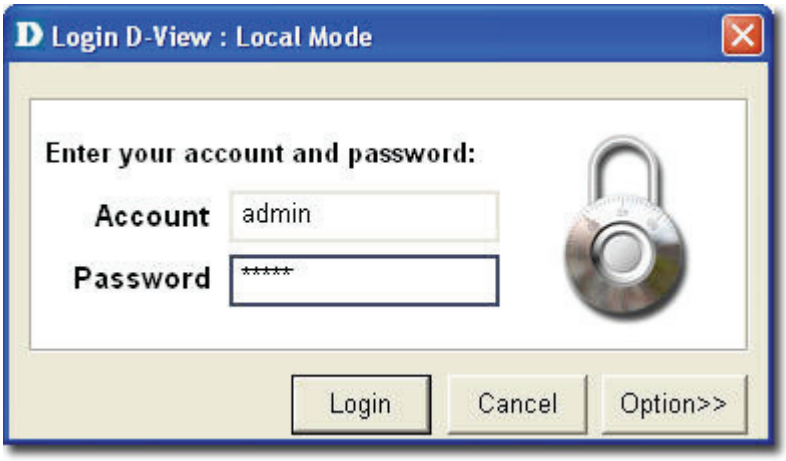


Figure 30: D-View Login screen

Click Option to login to D-View by using different domain-specific administrator accounts to view different topology maps.

Managed IP Feature

The **Managed IP** feature enables the administrator to control which domain can be managed by which user. After the user has successfully logged in with the domain's managed IP, the user will only be able to see that domain. The **Managed IP** feature differs between **Standard Edition** and **Professional Edition**.

- **Standard Edition:** Since D-View Standard is a standalone platform, the **Managed IP** feature is used to control which user can manage which domain locally. The domain can be divided by different departments or locations, with each department or location having a dedicated user who monitors the network status.
- **Professional Edition:** D-View Professional supports Client-Server architecture, thus allows for users to install D-View Professional to different locations. Each user can manage and monitor their responsible domain.

The administrator at the company headquarters can user the **Super Domain** account to manage and monitor all domains.

The user can also configure each account's access rights to limit features available while using D-View. This can be done by accessing **System > Administrator Manager**.

To enable **Managed IP** click **Option** on the D-View login screen.

Figure 31: D-View Login screen option button

Figure 32: D-View Login screen Managed IP feature

To configure Managed IP:

1. Click **System > Domain Manager**.

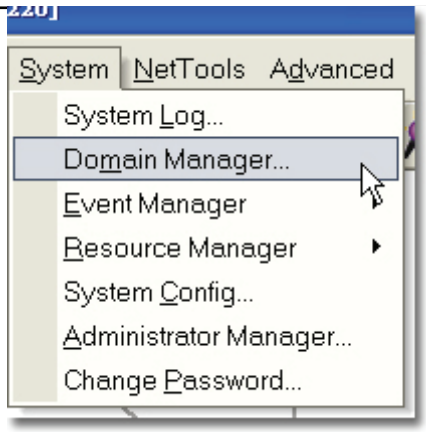


Figure 33: Domain Manager selection

2. Select a domain.
3. Click on the **Workstation** tab.

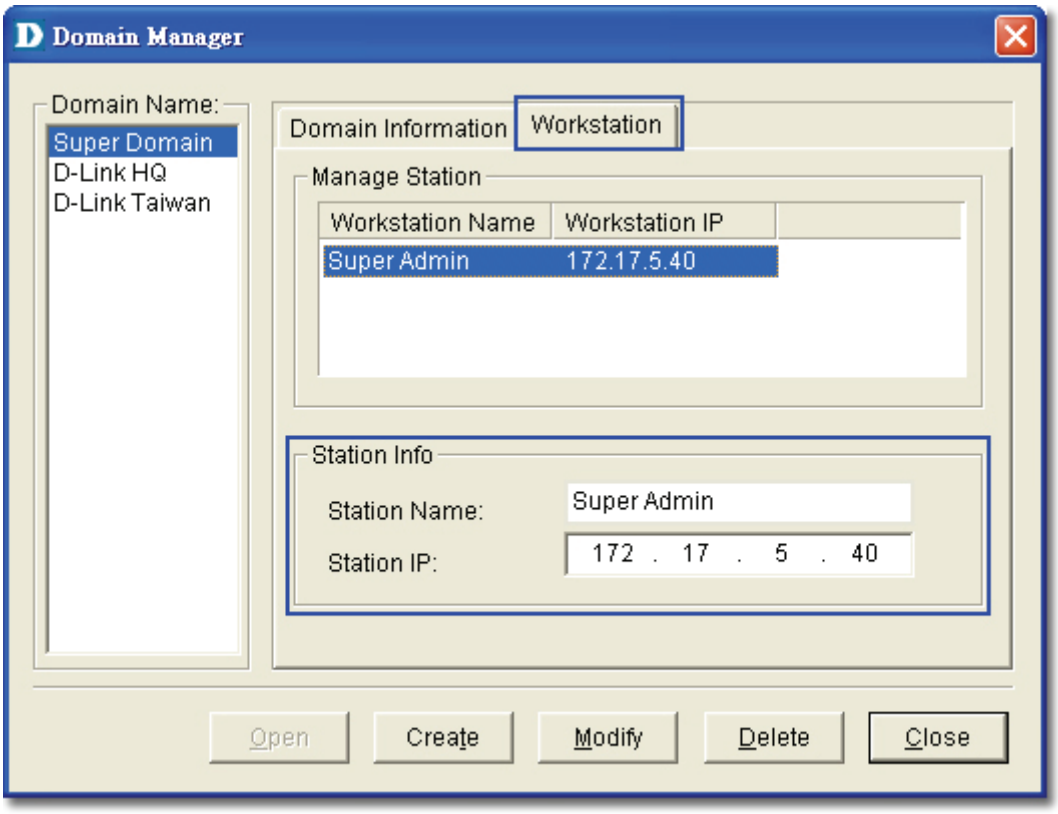


Figure 34: Domain Manager

4. Enter the **Station Name** and **Station IP**.

Repeat the above process for all domains.

When logging in using **Super Domain**, the administrator can manage and monitor all domains.

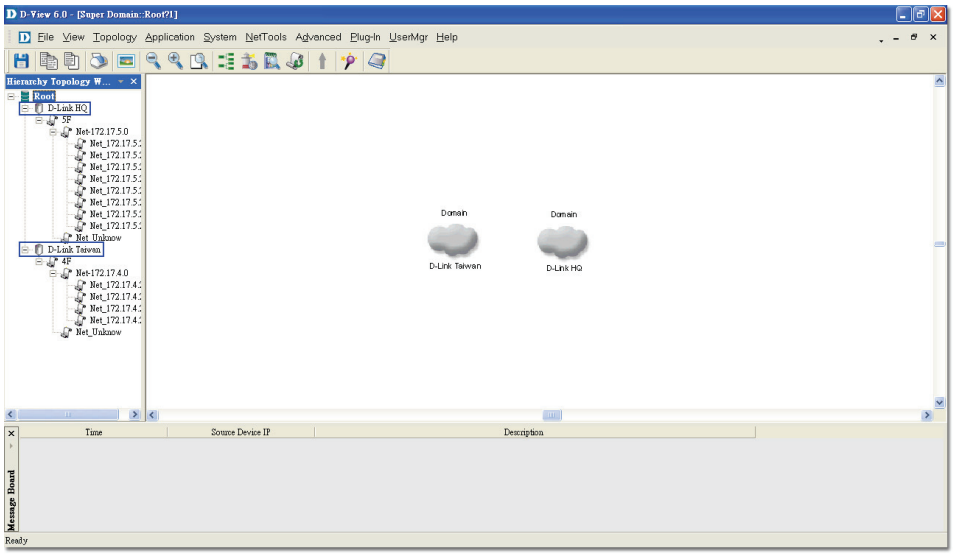


Figure 35: Super Domain

When logging in using the account for the company headquarters, the administrator can only manage and monitor the devices situated in the headquarters.

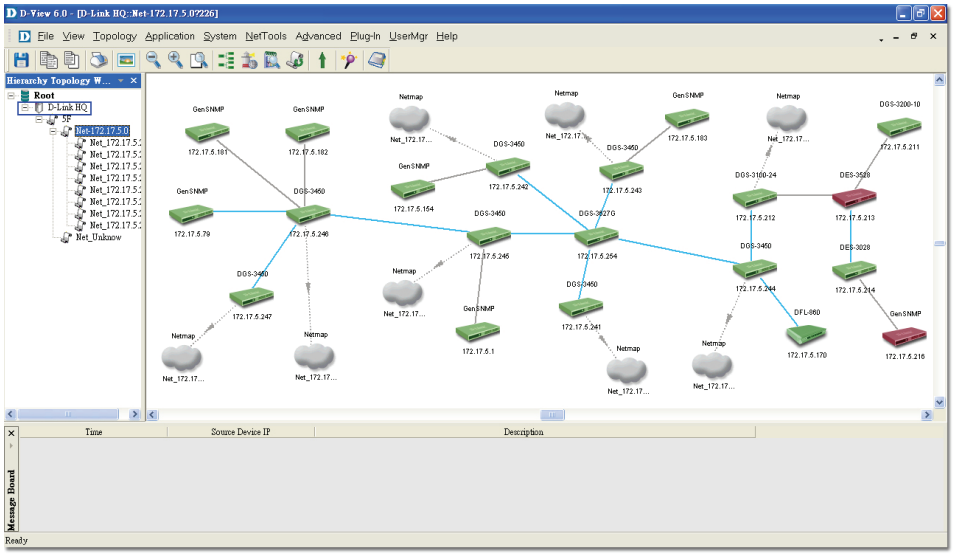


Figure 36: Headquarters account

When logging in using the account for branch office, the administrator can only manage and monitor the devices situated in the branch office.

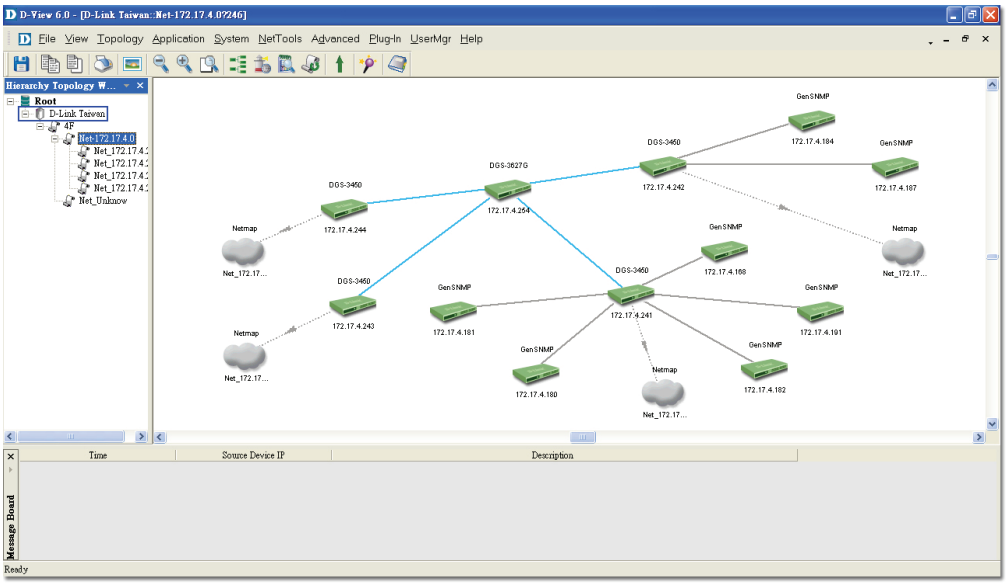


Figure 37: Branch office account

System Configuration

D-View supports two modes of authentication – **Local** and **Radius Authentication**. To configure the root domain name, management station and authentication information, go to **System** > **System Config**.
By default D-View uses **Local Authentication**.

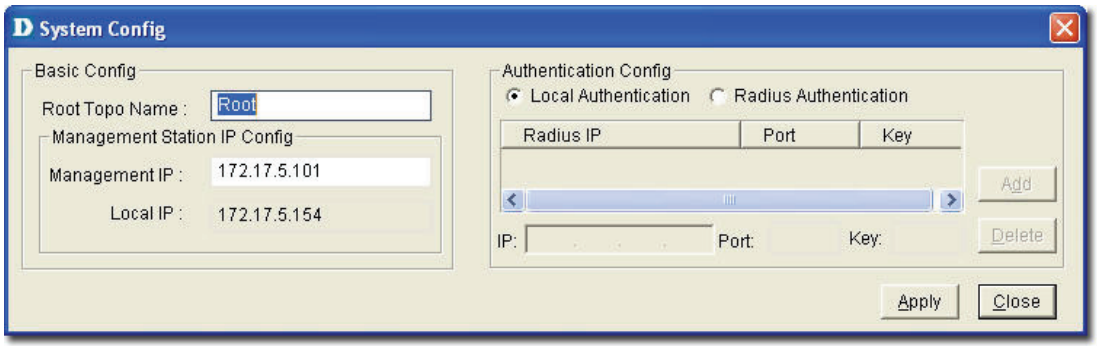


Figure 38: System Config screen

Local Authentication

- The account and password information is stored in the D-View database.

Radius Authentication

- The information is stored in the Radius server database.
- If the account and password information entered is valid, the server accepts the authentication and allows the administrator to manage and monitor the network.

Domain Manager

In a real environment administrators often need to manage multiple domains of the network. D-View can divide the entire network into many designated domains for administrators to manage different network.
An administrator needs to create a domain before working on any topology. When creating a new domain, the administrator should allocate IP address of the workstation.
Use **Domain Manager** to create, delete and modify the domain information.

After logging in, D-View creates a Super Domain and the IP address of the workstation by default. A super domain is a virtual domain which manages the topologies of all the domains. Refer to Creating a Topology to manually create a topology using Domain Manager.

Startup Wizard

The **Startup Wizard** helps you create a Topology. The Wizard will automatically create a new topology based on the information you provide.
To create a topology using the Startup Wizard:

5. Click **File> Startup Wizard**. The **Startup Wizard** screen displays.

Figure 39: Startup Wizard screen

6. Click **Next**. The **Domain Manager** screen displays.

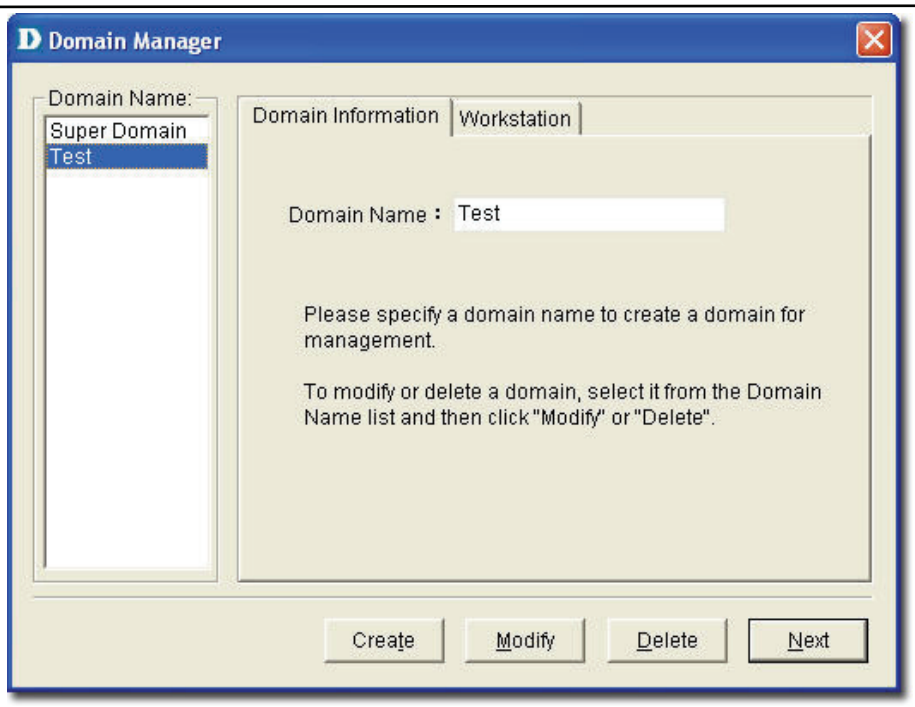


Figure 40: Domain Manager screen

7. Enter the name of your new **Domain**.
8. Click **Next**. The **Add Netmap** screen displays.

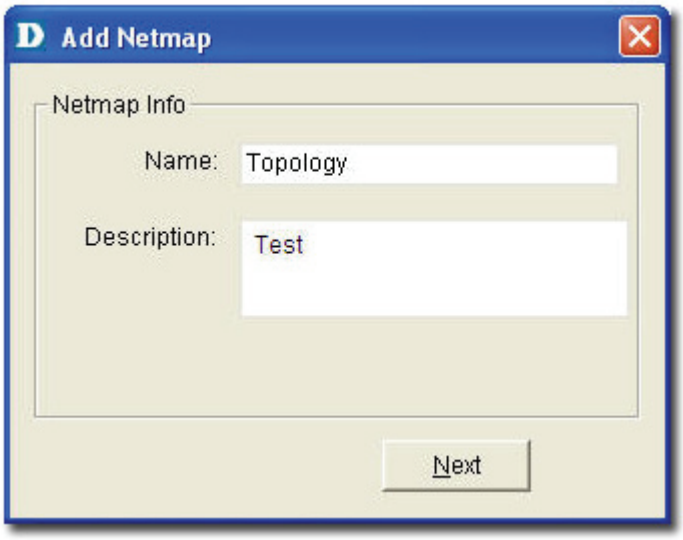


Figure 41: Add Netmap screen

9. Enter the **Netmap Name** and **Description**.
10. Click **Next**. The **Select Network Adapter** screen displays.

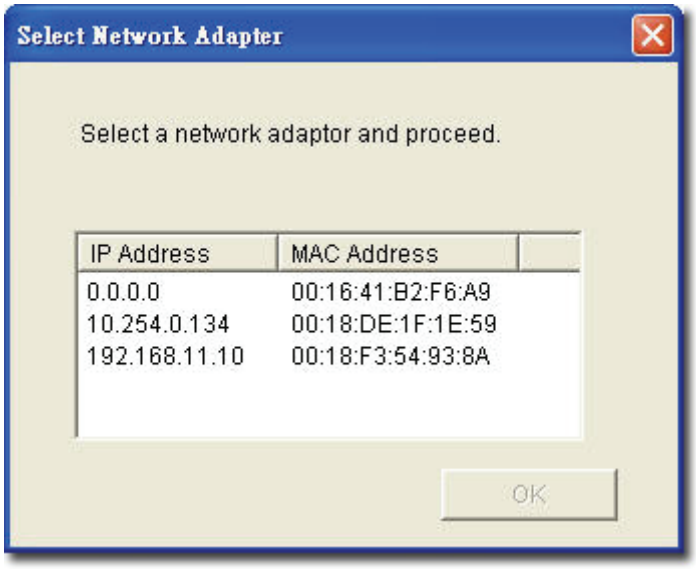


Figure 42: Select Network Adapter screen

11. Select a network adapter to build the topology.
12. Click **OK**. The **Topology Generator Wizard** screen displays.

Figure 43: Topology Generator Wizard screen

13. Select either **Local Network** or **Designated Network**.
    Local Network accesses devices in the local network and **Designated Network** accesses devices by specifying the IP range.
14. Enter a name for Topology Generator analysis.
15. Click **Next**. The **Topology Analysis Configuration** screen displays.

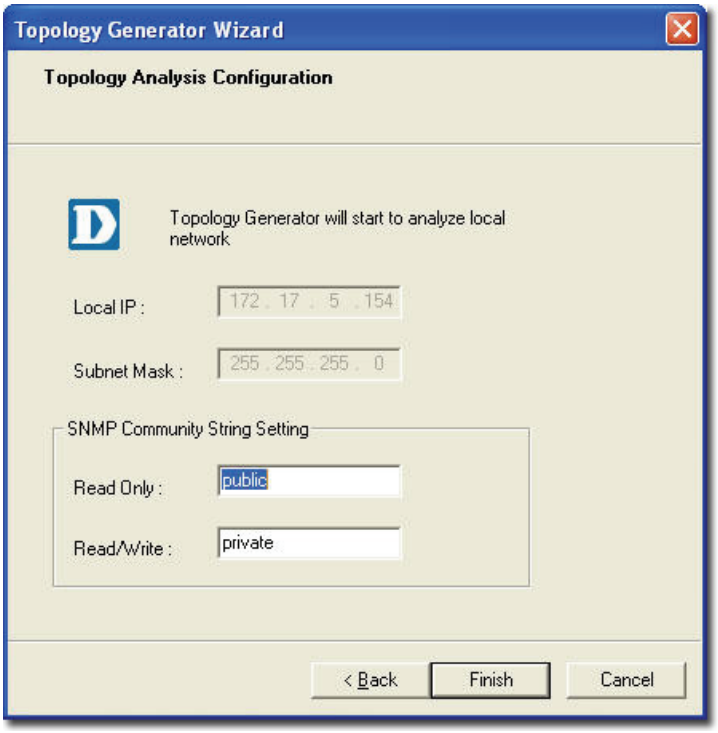


Figure 44: Topology Analysis Configuration screen

16. The topology generator analyzes the local network for the IP address and subnet mask. The **SNMP Community String Setting** is by default defined in D-view.
17. Click **Finish** to generate the topology. The **Topo Export** screen displays.

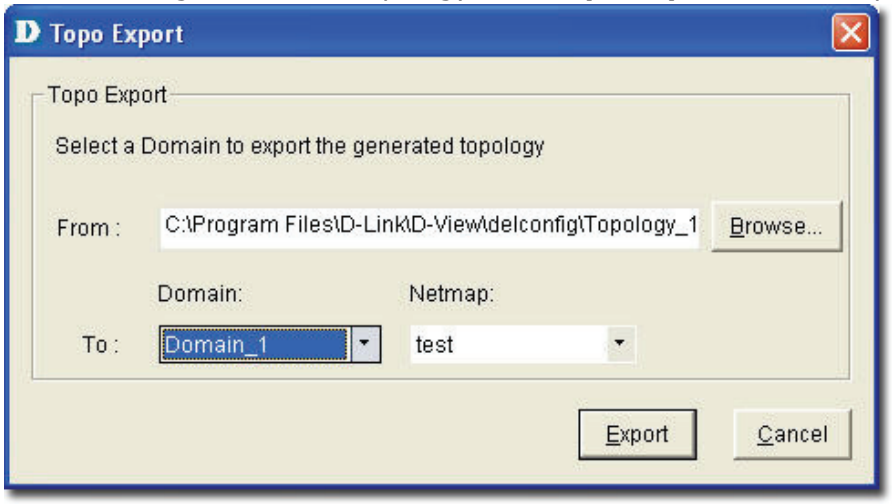


Figure 45: Topo Export screen

18. Click **Export** to export the generated topology to the Netmap. D-View displays the status of the export.

After completing the startup wizard's initial process, you can manage and monitor devices as described in the following chapters.

Working with Topologies

CREATING A TOPOLOGY

In D-View there are two ways to create a topology. They are:

- Using **Startup Wizard**: The wizard guides the users to create a topology. Refer to Startup Wizard create a topology.
- Create a topology manually

To manually create a topology:

1. Go to **System** > **Domain Manager** and create a new **Domain** to manage the topology.

Super Domain is by default a virtual domain from which the topologies of all other existing domains can be managed.

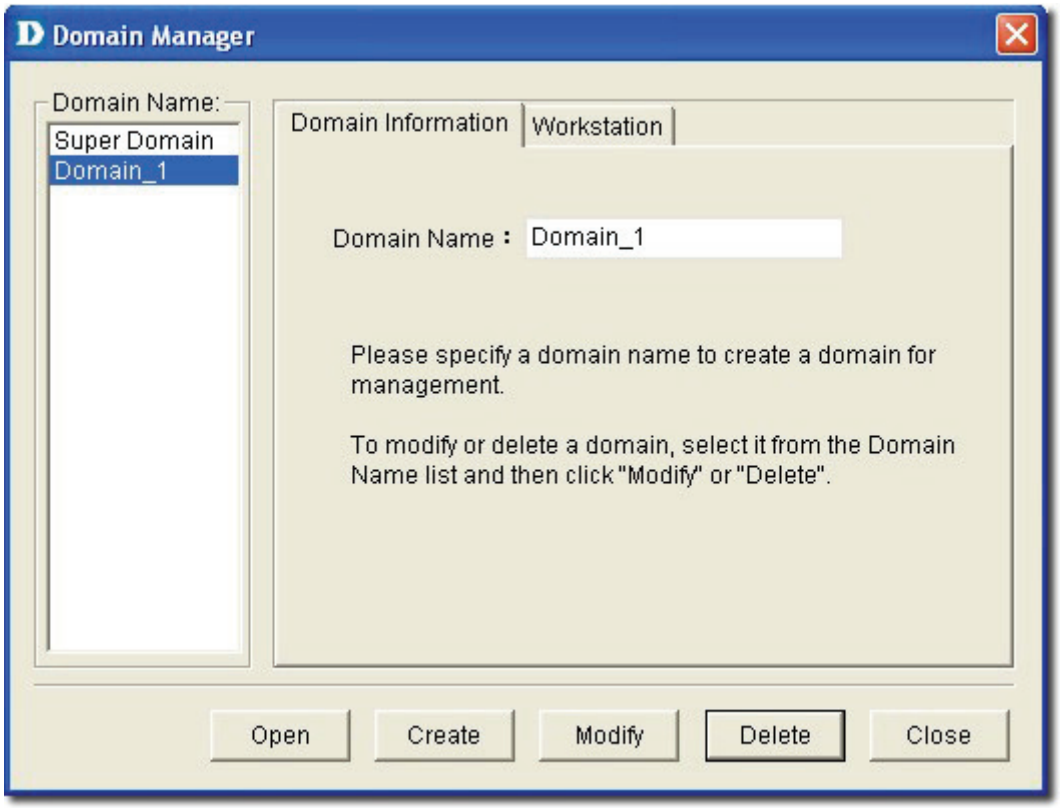


Figure 46: Domain Manager screen

2. Create a netmap. To create a netmap, right-click on the domain in the **Hierarchy Topology Workplace**, and select **Add Netmap**.

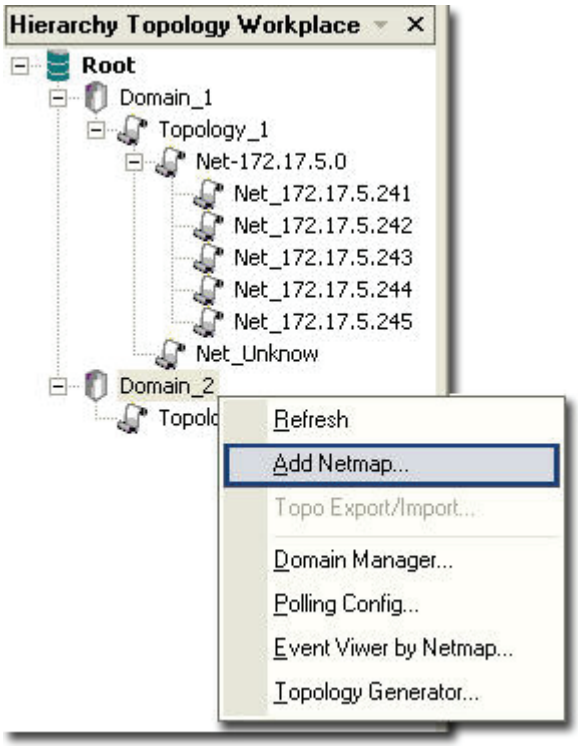


Figure 47: Hierarchy Topology Workplace screen

3. The **Add Netmap** screen displays.

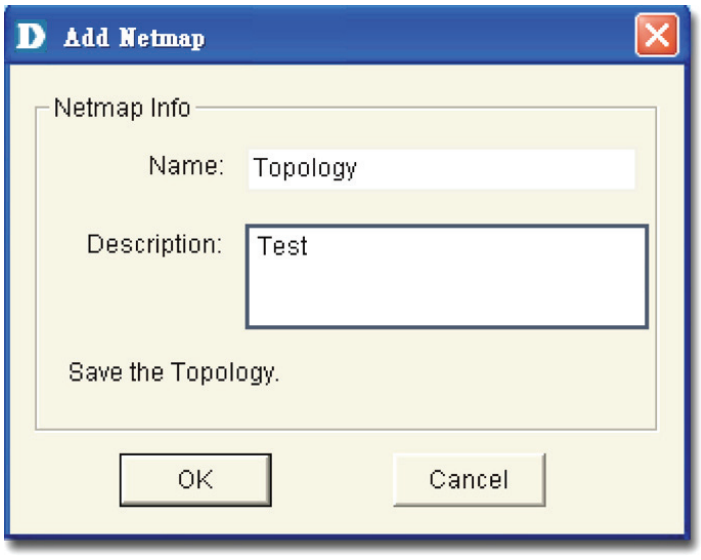


Figure 48: Add Netmap screen

4. Enter the **Name** and **Description** for the Netmap.
5. Click **OK**.

Make sure to save the changes made to the database before you proceed.

6. There are three ways to accomplish the next task. They are:
   - Go to **NetTools > Device Discovery** to search for and add devices into the Netmap manually. Then create links between the devices. Refer to Device Discovery for more information.

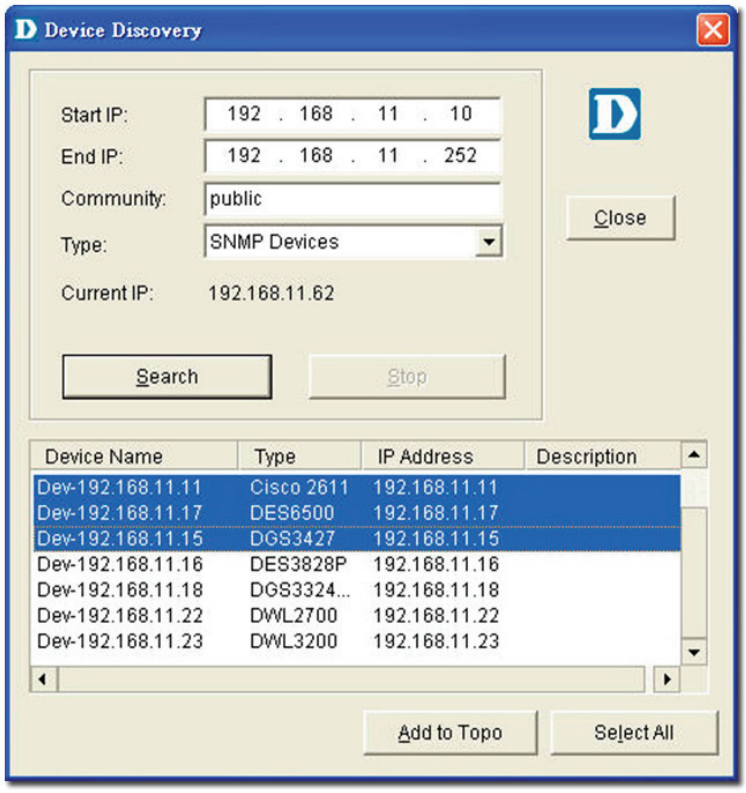


Figure 49: Device Discovery screen

- From the **Topo Manager Toolbar**, Click **Add Devices** [ ]. OR use the **Copy/Paste** function. Refer to Copy/Paste for more information.
- Continue to **Export** your topology. Refer to Using Topo Export/Import for more information.

CREATING ADMINISTRATOR-SPECIFIC TOPOLOGIES

D-View manages the entire topology in domain mode; administrators can create different topology maps to be managed by different administrators. Only the administrators in the Super Domain can manage the entire network.

To create multiple topologies with Domain Manager:

1. Login to D-View with **Super Domain** administrator access.
2. Go to **System > Domain Manager** and then create two domains. For example: Domain_1, Domain_2.

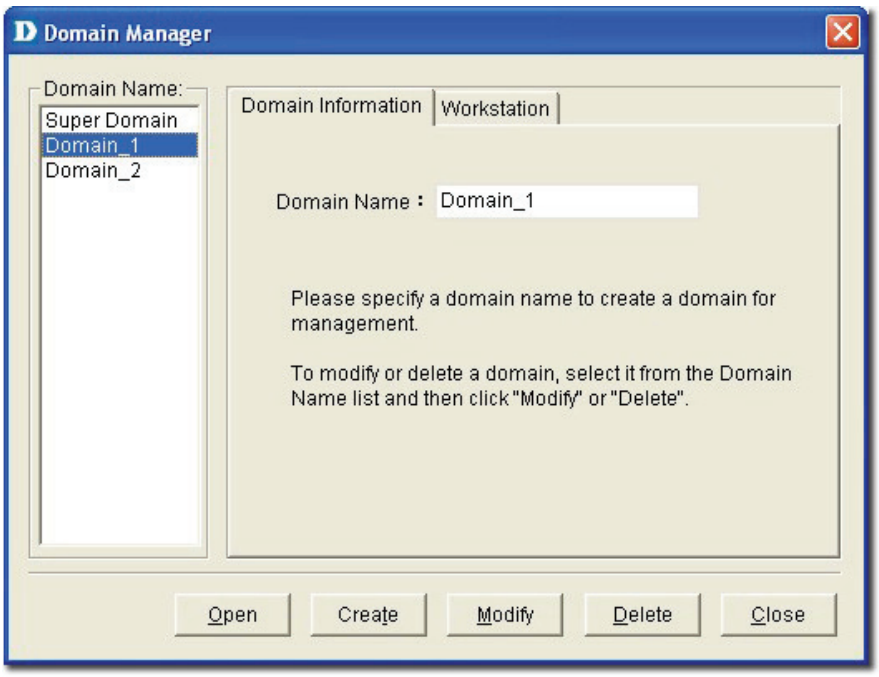


Figure 50: Domain Manager screen

3. Select a domain, update the **Workstation** information and then click **Create** to define the management workstation in D-View. For example: Domain_1, Station_1 and IP address.

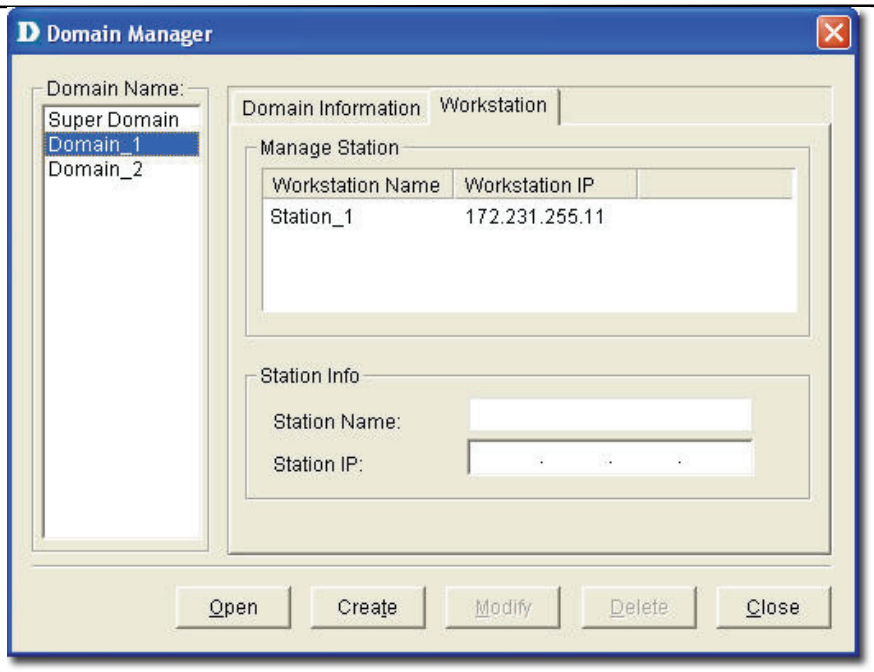


Figure 51: Domain Manager: Workstation screen

4. Repeat the previous step for the other domain.
5. Create a topology for each domain.

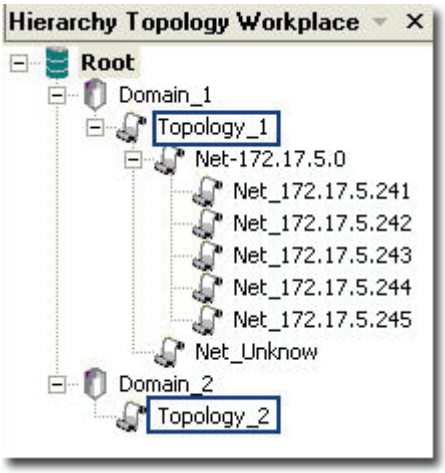


Figure 52: Hierarchy Topology Workplace

6. Login to D-View by using different domain-specific administrator accounts to view different topology maps. For example: Click **Option** to login with **Domain_1** administrator account by using **Domain_1 Station:** 172.231.255.11.

Figure 53: Login screen

7. This administrator can view only the **Domain_1** topology.

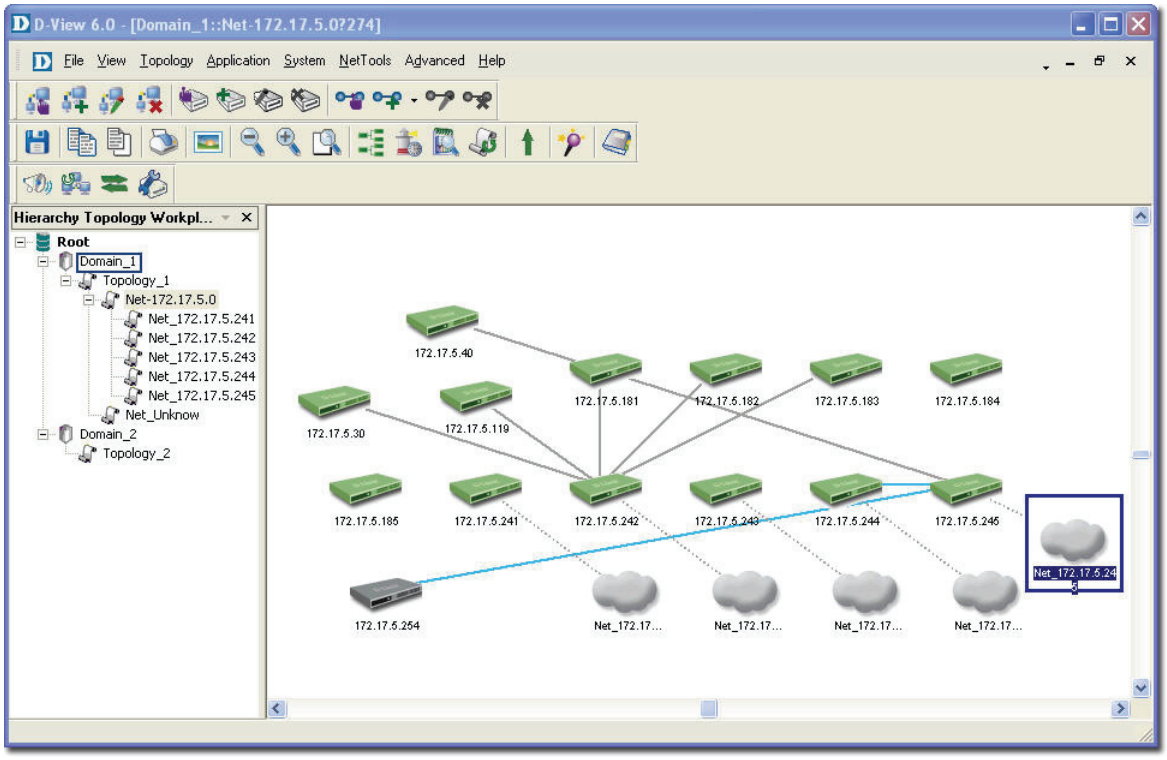


Figure 54: Domain_1 window

USING TOPO EXPORT/IMPORT

D-View allows you to export to or import from an XML file. Use this feature to make regular backups.

To export or import topology information:

1. Go to **Application > Topo Export/Import**. The **Topo Export/Import** screen displays.

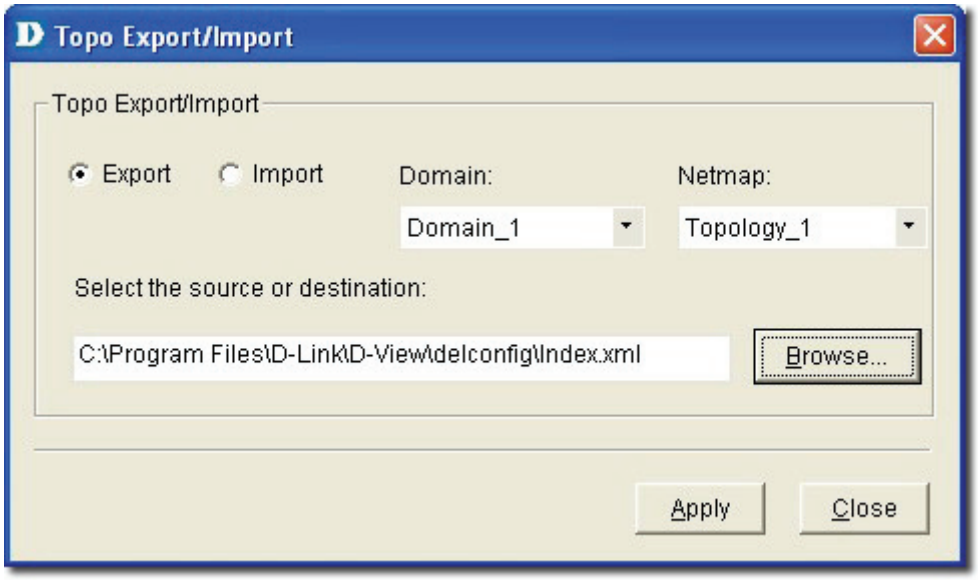


Figure 55: Topo Export/Import screen

2. Select either **Export** or **Import**.
   - **Export:** Backup/save topology data to an external XML file.
   - **Import:** Restore topology data from an XML file.
3. Select the **Domain**.
4. Select the **Netmap**.
5. Browse to select the file to export to or import from.
6. Click **Apply**.

Refer to Restoring and Backing Up D-View to restore and backup D-View.

TOPOLOGY GENERATOR PRINCIPLE

Using **ARP** (Address Resolution Protocol) and forwarding table information in devices, D-View creates a topology for a specific network. The following steps describe the principle behind the **Topology Generator:**

1. Discovers the devices by getting the ARP information in devices, and identifies the relationship among devices by their MAC or IP address.
2. Identifies the device type.
3. Retrieves the forwarding table information in switches to obtain the relationship among switch ports and MAC address of the devices.
4. Creates a Topology.

The generated topology can be incorrect if the switches' forwarding table information is incorrect or incomplete. The topology created by Topology Generator can be considered as a reference in completing the actual topology map.

USING TOPOLOGY GENERATOR

Use the **Topology Generator** to create the topology map.

To use the Topology Generator:

1. Go to **NetTools** > **Topology Generator.** The **Topology Generator Wizard** screen displays.

Figure 56: Topology Generator Wizard screen

2. Select the **Analysis Mode**.
3. Enter the **Topology** Name.
4. Click **Next**. The **Topology Analysis Configuration** screen displays. The topology generator analyzes the local network for the IP address and Subnet Mask. The **SNMP Community String Setting** is by default defined in D-View.

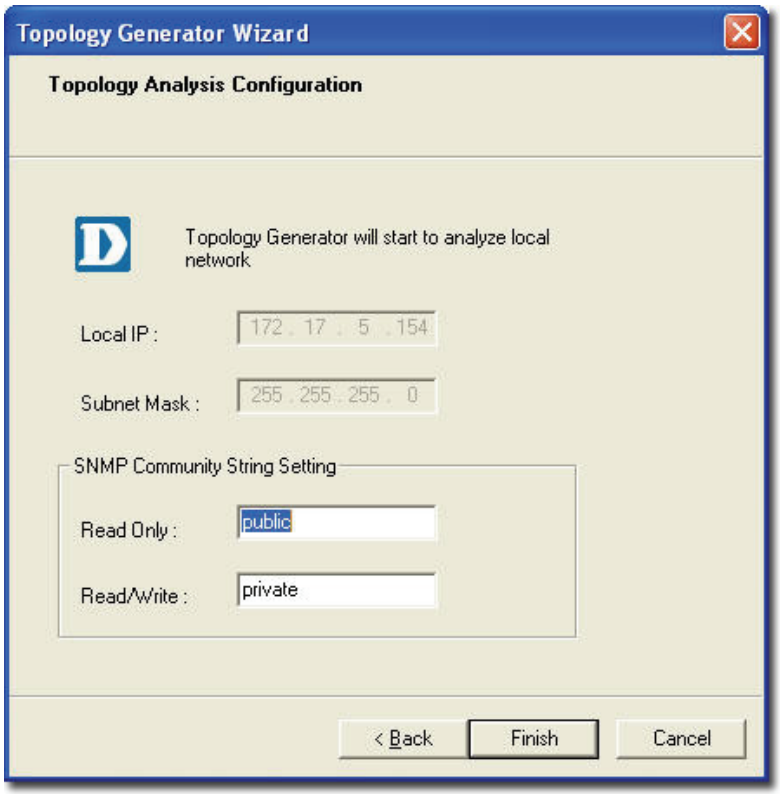


Figure 57: Topology Analysis Configuration screen

5. Click **Finish** to generate the topology. The new topology displays in the window.

For a designated network, enter the IP address and ensure that the D-View management console can access the designated subnet.

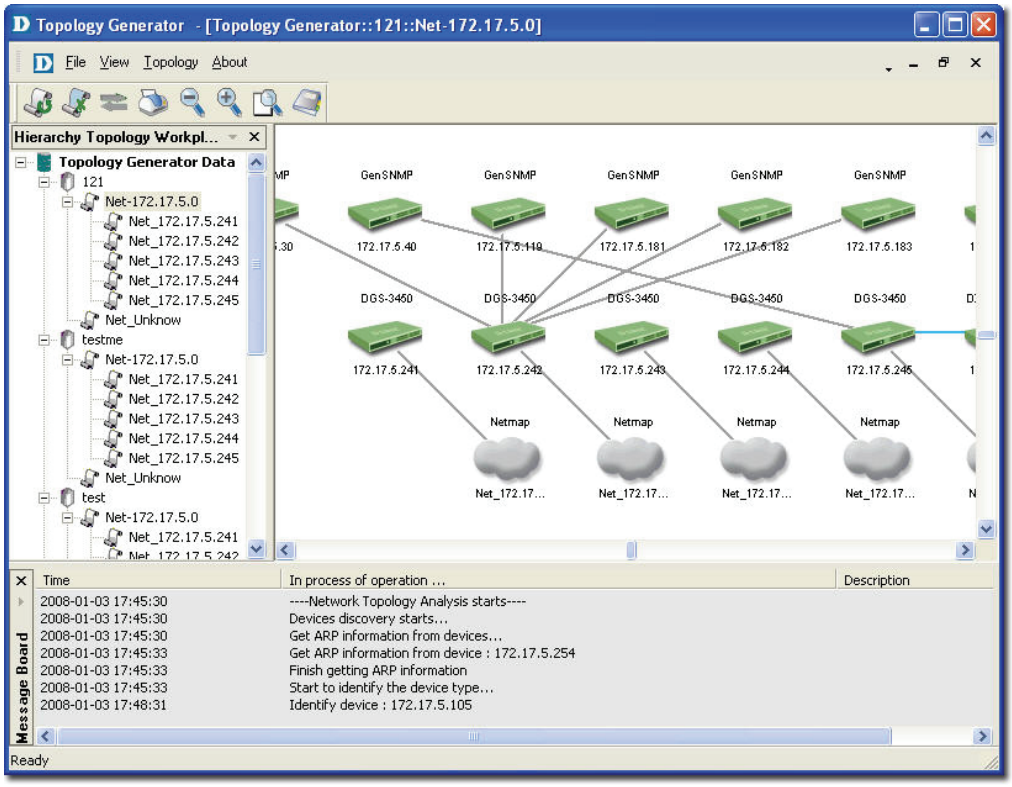


Figure 58: Generated Topology window

6. Go to **Topology** > **Topo Export** or select and right click on the netmap of the generated Topology to select **Topo Export**.

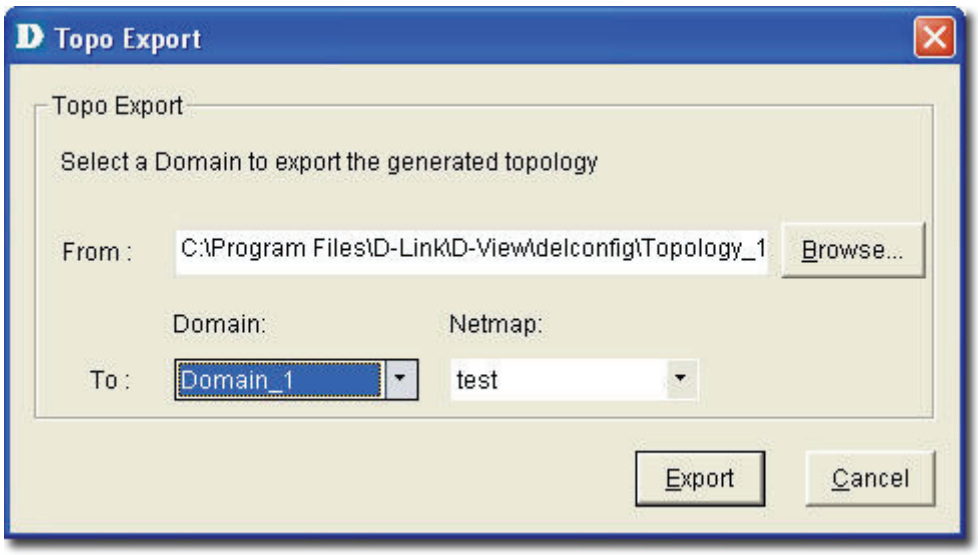


Figure 59: Topo Export screen

7. Click **Export** to export the generated topology.

REARRANGING THE TOPOLOGY

Manually rearranging multiple devices and links in a topology is a laborious and difficult process. But with D-View, you can:

- **Rearrange Totally**
- **Rearrange by step**

Using Rearrange Totally

Open and select a device in the topology. Go to **Topology** > **Rearrange Totally**. The system will rearrange the linked devices in hierarchy considering the selected device as the topmost device.

Using Rearrange by step

Open and select a device in the topology. Go to **Topology > Rearrange by step.** The system will rearrange the linked devices in hierarchy considering the selected device as the top device.

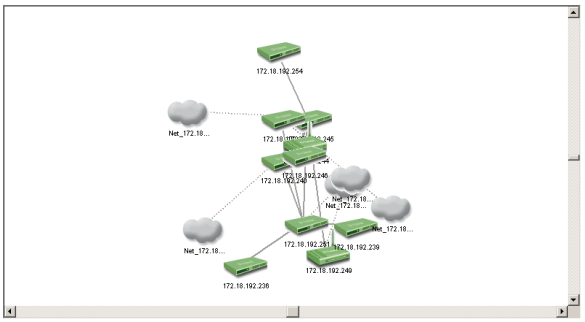
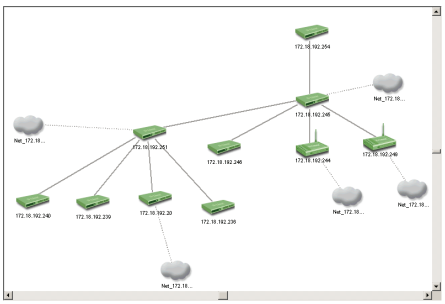
Before Rearranging	After Rearranging
	

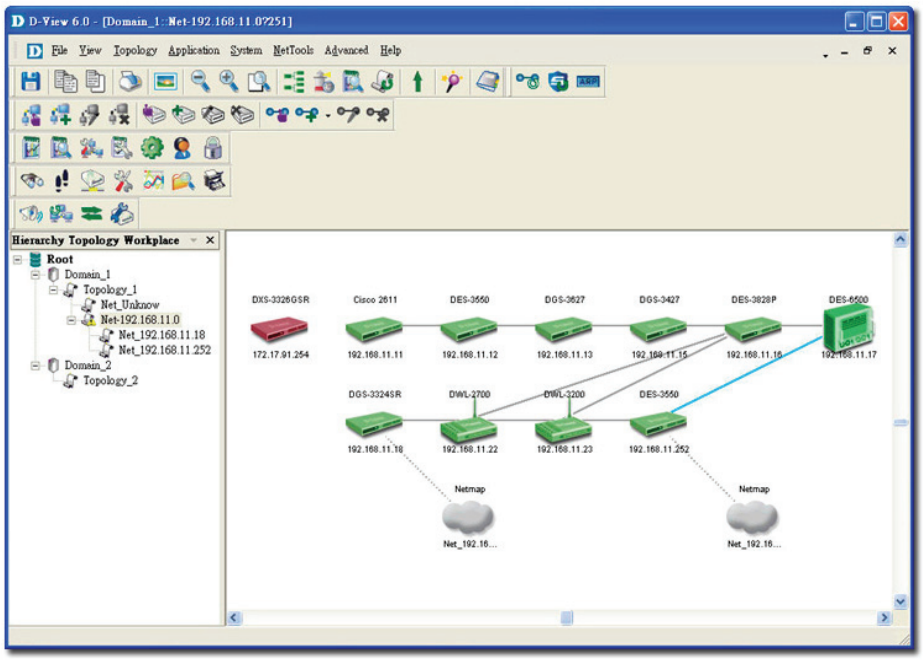
Figure 60: Topology before and after rearranging

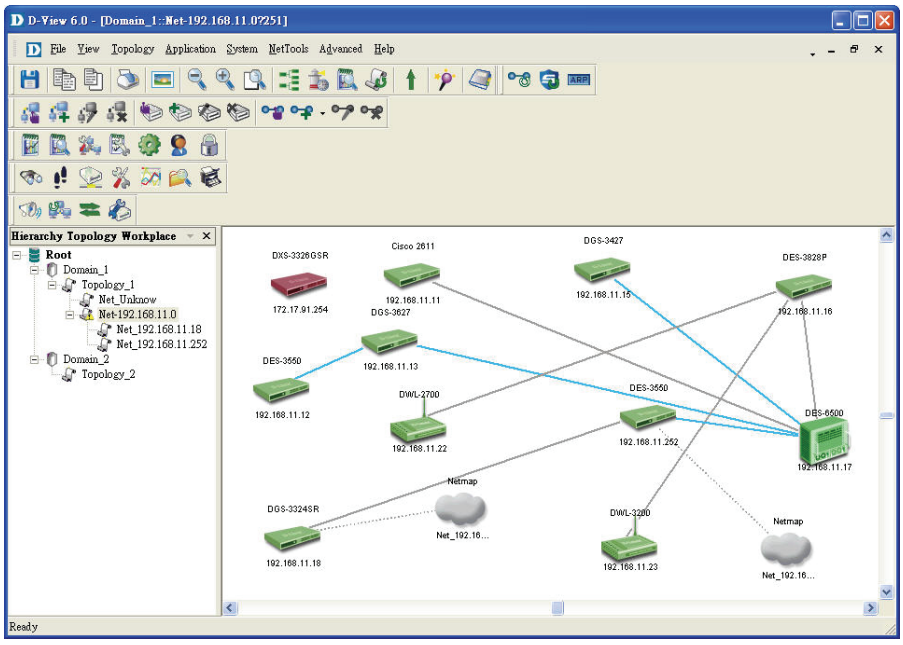
Rolling Back a Topology

After rearranging the topology, you can restore the saved topology that was created initially from the database.

To Rollback a Topology:

Go to **Topology > Topology Rollback**. The Topology reverts to the previous settings. The following screenshots displays the sequence of steps by using the Topology Rollback function.





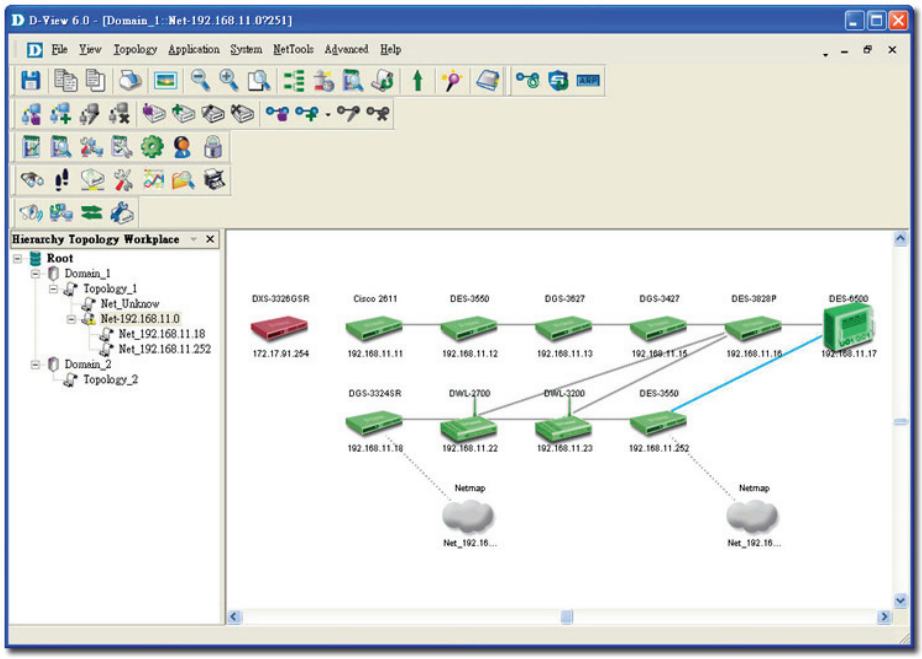


Figure 61: Sequence of steps displaying the Topology Rollback function

Managing and Monitoring Devices

IDENTIFYING DEVICES

To view the installed device modules, go to **Help** > **Devices Supported**. Information about all the supported devices is displayed. D-View, by default, supports all D-Link devices that have been added to D-View.

If you cannot find the device modules in the list, download and install the device management modules from the D-Link Website.

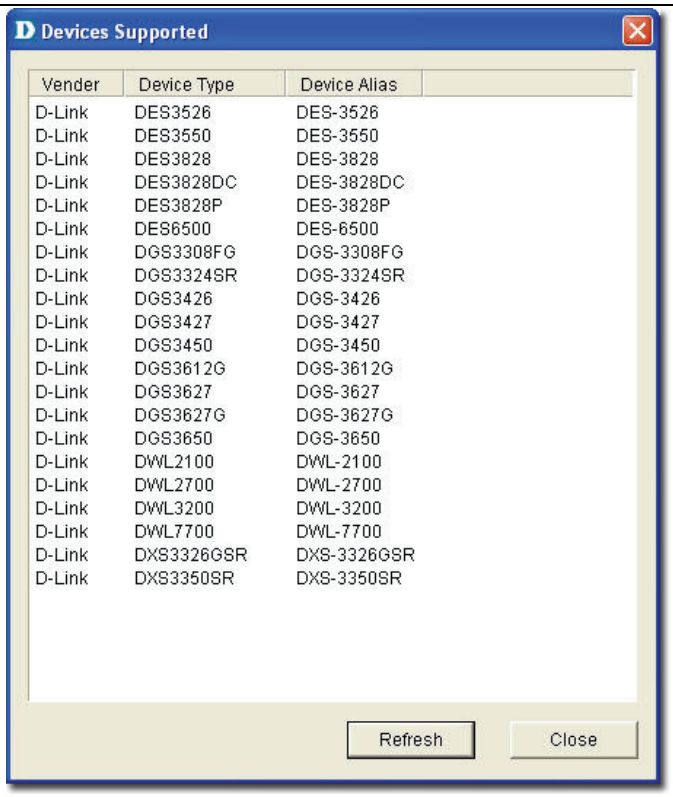


Figure 62: Devices Supported screen

Refer to Customizing Devices to extend the device module list.

MULTI-VENDOR SUPPORT

Only the following modules can be used by third-party devices:

- **GenSNMPDeviceModule:** D-View recognizes SNMP enabled devices irrespective of device type, vendor and model number. Refer to Retrieving OID of the device for more information.
- **MIB Browser/Compiler:** The MIB compiler translates the MIB from its normal ASN.1 format to a format that is comprehensible by other applications. Refer to Managing Devices with MIB Compiler for more information.
- **Telnet, Web management tools:** Refer to Management Methods for more information.
- Monitoring performance status by **ICMP**/**SNMP**. Refer to Setting the Devices to Poll for more information.
- Extension of supported device types with **Device Customization** functional module. Refer to Customizing Devices for more information.

CUSTOMIZING DEVICES

D-View provides a flexible method to extend devices that can be identified and managed by configuring the interface between platform and device module.

To customize devices:

1. Go to **Application** > **Device Customization.** The **Device Customization** screen displays.

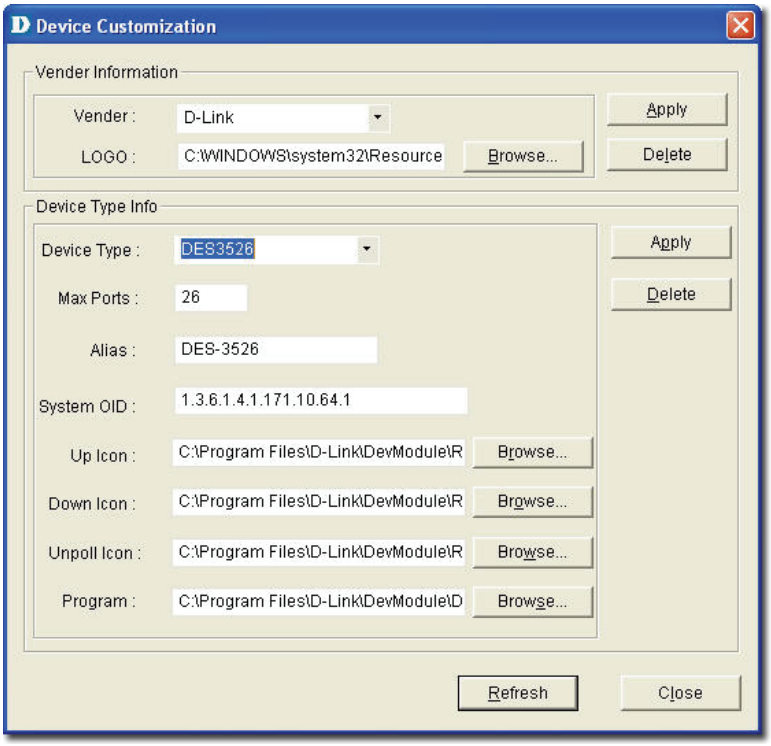


Figure 63: Device Customization screen

2. From the **Device Customization** screen, you can modify the device type properties in the dialog.
   - **Vendor:** Select/enter a vendor from the drop-down list.
   - **Logo:** Select a logo for the device module.
   - **Device Type:** Select/enter the device type.
   - **Max Ports:** Enter the maximum number of ports, depending on the device.
   - **Alias:** Enter an alias name for the device.
   - **System OID:** Enter the OID value of the device. Refer to Retrieving OID of the device to obtain the OID of a device.
   - **Up, Down, Unpoll icons:** Browse to define and customize the device icons.
   - **Program:** Specify the location of D-View module. Double-click on the device icon in the topology to manage multiple devices through a D-View Module (graphic interface).
3. Click **Apply** to save the Device Type info into the database.
4. Click **Refresh** to clear the fields.

HOW TO CONFIGURE DEVICES NOT IN SUPPORTED LIST

To verify if a switch is supported by D-View 6.0, go to **Help > Devices Supported**.

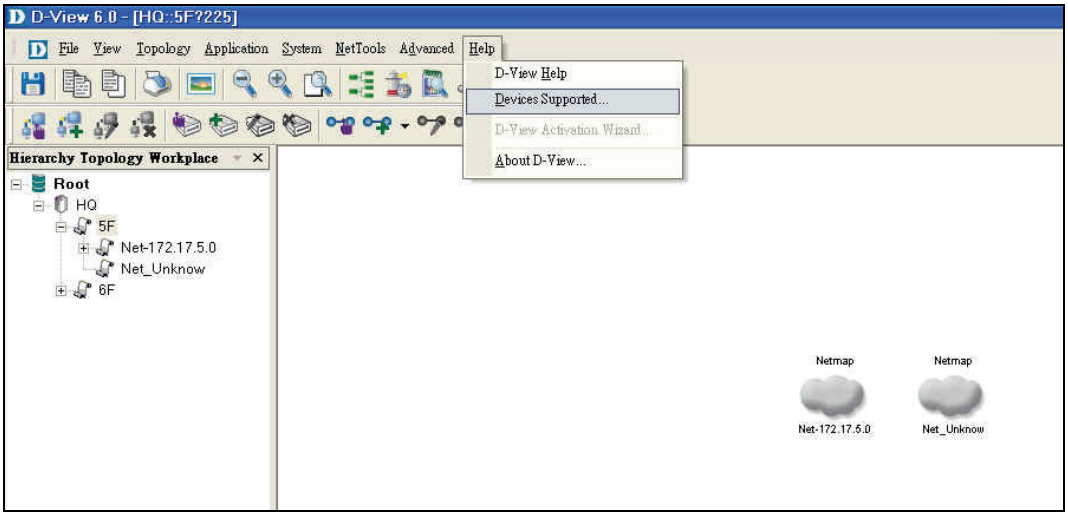


Figure 64: Devices Supported function

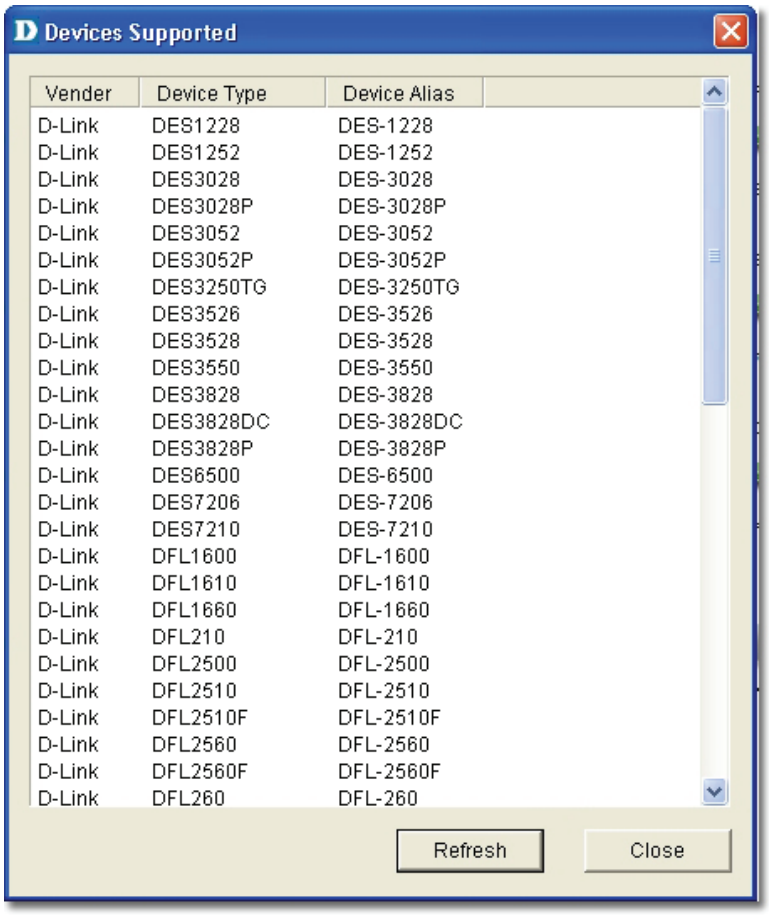


Figure 65: Devices Supported list

Discover Devices

In order to discover a device, follow the steps below. The DES-3028 will be used as an example for Device Discovery.

To search for the device and then add it to the topology map go to **NetTools > Device Discovery.**

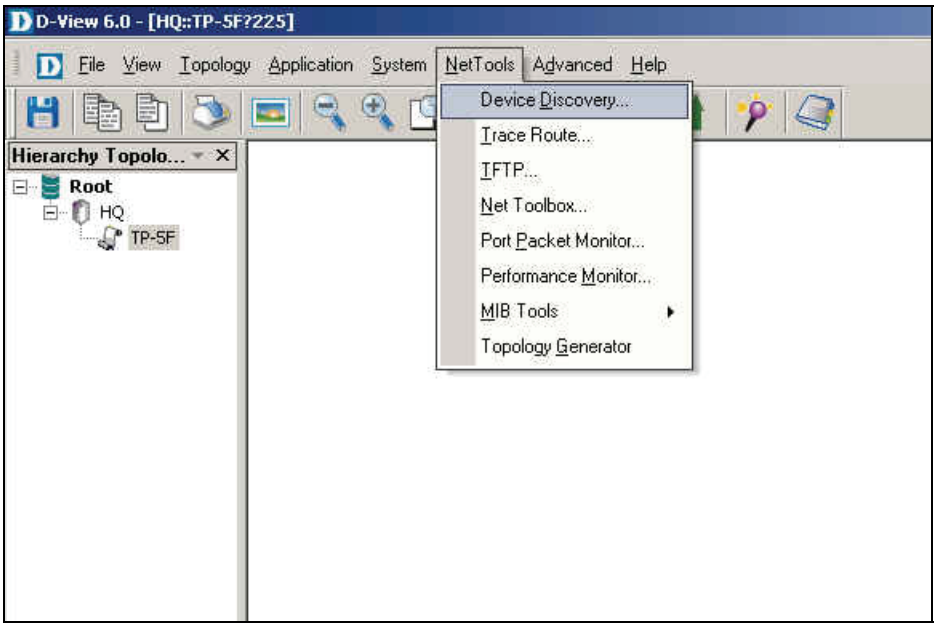


Figure 66: Device Discovery function

Enter the information related to the switch:

- IP address.
- Community name.

Next, click **Search.** Select the discovered device and click **Add to Topo.**

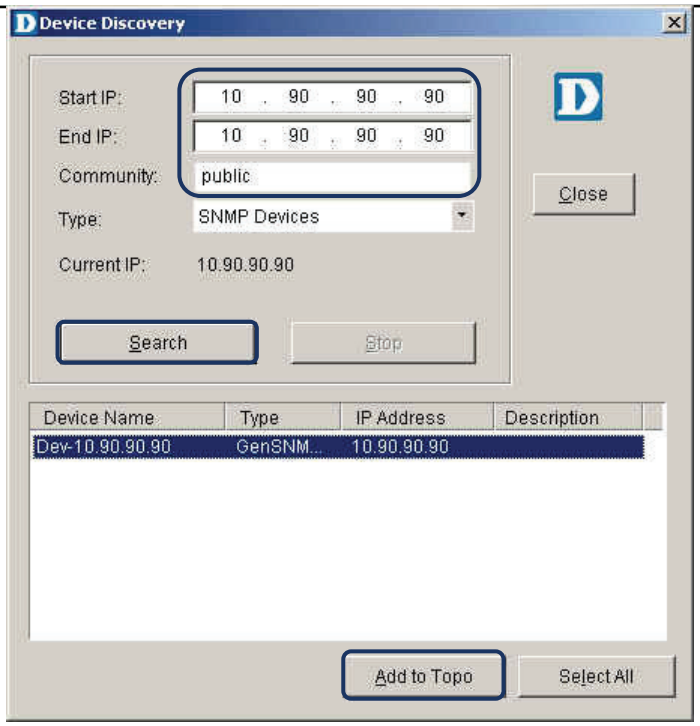


Figure 67: Device Discovery screen

To change the device type:

1. Double click the device icon on the topology map to launch the D-View module.

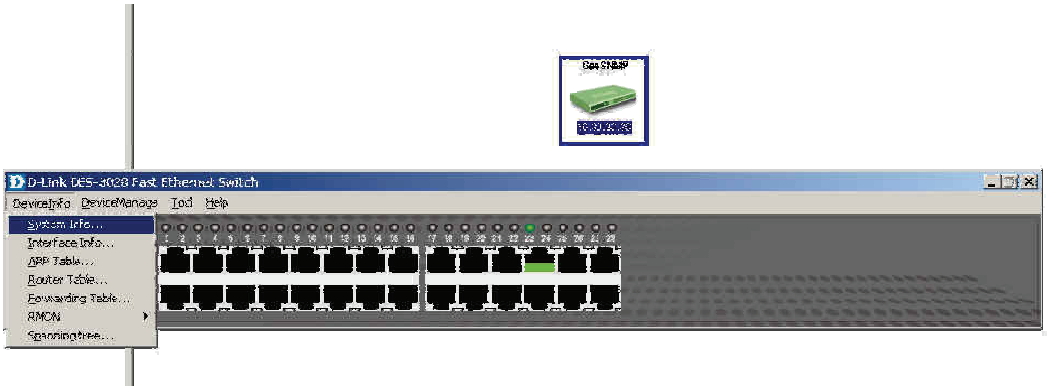


Figure 68: GenSNMP D-View module

2. Check device's OID information, go to **DeviceInfo > System Info.**

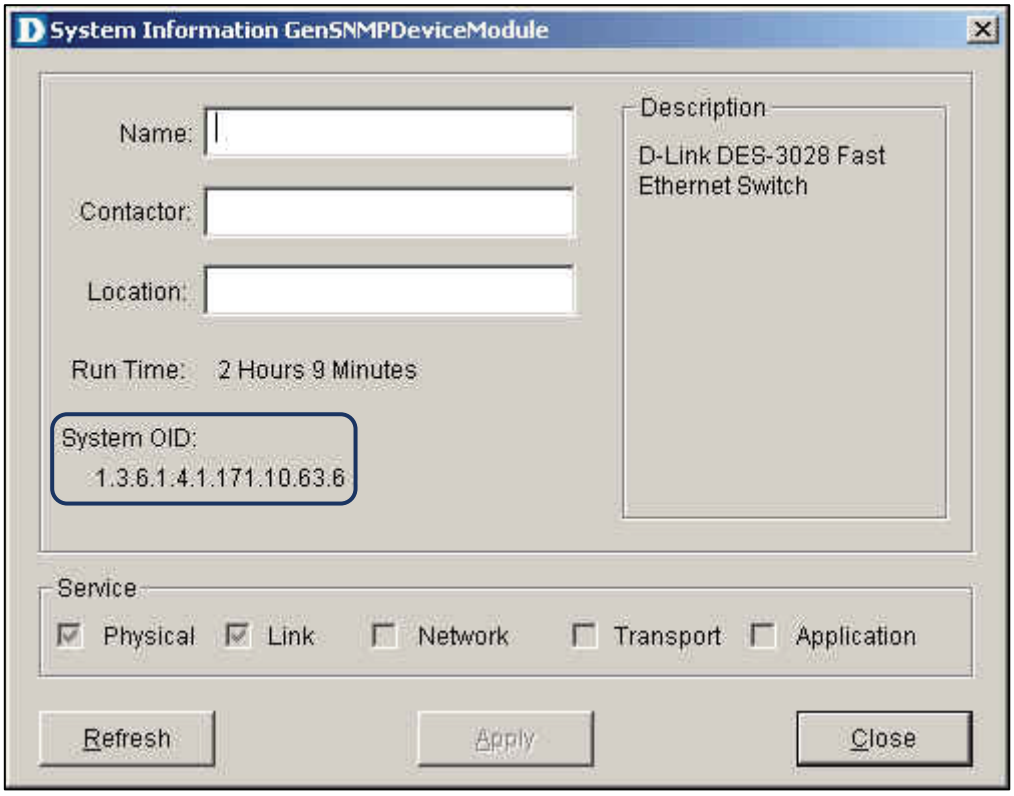


Figure 69: System Information screen

3. Launch the Device Customization tool and add the OID information to D-View's database, go to **Application > Device Customization.**

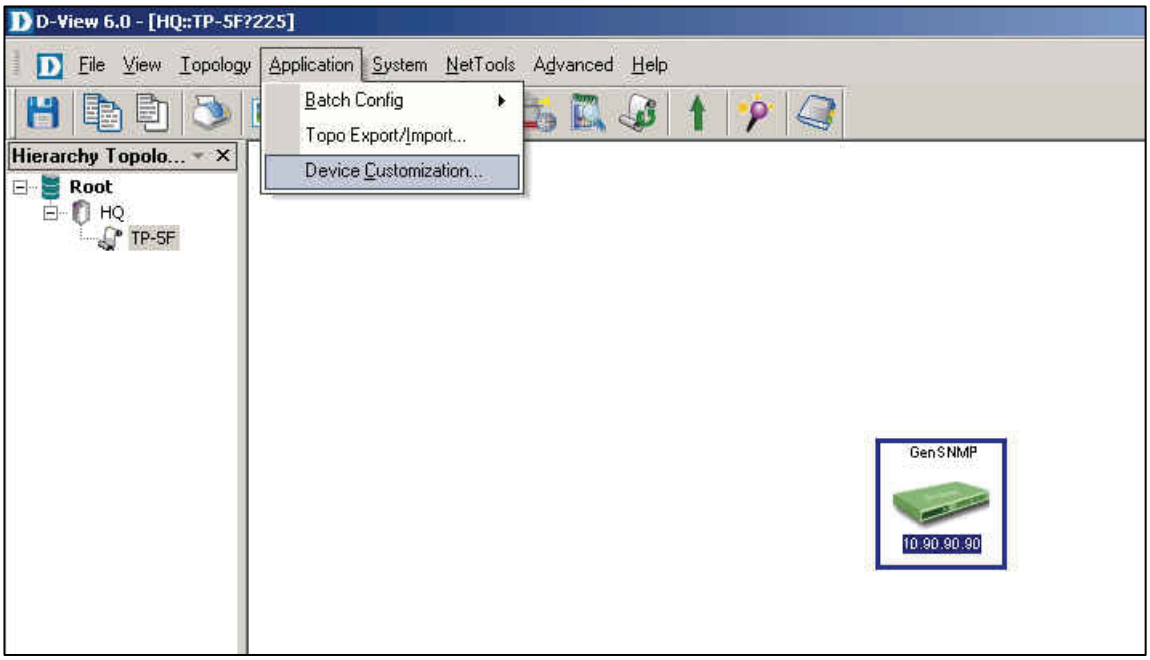


Figure 70: Device Customization function

4. Enter the vendor's information.
   - Vendor: Enter vendor's name.
   - Logo: Upload a logo for the vendor.

5. Enter the device type.
   - Device Type: Enter the model name.
6. Enter the alias name & OID.
   - Alias: The name entered is displayed on the topology map.
   - System OID: Device's OID number.
7. Click **Apply**.

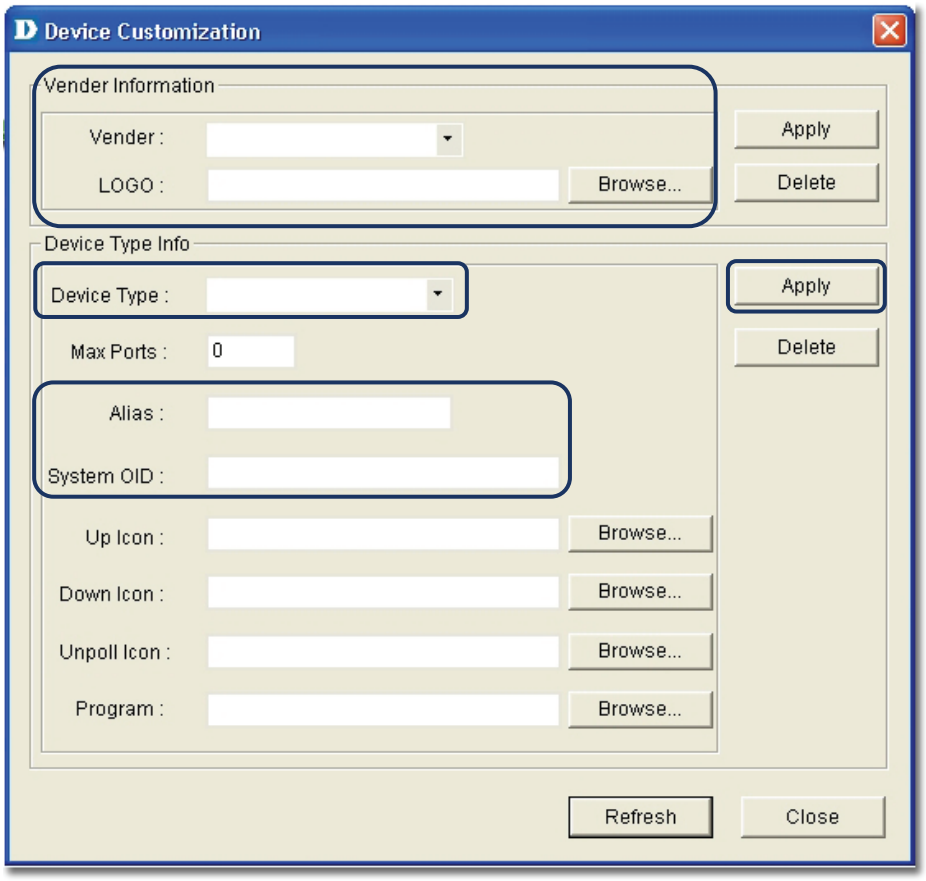


Figure 71: Device Customization screen

There are two **Apply** buttons in the **Device Customization** window:

Vendor Information:

- If the vendor's name is not seen in the list, you can create a new one.
- Enter the vendor's name and click **Browse** to upload a logo, then click **Apply.**

Device Type Info:

- To add a new device module into D-View's database, enter the vendor's information.

If the model name did not change, be sure to execute **Device Type Check** to update the database. Save the changes.

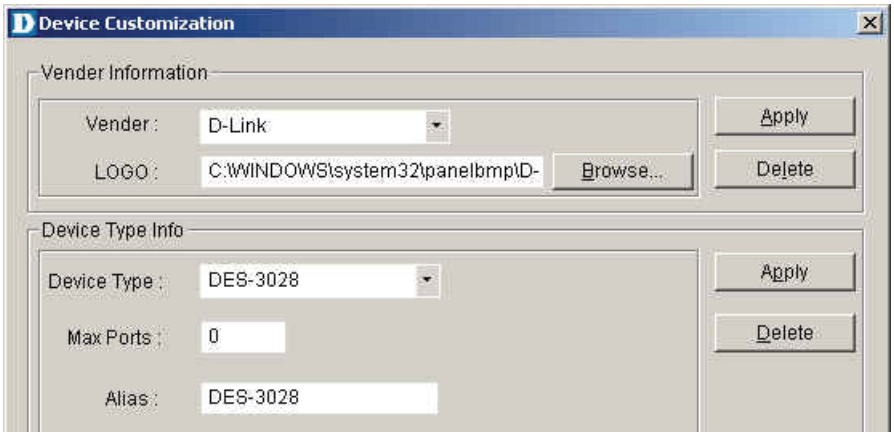


Figure 72: Device Customization

The purpose of Device Type Check is to update the customized information to the database.

1. Launch the **Device Type Check** function, go to **Advanced > Device Type Check.**

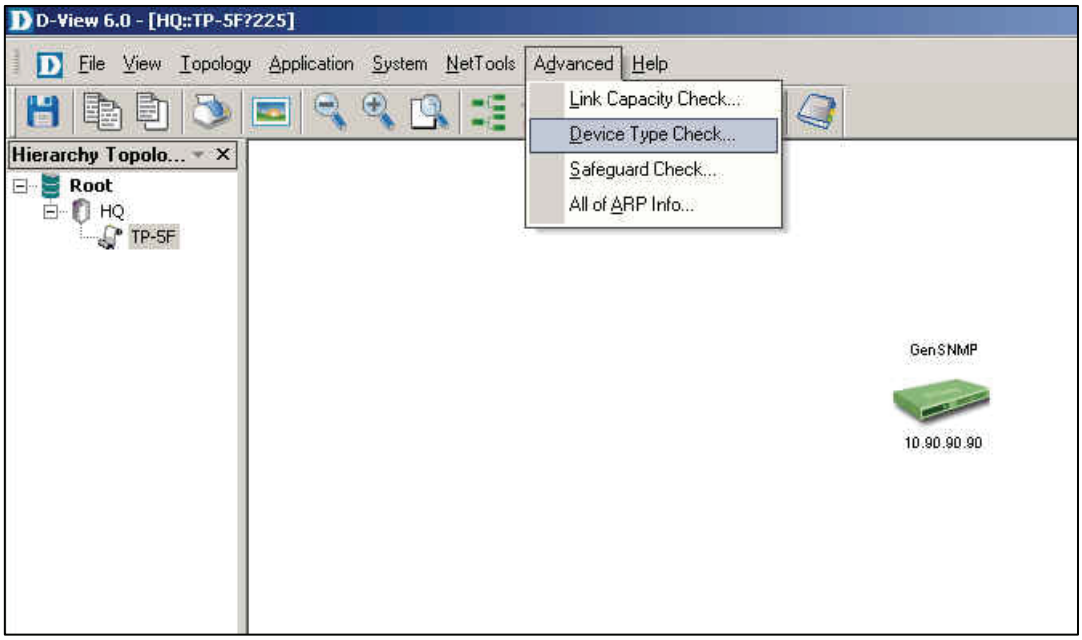


Figure 73: Device Type Check

2. Click **Check** to load the data from the database.
3. Click **Update** to update the database with the correct model name.

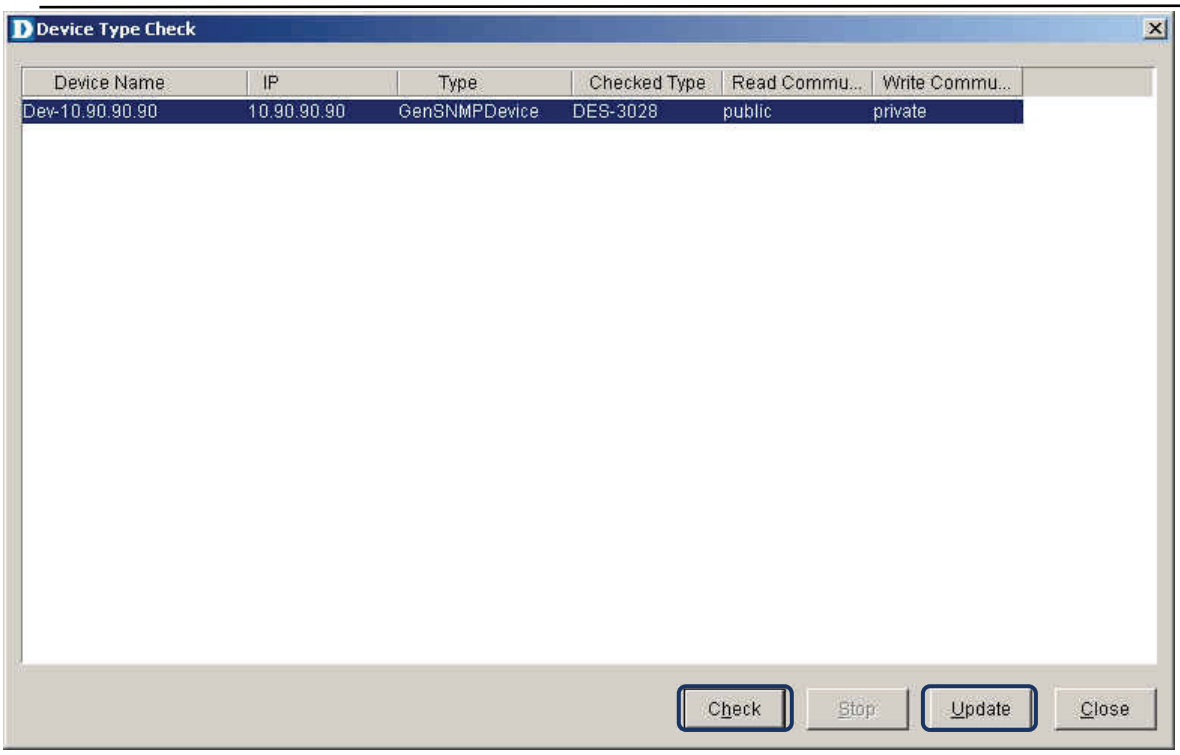


Figure 74: Device Type Check

In this case, the model name changes from GenSNMP to DES-3028. Click **Save** to save the changes.

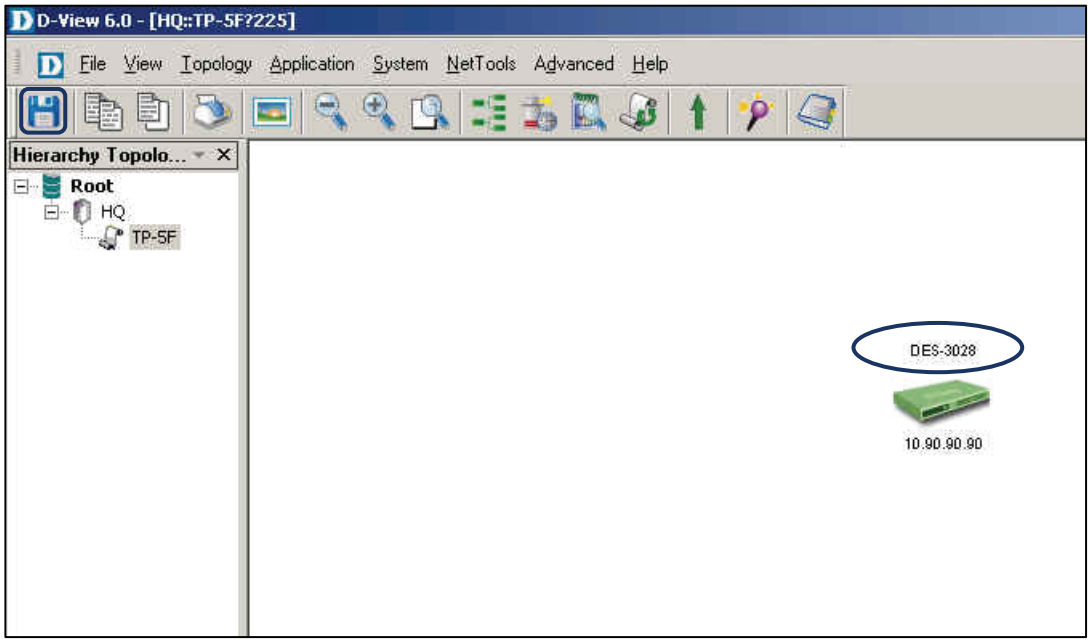


Figure 75: DES-3028 identified in the topology

In order to configure the Batch Config support for DES-3028's firmware update, the associated function OID for the device has to appear in the list.

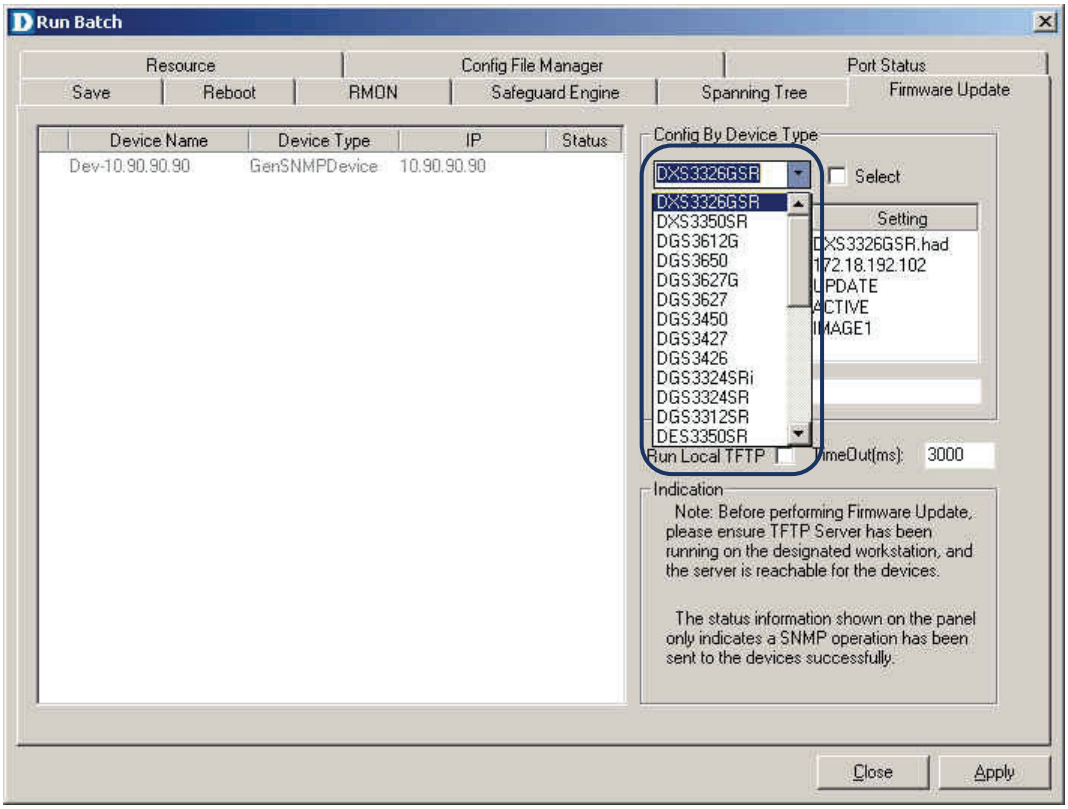


Figure 76: DES-3028 not in the list

To customize DES-3028's associated OID functions, add DES-3028 to the firmware update supported device list

1. Open **Advanced Option** to customize the OID function, go to **Application > Batch Config > Advanced Option.**

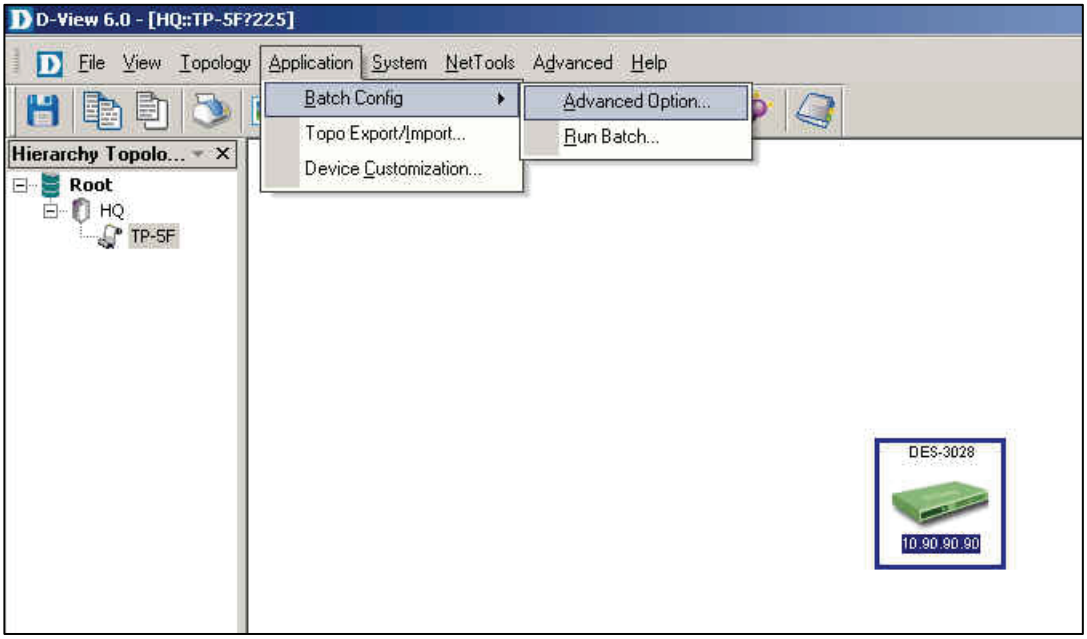


Figure 77: Advanced Option function

2. Select **FIRM** in the functions list and then click **Next**.

3. Search for DES-3028 in the **Device Types supported by...** list.
4. Click **Add** to add to the **Configured Devices Types** list.

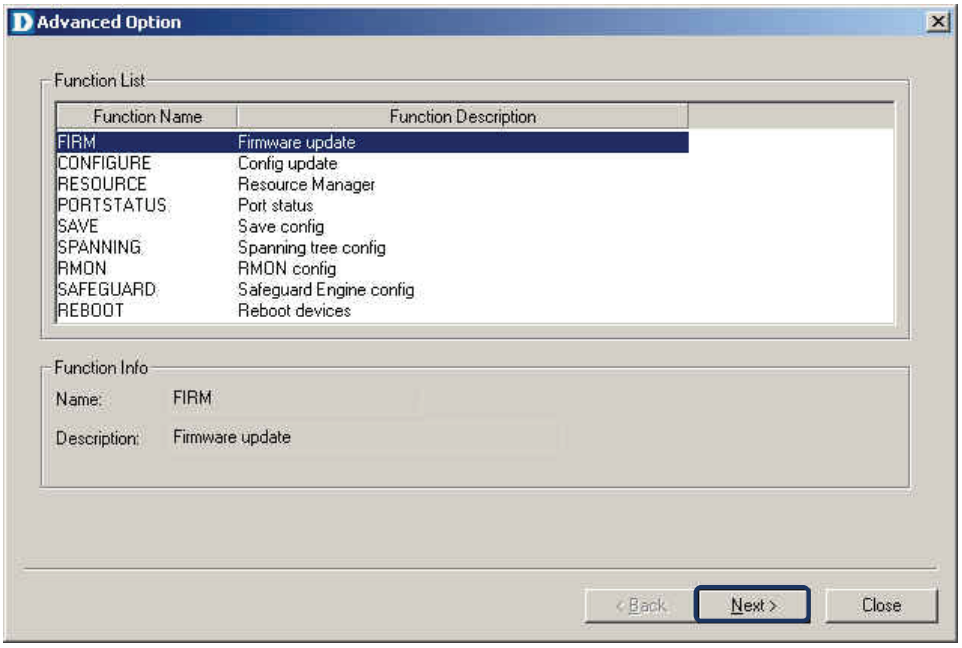


Figure 78: Firmware Update function

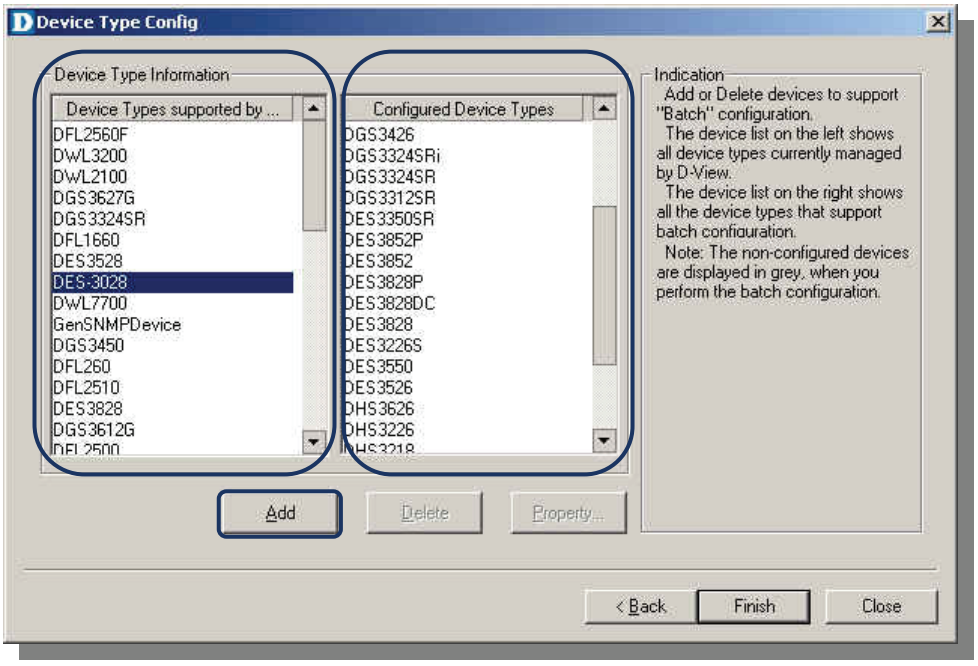


Figure 79: Adding DES-3028 to the support list

5. Select DES-3028 and then click **Property** to configure the OID function.

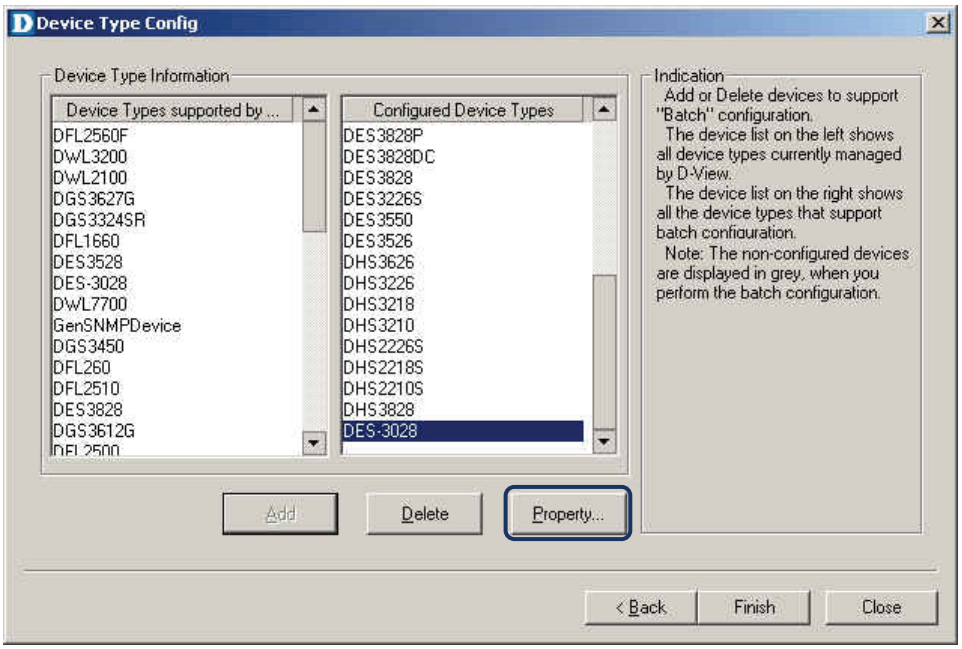


Figure 80: Device Type Config

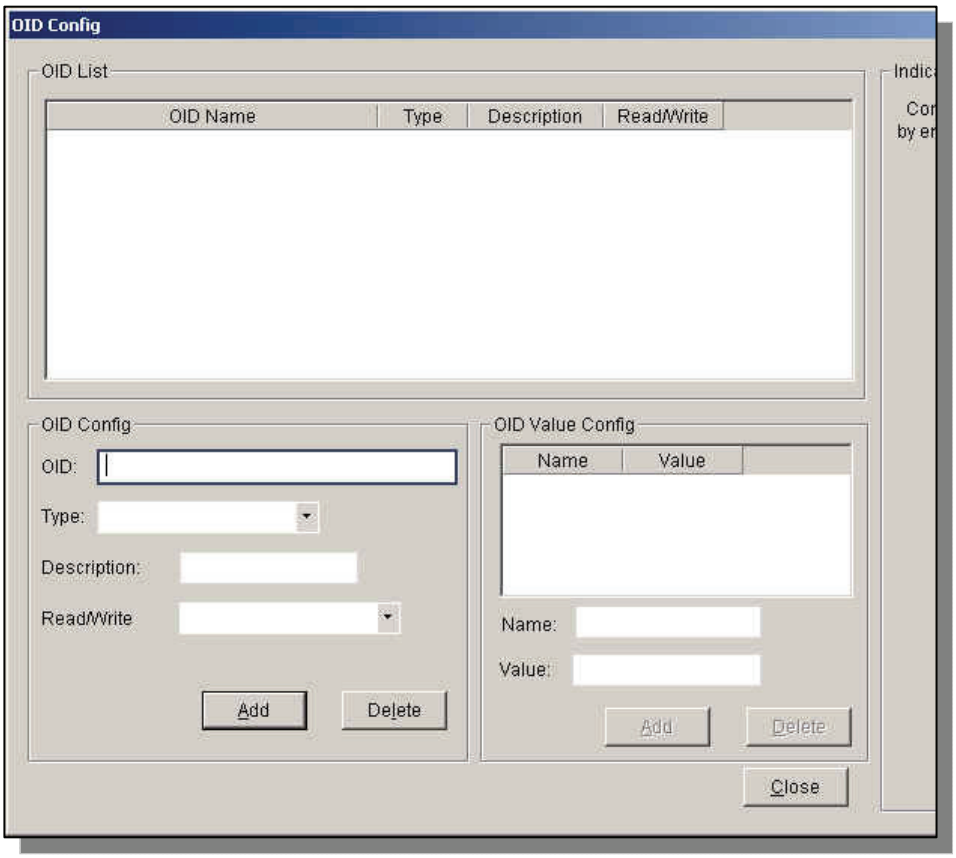


Figure 81: OID Config screen

Follow these steps to retrieve the OID information:

1. Open the MIB compiler to query the OID information.

   Go to **NetTools > MIB Tools > MIB Compiler.**

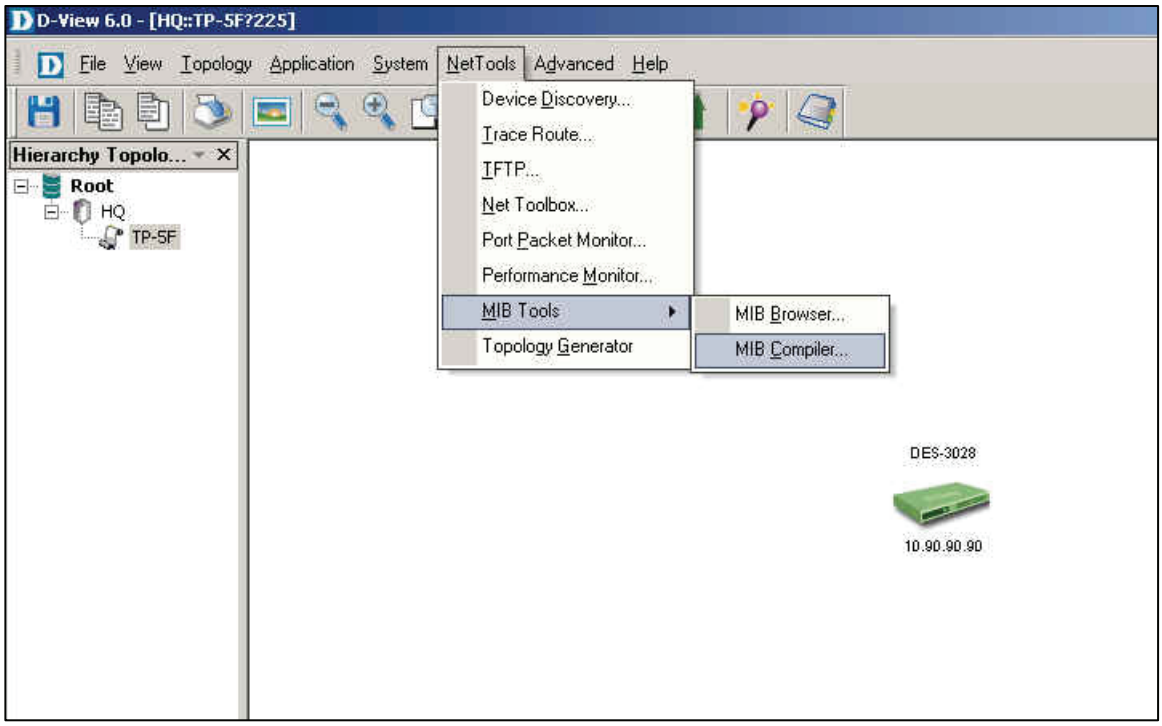


Figure 82: MIB Compiler

2. Click **Compile** to open the dialog window.
3. Browse and open the Genmgmt.mib file for compilation.
4. Enter the MIB file's location.

Figure 83: MIB Compiler

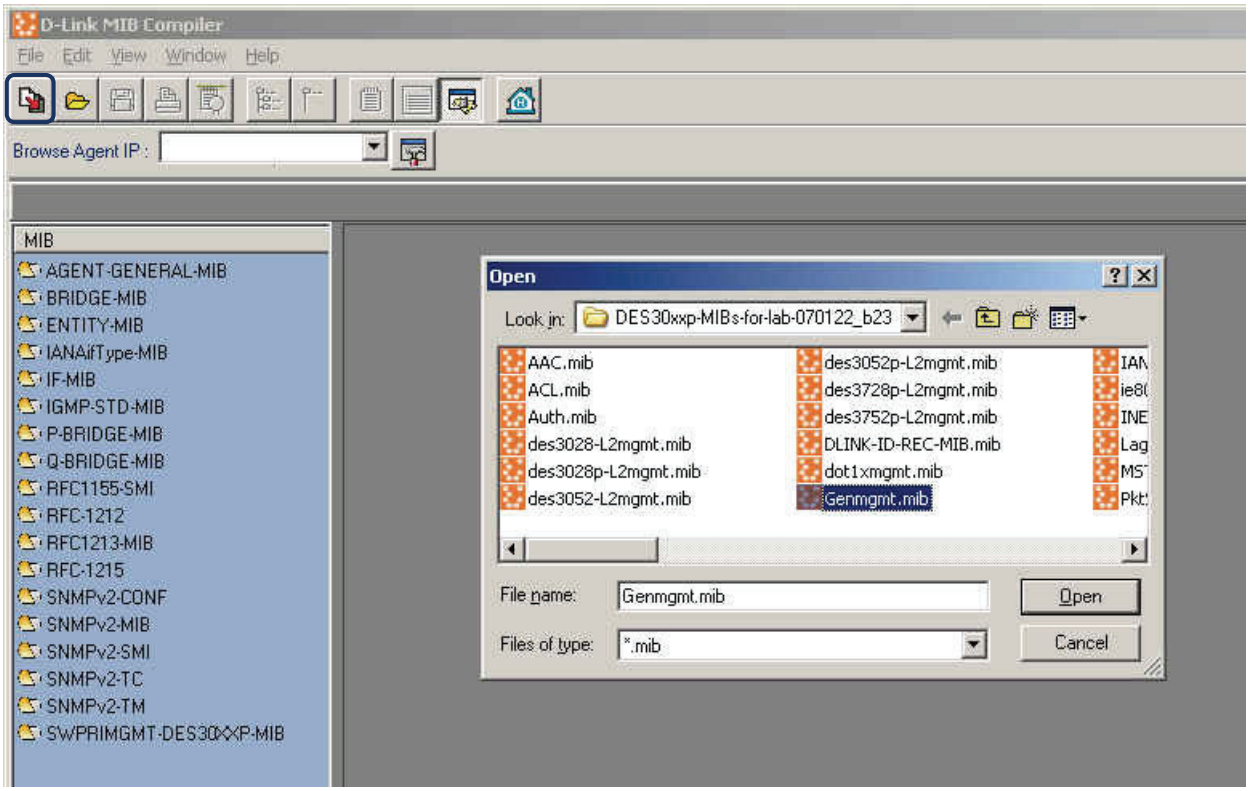


Figure 84: MIB Compiler

5. Select **agentBscSwFileLoadType** from the MIB Tree, the OID is displayed in the right window. This allows you to view information about uploaded and downloaded firmware.
   - The number in the **Value List** will control the upload or download action.

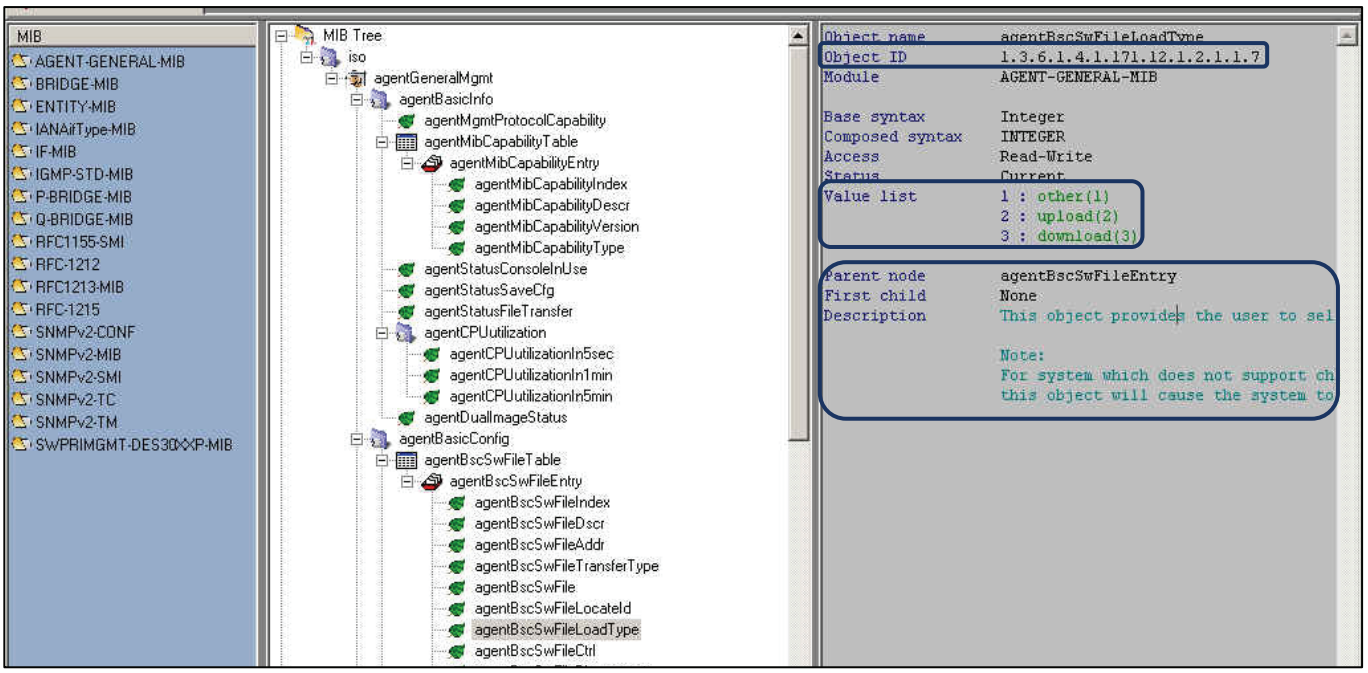


Figure 85: MIB Compiler screen

This slide refers to the DGS-3450 model's configuration; please configure the same for the DES-3028.
OID 1.3.6.1.4.1.171.12.1.2.1.1.7 refers to the file name.

1.3.6.1.4.1.171.12.1.2.1.1.7.***1***, here 1 refers to the index.

Value list defines the types of actions:

- 2: Upload (backup firmware).
- 3: Download (update firmware).

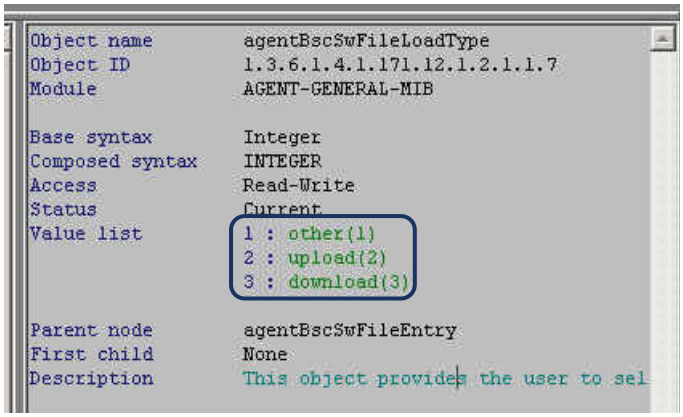


Figure 86: MIB Value description screen

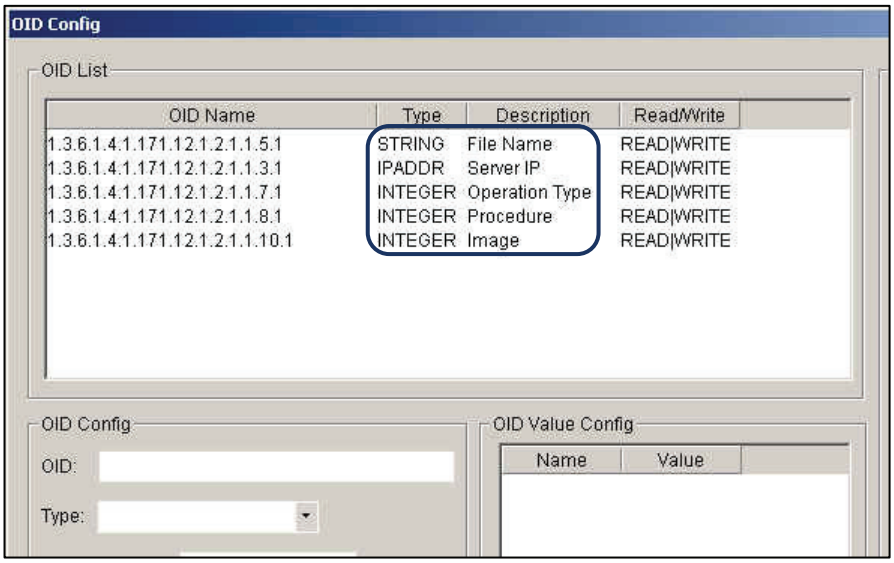


Figure 87: OID Parameter screen

6. Check the File Name's OID number and update the fields in **OID Config**, as seen in the screen below. Use the MIB-Compiler to enter the parameters.

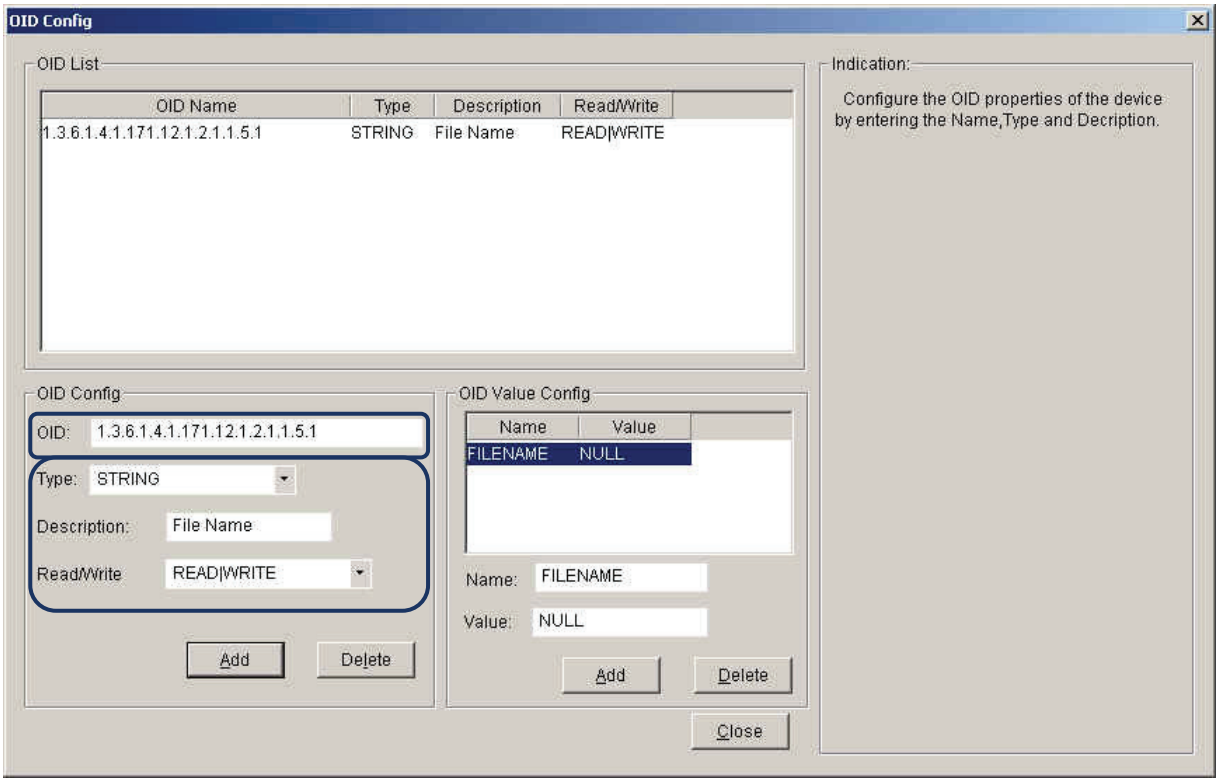


Figure 88: OID Config screen

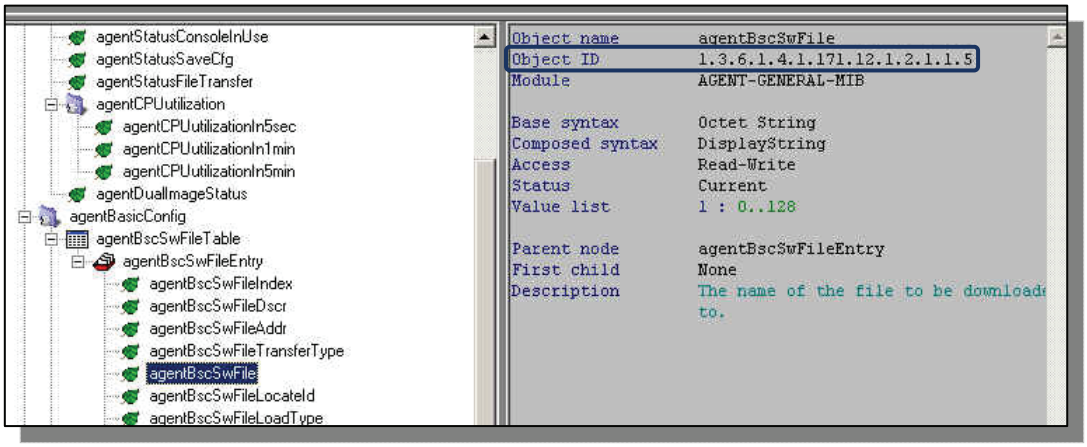


Figure 89: OID Information Query in MIB Compiler

7. Select **FileName** and enter the values of the OID Value Config information.
   - Name: Enter file name.
   - Value: Defines the input format and the space to store data.

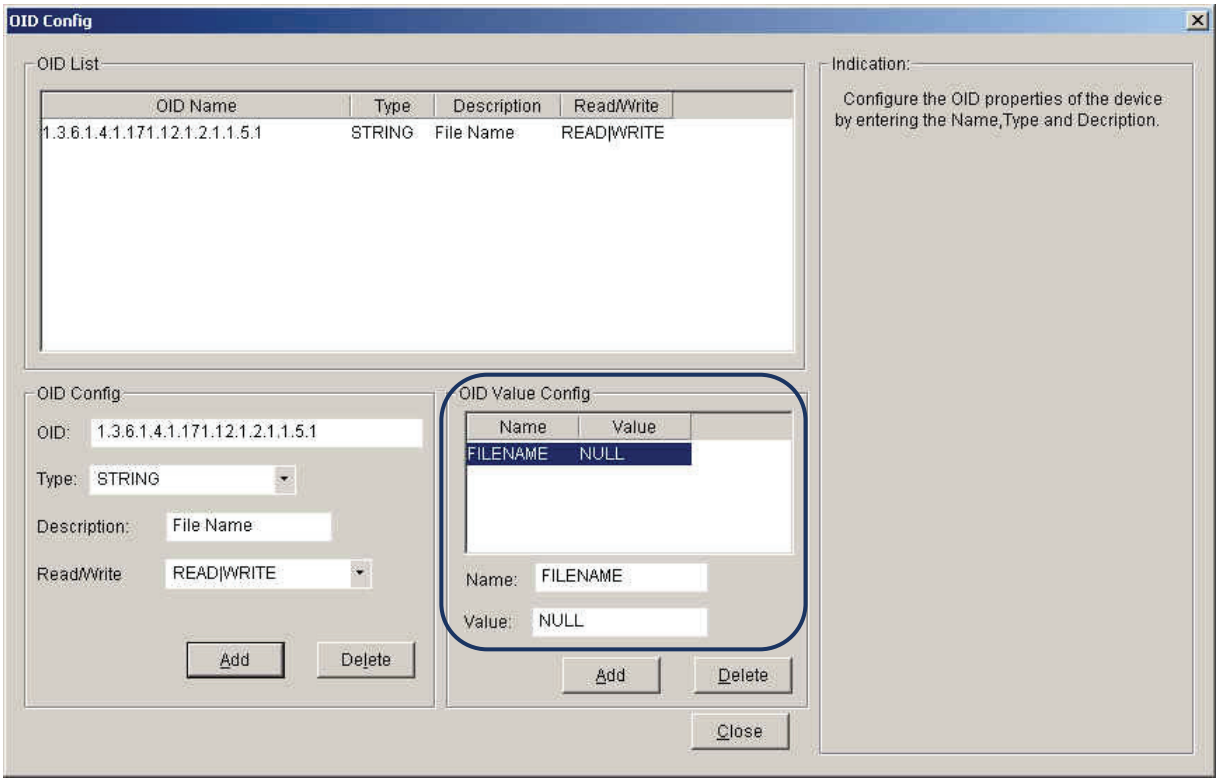


Figure 90: OID Value Configuration

8. Add **Server IP** to the OID list.
   - Follow the on-screen icons.
   - There is no "value" description in MIB file, please enter 1.

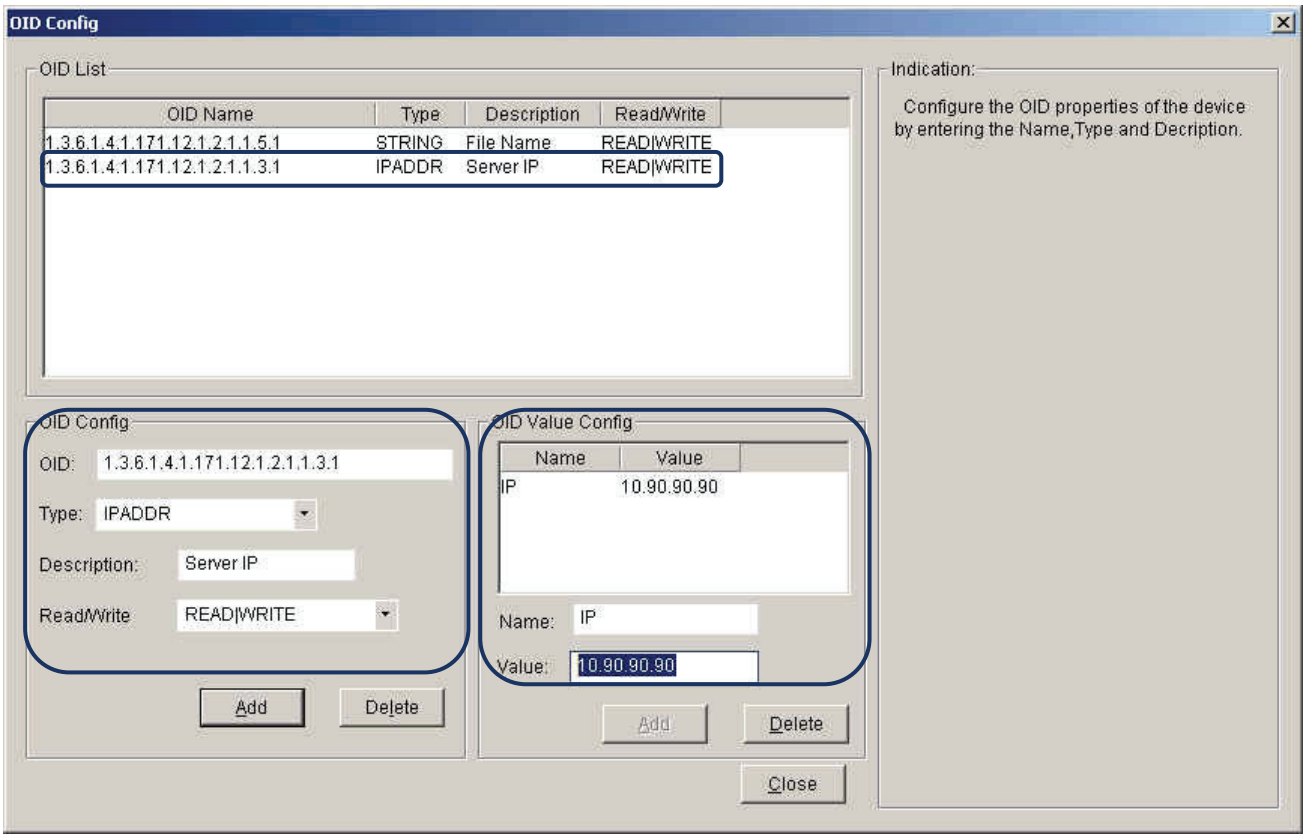


Figure 91: Server IP Parameter Configuration

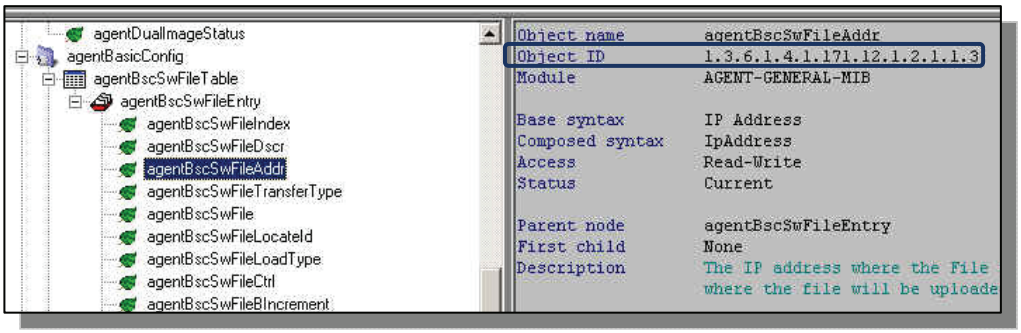


Figure 92: OID Information Query in MIB Compiler

9. Add **Operation Type** to the OID list.
   - Repeat the previous procedure.
   - Enter the values: 2 for backup and 3 for update.

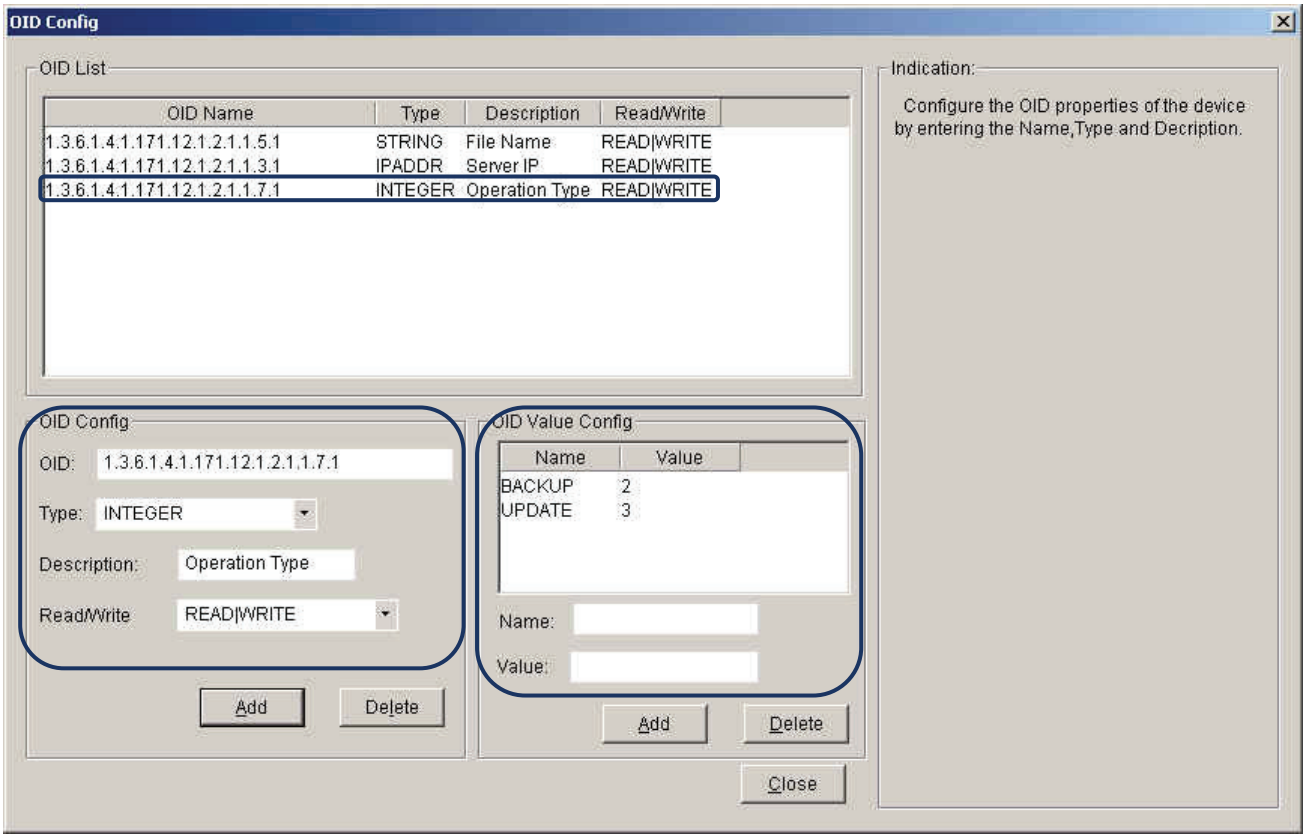


Figure 93: Operation Type Parameter Configuration

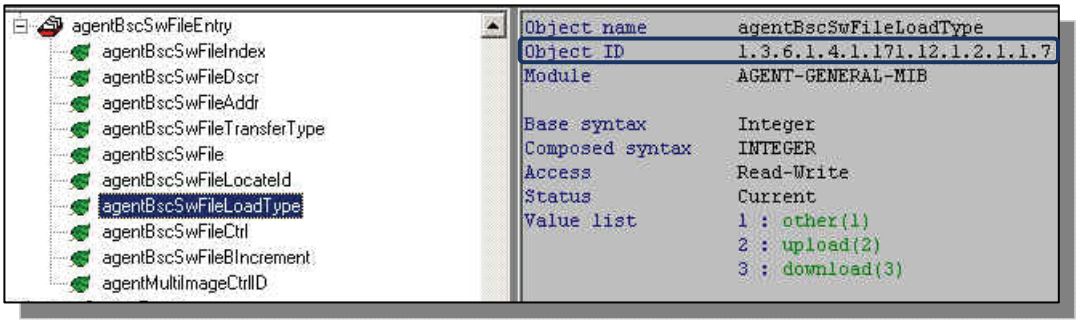


Figure 94: OID Information Query in MIB Compiler

10. Add **Procedure** to the OID list.

- Repeat the previous procedure.
- Enter the values: 2 for inactive and 3 for active.

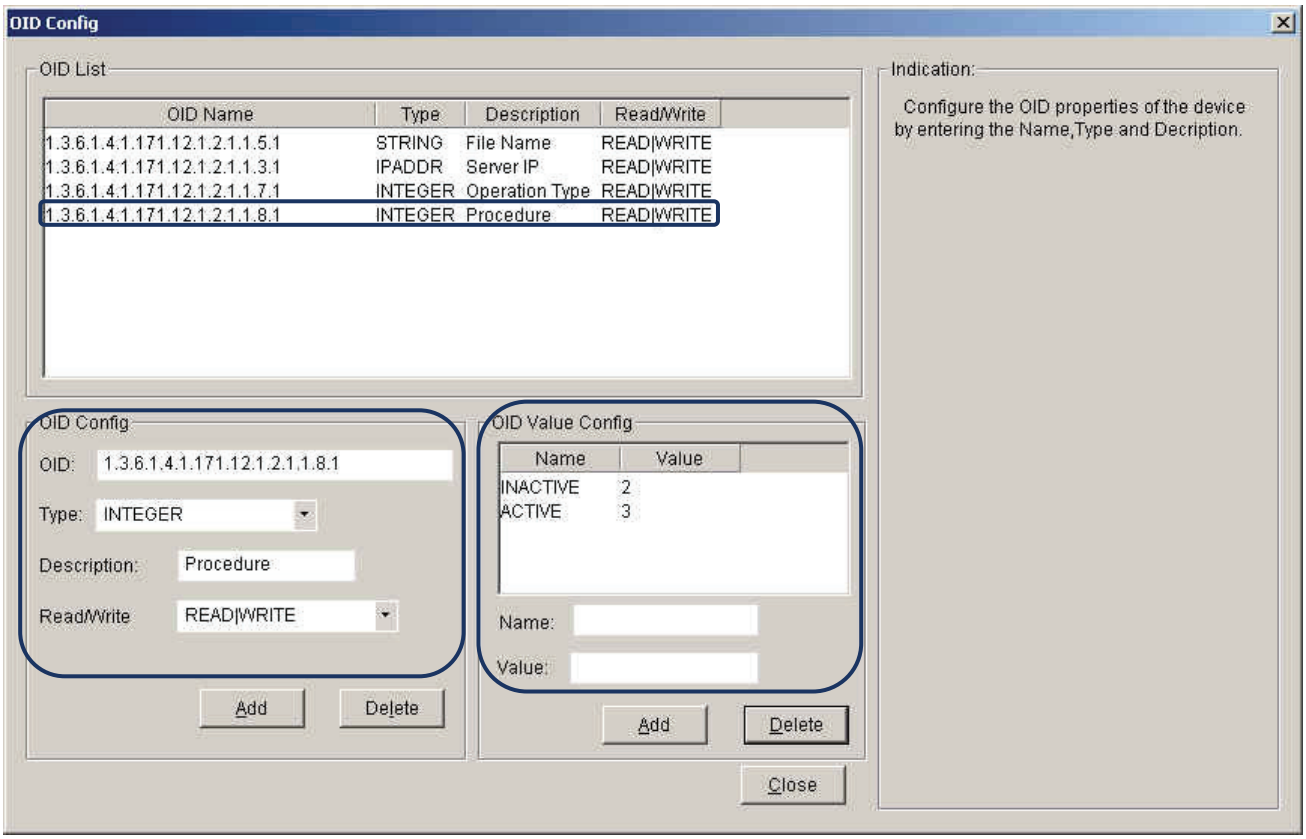


Figure 95: Procedure Parameter Configuration

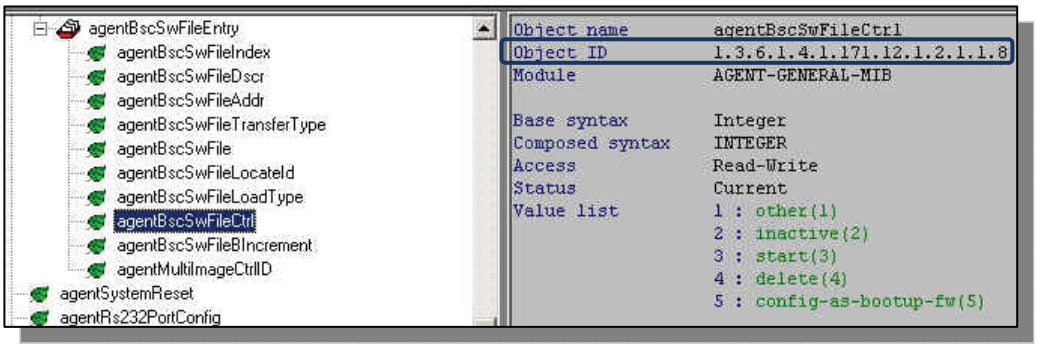


Figure 96: OID Information Query in MIB Compiler

11. Add **Image** to the OID list.
    - Repeat the previous procedure.
    - Enter the values: 1 for Image1 and 2 for Image2.

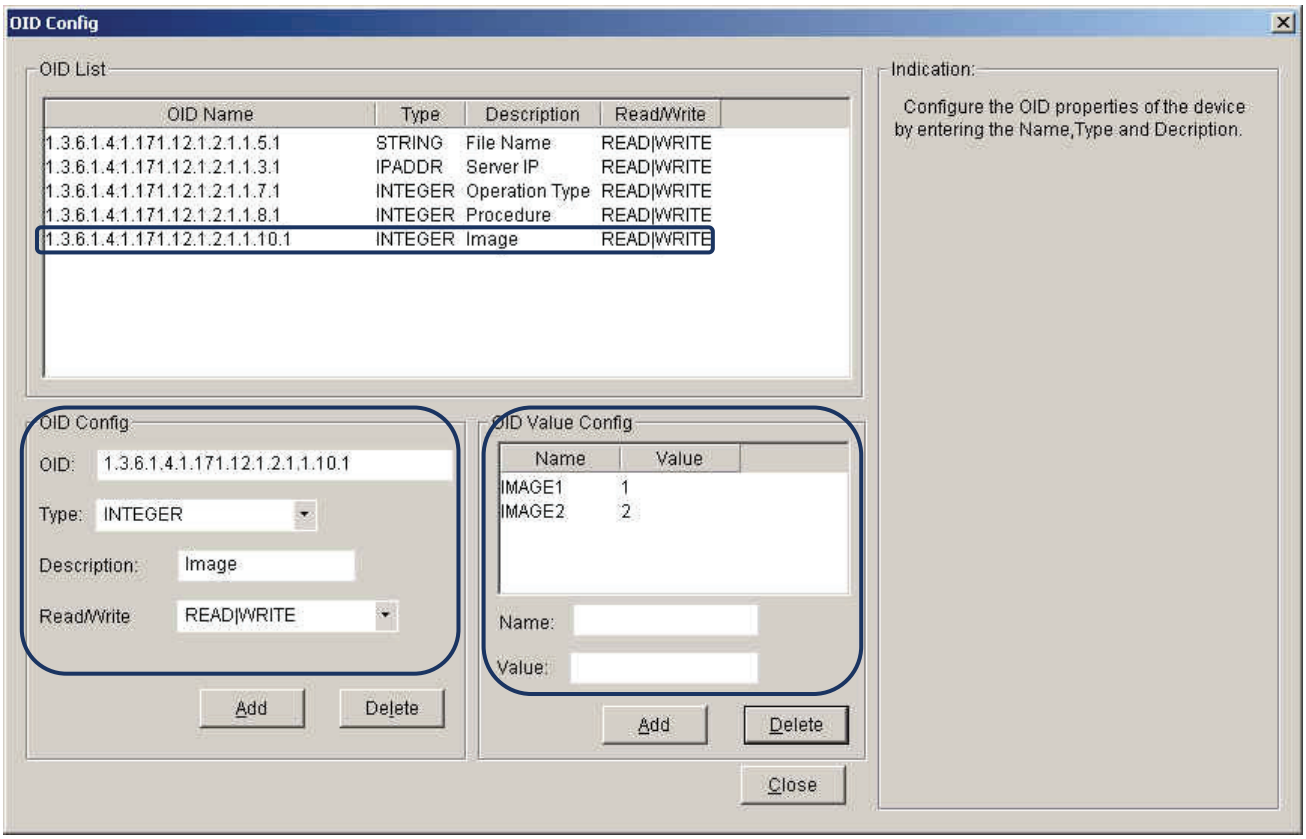


Figure 97: Image Parameter Configuration

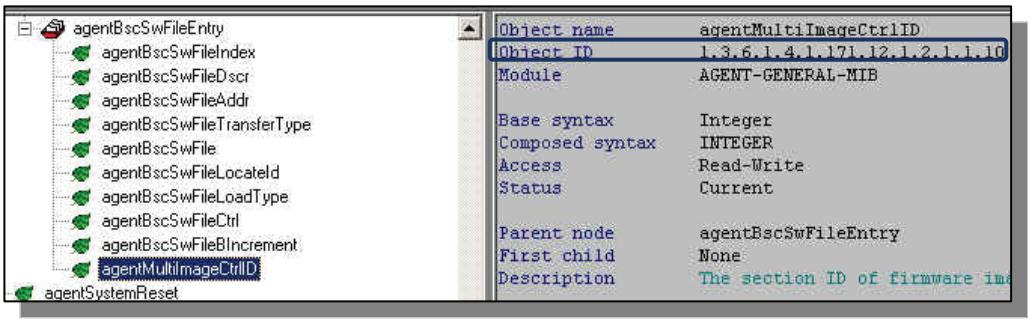


Figure 98: OID Information Query in MIB Compiler

12. Launch the **Run Batch** function. *Go to **Application > Batch Config > Run Batch.***
Be sure to enter the parameters correctly to avoid error messages.

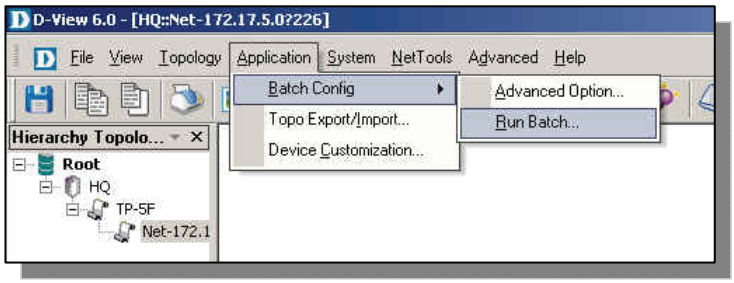


Figure 99: Run Batch function

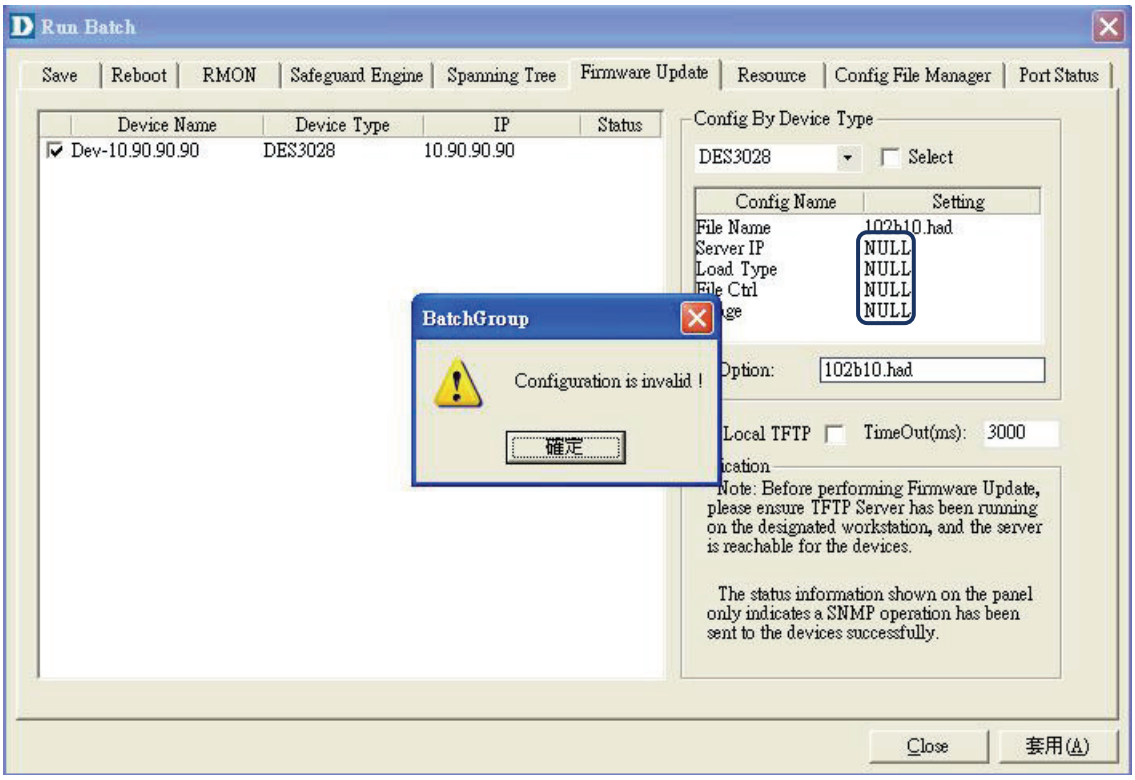


Figure 100: Error message during first process initiation

- DES-3028 is now in the list.
- The parameters you configured are in the list now. Select the appropriate information to proceed with the firmware procedure.
- Select **Run Local TFTP** to implement the firmware procedure.

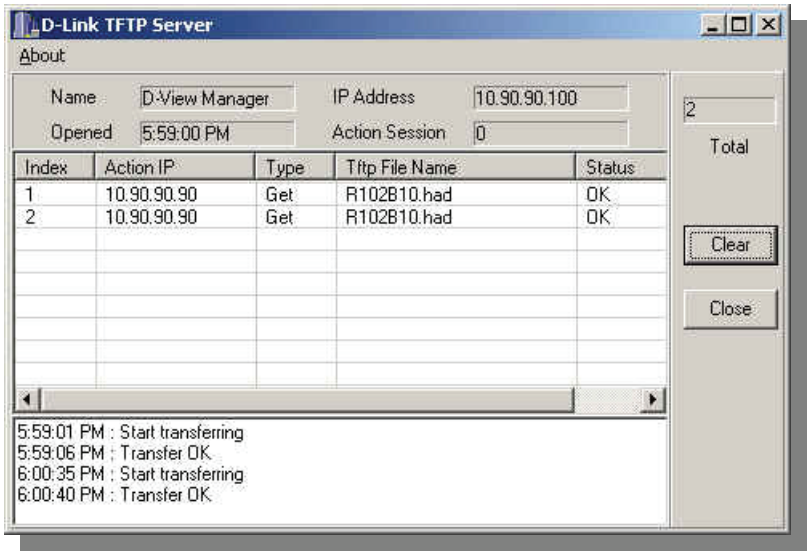


Figure 101: TFTP Server

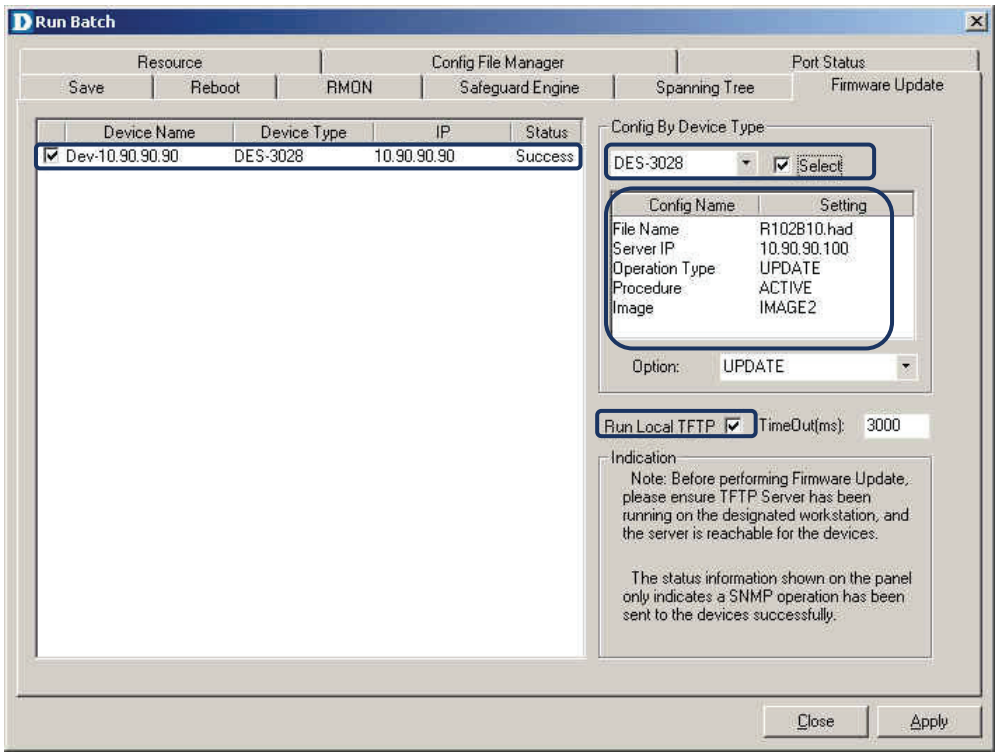


Figure 102: Configured Parameters in Run Batch screen

In order to Batch Config the reboot function for the DES-3028 follow the steps below:

- As seen in the screen below, DES-3028 is greyed-out which means that the reboot function does not support DES-3028 model.

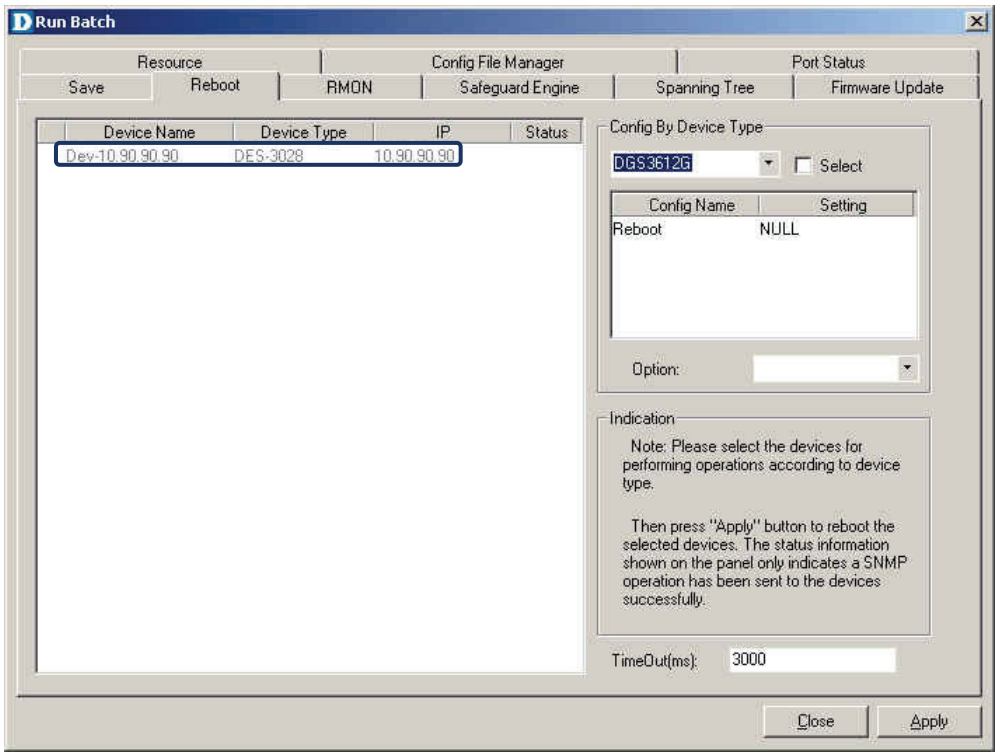


Figure 103: DES-3028 not in supported list

1. Open **Advanced Option** and select **Reboot.**
   - Please refer to previous session on how to launch the Advanced Option.
2. Select DES-3028 and add it to the Configured Device Types list.

- Click **Property** to edit OID.

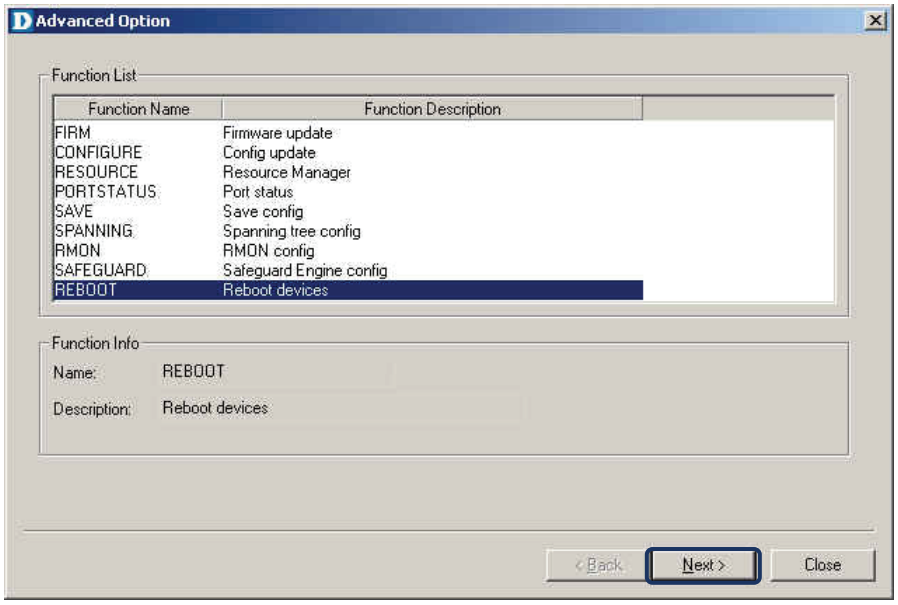


Figure 104: Reboot function

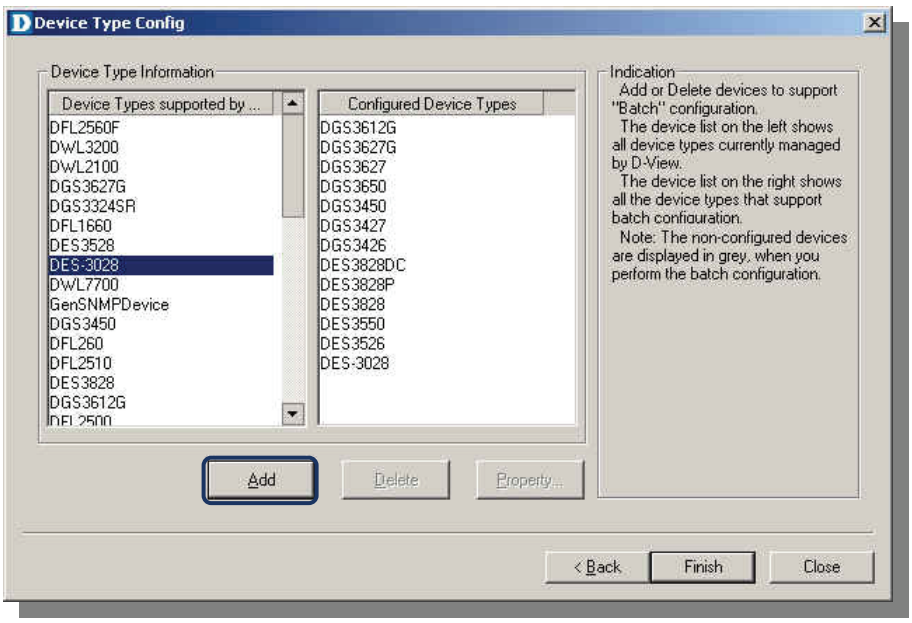


Figure 105: Adding of DES-3028 to list

3. Update the fields in the OID Config as seen in the screen below.
   - DES-3028 can now be seen in the list.
   - Click **Apply** to reboot the switch.

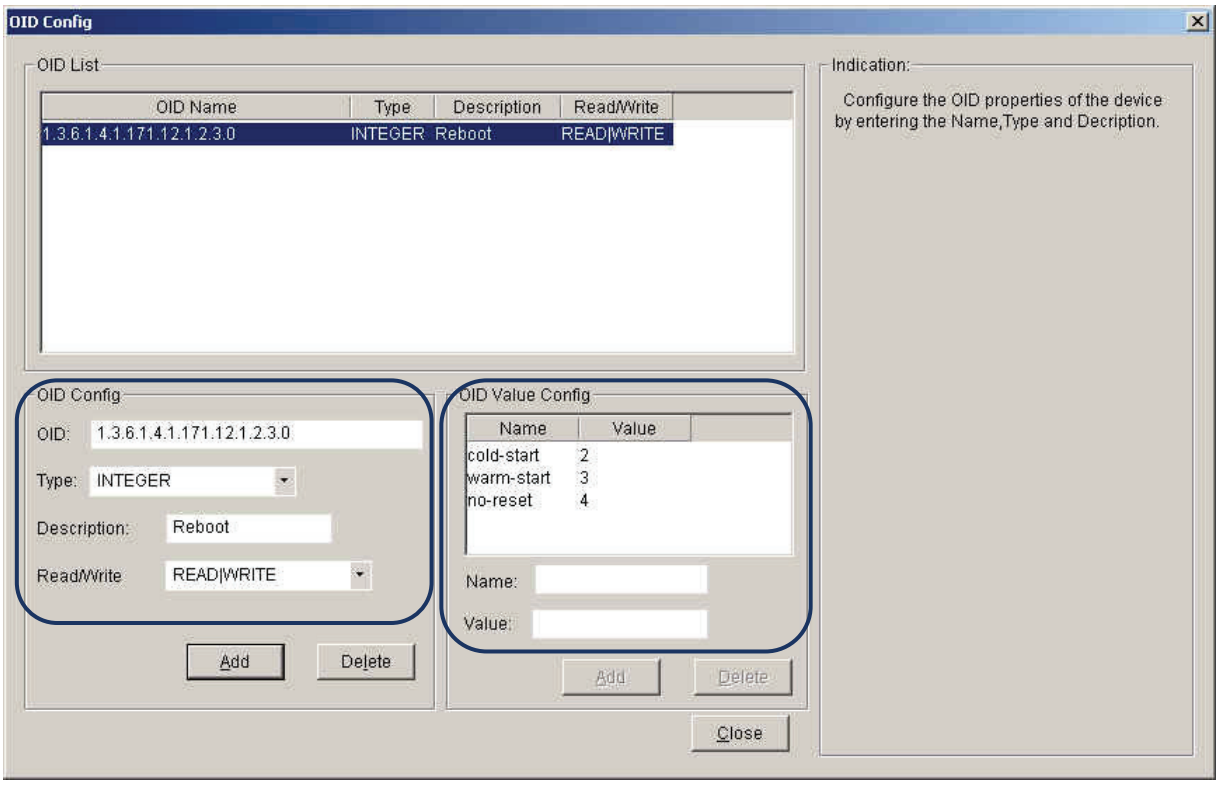


Figure 106: Reboot Parameter Configuration

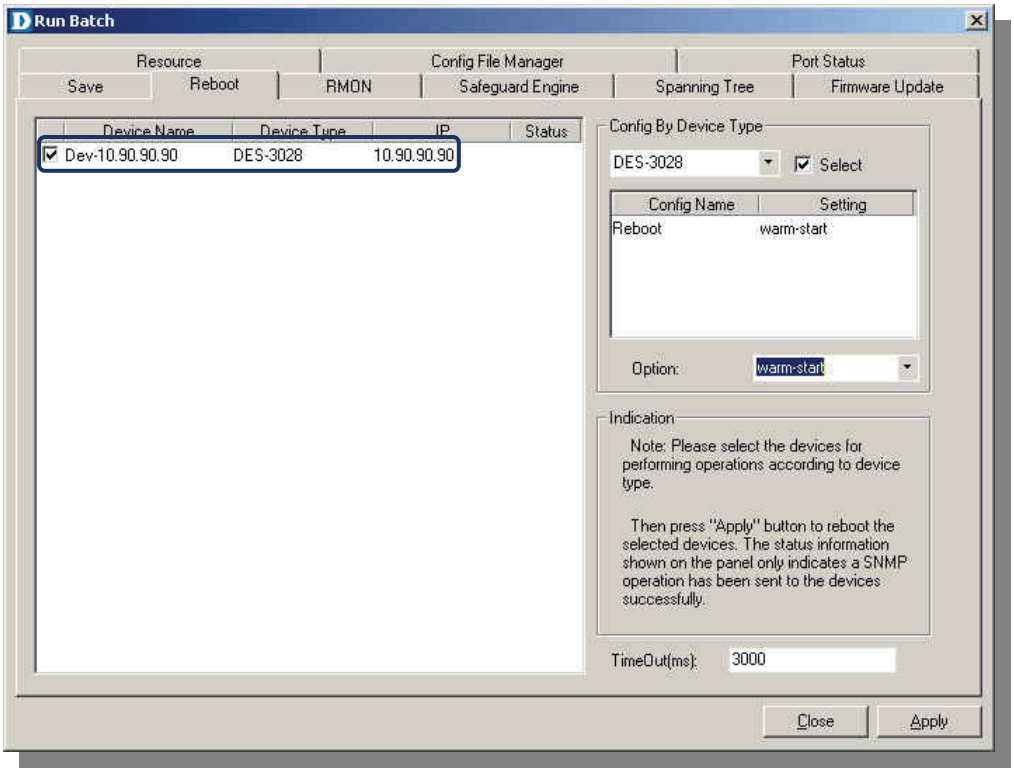


Figure 107: Reboot Function execute

THIRD PARTY DEVICES: CISCO CATALYST 2960

For Cisco's Catalyst 2960 follow the steps below:

1. Double-click the icon to launch GenSNMP D-View module. Confirm the Catalyst 2960's system OID information, go to ***DeviceInfo > System Info.***

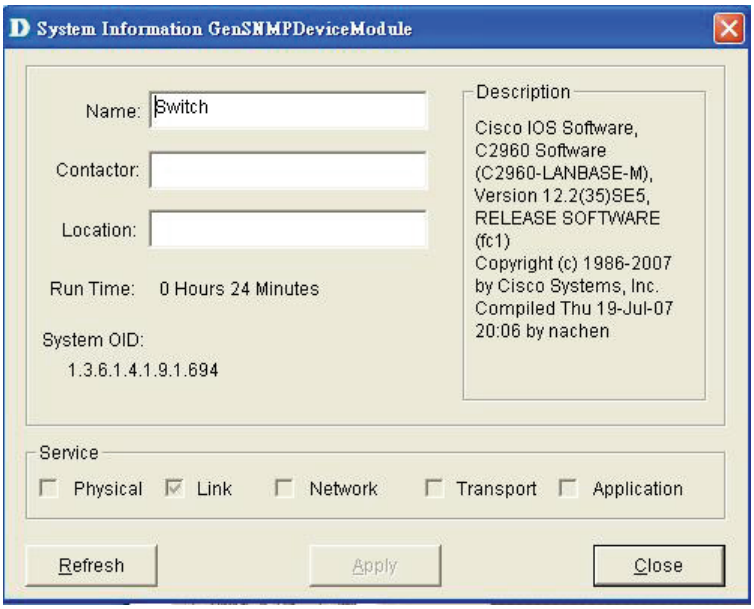


Figure 108: System OID Query

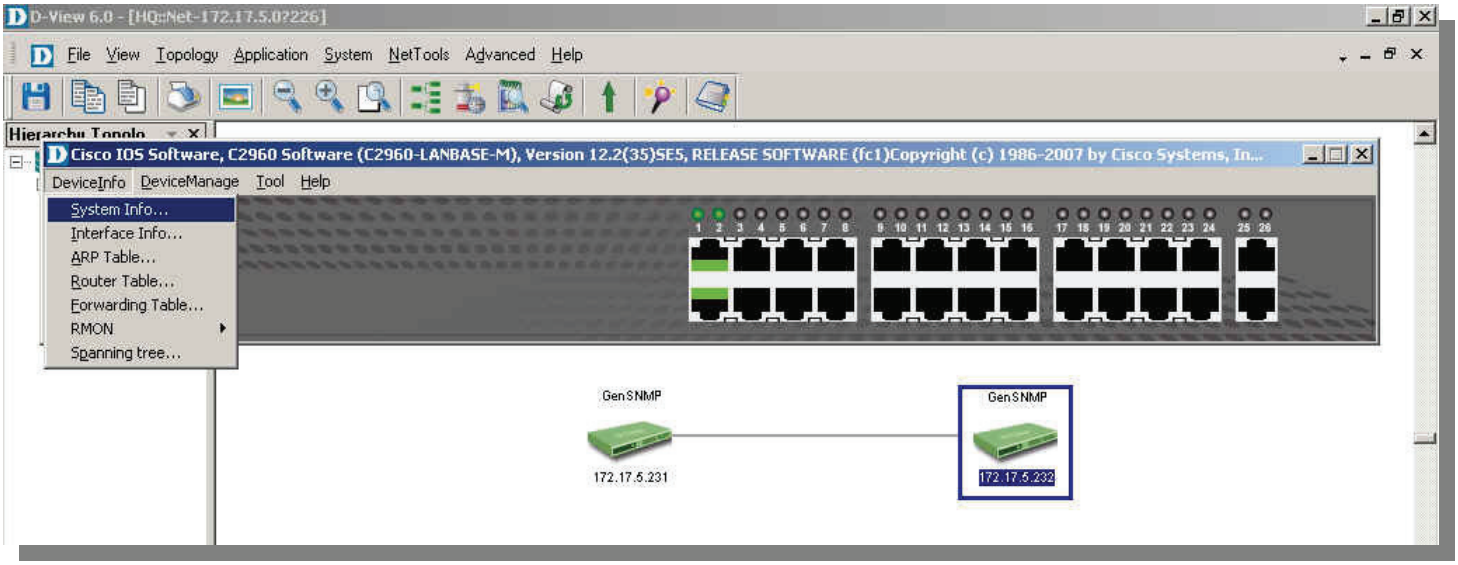


Figure 109: GenSNMP D-View module

2. Open **Device Customization** to configure the Catalyst 2960.
   - Update the necessary fields.
   - The updated content will be displayed in the topology map.

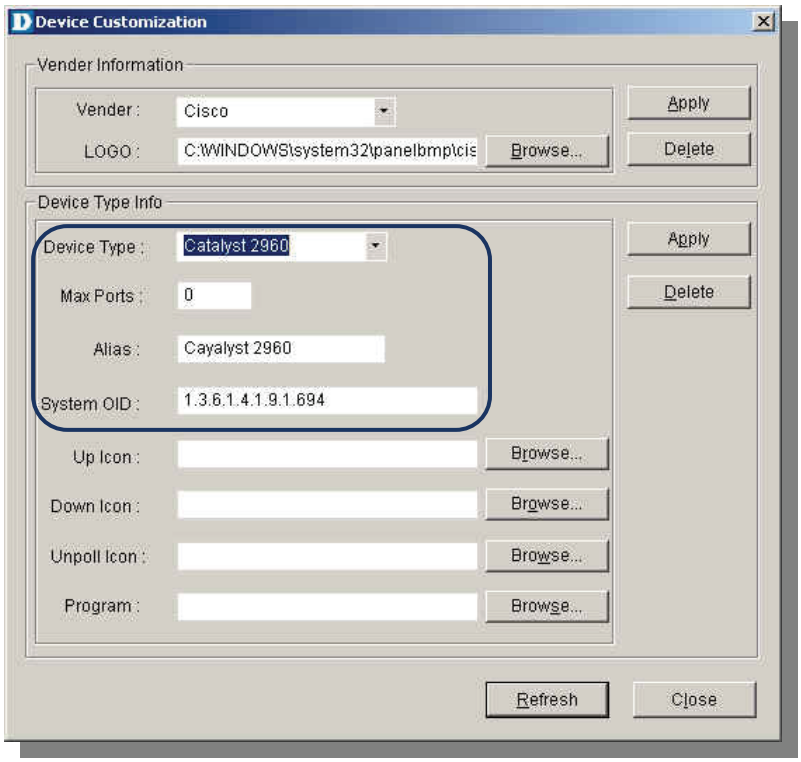


Figure 110: Parameter Configuration

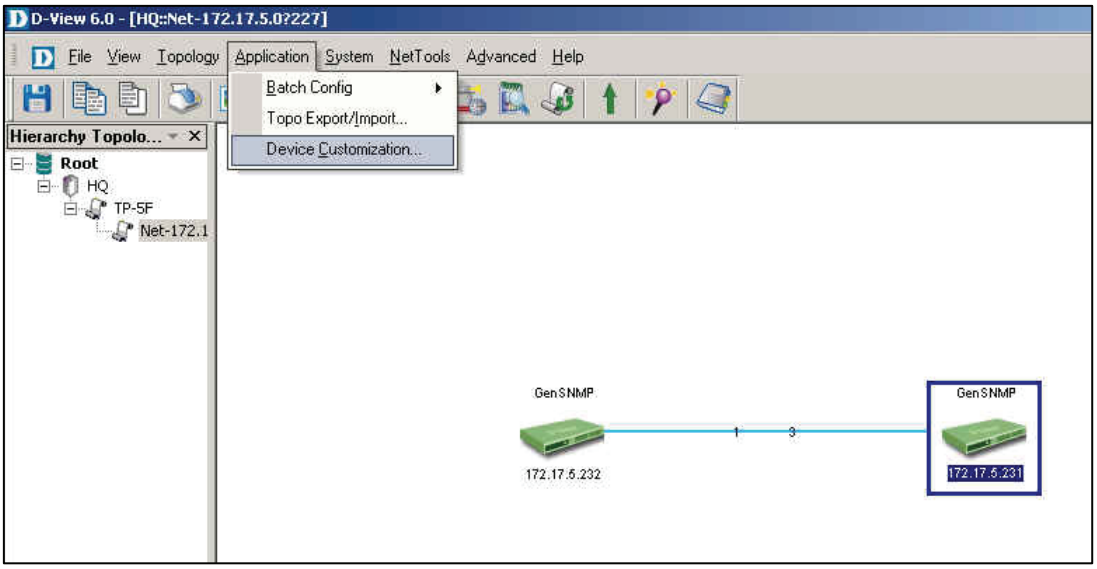


Figure 111: Device Customization

To perform the Device Type Check:

1. Open **Device Type Check...** to update the database, go to ***Advanced > Device Type Check.***

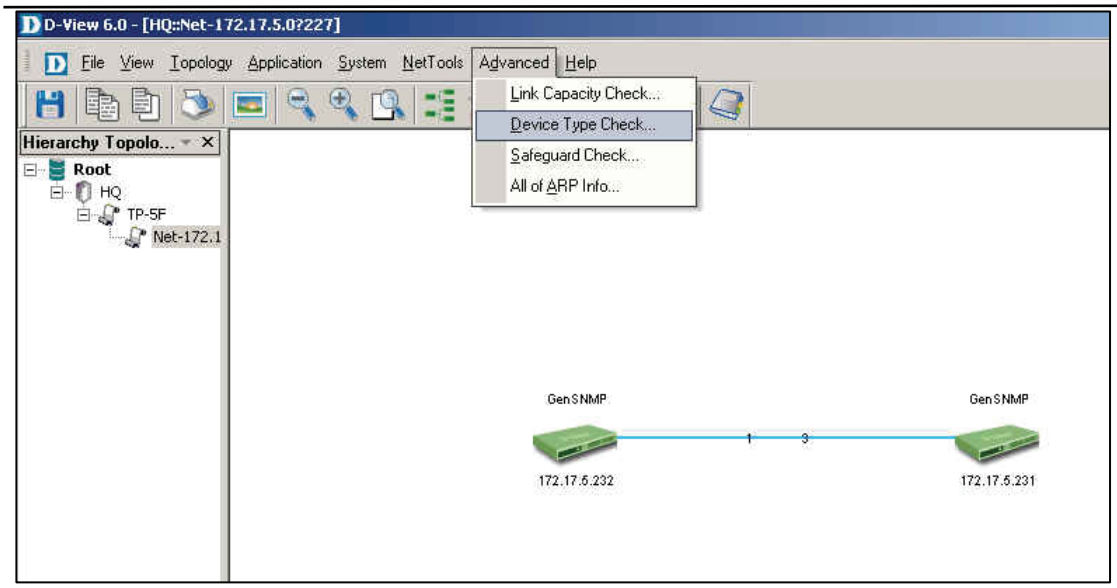


Figure 112: Device Type Check

2. Click **Check** and then press **Update** to update the database.
   - Save the changes.

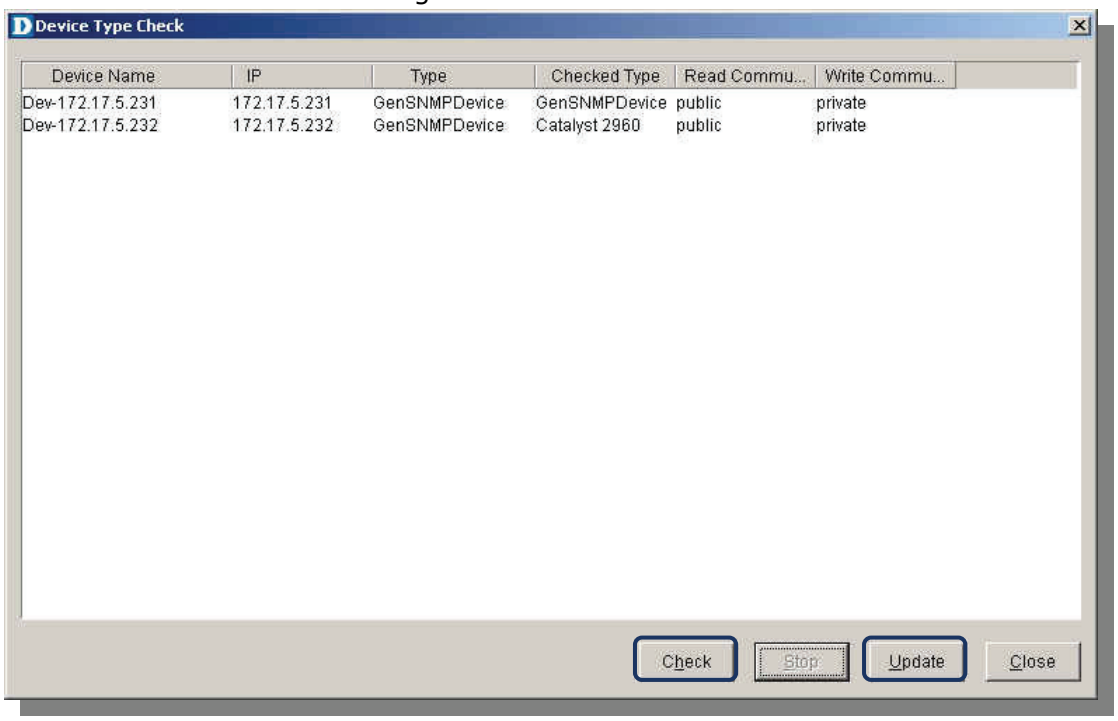


Figure 113: Device Type Check screen

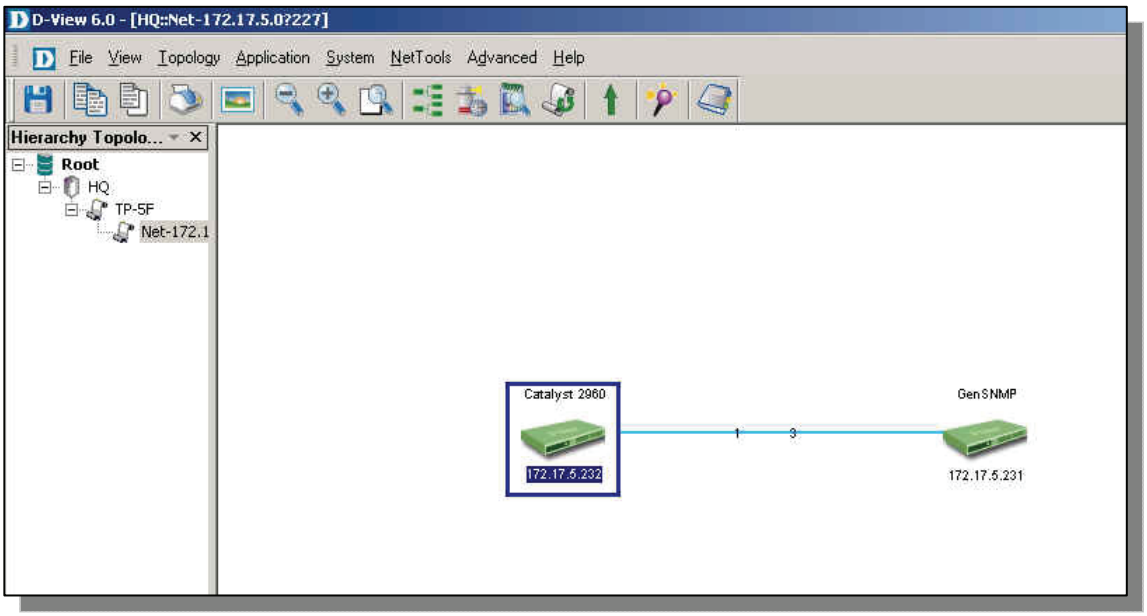


Figure 114: Saving changes

To set up Batch Config to support Catalyst 2960:

1. Open **Advanced Option...** to configure 2960.
    - If the device type is not activated it means the device is not supported by D-View.

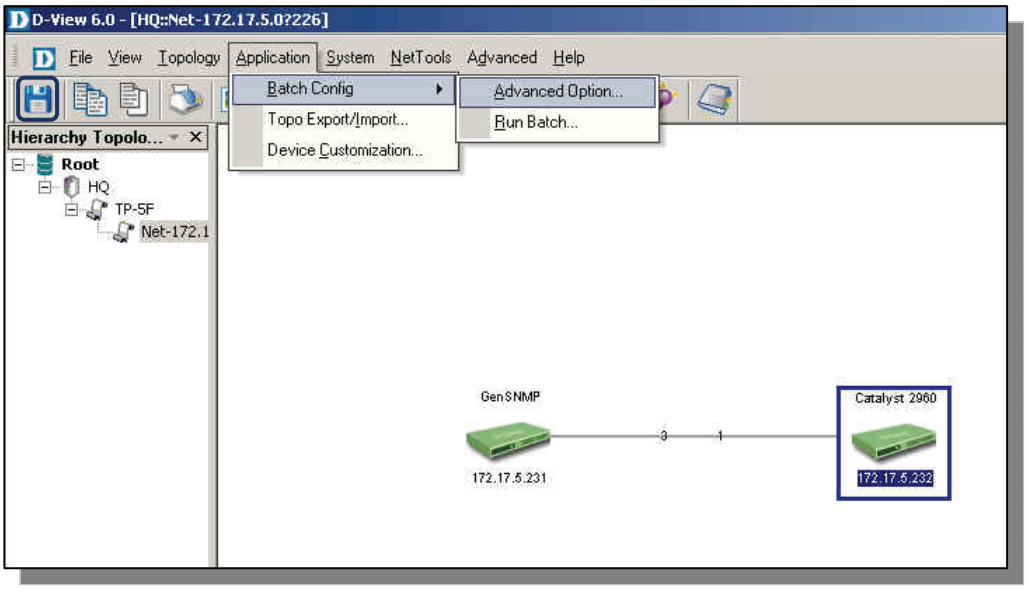


Figure 115: Advanced Option Function

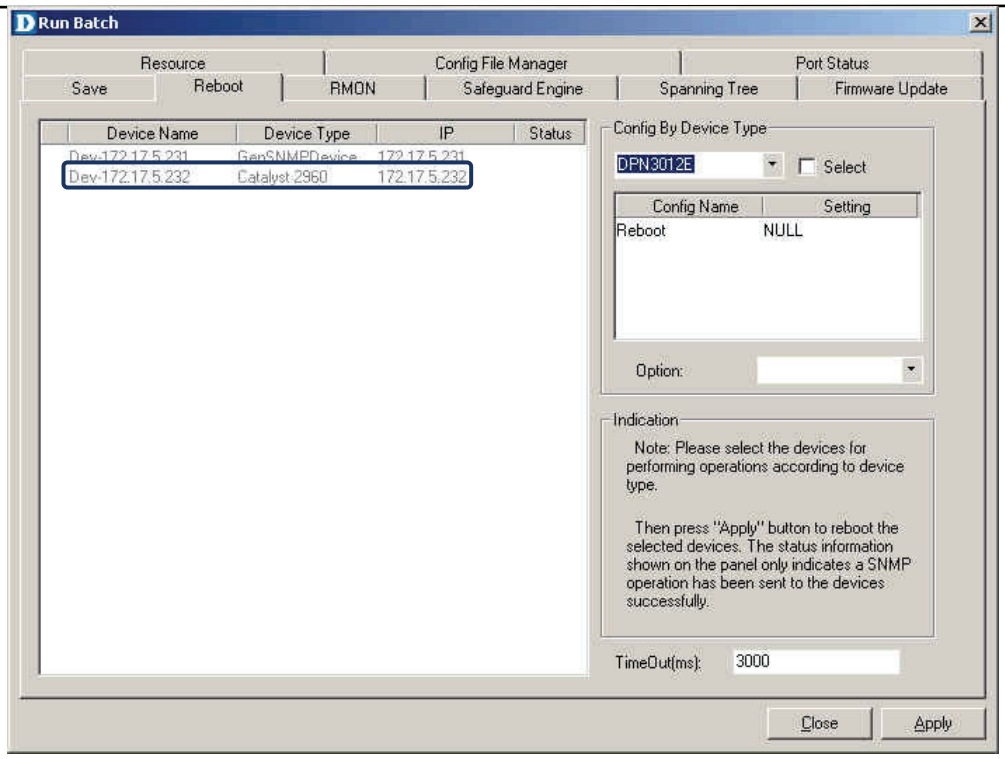


Figure 116: Cisco 2960 not in the supported list

2. Select **Firmware** and then click **Next**.
3. Add Catalyst 2960 into the list and click **Property** to configure the OID information.

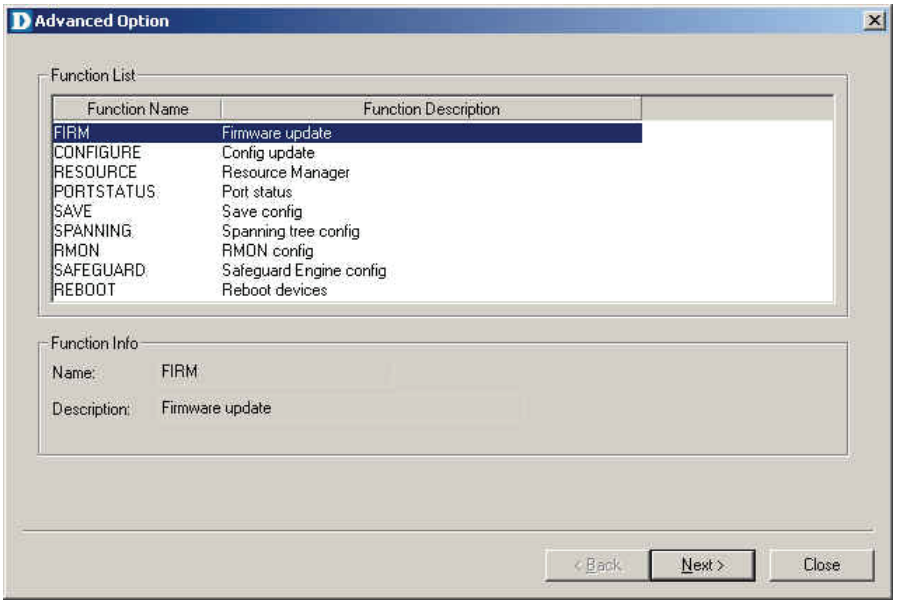


Figure 117: Firmare Update Function

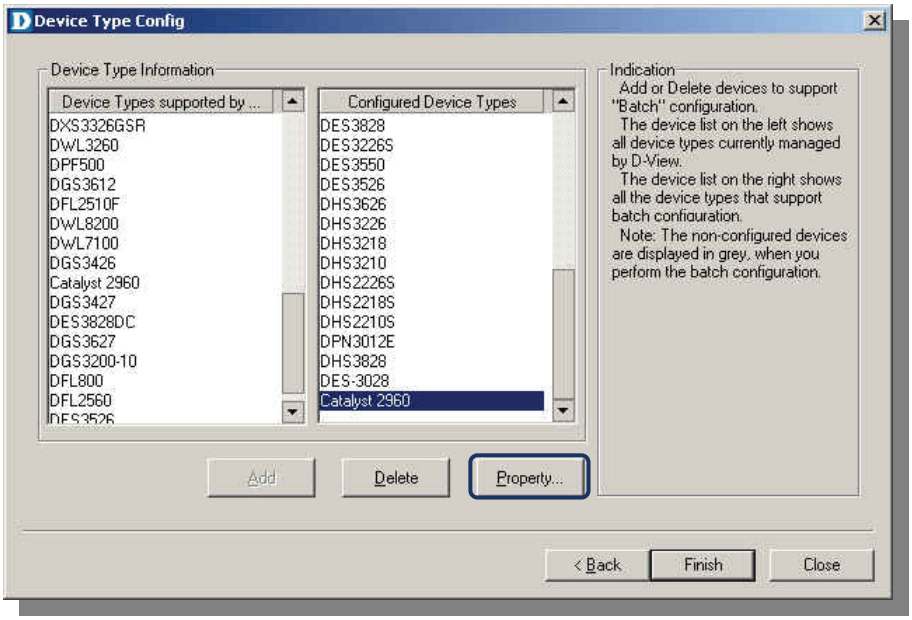


Figure 118: Adding Cisco 2960 to list

4. Update the related OID information as follows:
   - Configure the Protocol Type.
   - Configure the Source File Type.

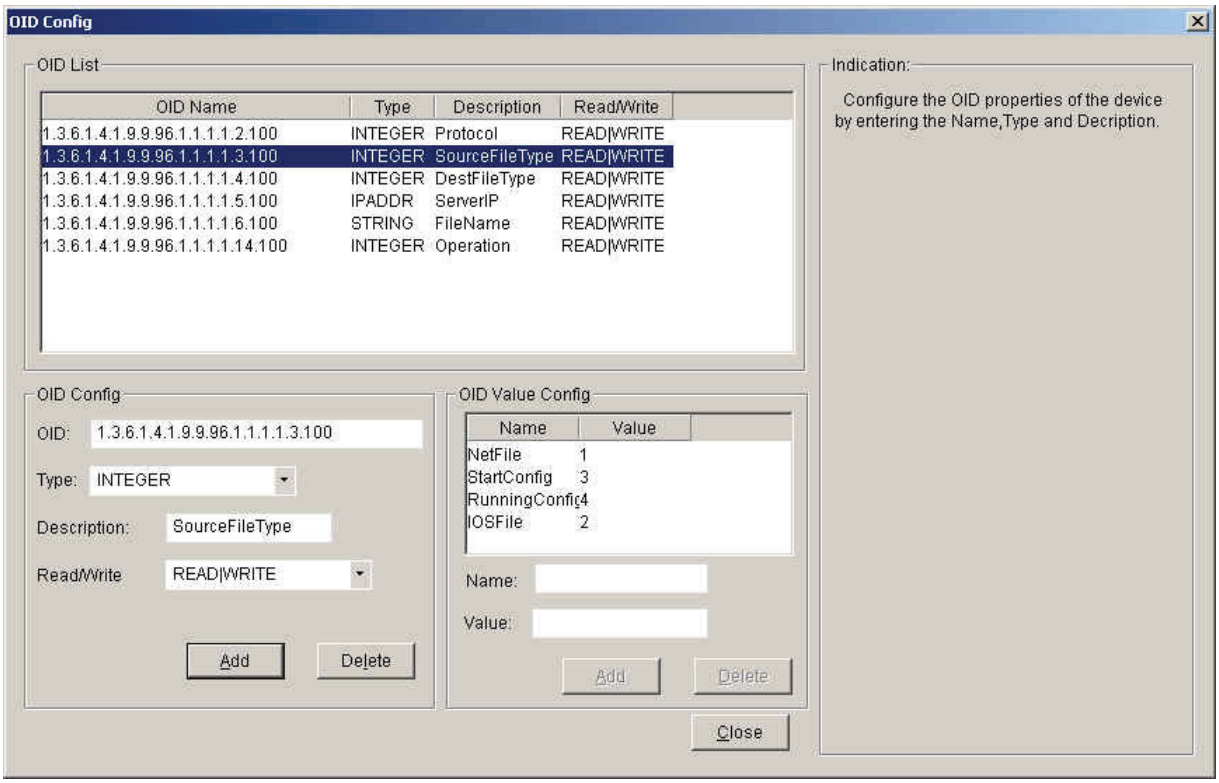


Figure 119: Parameter Configuration

   - Configure the Destination File Type.
   - Configure the TFTP server IP address.

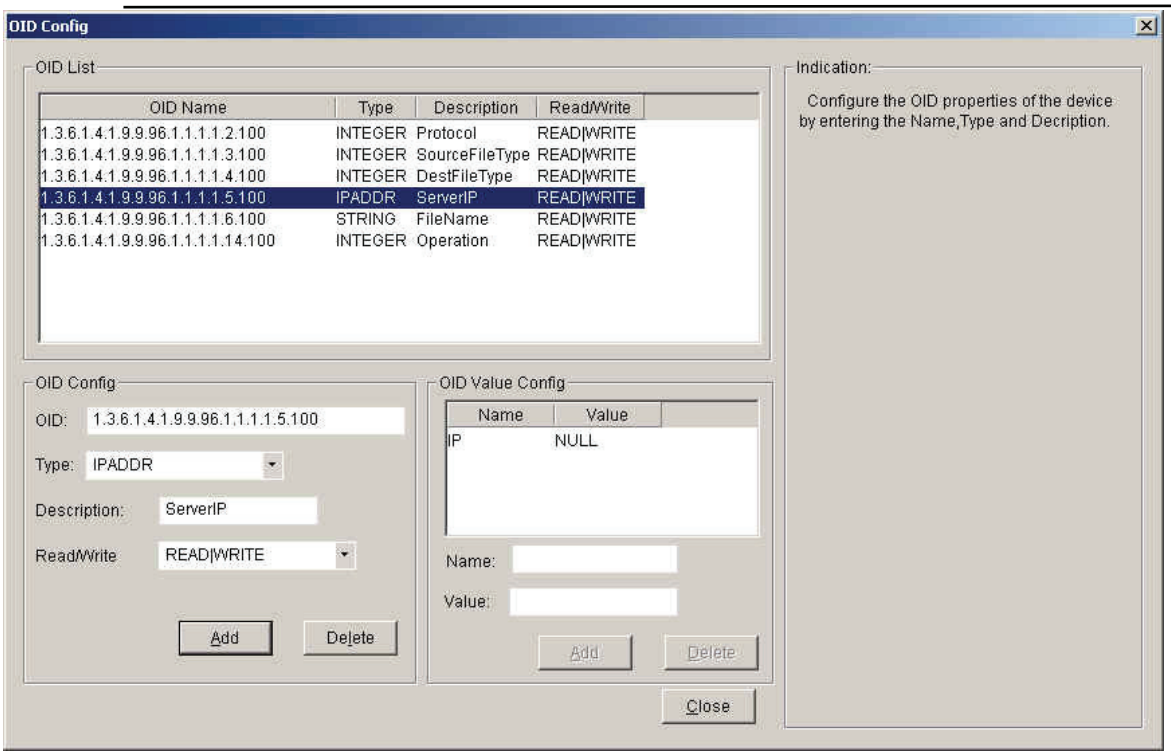


Figure 120: Parameter Configuration

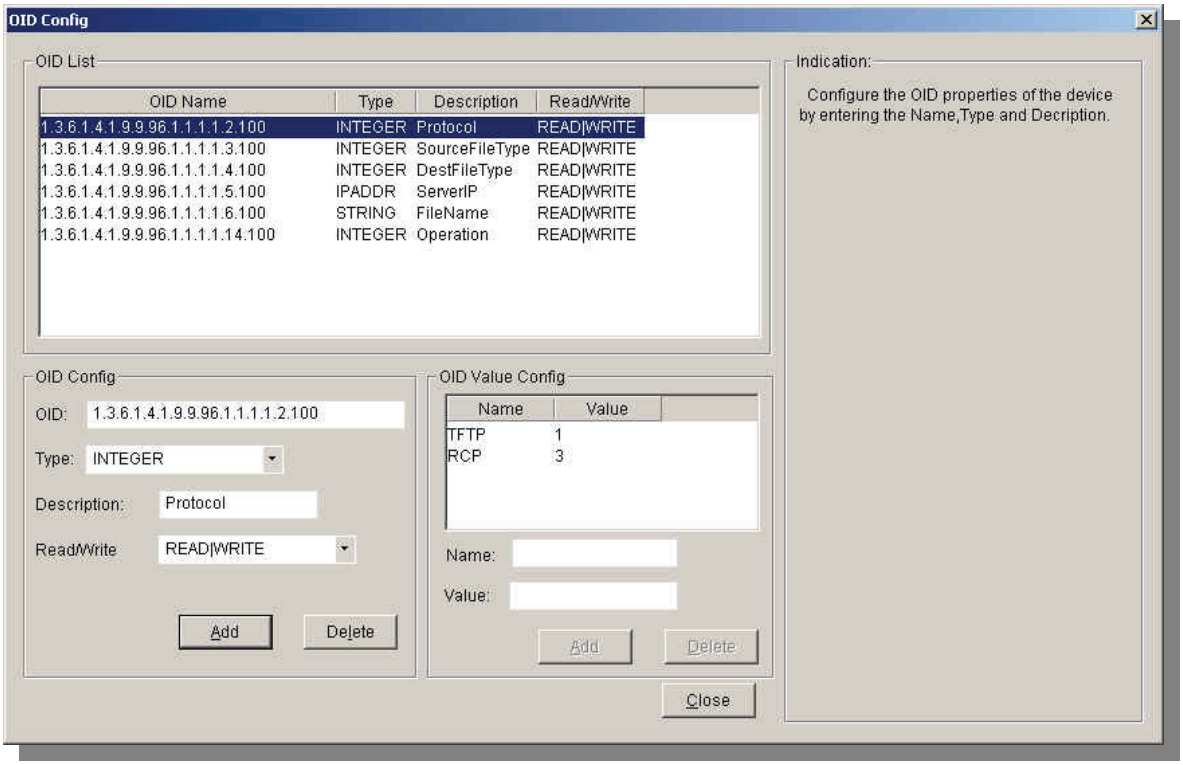


Figure 121: Parameter Configuration

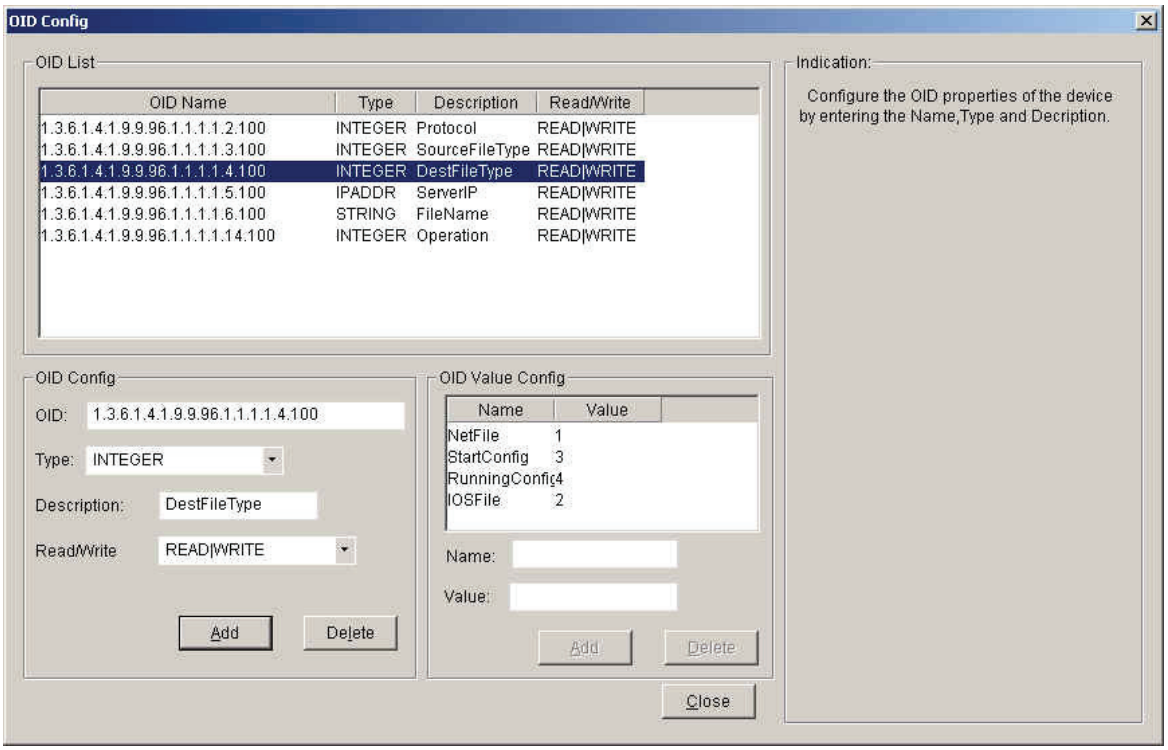


Figure 122: Parameter Configuration

- Configure the File Name.
- Configure the Operation, Create or Delete.

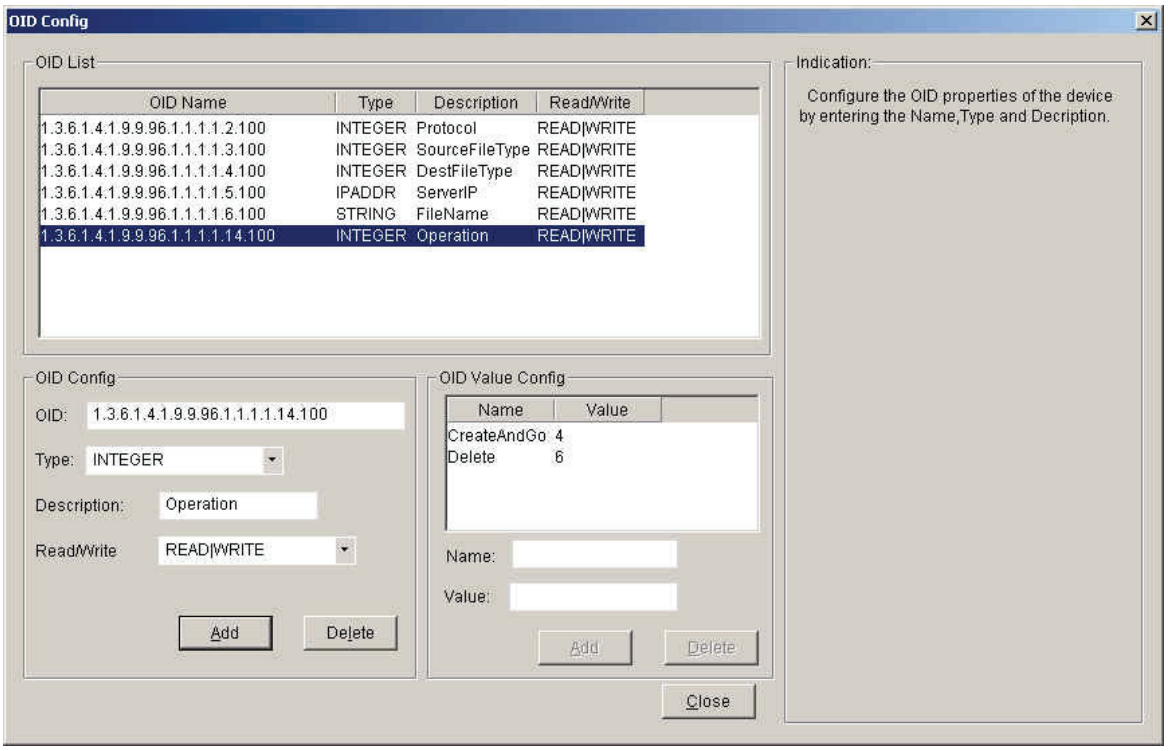


Figure 123: Parameter Configuration

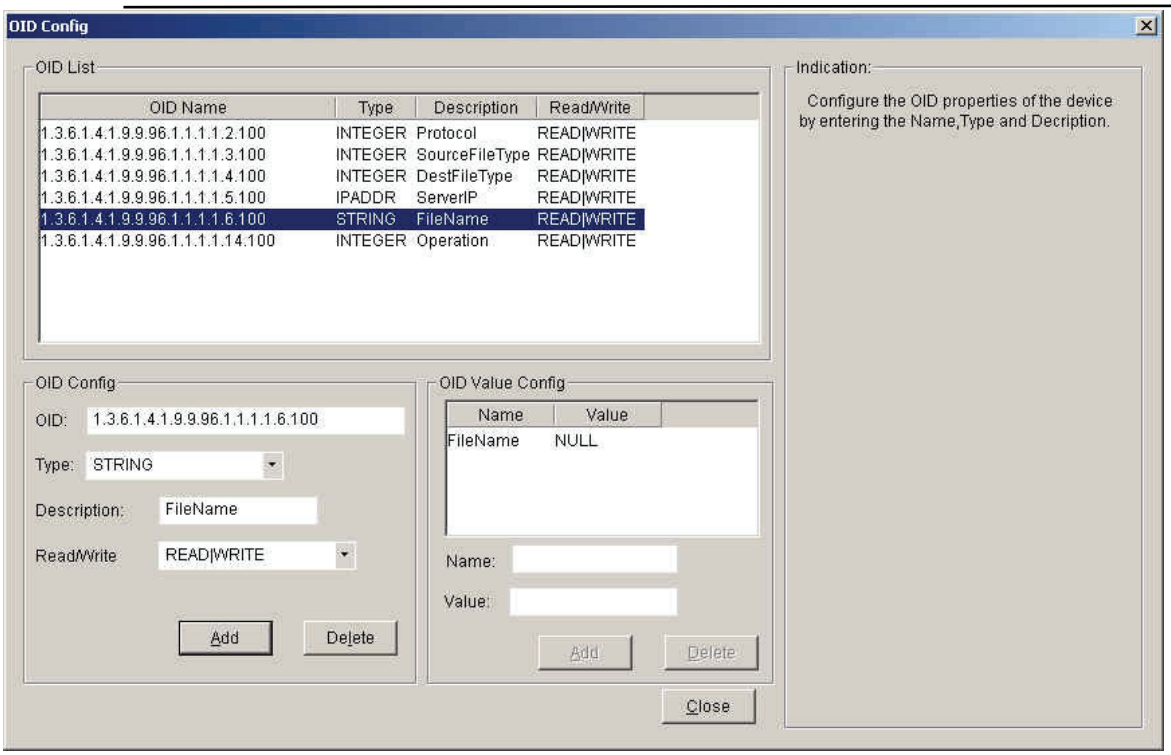


Figure 124: Parameter Configuration

To back up Catalyst 2960's configuration file:

Because of the difference in the MIB design between D-Link and Cisco, you have to implement the backup via Firmware Update function. There are a few limitations in the current design, such as:

- There are no problems with one to one relationship (backup one config to a tftp server).
- One to many is the appropriate way to run this function (one config file to many switches). Use the config file for multiple switches, the IP address for each device needs to be modified.
- Many to one relationship is not recommended (many switches to a tftp server). The configuration file will be overwritten on that single config file.

The terminology definition:

- NetFile: refers to TFTP, please select this option if the destination is TFTP server.
- Operation: please select **Create and Go** to process the task.
- According to Cisco's MIB document, the IOS update via SNMP is not supported.

Follow these steps to backup 2960's configuration file:

1. Open **Run Batch.**
2. Select the **Firmware Update** tab to back up the configuration.
3. Select the appropriate action and enter the information.

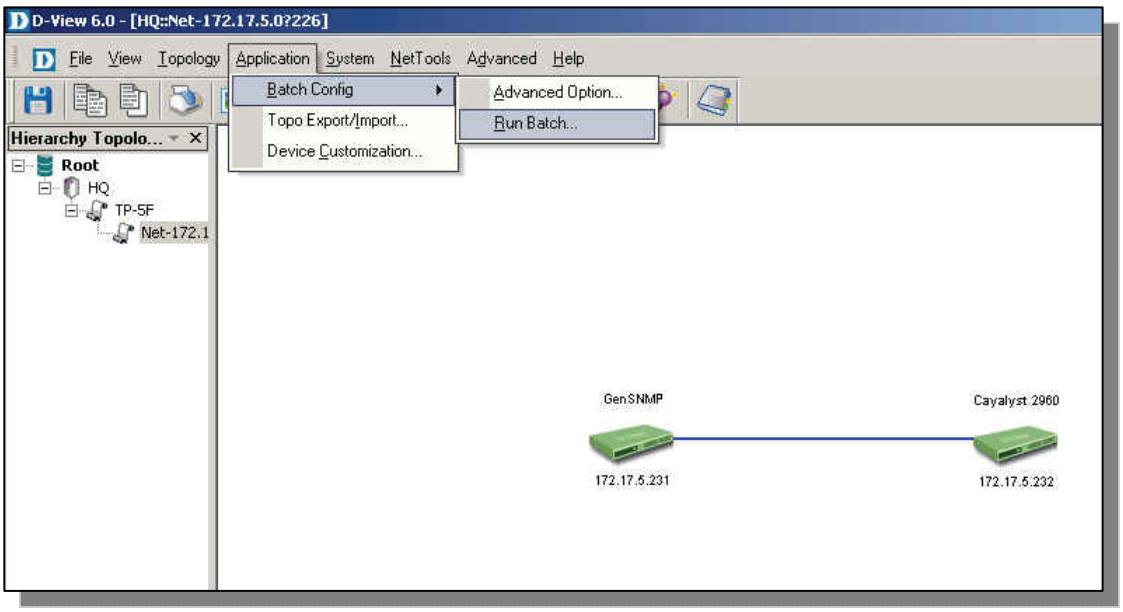


Figure 125: Run Batch function

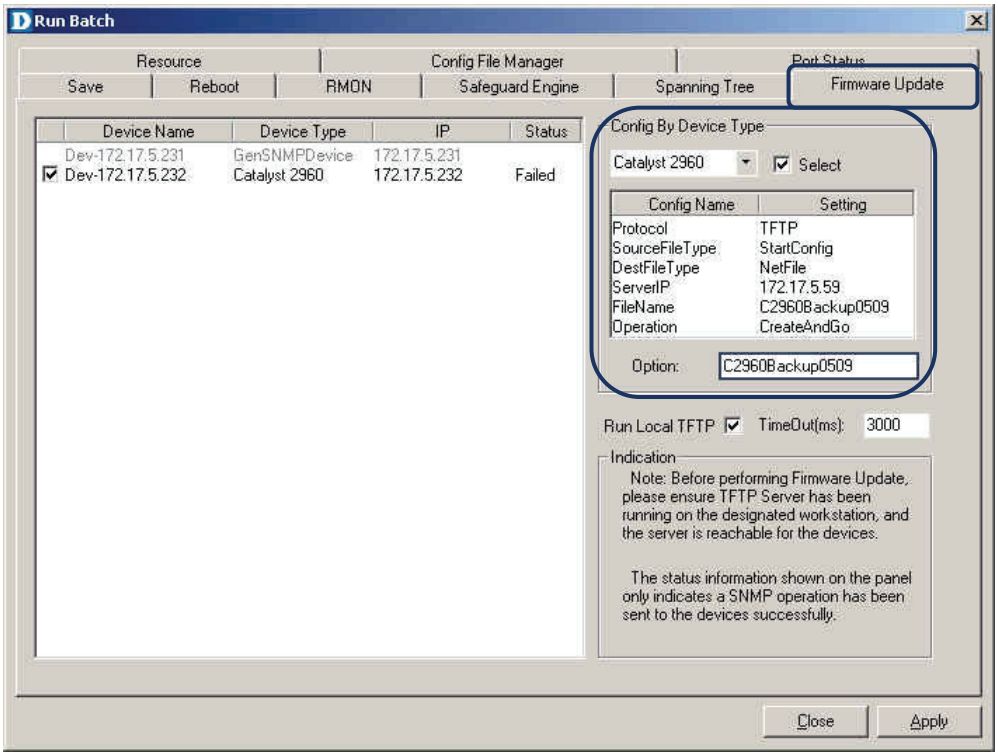


Figure 126: Firmware Update Selection screen

4. After all the parameters are set, click **Apply.**
   - The status is displayed in the TFTP's directory

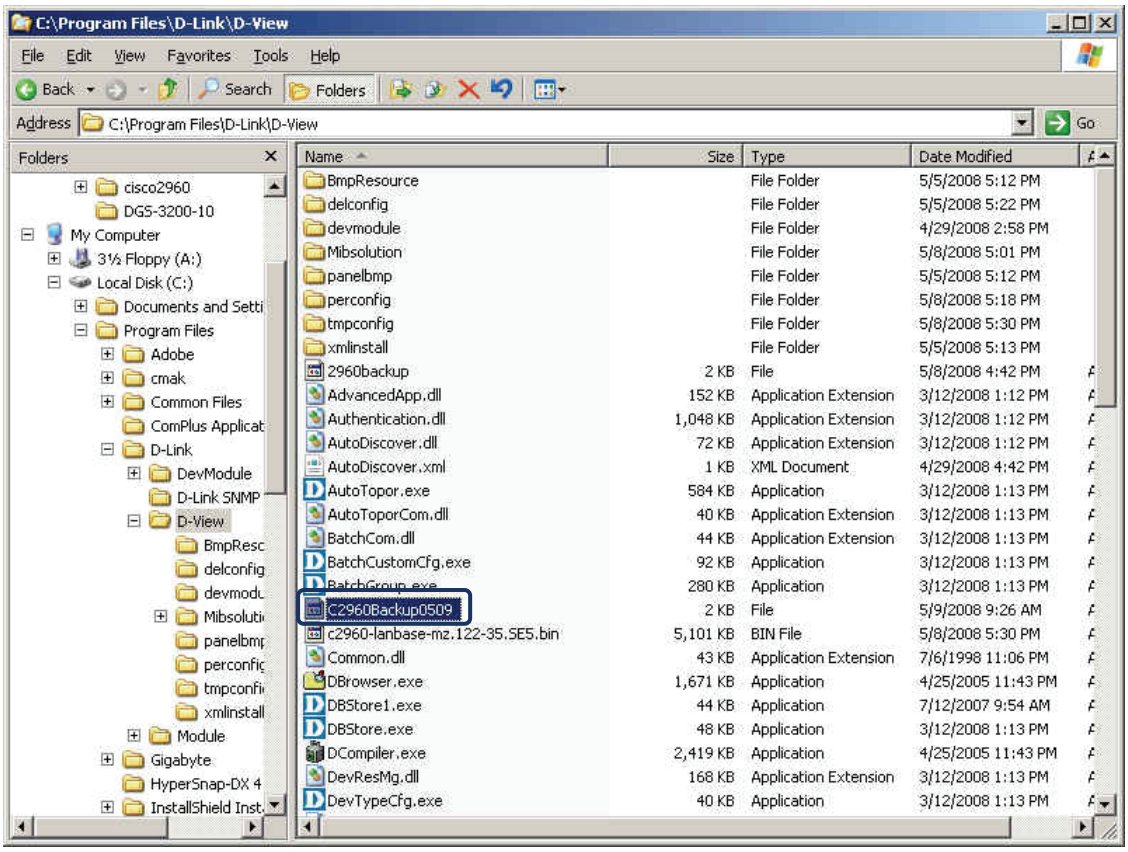


Figure 127: File Backup Configuration

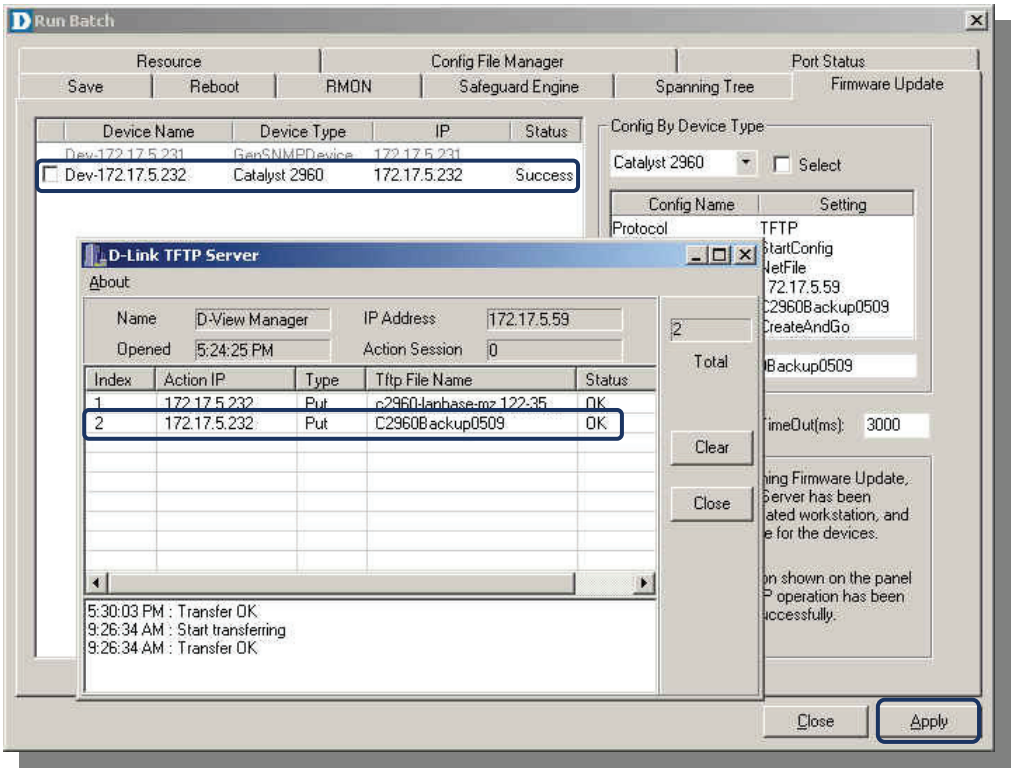


Figure 128: Apply to back up

To configure Batch Config to support the reboot function for Catalyst 2960:

1. Open **Advanced Option** and select **Reboot** to add 2960 into the list. Click **Next** to

continue. Go to ***Application > Batch Config > Advanced Option.***

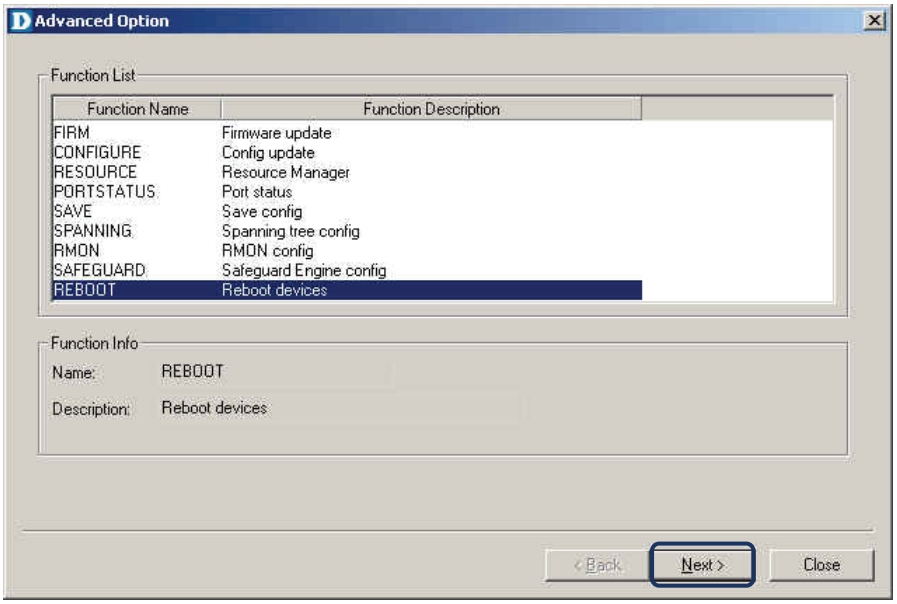


Figure 129: Reboot function selection

2. Add Catalyst 2960 to the list and click **Property** to configure the OID information
   - Follow the on-screen icons to add the 2960.

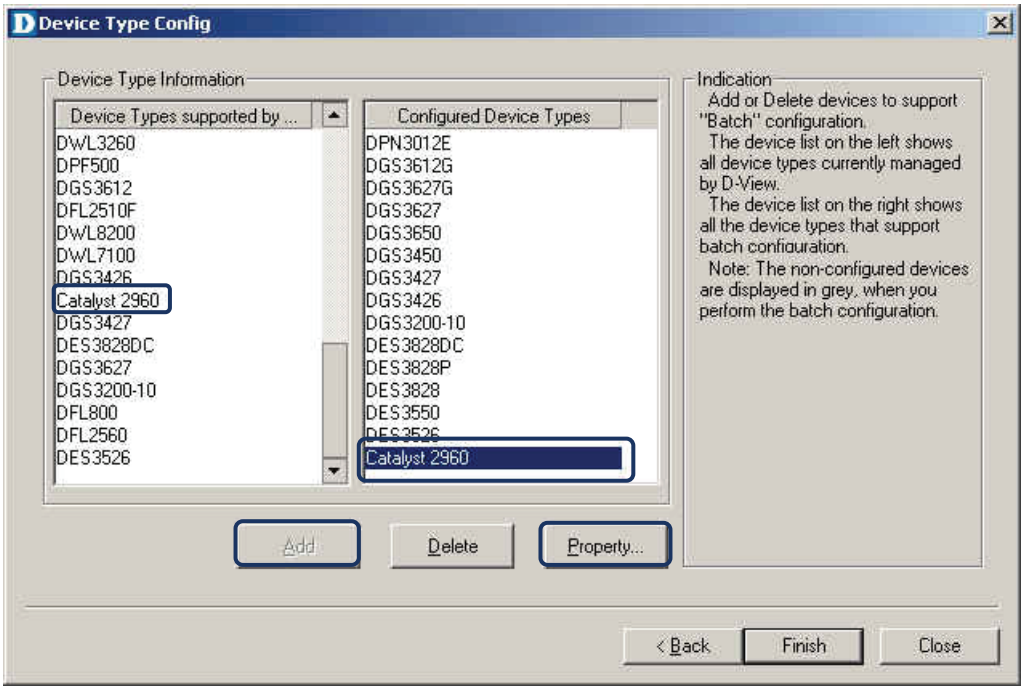


Figure 130: Device Type Config

3. Enter the OID information and click **Add.**
4. Select the added OID information.
5. Add the OID value as seen in the screen below.

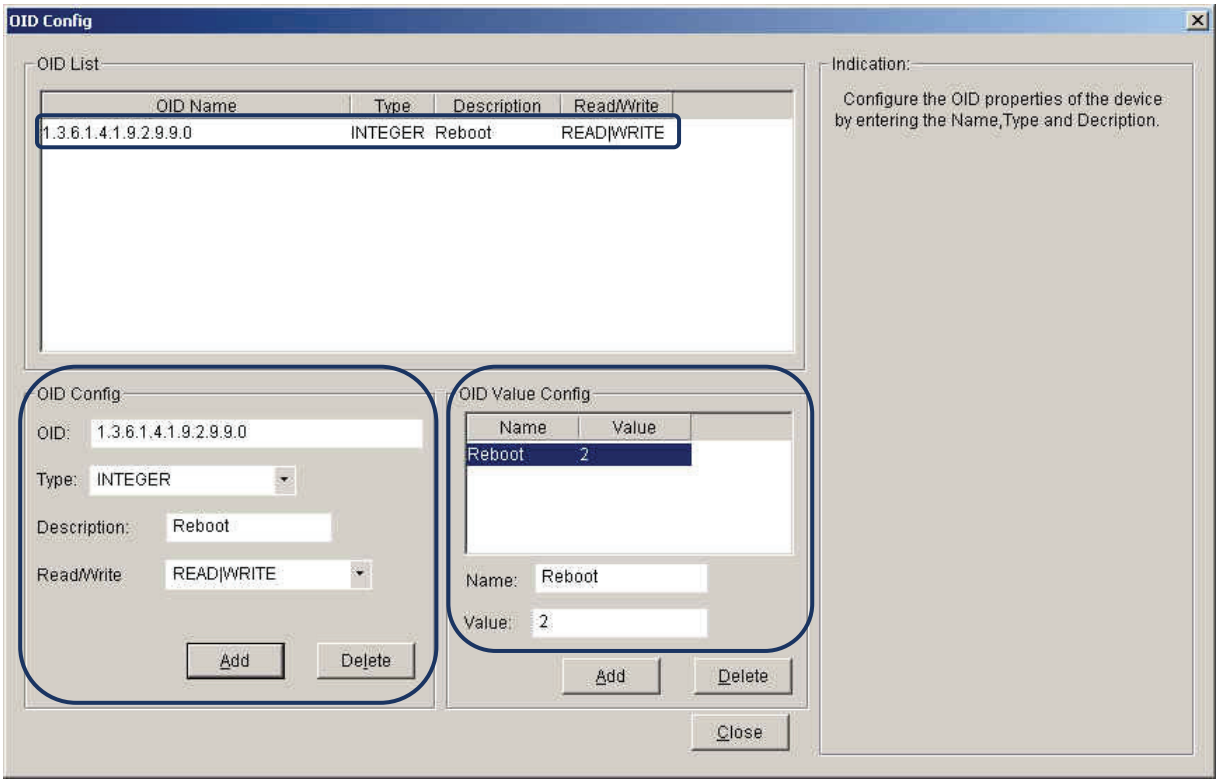


Figure 131: Reboot Parameter Configuration

6. Select the **Reboot** tab to reboot the switch.
   - Follow the on-screen icons to reboot the switch.

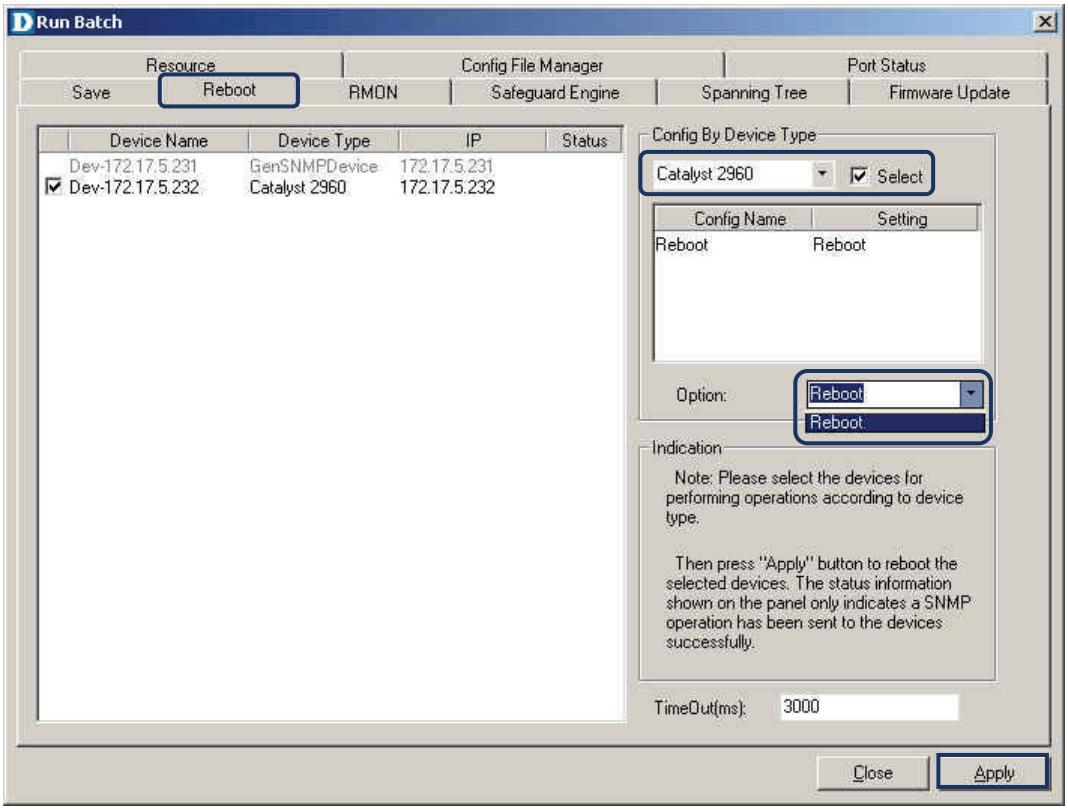


Figure 132: Reboot Function execute

MANAGING DEVICES WITH DEVICE PANEL SIMULATION

Double-click on a switch icon in the topology window of D-View 6.0 to open a new window. This window graphically represents the front panel of the switch. Different management tasks can be started via context menus that appear in the Device Panel Simulation.

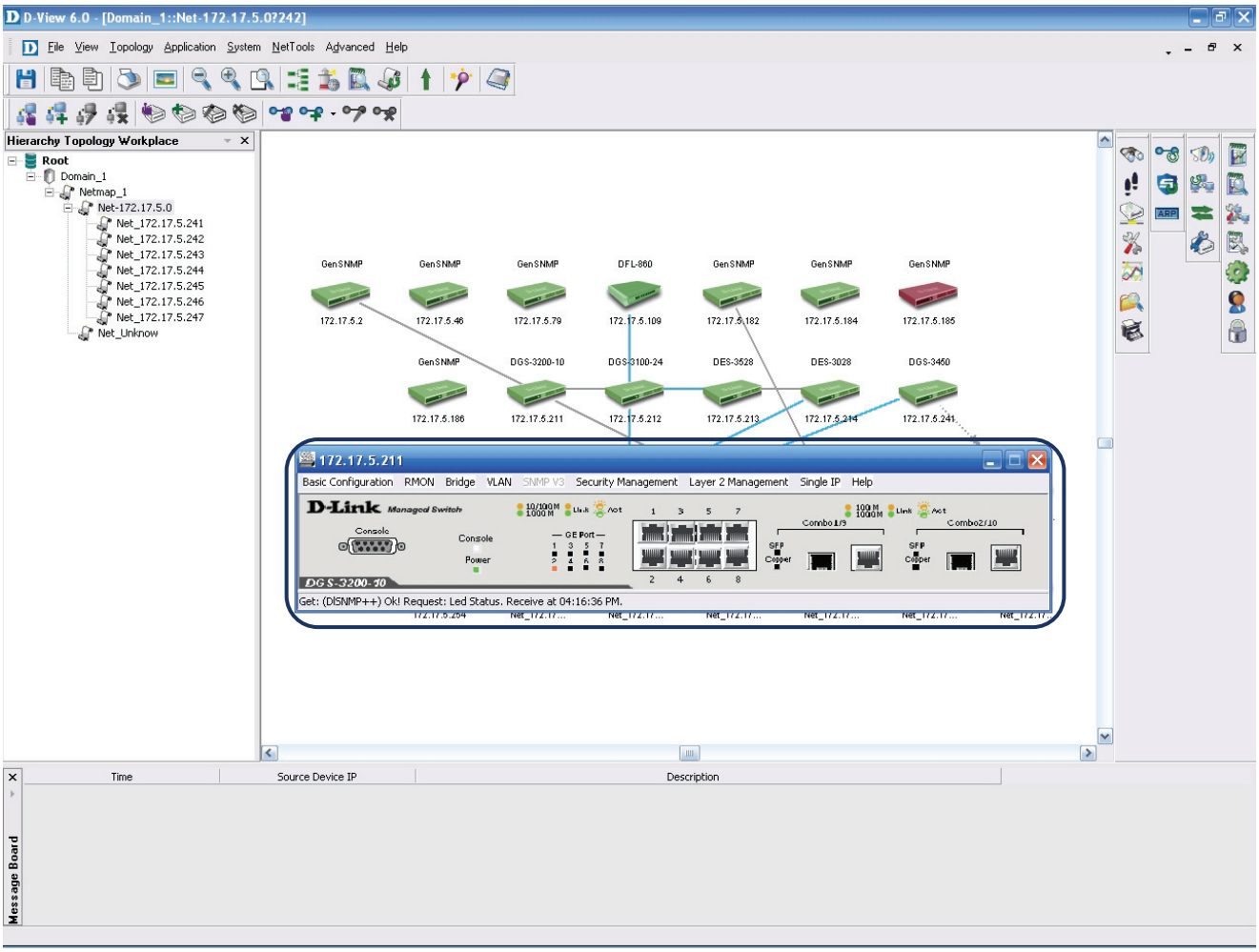


Figure 133: Opening the Device Panel Simulation

The Device Panel Simulation also displays LEDs situated on the physical switch. The following image shows the Device Panel for the DGS-3100. The context menus can be seen on the upper part of the window, ports and LEDs are shown in the graphical representation of the switch. LEDs show status information about Power, Console, RPS, Fan Errors, and individual ports.

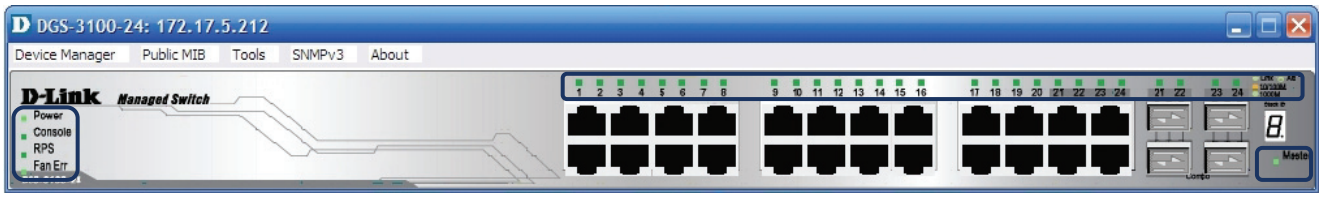


Figure 134: Panel Simulation for the DGS-3100 switch

Point the cursor to the context menu to start management tasks for the corresponding switch.

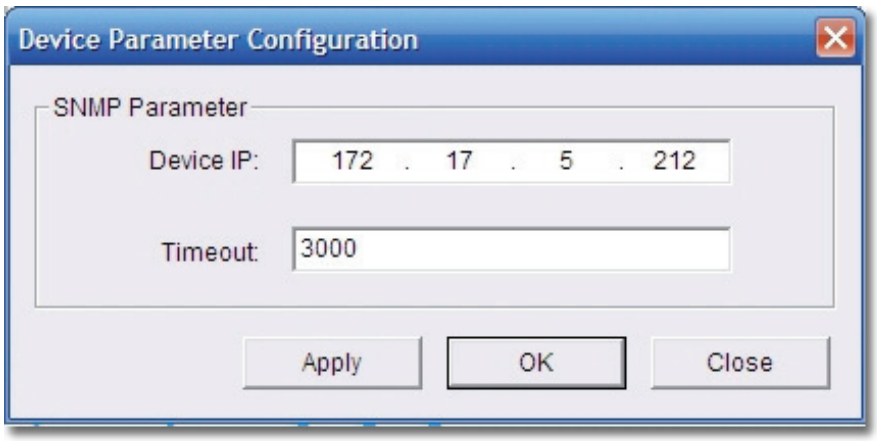


Figure 135: Device Parameter Configuration

Point the cursor to a port and click on it to open the Port Configuraton Window.

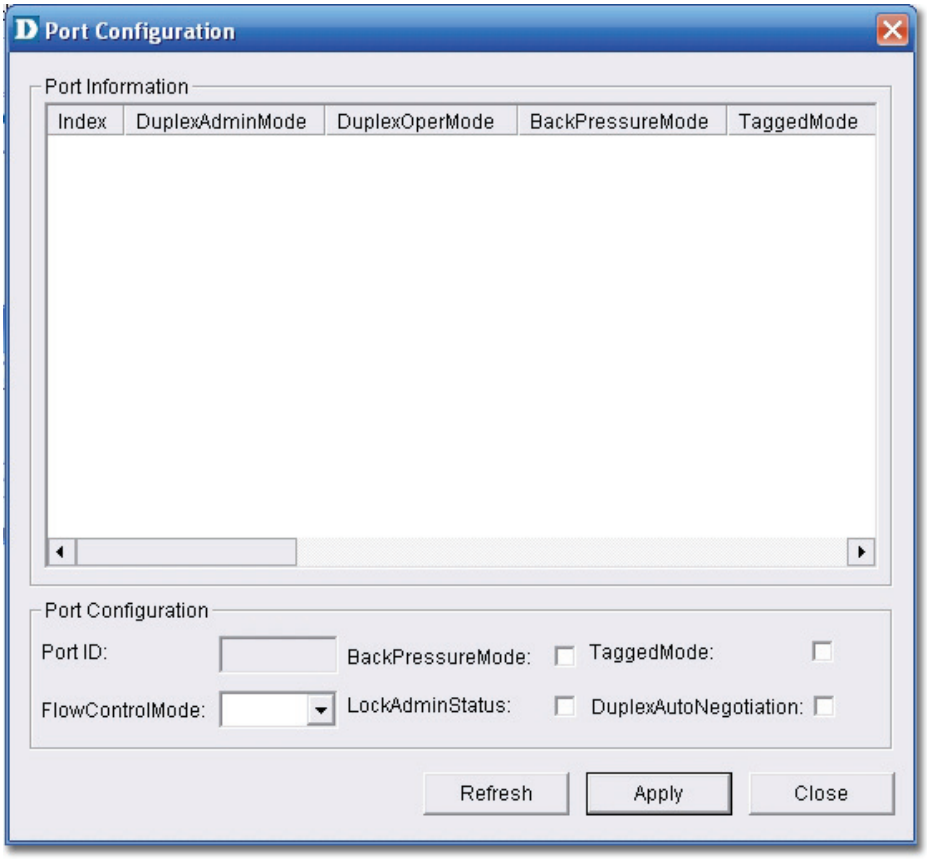


Figure 136: Port Configuration window

Several switches can be managed and monitored at the same time using the Device Panel Simulation.

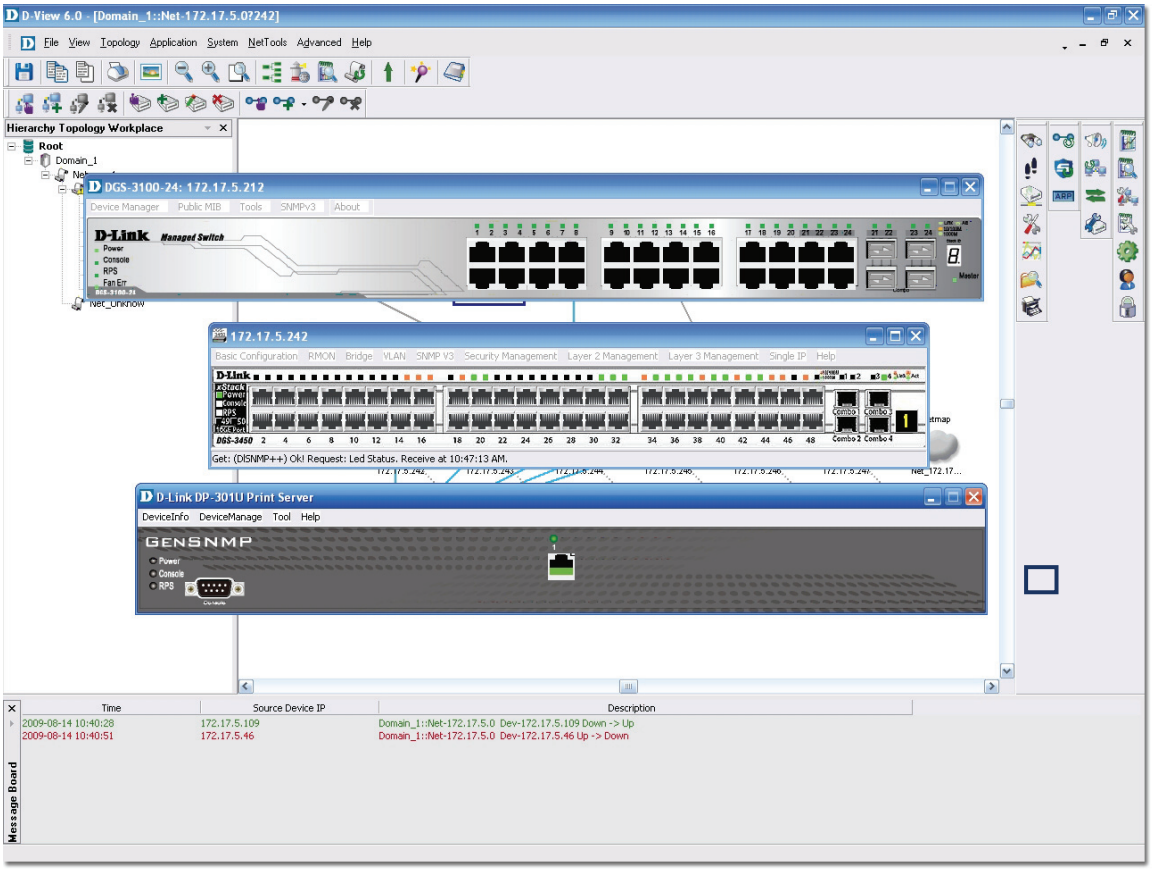


Figure 137: Device Panel modules

MANAGING DEVICES WITH MIB COMPILER

The **MIB Compiler** is used for configuring non-D-Link devices, through a MIB file. The MIB compiler translates the MIB from its normal ASN.1 format to a format that is comprehensible by other applications. The benefits of using the MIB compiler are that you can query data and configure the settings for a third party device with the help of D-View.

To manage devices with MIB Compiler:

1. Go to **NetTools** > **MIB Tools** and then select **MIB Complier**. The **D-Link MIB Compiler** screen displays.

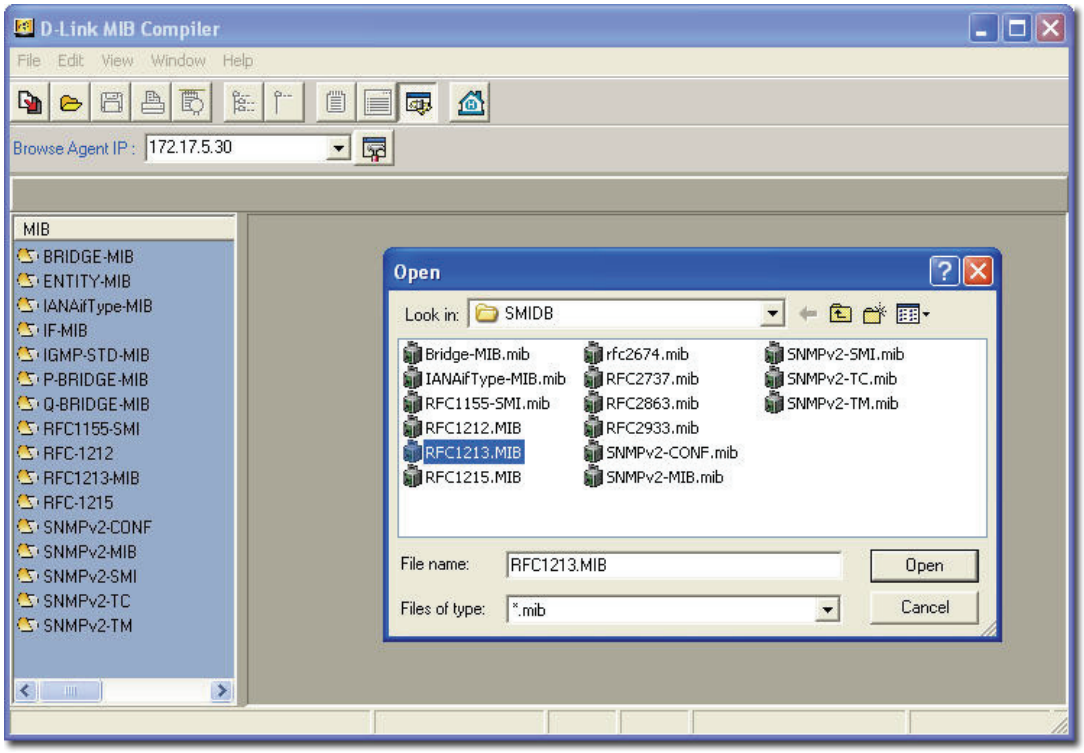


Figure 138: D-Link MIB Compiler screen

2. Open the `rfc1213` file for modification. D-View loads the compiled MIB file.

Typically, D-View identifies the device type by retrieving the OID value 1.3.6.1.2.1.1.2.0 from the RFC1213 MIB file.

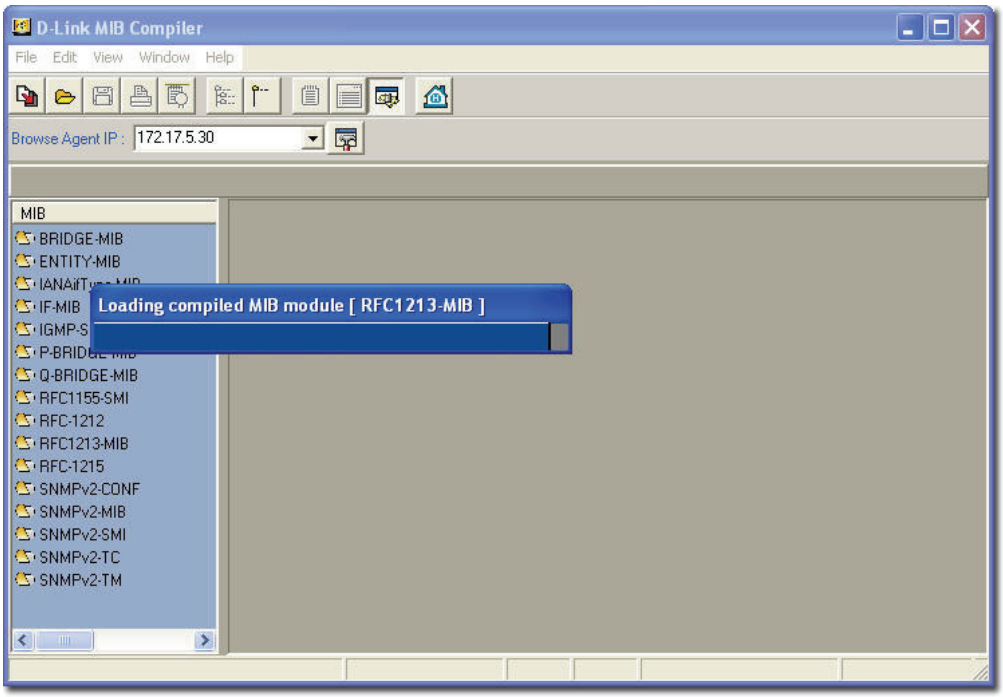


Figure 139: Loading compiled MIB Module screen

3. For example, right-click on `sysLocation` and select **Info** in the MIB tree.

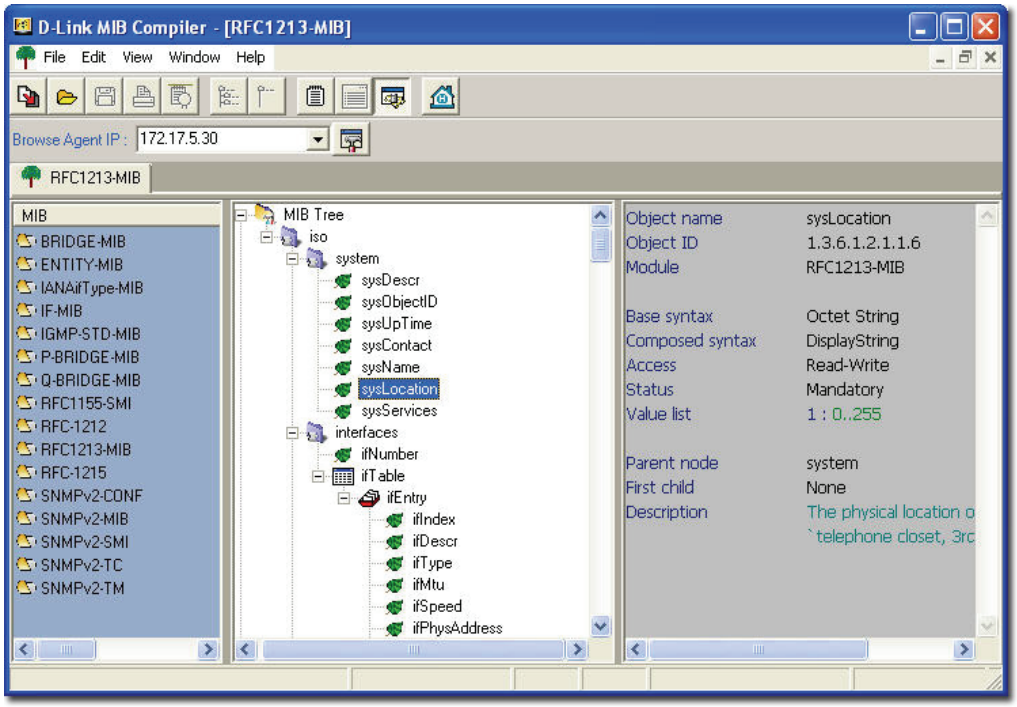


Figure 140: MIB Tree screen

The **Browse Result Node: sysLocation** screen displays.

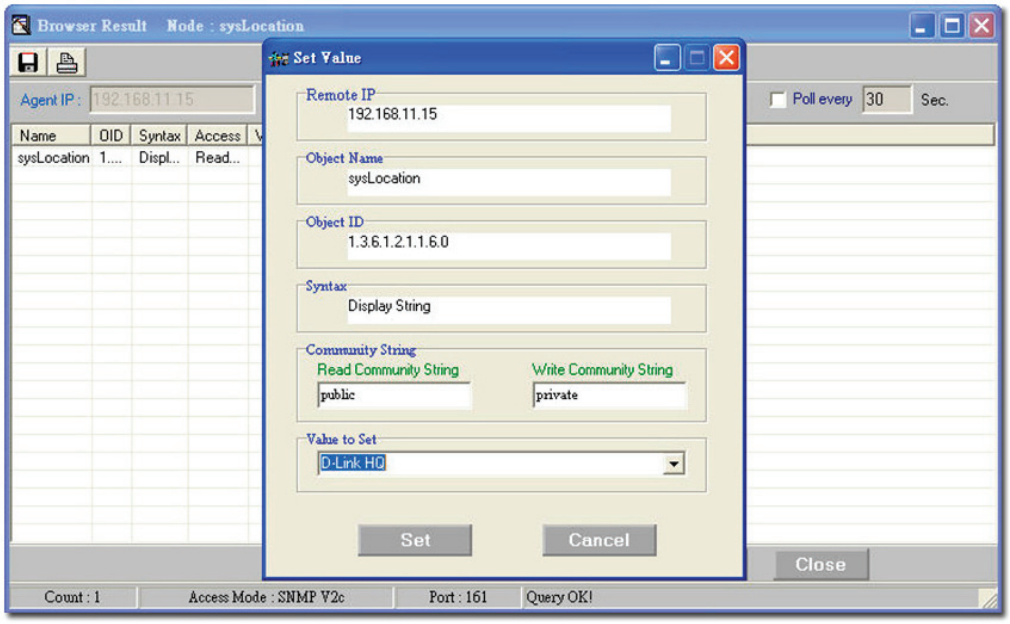


Figure 141: Set Value screen

4. Click **Query** to get the value of the device.
5. Click **Set** to set change the value for `sysLocation`.
6. Make a note of the **OID** value of the device.

Use MIB Browser to browse MIB files after compilation.

Setting Up SNMP Configuration to Retrieve Device Information

1. Click **SNMP Configuration** from the **MIB Complier** screen. **The SNMP Configuration** screen displays.

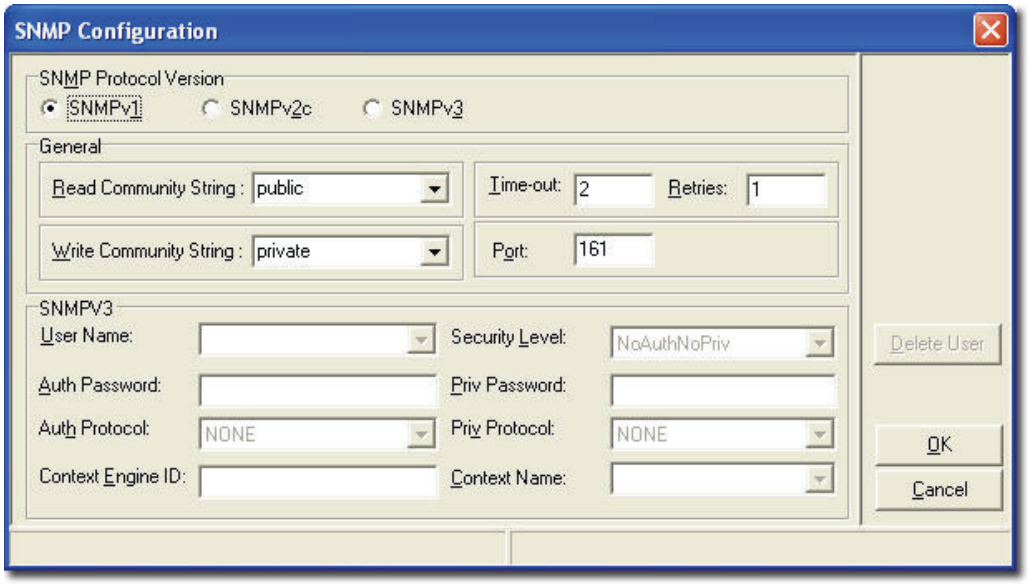


Figure 142: SNMP Configuration screen

2. Select the **SNMP Protocol Version**.
3. Enter the community string to access devices through SNMP.

If you select SNMPV3, update the SNMPV3-specific fields and access devices respectively.

4. Click **OK** and manage the selected device using **MIB Compiler**.

RETRIEVING OID OF THE DEVICE

To identify non D-Link devices, the administrators must first retrieve the OID of the device and then customize them to add to D-View.

Ensure the device is online to retrieve the OID of the device.

To retrieve the OID of the device:

1. Go to **NetTools** > **MIB Tools** > **MIB Compiler**. The **MIB Compiler** screen displays.

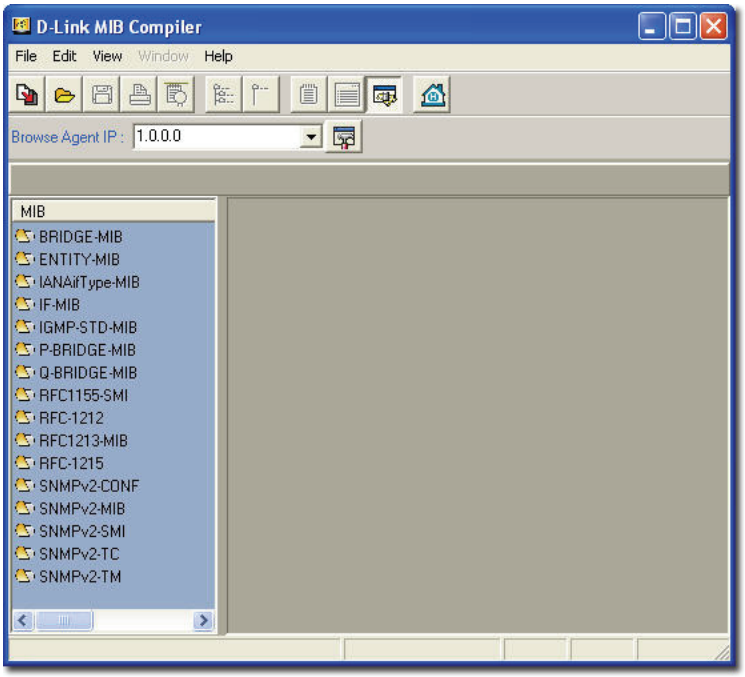


Figure 143: MIB Compiler screen

2. Enter the device IP address.
3. Set the **SNMP Configuration**. Refer to Setting Up SNMP Configuration to Retrieve Device Information from devices.
4. Compile the `RFC1213` MIB File and select `sysObjectID` from the MIB tree.
5. Right-click `sysObjectID` and select **Info**. The **Browser Result** screen displays.
6. Make a note of the OID value of the device.

OR

1. For a non-designated device module, D-View will identify the device as **GenSNMPDevice** type.
2. Double-click on the device. The graphical interface of the device displays.
3. Go to **Device Info** and then select **System Info**. The **System InfoGenSNMPDevice Module** screen displays.

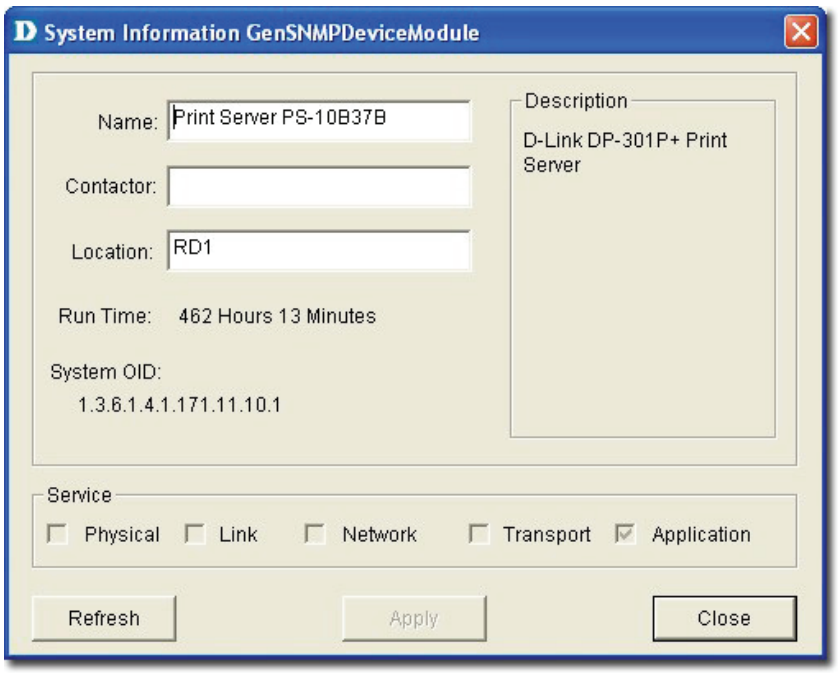


Figure 144: System InfoGenSNMPDeviceModule screen

4. From the **System InfoGenSNMPDeviceModule** screen, modify the device type properties in the dialog.
   - **Name:** Enter the name of the device.
   - **Contactor:** Enter the name of the user responsible for managing the device.
   - **Location:** Enter the location of the device.
   - **Run Time:** Displays the run time of the device.
   - **Service:** Displays the OSI layers the device supports.
5. Click **Apply** to save the changes.
6. Click **Refresh** to view the updated information.

BATCH CONFIGURATION

The **Batch Configuration** tool allows you to execute a sequence of operations in D-View, for example: Save Configuration and Retrieve Port Status. With Batch Configuration you can configure multiple devices simultaneously. Since all the configurations are similar, only one has been described below.

Remember to configure the OID information before using the Run Batch tool.

To configure the OID information of SafeGuard Engine:

1. Go to **Application** > **Batch Config**> **Advanced Option**. The **Advanced Option** screen displays.

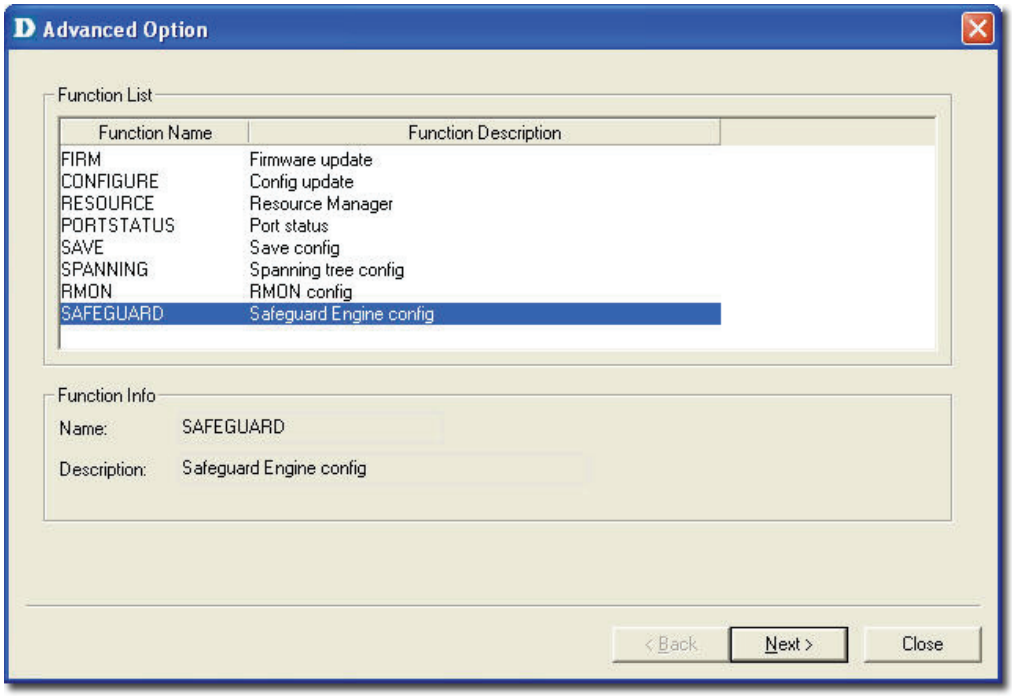


Figure 145: Advanced Option screen

2. D-View supports a list of batch function templates. They are:
   - **FIRM:** Download firmware from the switch to the TFTP server or upload firmware to the device.
   - **CONFIGURE:** Download/Upload config information in the device.
   - **RESOURCE:** Retrieve/Set the information about name, location, contact of the device.
   - **PORTSTATUS:** Retrieve/Set the **Port Enable** status.
   - **SAVE:** Save the configuration changes in a device.
   - **SPANNING:** Enable/Disable the **STP** status in device.
   - **RMON:** Enable/Disable the **RMON** status in device.
   - **SAFEGUARD:** Enable/Disable the **SAFEGUARD** status in device.
3. Select **SAFEGUARD** and then click **Next** to continue. The **Device Type Config** screen displays.

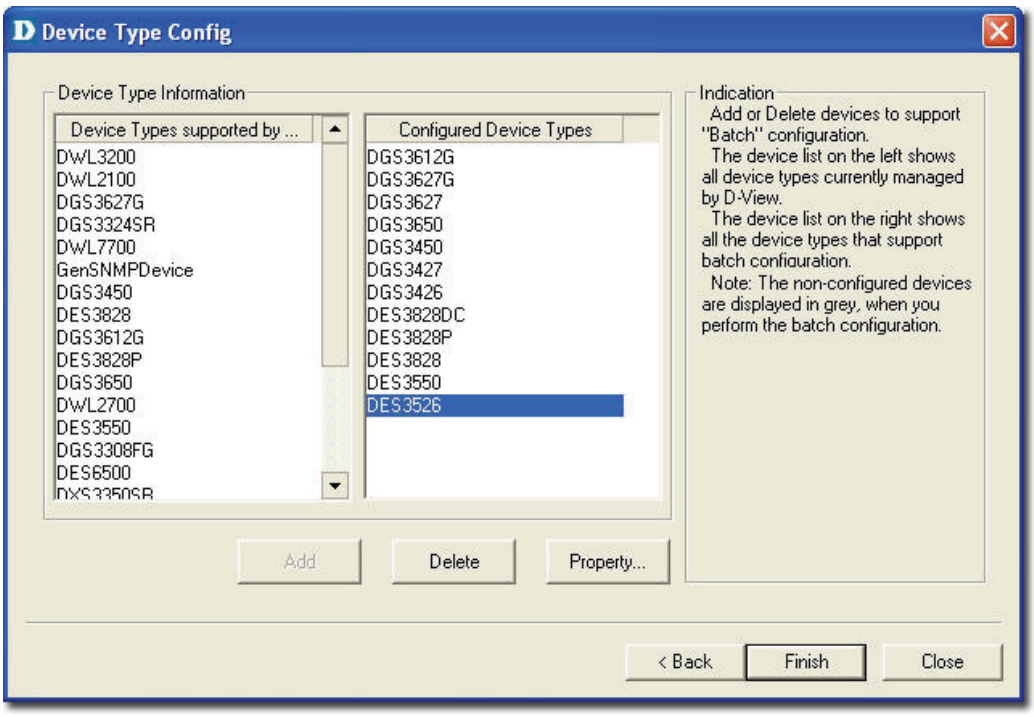


Figure 146: Device Type Config screen

4. The devices can be added or deleted to support batch configuration.
5. Click **Property** to configure the OID properties of a device type. The **OID Config** screen displays.

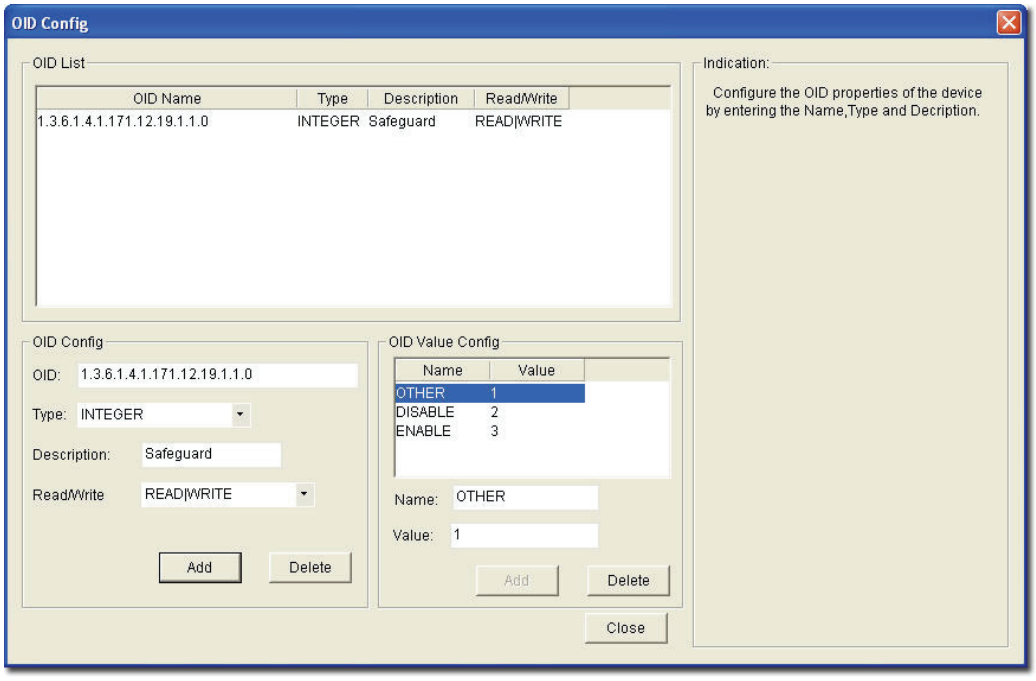


Figure 147: OID Config screen

6. Enter the values of the **OID Config** information.
7. Enter the values of the **OID Value Config** for each OID.
   - 1 – Other
   - 2 – Disable
   - 3 – Enable
8. Click **Add** to configure the OID value of **Safeguard Engine**.

Backup and Update the Devices' Configuration

Use the **Batch** tool to backup and update the devices' configuration.

1. Go to **Application** > **Batch Config** > **Run Batch** or right-click and select **Run Batch** from the popup menu after selecting the devices in the opened topology. The **Run Batch** screen displays.

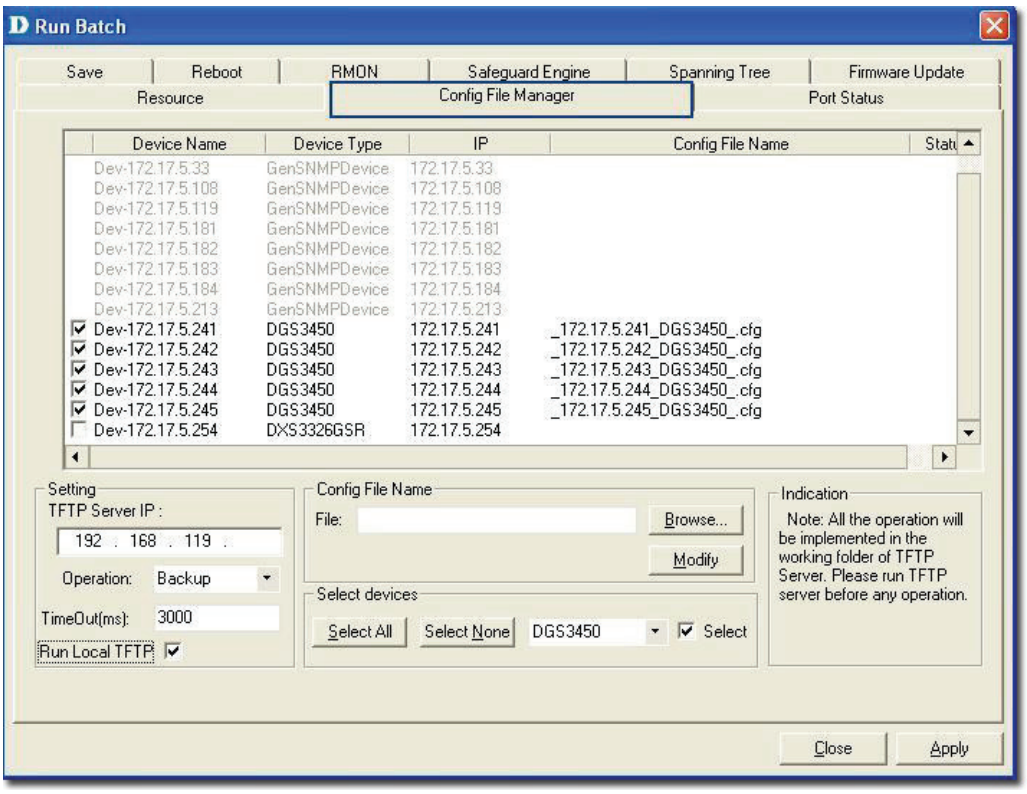


Figure 148: Run Batch screen

2. A brief description of other tabs is given below:
   - **Save:** Save device configuration.
   - **RMON:** Enable/Disable RMON status to monitor device performance.
   - **Safeguard Engine:** Enable/Disable safeguard status. Refer to Using Safeguard Check for more information.
   - **Spanning Tree:** Enable/Disable the status to prevent undesirable loops in the network.
   - **Firmware Update:** Upload/Download firmware through TFTP server.
   - **Resource:** Select to update the resource information for a specific device.
   - **Config File Manager:** Update and backup configuration files from the TFTP server.
   - **Port Status:** Select to view the port status of the device.
3. Select the **Config File Manager** tab. The **Config File Manager** tool helps the administrators to perform the following actions.
   - **TFTP Server IP:** Enter the IP address on which the TFTP server program runs.

- **Operation:** Select the mode of operation- Backup or Update.
- **TimeOut:** SNMP timeout value.
- **Run Local TFTP:** Select to use the TFTP server tool provided by D-View. The **D-Link TFTP Server** screen displays.

4. Click **Apply** and monitor the running status of the TFTP Server.

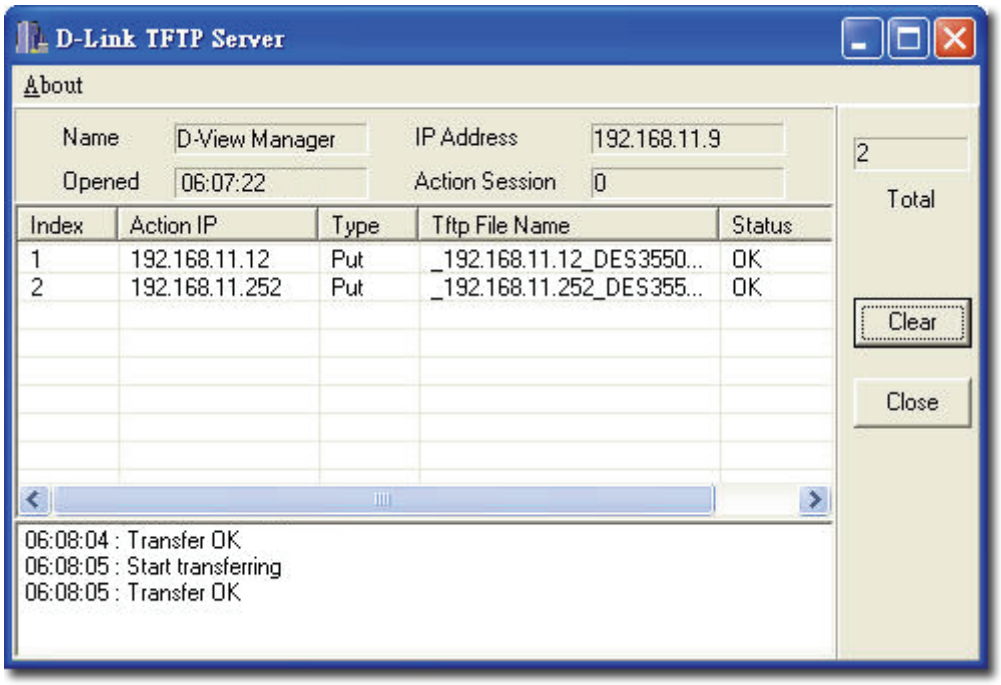


Figure 149: D-Link TFTP Server screen

5. The **Config File Manager** enables uploading of the configuration files to the device through TFTP server. Administrators can make the required changes to the file and then upload this file to the device. It reduces the administrators' time when a similar configuration has to be made to several similar devices. The status displays **OK**, when the transaction is successfully completed. Refer to TFTP for more information.

Using Device Type Check

Use **Device Type Check** to check the network for new and updated devices.

1. Open the **Topology** and select the device that needs to be monitored.

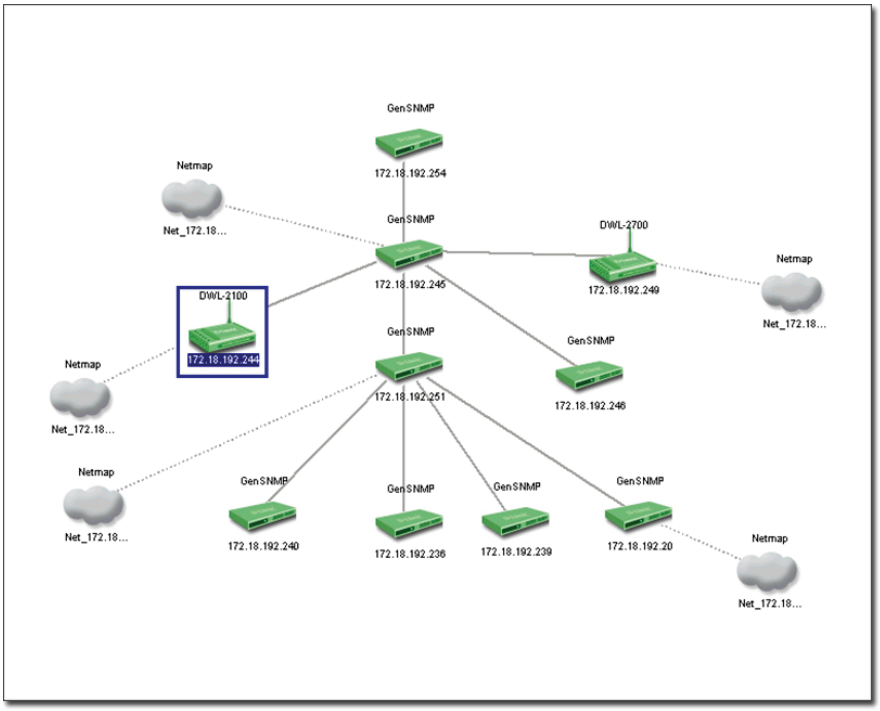


Figure 150: Generated Topology window

2. Go to **Advanced** > **Device Type Check**. D-View scans the devices in the open topology.

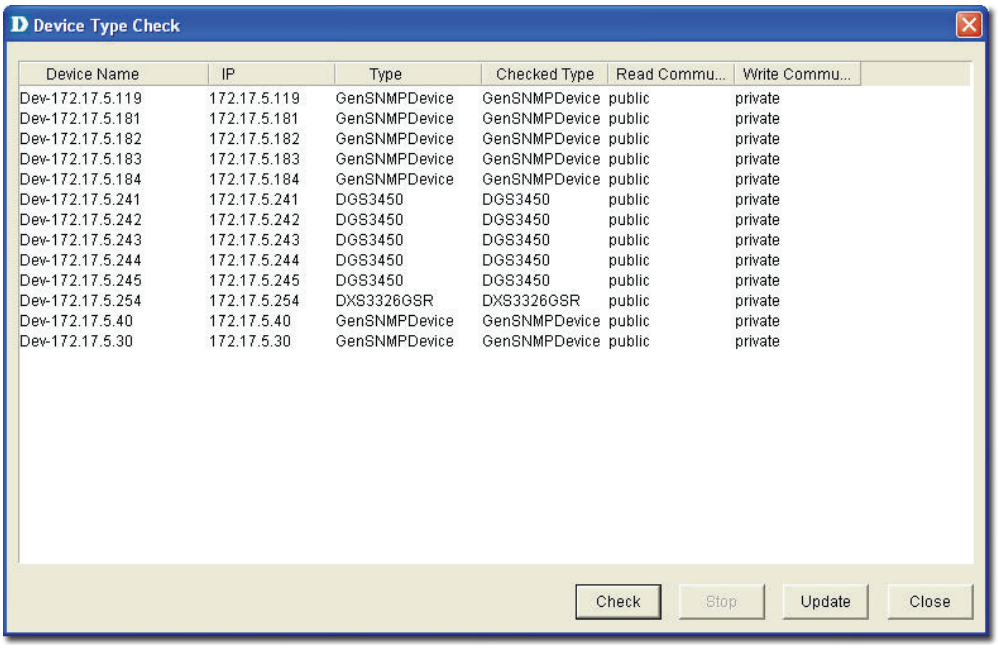


Figure 151: Device Type Check screen

3. Click **Check** to manually scan the device.
4. Select one or more devices and click **Update**. D-View refreshes the information of the selected devices.

Using Safeguard Check

Malicious hosts on the network could attack the Switch through various methods (for example, packet flooding). To overcome this situation, D-View uses **Safeguard Engine** to protect switches from malicious traffic flood. This minimizes the workload of the switch during the attack. The Switch, therefore, is capable of forwarding essential packets even during limited bandwidths.

By default, the safeguard status of all devices is disabled.

To configure the safeguard status:

1. Go to **Application** > **Batch Config** > **Run Batch**
   Or
   In the opened topology select the device and right-click and select **Run Batch**.
   The **Run Batch** screen displays. You can now enable or disable the devices' Safeguard Engine.

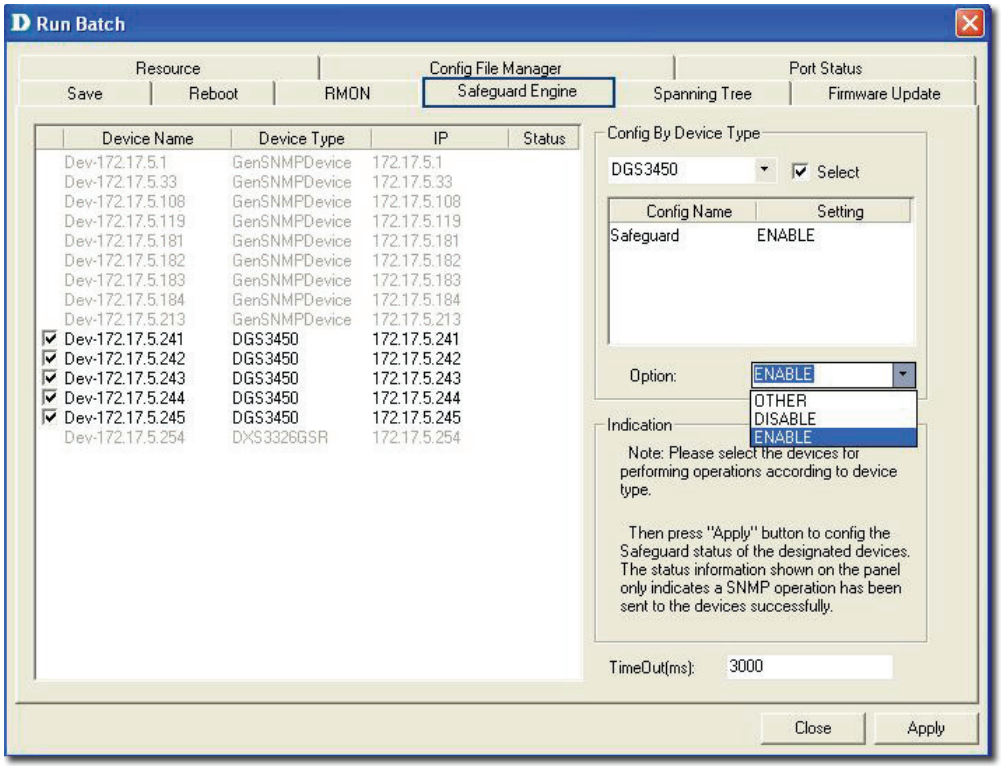


Figure 152: Run Batch: Safeguard Engine screen

2. Check the devices and then select **ENABLE** from the **Option** drop-down list.
3. Click **Apply** to enable the **Safeguard Engine** status of the selected devices.
4. Go to **Advanced** > **Safeguard Check** for the updated enable status of the selected devices. The **Safeguard Check** screen displays.

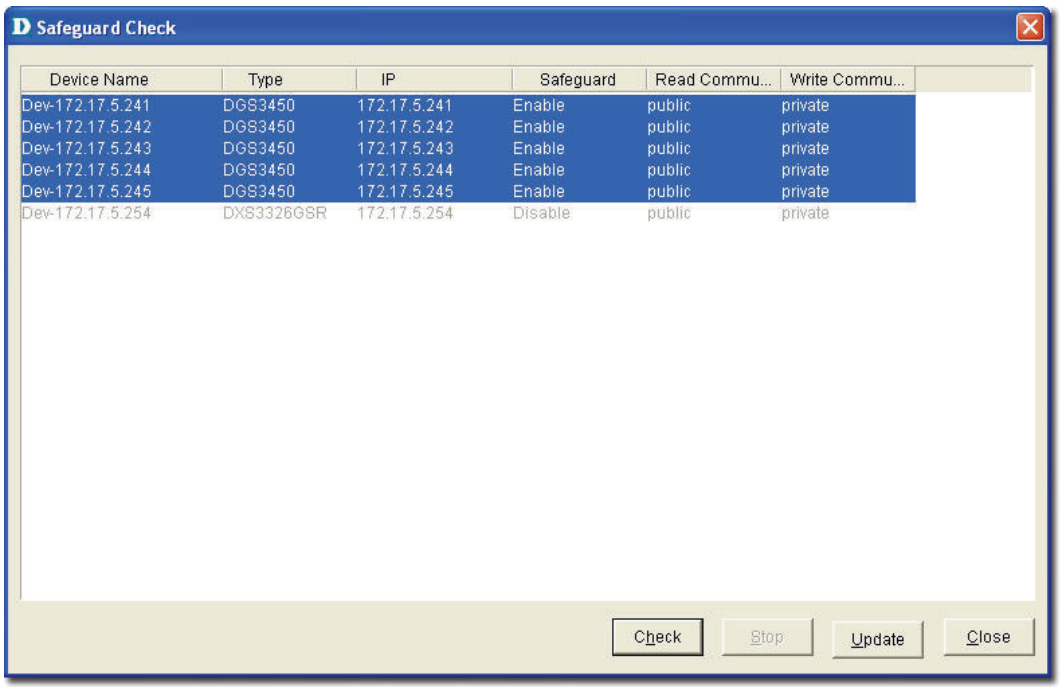


Figure 153: Safeguard Check screen

5. Click **Check** to manually scan the safeguard status of the device.
6. Click **Update** to refresh the updated information.
7. Click **Close** to exit the window.

The **Safeguard Engine** icon is displayed on the top left-hand corner of the device in the topology.

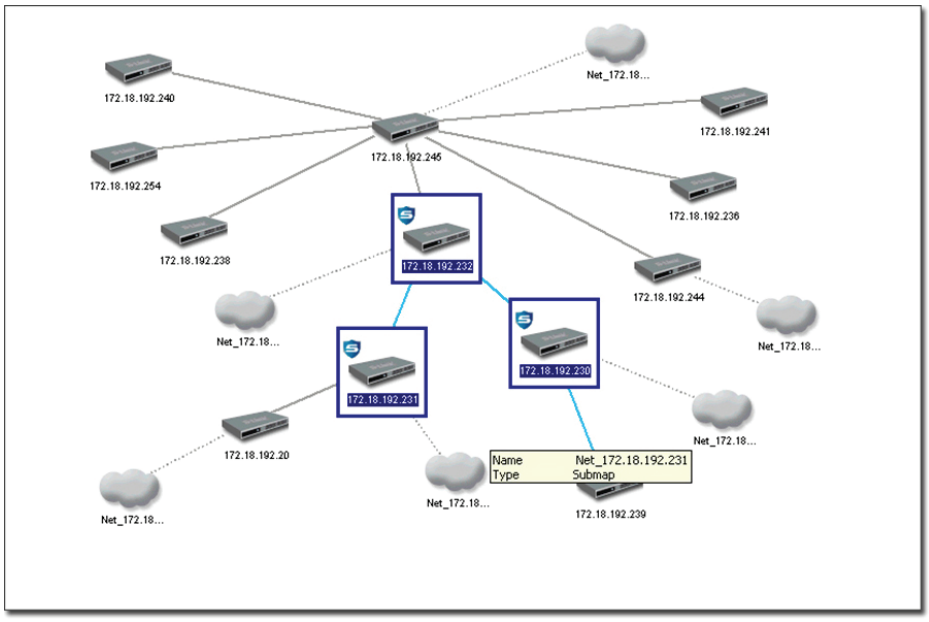


Figure 154: Topology indicating the Safeguard Engine enabled for certain switches

The Safeguard status is not saved into the database; the status value is only for the opened topology.

Labeling Devices

There are two types of labels in D-View:

- **Device Label** – Used to label the device. Administrators can set what details should be displayed.
- **Link Label** – Used to label the connectors connecting two or more devices.

By default, D-View displays the IP addresses under the device icon in a topology.

Device Label

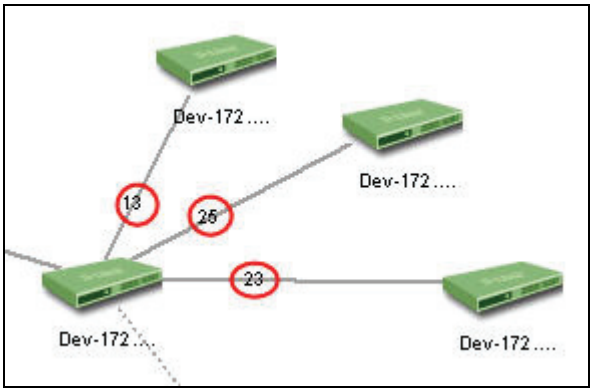
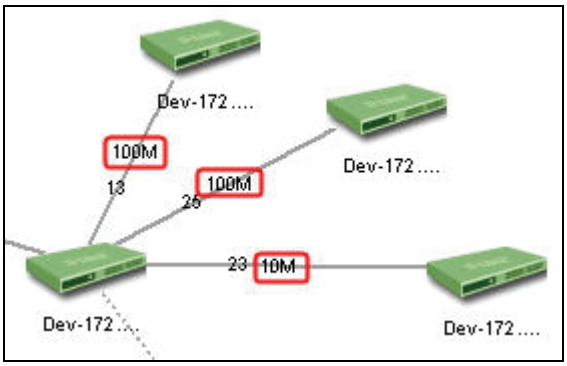
To change the **Device Label**, go to **Topology** > **Device Label** and select a type.

The following table lists the different types of **Device Labels**.

DEVICE LABEL	DESCRIPTION	EXAMPLE
Device Name	The device name is displayed under the device icon.	
Device IP	The device IP address is displayed under the device icon.	
Device Type	The device type is displayed above the device icon.	
Safeguard Engine	The Safeguard status is displayed on the top left corner of the device icon. The Safeguard status can be checked and updated by calling Using Safeguard Check function module.	
Hide Info	Hides the information of the devices.	

Link Label

To change the **Link Label**, go to **Topology** > **Link Label** and select a type. The following table lists the different types of **Link Labels**.

DEVICE LABEL	DESCRIPTION	EXAMPLE
Link Port	Displays the port number used to connected the two devices.	
Link Speed	Displays the maximum connection speed between the two devices.	

Editing Device Information

D-View can store device-related information such as name of the device, the port it uses, interface configuration details, vendor, and so on.

To edit device information:

1. Select the device from an open topology and then go to **Topology** > **Device Manager** > **Edit Device**. The **Edit device** screen displays.
   OR
   Right-click on the device and select **Property** to edit the properties of the device. The **Edit Device** screen displays.

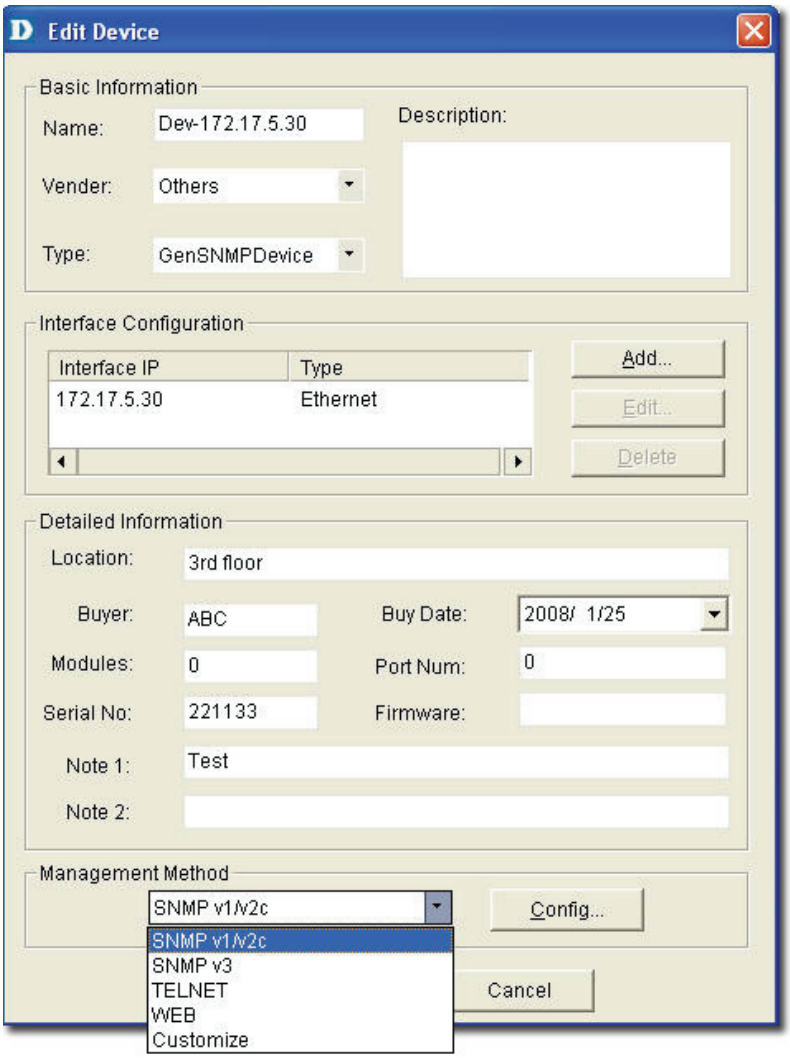


Figure 155: Edit Device screen

2. Enter the **Basic Information** for the device. Basic Information comprises **Name**, **Vendor**, **Type**, and **Description** of the device.
3. Configure the **Interface IP**. Click **Add** to add a new Interface IP, **Edit** to update an existing Interface IP, or **Delete** to remove an existing Interface IP.
4. Enter the **Detailed Information** for the device. Detailed Information comprises the **Location**, **Buyer**, **Modules**, **Serial No.**, **Buy Date**, **Port Num**, and **Firmware** of the device.
5. Configure the **Management Method**. Refer to Management Methods for more information.
6. Click **Apply**.

Management Methods

D-View allows administrators to manage multiple device modules simultaneously, using different management methods. When administrators need to configure the device, D-View opens the designated management tool.

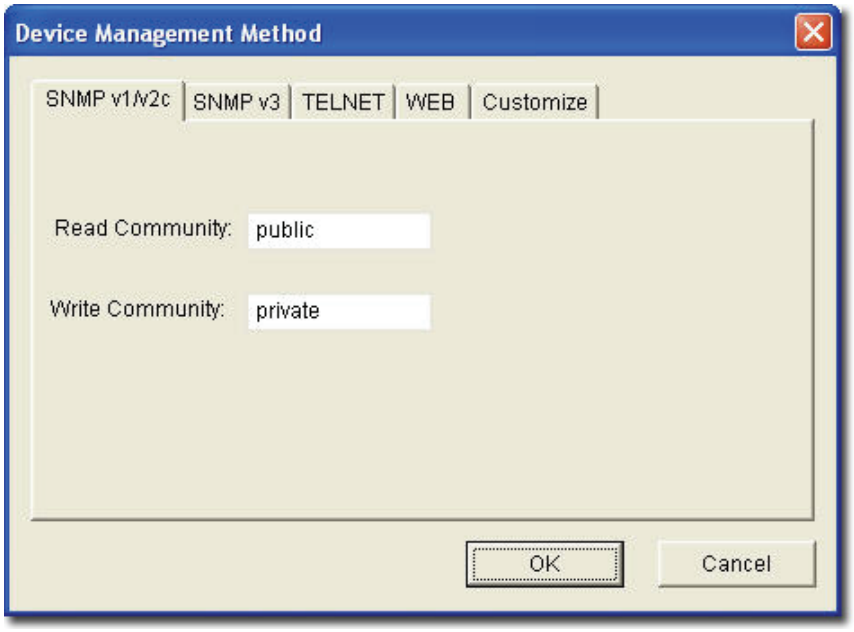


Figure 156: Device Management Method screen

D-View includes the following methods for managing a device:

- **SNMP v1/v2c:** D-View will use device modules that support SNMP v1/v2c to manage the device.
- **SNMP v3:** D-View will use device modules that support SNMP v3 to manage the device.
- **TELNET:** D-View will use the telnet tool embedded in the OS to manage the device.
- **WEB:** D-View will use web browser (IE) tool imbedded in the OS to manage the device.
- **Customize:** D-View will use the designated program to manage the device.

MANAGING EVENTS

Events are one of the core functions of D-View. In fact, the main function of D-View can be described as detecting changes within the network, and every change can be thought of as an event. The following sections will discuss **Events** in detail.

Setting Poll Parameters

Parameters for the polling include poll interval and poll timeout.

To set the Polling Parameters:

1. Go to **System** > **Event Manager** > **Polling Config** > **Set Parameter** tab.

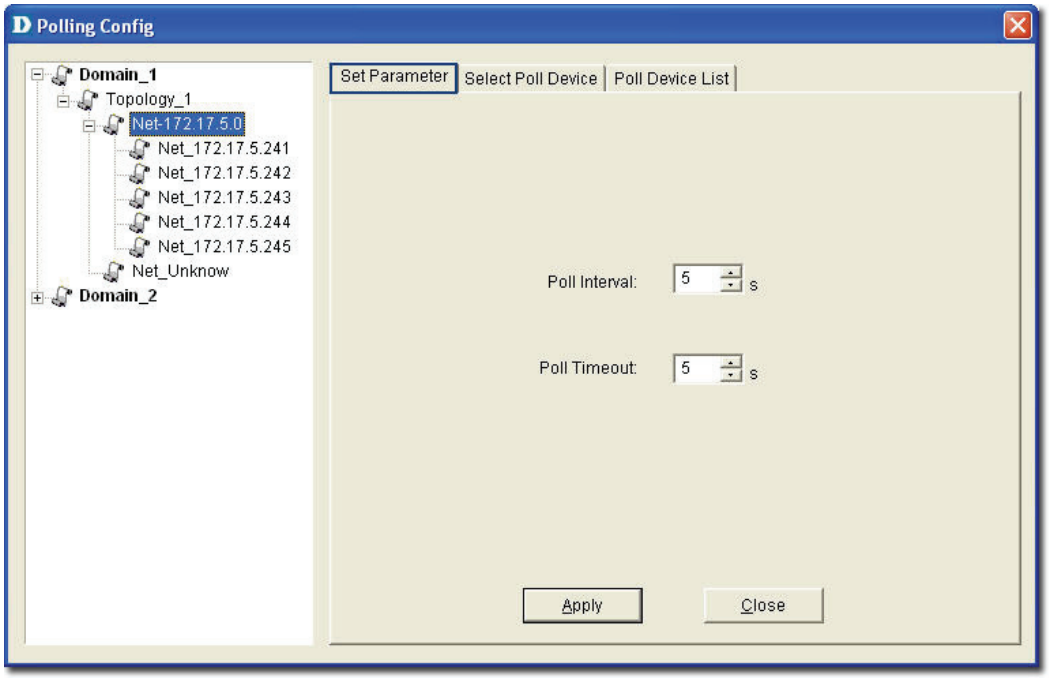


Figure 157: Set Parameter screen

2. Set the **Poll Interval** in seconds. D-View polls the devices at the set time interval.
3. Set the **Poll Timeout** in seconds. D-View stops polling the device after the timeout period.
4. Click **Apply**.

Setting the Devices to Poll

To monitor the status of the devices, add the devices to the poll list. You can also delete the devices if you no longer want to monitor the device status.

When the devices are added to the poll list, the device icon color changes from grey to green.

To configure the Poll List:

1. Go to **System** > **Event Manager** > **Polling Config** > **Select Poll Device** tab.

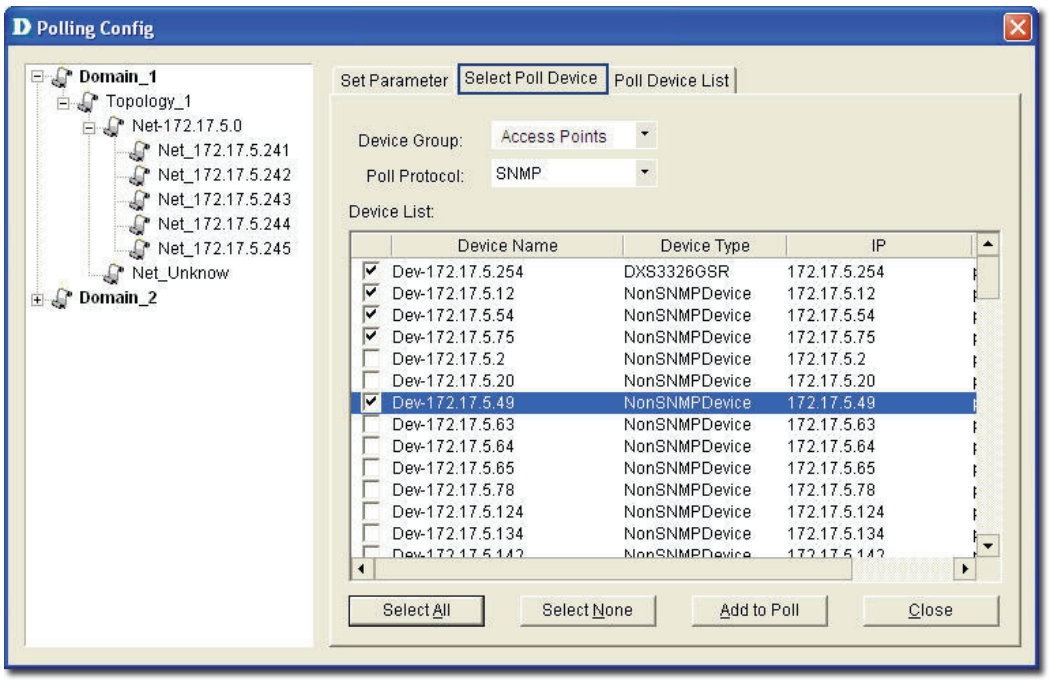


Figure 158: Select Poll Device screen

2. Select the **Device Group**. Refer to Grouping Devices using Device Manager for more information on grouping devices.
3. Select the **Poll Protocol**. The two options to poll the network devices periodically are **SNMP** (Simple Network Management Protocol) and **ICMP** (Internet Control Message Protocol). The default poll protocol is **ICMP**.
4. Select devices and then click **Add to Poll** to add to the poll list.

From the topology, select the device and right-click to select **Add to Poll List** or **Delete from Poll List** from the popup menu.

*By default, when the topology is imported, the devices are in an **unpoll** status.*

*The status of the device is changed to **Up** or **Down** when the device is added manually.*

Viewing the Poll Device List

The **Poll Device List** displays the list of devices after generating the Topology.

1. Go to **System** > **Event Manager** > **Polling Config** > **Poll Device List** tab.

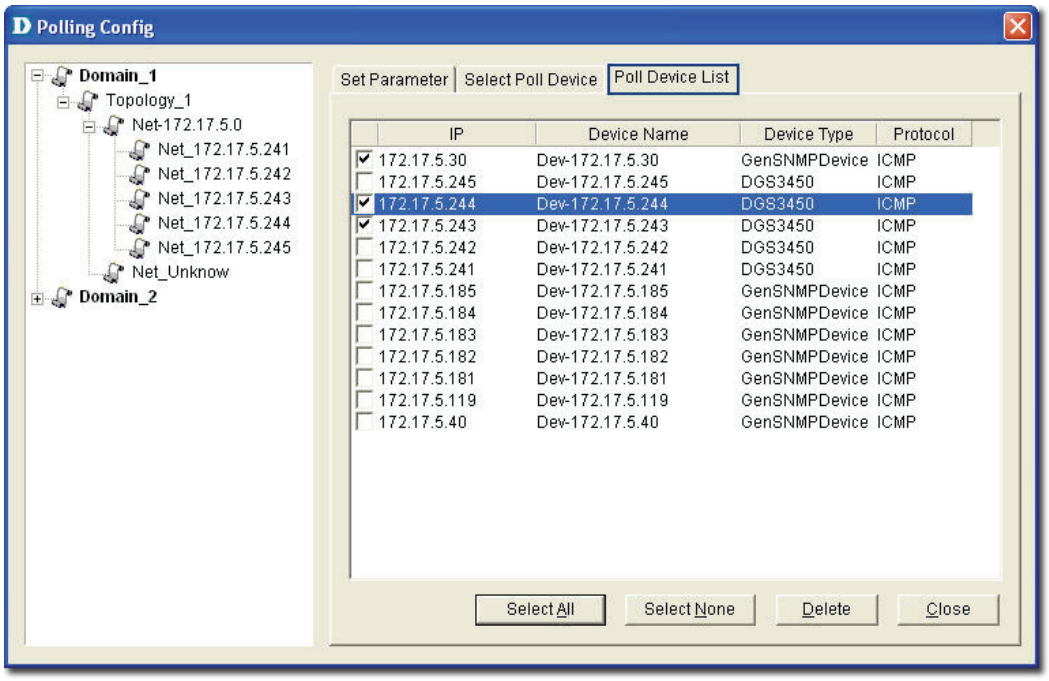


Figure 159: Poll Device List screen

2. From here you can delete devices you've added to the list.

From the topology, select the device and right-click to select **Add to Poll List** or **Delete from Poll List** from the popup menu.

Grouping Devices using Device Manager

For monitoring similar devices, you can group devices of the same type using the **Device Group Manager**.

1. Go to **System** > **Event Manager** > **Device Group Manager**. The **Device Group Manager** screen displays.

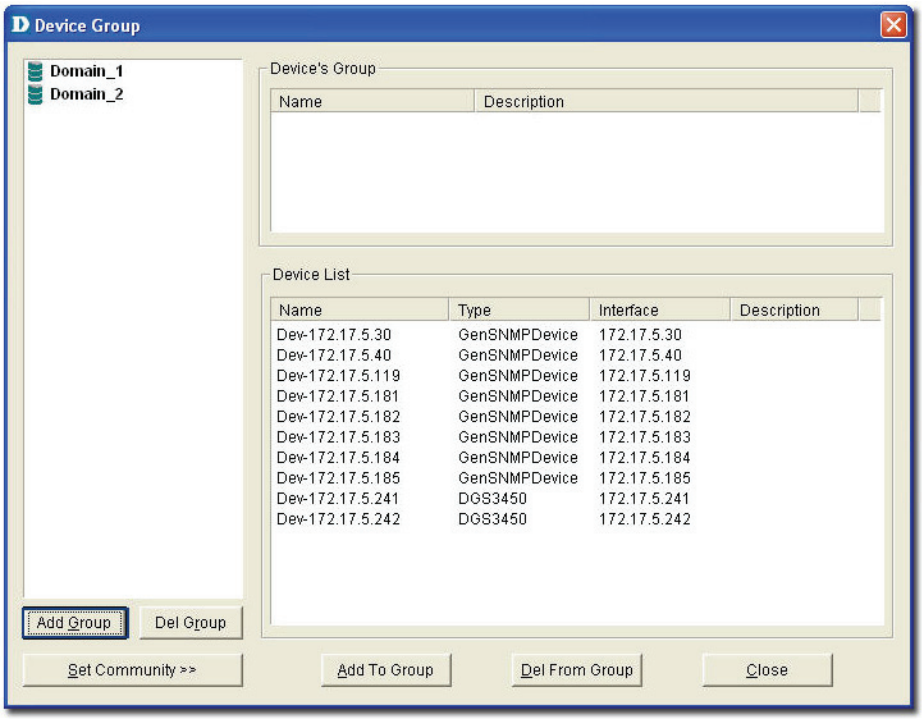


Figure 160: Device Group screen

2. Click **Add Group** to create a group. The **Add Group** screen displays.

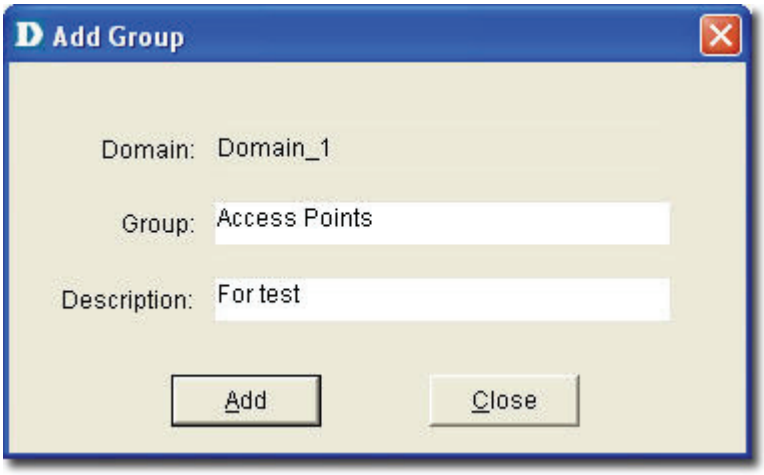


Figure 161: Add Group screen

3. Enter the name of the Group.
4. Enter a brief **Description** of the group.
5. Click **Add.** The group is created.
6. Next, select devices from the device list you want to add to this group and click **Add To Group**. The **Add Device to a group** screen displays.

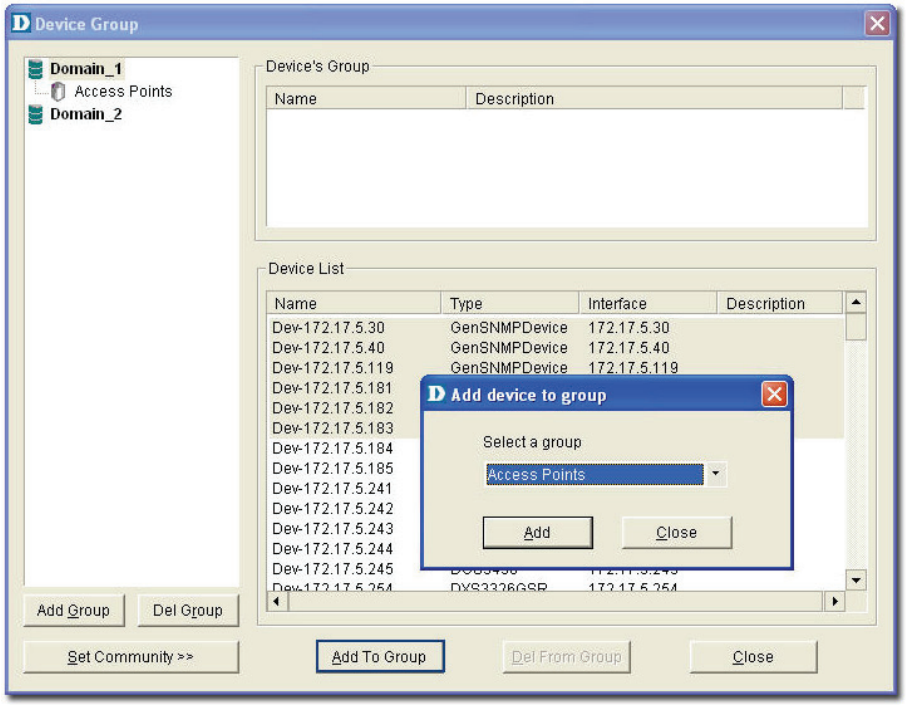


Figure 162: Add device to group screen

7. Select the group from the list.
8. Click **Add**. The devices are added to the group.

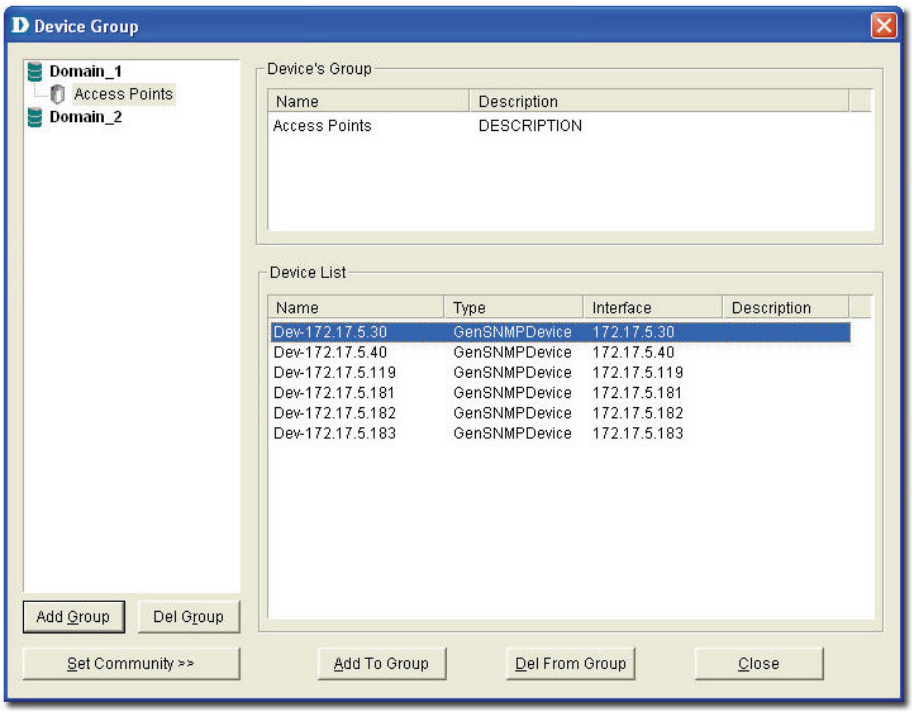


Figure 163: Device Group screen

9. Click **Set Community** to change the read/write community of devices.

Configuring Device Events

After defining the poll list, configure the event process mechanism for a device or a group of devices when an event occurs.

To configure Device Events:

1. Go to **System** > **Event Manager** > **Device Event Config**. The **Event Configuration** screen displays.

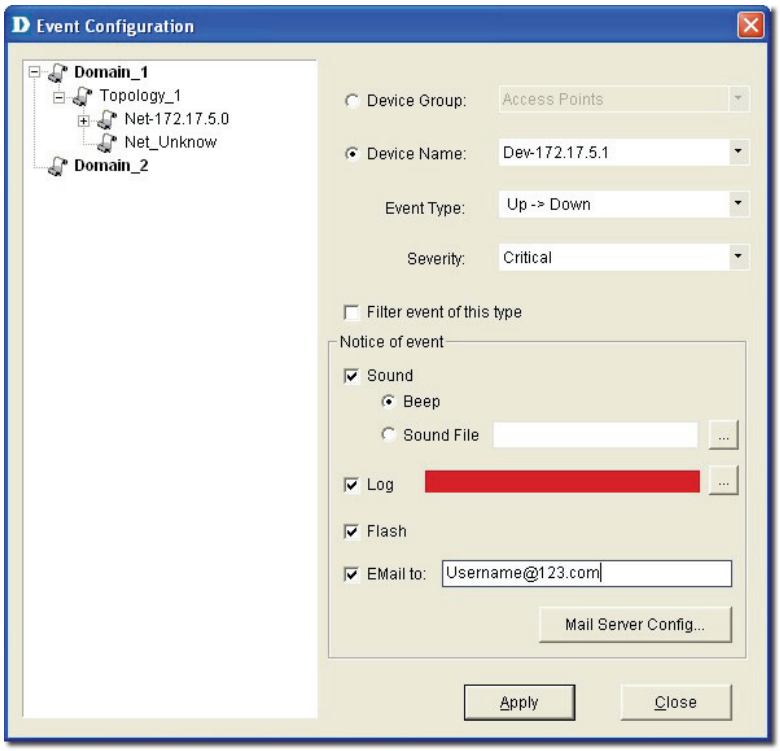


Figure 164: Event Configuration screen

2. Select a **Device Group** or a **Device Name**.
3. Select the **Type** of event. The different events are:

TRAP	INDICATION
Up -> Down	The link between the device and the workstation (D-View) is disconnected.
Down -> Up	The link between device and the workstation is connected.
Cold Start	Device sends **Cold Start** trap message when the device is powered off/on.
Warm Start	Device sends **Warm Start** trap message when the device has been rebooted.
Link Down	Device sends **Link Down** trap message when the status of an attached communication interface has changed from up to down.
Link Up	Device sends **Link Up** trap message when the status of an attached communication interface has changed from down to up.
Syslog Event	Device sends log messages to the syslog server.
Device Authentication Fail	Device sends **Authentication Fail** trap when the agent received a request from an unauthorized manager.
EGP Fail	In routers running the **Exterior Gateway**

	Protocol (EGP), an EGP Neighbor has changed to a down state.
Self-Defined Trap	Device sends the private trap defined by the users.
Threshold Event	Device sends the trap message, when D-View detects a threshold event. Whenever the exceeded count reaches the trigger value then a threshold event is generated.

4. Enable **Filter this type event** if you do not want to notify users of this event.
5. Set the notification options as required:

- **Sound:** D-View plays the selected sound file or beeps to notify users that an event has occurred.
- **Log:** Saves the event into database. Set the color of the Log messages displayed in the message board.
- **Flash:** The netmap icon in the Hierarchy Topology Workplace will flicker a warning sign.
- **EMail:** D-View notifies administrators of an event through an e-mail.
- **Mail Server Config:** Click to configure the mail.

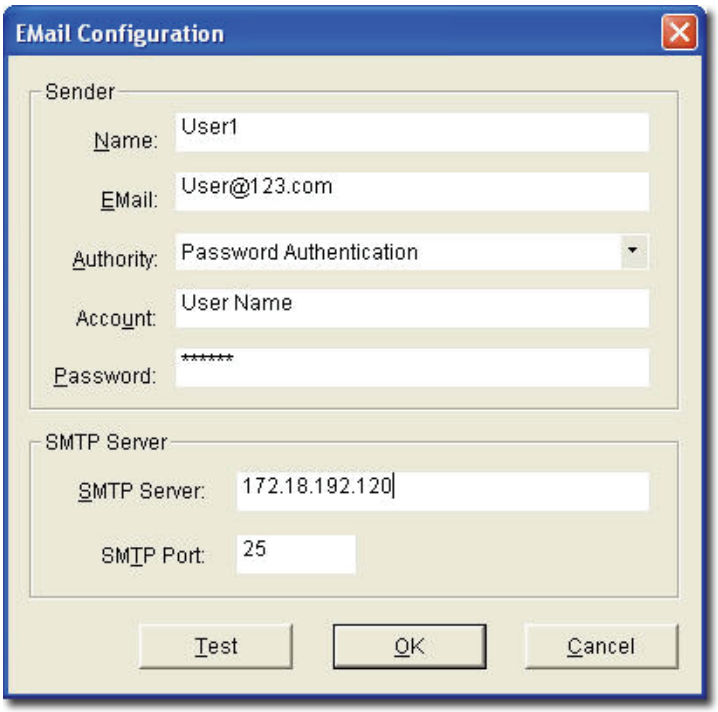


Figure 165: Email Configuration screen

- **Sender:** Update the Sender's information by entering the name, email, authority, account and password.
- **SMTP Server:** Enter the IP address of the device. SMTP is a server program that lets you send email messages directly from your computer.
- **SMTP Port:** Enter the **SMTP Port** number to connect to the server.
- Click **Test** to connect to the mail server.

Retrieving Device Event Logs

D-View saves all events into the database as and when they occur. Retrieve the **Device Event Log** to view event information.

1. **Event Viewer by Netmap:** To view events occurred for a selected Netmap go to **System** > **Event Manager** > **Event Viewer by Netmap**.

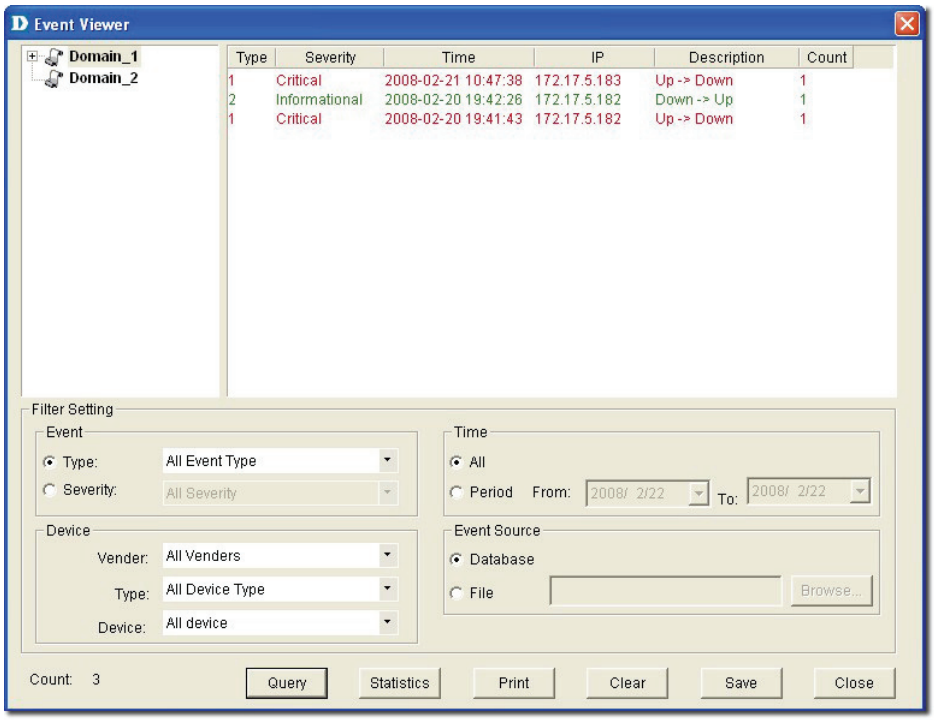


Figure 166: Event Viewer by Netmap screen

2. **Event Viewer by IP:** To view events occurred for a selected IP address go to **System** > **Event Manager** > **Event Viewer by IP**.

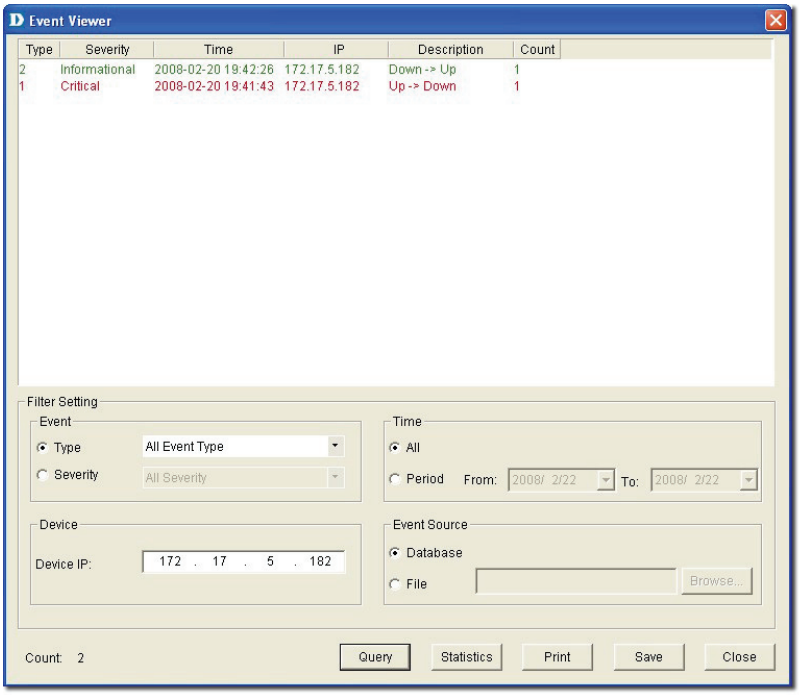


Figure 167: Event Viewer by IP address screen

3. From here, you can further filter the events. Select from the following to filter the events:
   - **Filter Setting:** Administrators can set filters such as event type and level of severity.
   - **Device:** Select device information such as the IP address, vendor name and device type from the drop-down list.
   - **Time:** Set the time interval at which the event has occurred.
   - **Event Source:** Select the source of the event saved in the database or stored in a file.
4. Save the settings and click **Query** to query the database and a list of devices are displayed depending on the filter setting.
5. Click **Statistic** to view event statistics by event type, manufacturer, severity and device type.

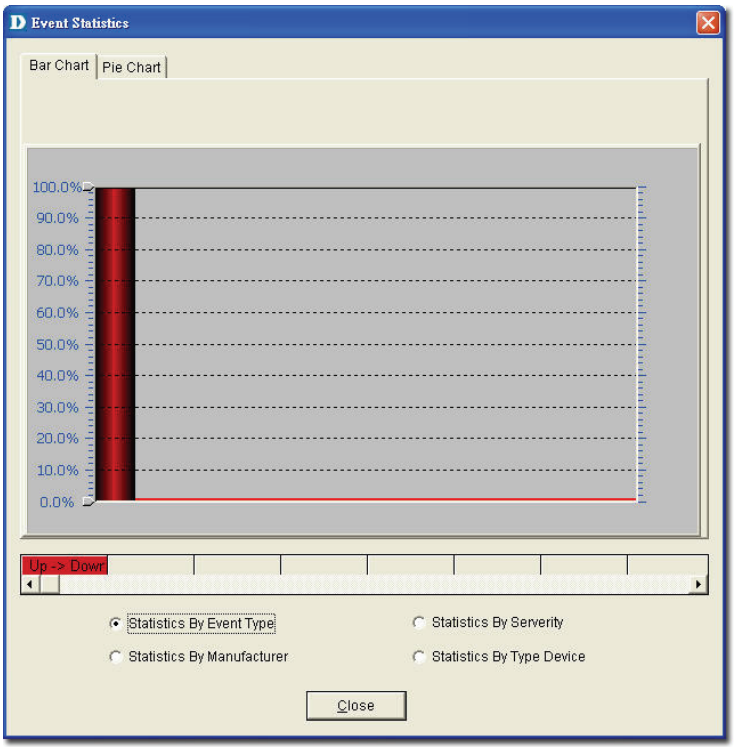


Figure 168: Event Statistics: Bar Chart screen

   - **Bar Chart:** Illustrates the event statistics by **Event Type**, **Manufacturer**, **Severity** and **Device Type**.

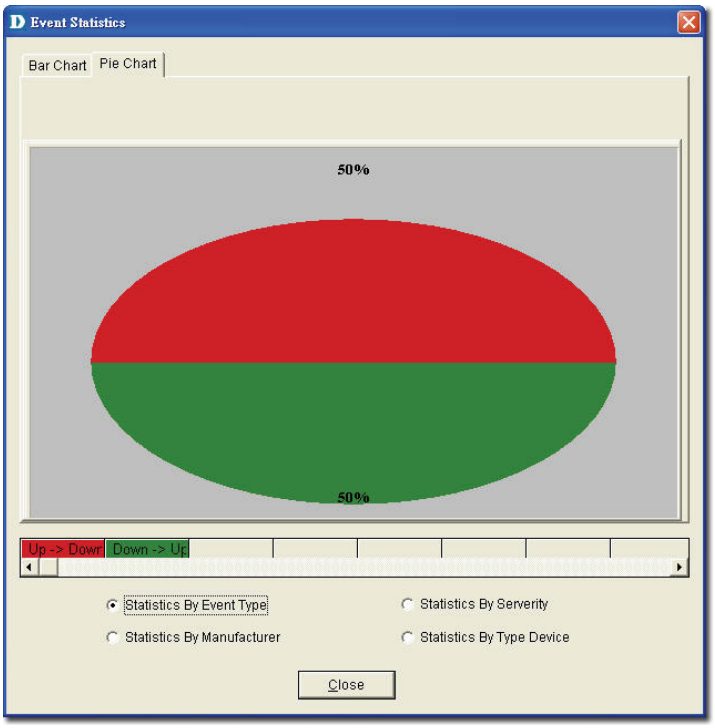


Figure 169: Event Statistics: Pie Chart screen

- **Pie Chart:** Illustrates the event statistics by **Event Type**, **Manufacturer**, **Severity** and **Device Type**.

Defining Trap Information

D-View monitors device events by polling devices by sending ICMP or SNMP packets positively and using **Trap Editor** to retrieve trap information passively.

D-View retrieves and parses trap information from devices. In order to receive and parse the private trap information from a designated device, administrators need to customize the private trap information.

To customize trap information, retrieve the definition format from the device vendor.

To define trap information:

1. Go to **System** > **Event Manager** > **Trap Editor**. The **Trap Editor** screen displays.

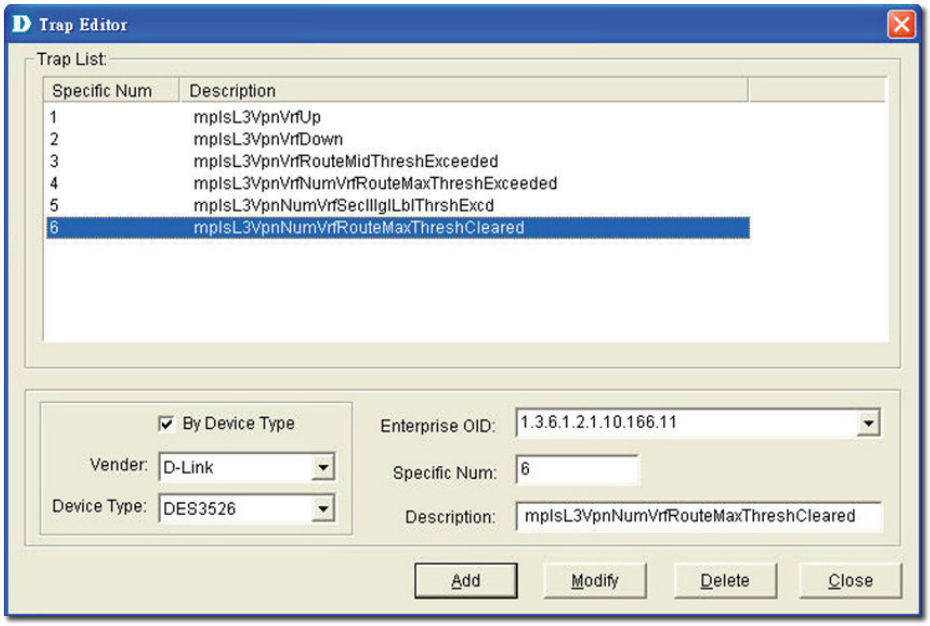


Figure 170: Trap Editor screen

2. Check **By Device Type** to select the **Vendor** name and **Device Type** from the drop-down list.
3. Enter the **Enterprise OID**. Contact D-Link support to obtain the trap OID.
4. Enter the **Specific Num**. The **Specific Num** associates with the specific trap action. The **Enterprise OID** and the **Specific Num** define the designated type of trap.
5. Type the **Description** of the message, for the designated trap.
   For example:
   The enterprise OID is **1.3.6.1.2.1.10.166.11**
   The specific number 6 here represents **mplsL3VpnNumVrfRouteMaxThreshCleared** trap message.

Locating the Switch Port

D-View provides an easy and effective way to inspect and report which network devices are connected to each switch port. Therefore it solves the problem of having to trace cables in order to see which port a network device is connected to, making it a very valuable tool for network and IT administrators.
Locate the switch port of the end user's computer with the MAC or IP address using **MAC Locator**.

1. Go to **System**> **Resource Manager** > **MAC Locator**. The **Mac Locator** screen displays.

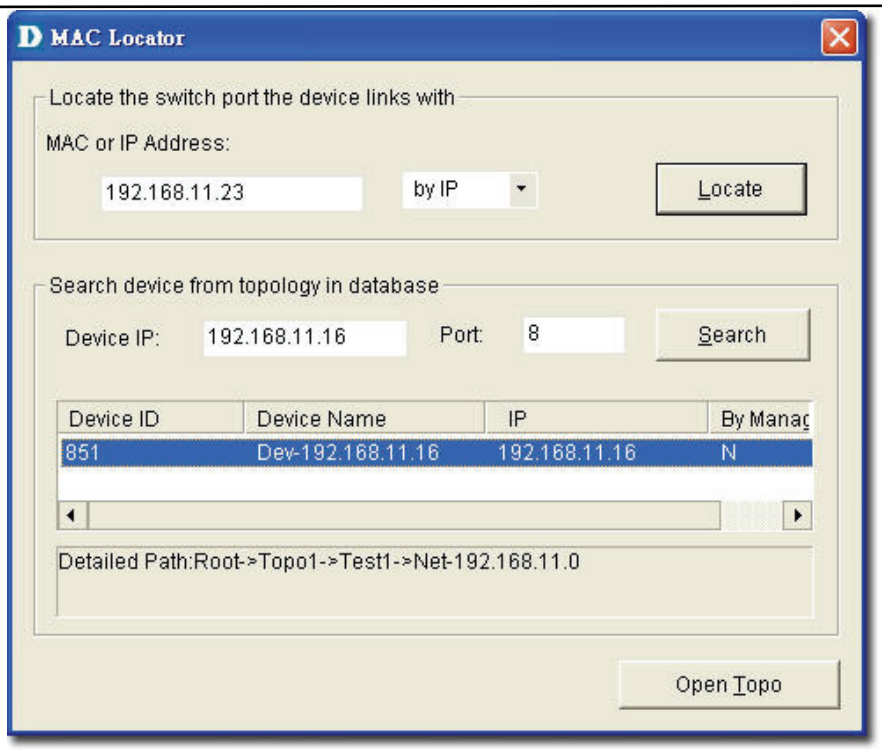


Figure 171: MAC Locator screen

2. Enter the MAC or IP address. Click **Locate**.
   D-View locates the specified device, if found.

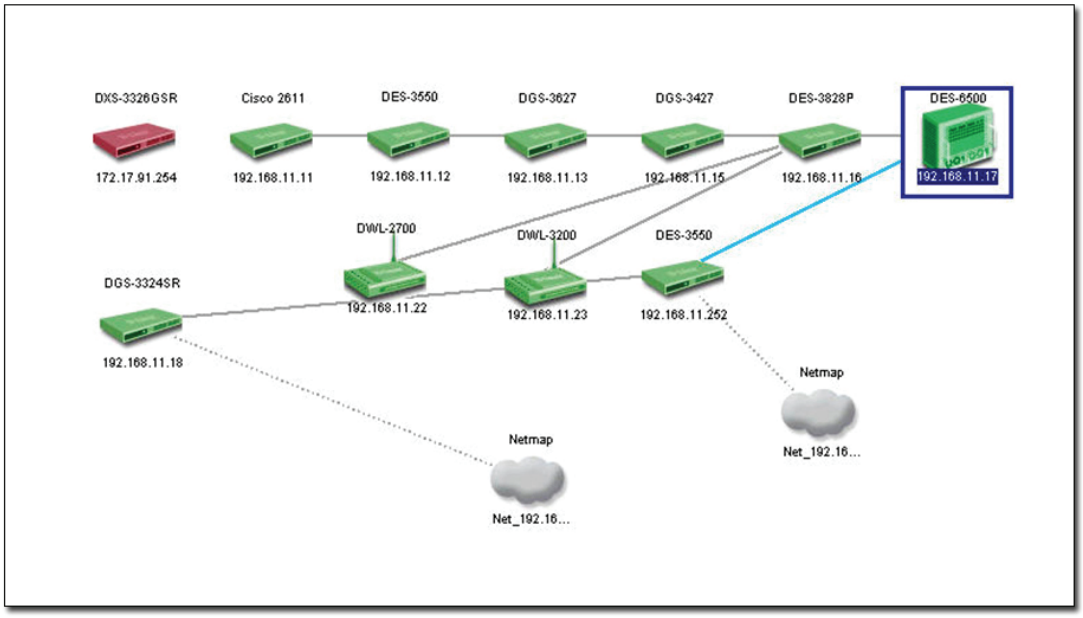


Figure 172: Specified device located in the Topology using MAC Locator

Monitoring the Link Status

D-view lets you monitor and modify the link status in a topology.

To monitor the Link Status:

1. Open the topology.
2. Go to **Topology** > **Link Label** and then select **Link Speed.** The status of the links is displayed.

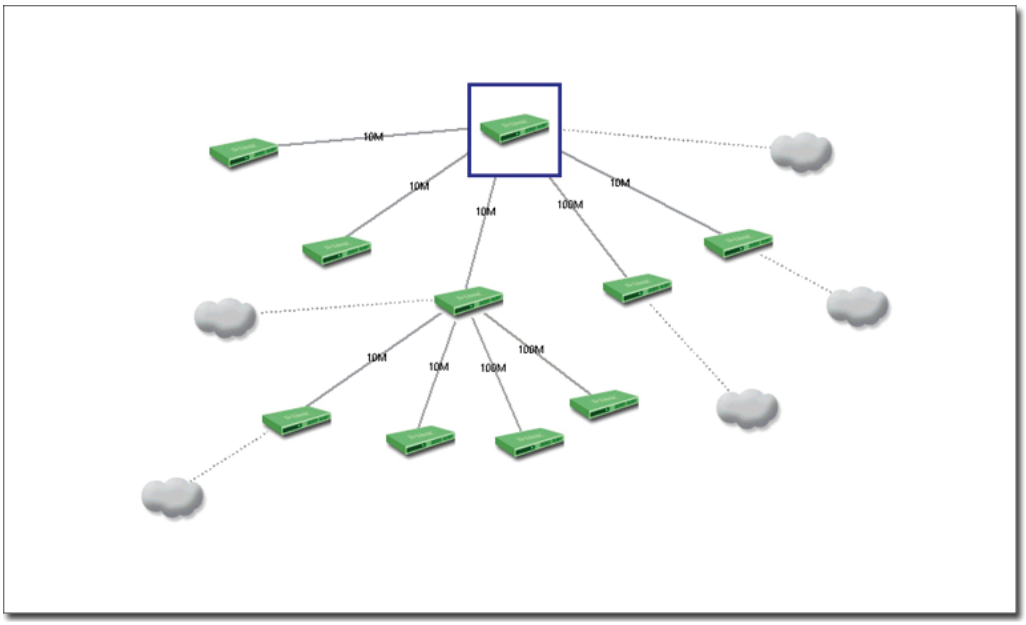


Figure 173: The Topology displays the Link status of the devices

3. Go to **Advanced** > **Link Capacity Check**, to monitor the link status of all the devices in a table.

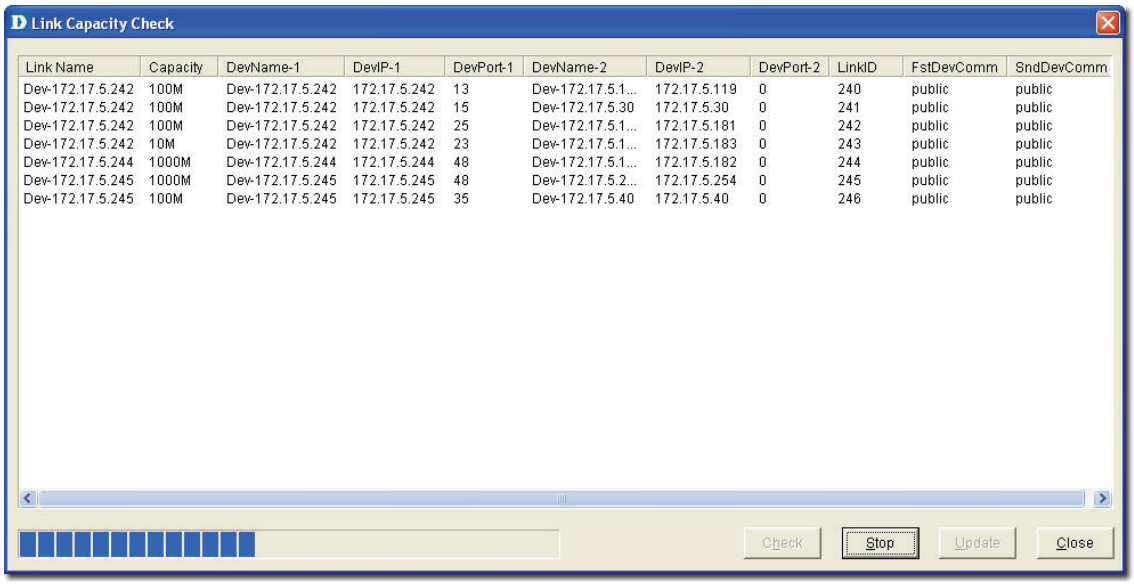


Figure 174: Link Capacity Check screen

4. Click **Check**. D-View checks the capacity of each device link port and displays the minimum capacity value of the link as seen in figure below.

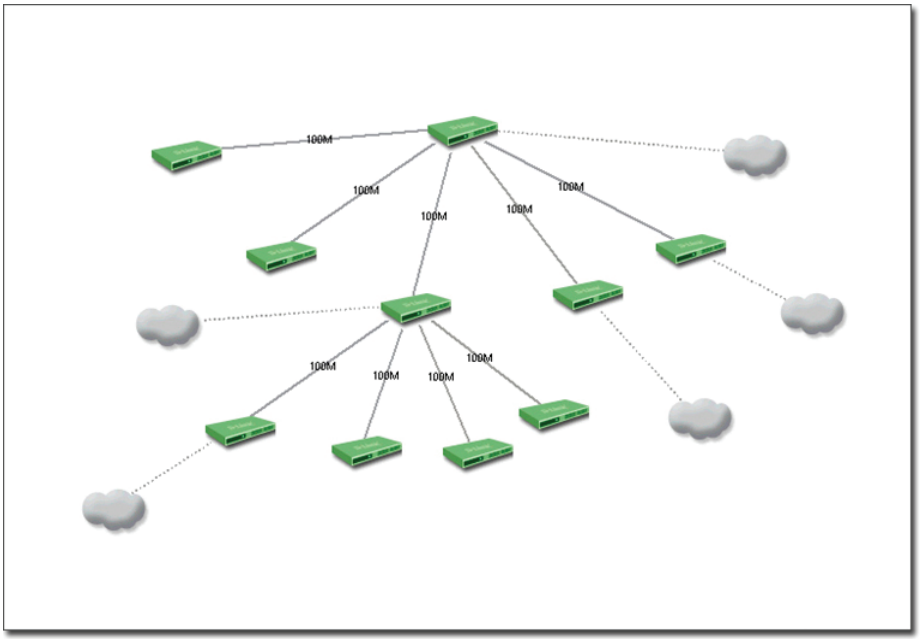


Figure 175: The Topology displays the link status after the Link Capacity check

By default, when a link is created between devices the link capacity is set to 100M.

To modify the Capacity Value:

1. Go to **Topology** > **Link Manager** > **Edit Link**. The **Edit Link** screen displays.
   OR
   In a topology, right-click on a link and then select **Property**. The **Edit Link** screen displays.

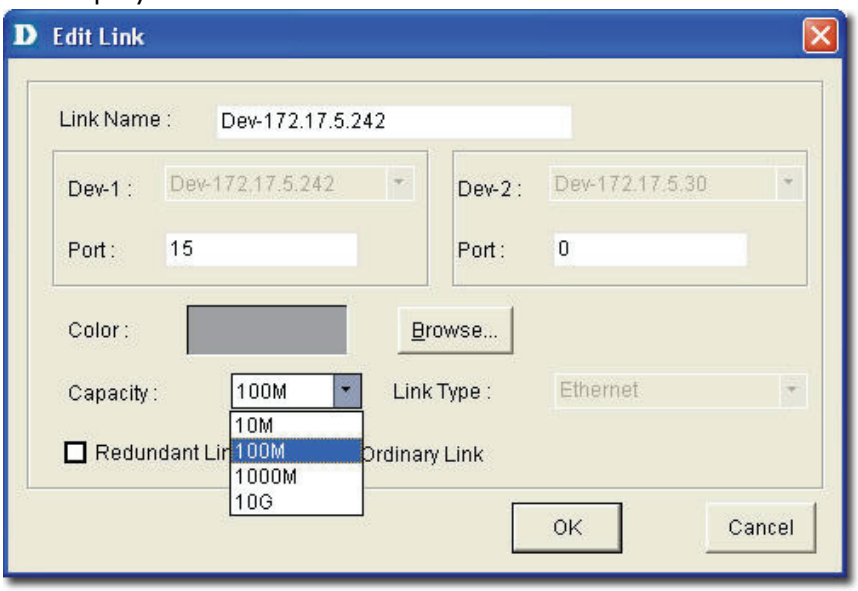


Figure 176: Edit Link screen

2. Update the **Capacity**. Select from **10M**, **100M**, **1000M**, or **10G**.
3. Click **OK**.

In order to obtain accurate results from the link capacity, ensure the port numbers between the devices are entered correctly.

Locating Devices

In D-View, you can locate devices using the Device Locator tool. Use **Device Locator** to find devices in multiple topologies by entering the **Device Name** or **IP address**.

1. Go to **System** > **Resource Manager** > **Device Locator**. The **Device Locator** screen displays.

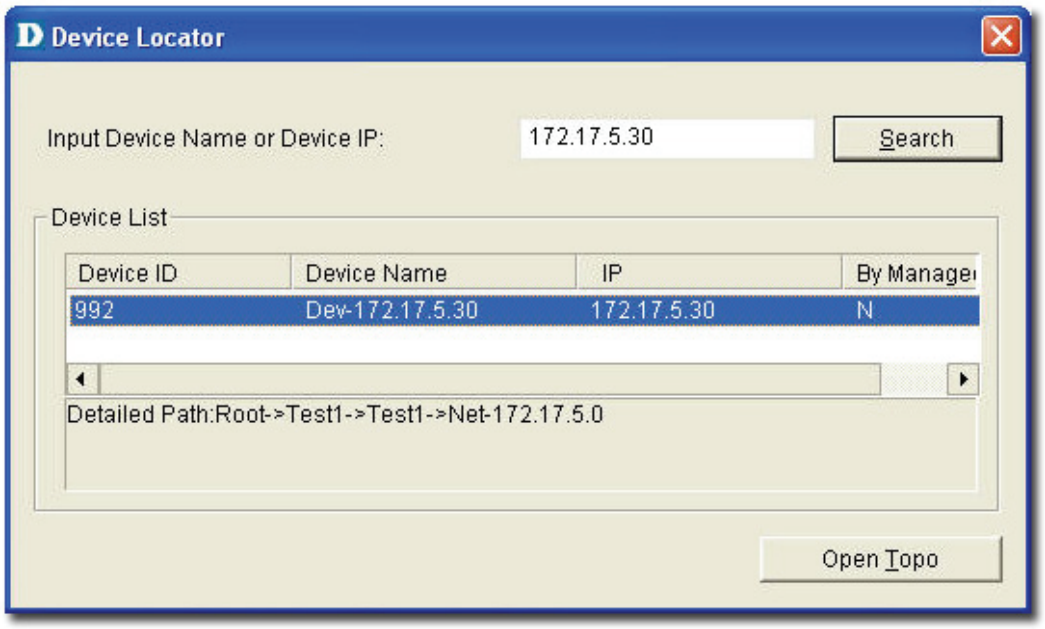


Figure 177: Device Locator screen

2. Enter the name or IP address of the device to be located.
3. Click **Search** to locate the device. The results are displayed.
4. Click **Open Topo** to locate the device in a topology.

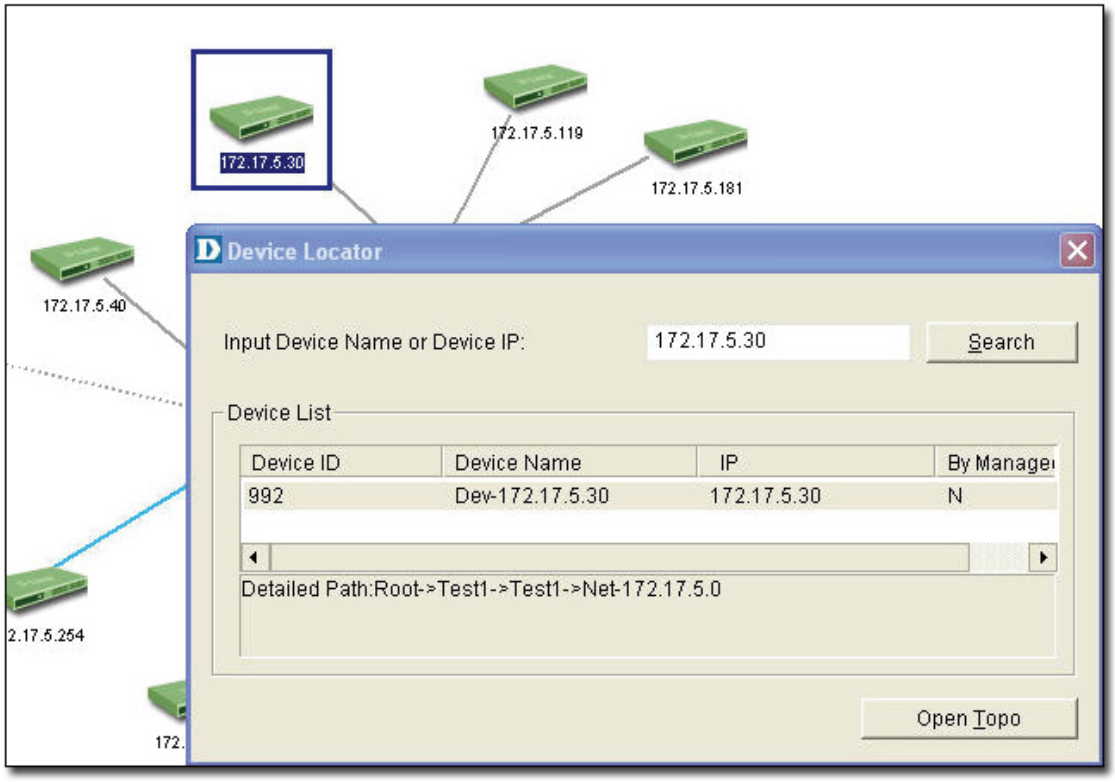


Figure 178: The Topology indicates the device located after using Device Locator tool

Entering User Information

In D-View, you can use the **Device Collector** tool to enter **User Information**.

To enter user information:

1. Go to **System** > **Resource Manager** > **Device Collector**. The **Device Collector** screen displays.
2. Use filter options to select the vendor's name and device type. A list of devices is displayed.

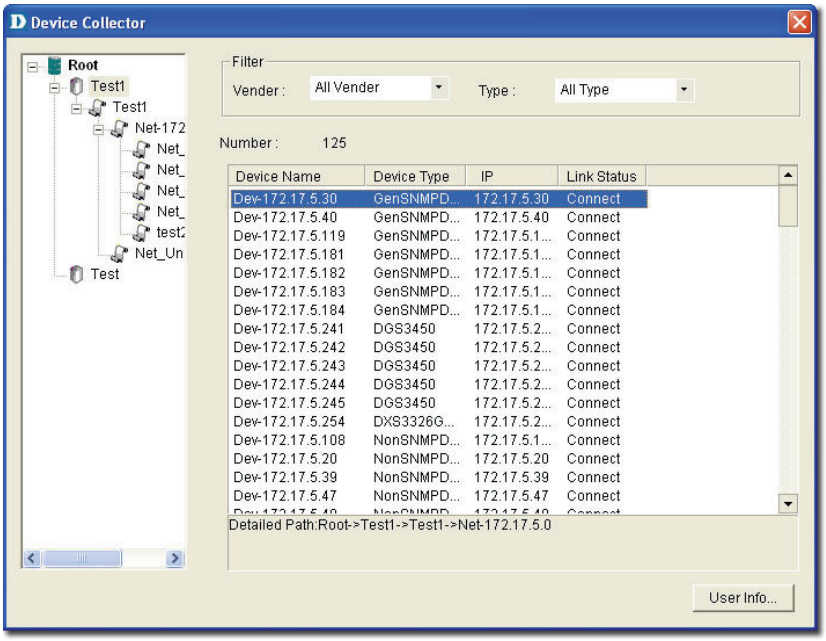


Figure 179: Device Collector screen

3. Select a device from the list and then click **User Info**. The **User Info** screen displays.

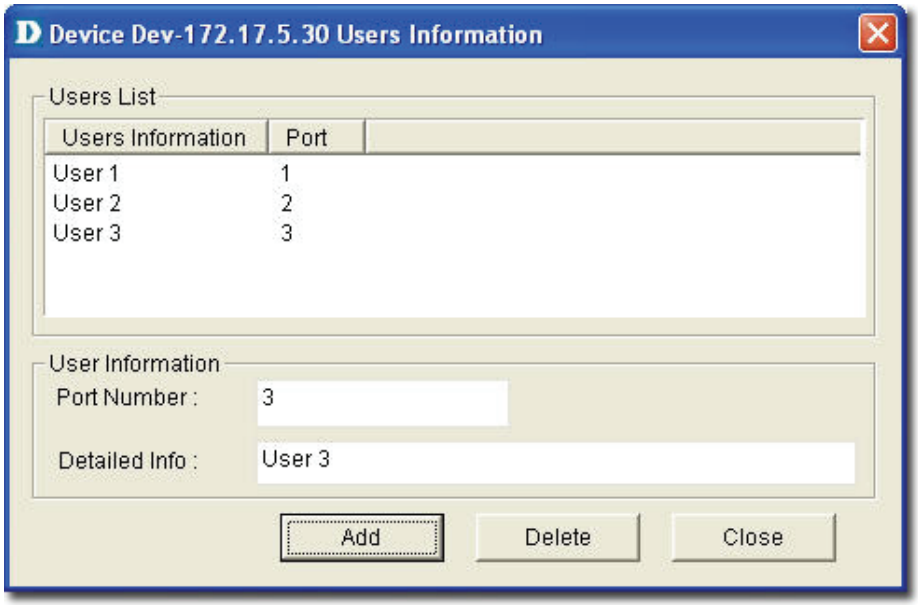


Figure 180: User Information screen

4. **Add**/**Edit**/**Delete** user information of the selected device.

Locating Users

In D-View, you can locate users using the **User Locator** tool. Use **User Locator** to find users connected with a particular device.

To Locate Users:

1. Go to **System** > **Resource Manager** > **User Locator**. The **User Locator** screen displays.

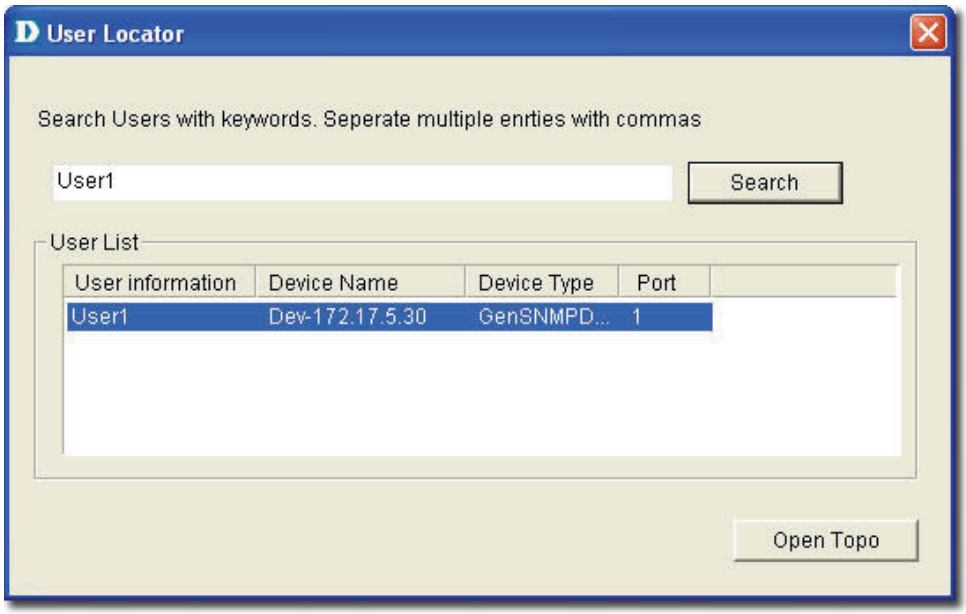


Figure 181: User Locator screen

2. Enter the user's name. Separate multiple entries with a comma (,).
3. Click **Search**. The search results are displayed.

4. Click **Open Topo** to locate the device in a topology.

User Statistics

User Statistics displays the users connected to particular devices.

To view User Statistics:

1. Go to **System** > **Resource Manager** > **User Statistics**.

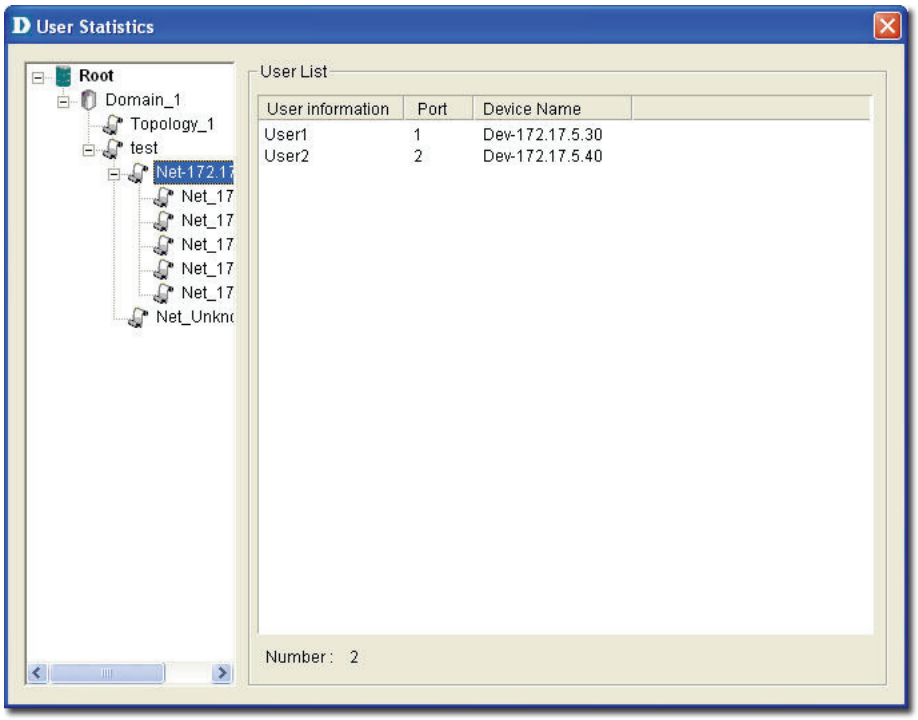


Figure 182: User Statistics screen

2. The users are displayed.

Device Statistics

Device Statistics can display information related to a vendor, buyer, or buyer date. For example, you can view all the devices sold by a particular vendor.

To view Device Statistics:

1. Go to **System** > **Resource Manager** > **Device Statistic**. The **Device Statistic** window displays.

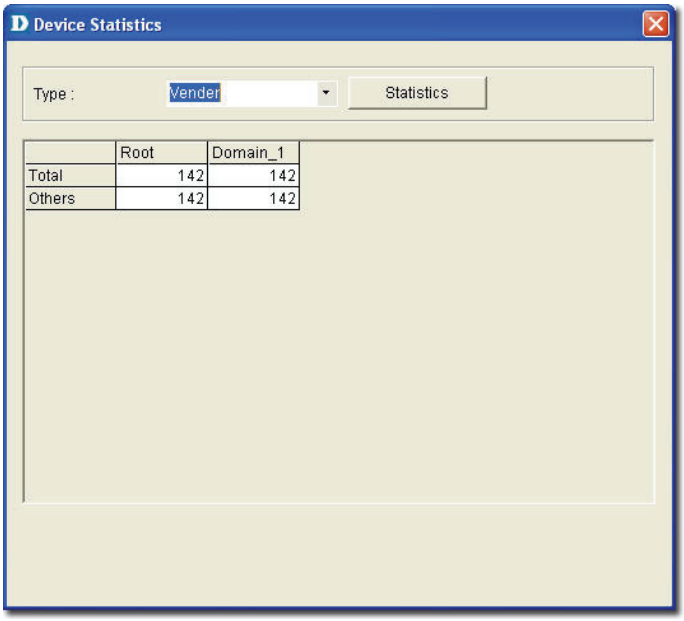


Figure 183: Device Statistic screen

2. View the devices in the domain. You can sort them by **Vendor**, **Buyer**, or **Buy Date**.

8

Basic Operations

View Options

Go to **Topology**> **View Options** to turn on or off the view options of the topology.

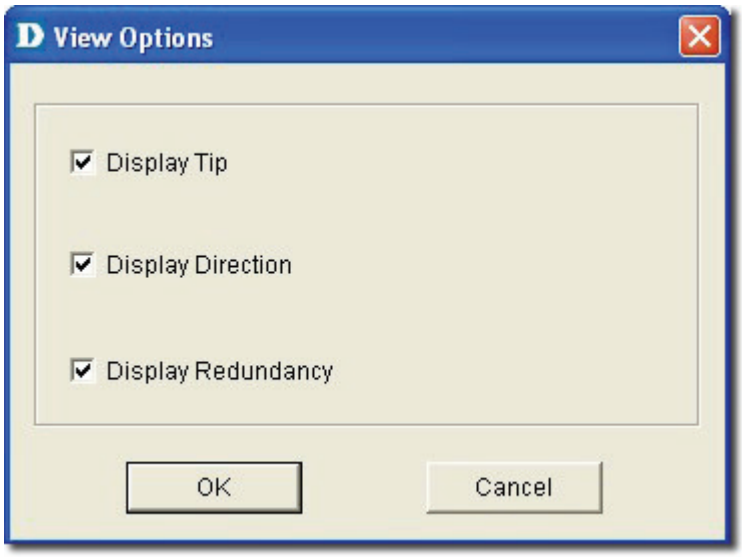


Figure 184: View Options screen

- **Display Tip:** Mouse over to view the net cell information in the topology.
- **Display Direction:** Displays the direction of link in the topology.
- **Display Redundancy:** Display the redundant link in the topology map.

Copy/Paste

Use **Copy**/**Paste** function to add devices to the topology.

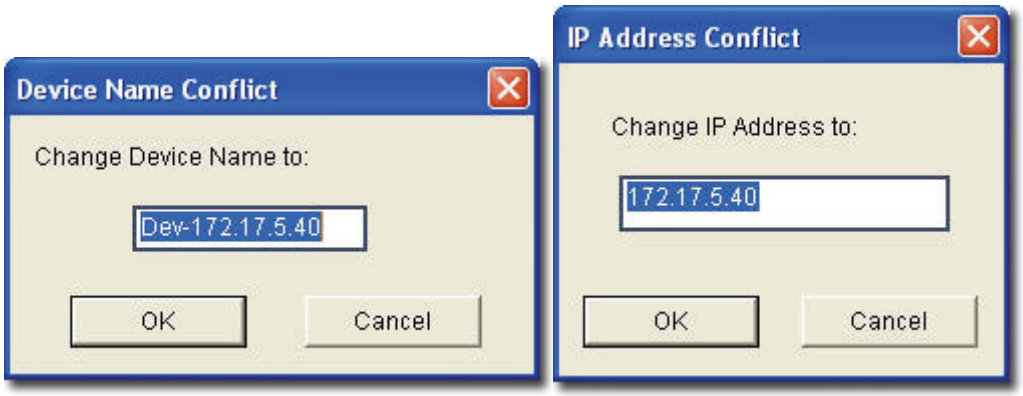


Figure 185: Device Name Conflict and IP Address Conflict

- **Copy:** Select a device and then go to **Topology** > **Copy** to copy the device icon from the topology map.
- **Paste:** Select a device and then go to **Topology** > **Paste** to paste the device icon into the opened topology.

Rename the device and IP address to paste the copied device icon in the topology.

Zoom In / Out / Fit

You can zoom in to get a close-up view of your topology or zoom out to see more.

- Go to **Topology** > **Zoom In** to zoom into the topology.
- Go to **Topology** > **Zoom Out** to zoom out of the topology.
- Go to **Topology** > **Zoom Fit** to fit the topology map in the current window.

Set Background

Go to **Topology** > **Set Background** to modify the background color of the topology.

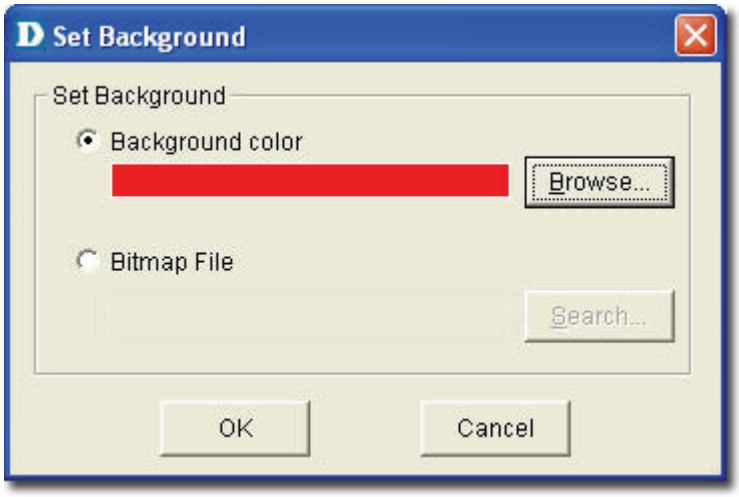


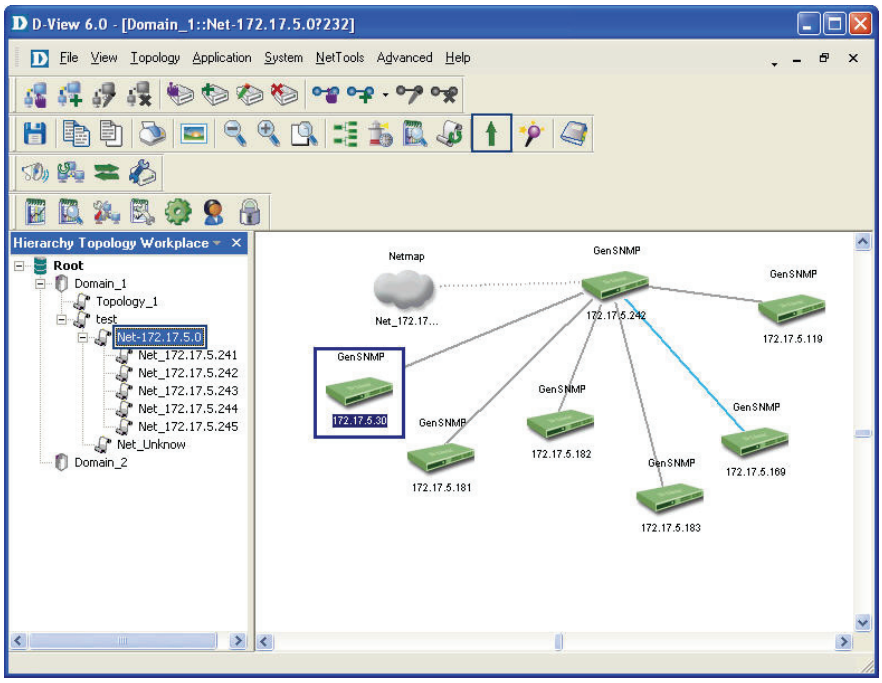
Figure 186: Set Background screen

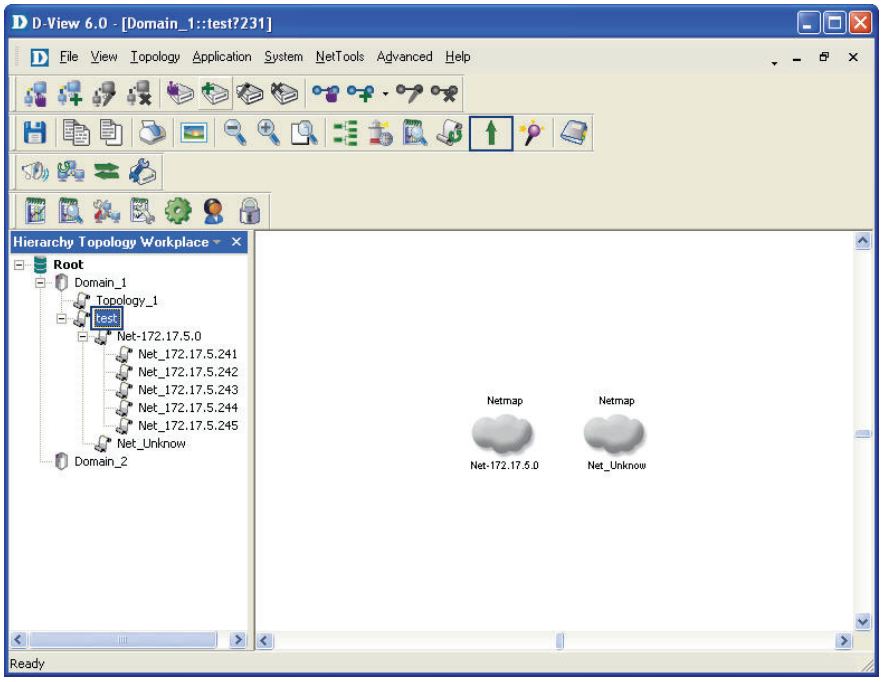
Upper Layer

Use Upper Layer to move to the parent level.

Go to **Topology** > **Upper Layer** or click from the **Main Toolbar** to get back to the first layer of the topology.

For example, if you are in the topology level, and you click Upper Layer, netmap level is displayed. Eventually, you will go to the root level.


D-View 6.0 - [Domain_1::Net-172.17.5.0?232]
File View Topology Application System NetTools Advanced Help
Hierarchy Topology Workplace
Root
Domain_1
Topology_1
test
Net-172.17.5.0
Net_172.17.5.241
Net_172.17.5.242
Net_172.17.5.243
Net_172.17.5.244
Net_172.17.5.245
Net_Unknow
Domain_2
Netmap
Net_172.17...
GenSNMP
172.17.5.242
172.17.5.119
172.17.5.30
172.17.5.181
172.17.5.182
172.17.5.169
172.17.5.183


D-View 6.0 - [Domain_1::test?231]
File View Topology Application System NetTools Advanced Help
Hierarchy Topology Workplace
Root
Domain_1
Topology_1
test
Net-172.17.5.0
Net_172.17.5.241
Net_172.17.5.242
Net_172.17.5.243
Net_172.17.5.244
Net_172.17.5.245
Net_Unknow
Domain_2
Netmap
Net-172.17.5.0
Netmap
Net_Unknow
Ready

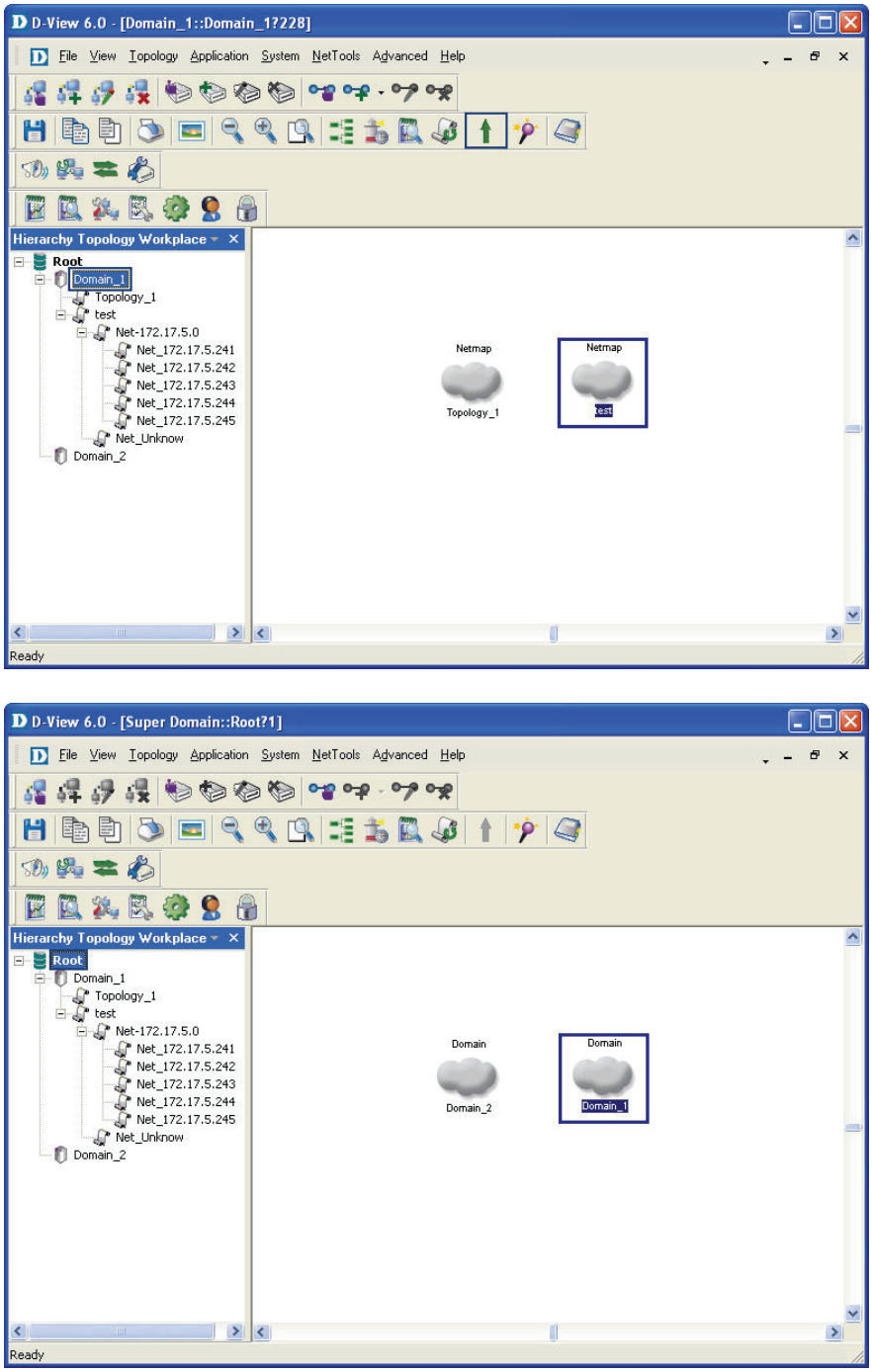


Figure 187: Sequence of steps navigating from the topology level to the domain.

System Log

The **System Log** stores logged events. The log records events such as additions, deletions, updates or error messages. Helps users identify and diagnose the source of current system.

To view logged events of the topology:

Go to **System** > **System Log**. The **System Log** screen displays.

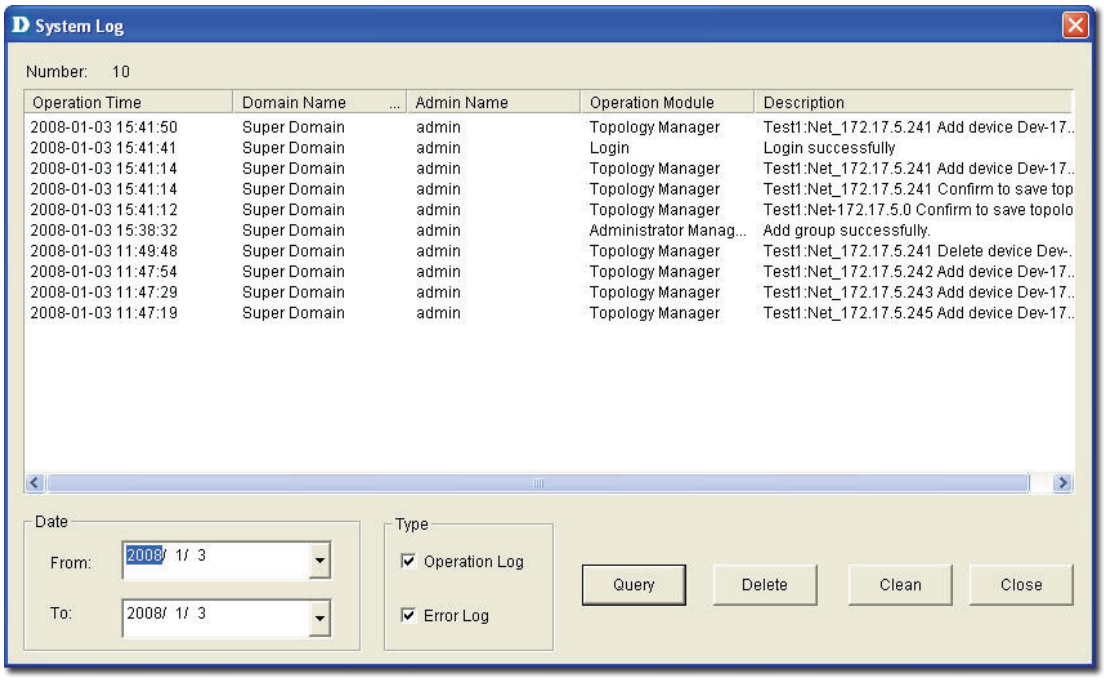


Figure 188: System Log screen

1. Select the **From** and **To** date, to view the events occurred in that time interval.
2. Select the type of log, **Operation** or **Error Log** or both.
3. Click **Query** to find the events that match the search criteria.
4. Click **Clean** to clear log messages.

Administrator Manager

Using the **Administrator Manager**, authorized administrators can create user groups. Administrator's define the access rights for each user group and then add users into the group.

To create a User Group:

1. Go to **System > Administrator Manager.** The **Administrator Manager** screen displays.

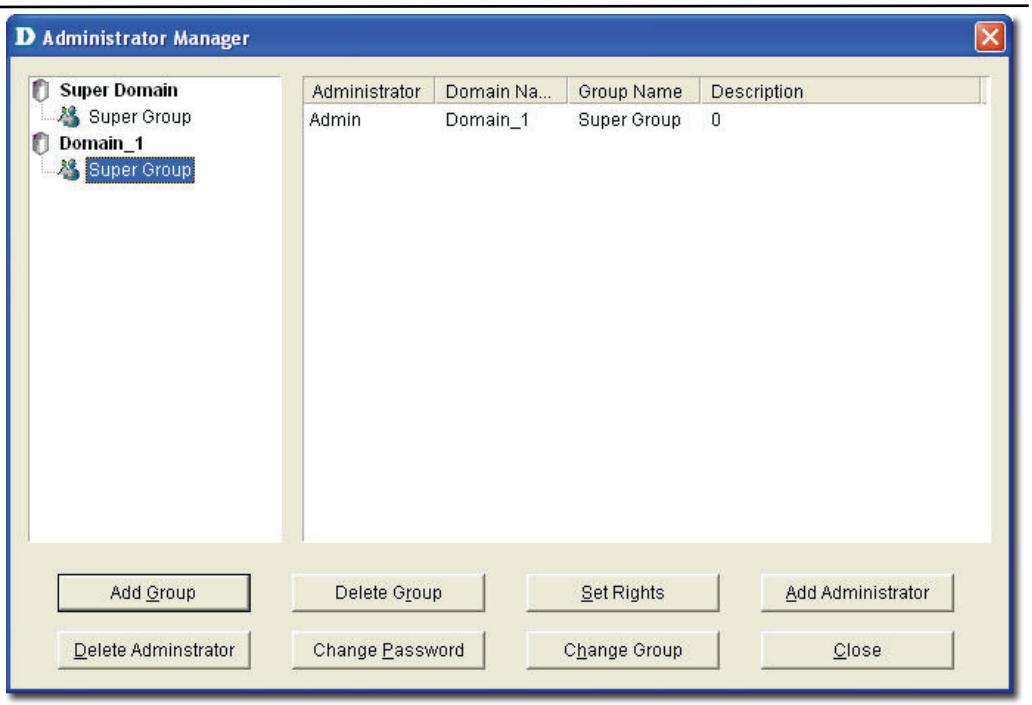


Figure 189: Administrator Manager screen

2. Select the domain for which you want to add a group.
3. Click **Add Group**. The **Add Group** screen displays.

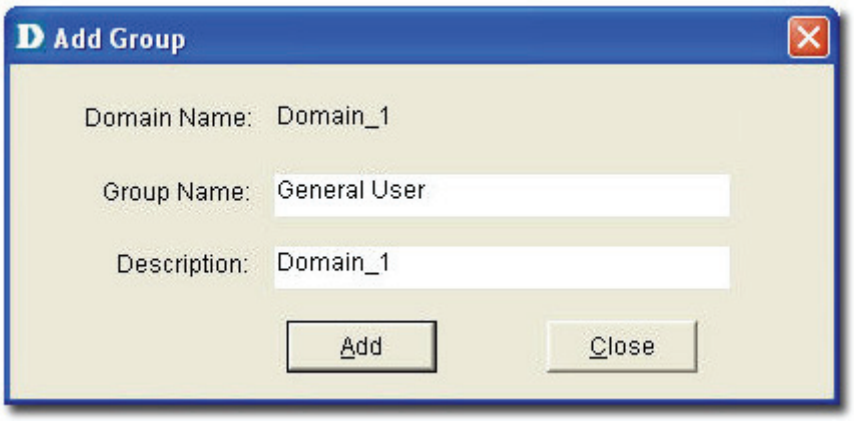


Figure 190: Add Group screen

4. Type the name of the group with description to which you want to assign this right and click **Add** to continue.

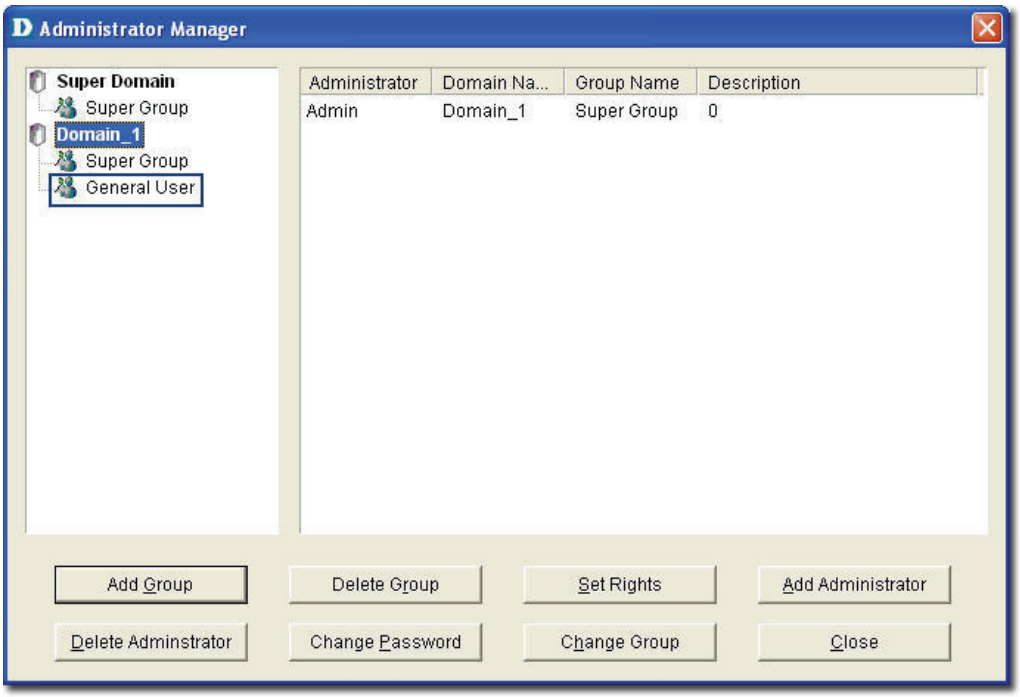


Figure 191: Administrator Manager: Add Group screen

5. Click **Add Administrator** to provide access rights to the user. The **Add Administrator** screen displays.

Figure 192: Add Administrator screen

6. Update the fields and then click **Add** to create an administrator account.
7. Click **Set Rights** in the Administrator Management screen. The **Set Rights** screen displays.

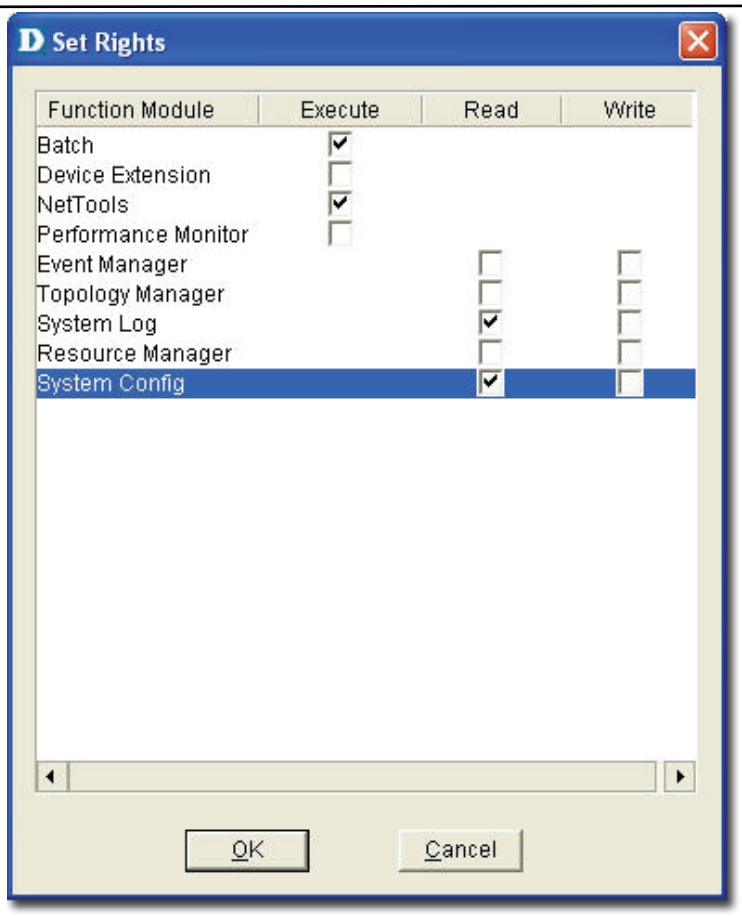


Figure 193: Set Rights screen

8. Check the specific functional modules boxes to assign rights (execute, read, write) to the user.
9. Click **OK** to apply the changes.

The changes made are reflected in the **System Log**.

Changing Password

D-Link recommends changing the password immediately after logging on for the first time and also on a frequent basis after that.

To change the password:

1. Go to **System** > **Change Password**.

Figure 194: Change Password screen

2. Enter the old password and then type your new password.

Restoring and Backing Up D-View

To restore and back up Topology data:

1. Select a topology.
2. Go to **Application** > **Topo Export/Import** to restore & back up topology data.
3. For data in D-View：
    a. **D-View 6.0 Standard Edition** - Back up **dvision3.mdb** file, in the installation folder. The file can be used to restore D-View by overwriting the current database dvision3.mdb.
    b. **D-View 6.0 Professional Edition**
    Backup Procedure:
        - Use the SQL Server 2000/2005 management tool to back up **Division3.mdf** and **Division3_Log.ldf** files.

    Restore Procedure:
        - Use the SQL Server 2000/2005 management tool to restore **Division3.mdf** and **Division3_Log.ldf** files.
        - Restart the **SQL Server** service.

NetTools

Device Discovery

D-View identifies a SNMP supporting device as a **GenSNMPDevice** and an ICMP supporting device as a **NonGenSNMPDevice**.
Use the **Device Discovery** tool to search and identify the type of devices in the designated network.

To manually add devices into the opened topology:

1. Go to **NetTools** > **Device Discovery**. The **Device Discovery** screen displays.

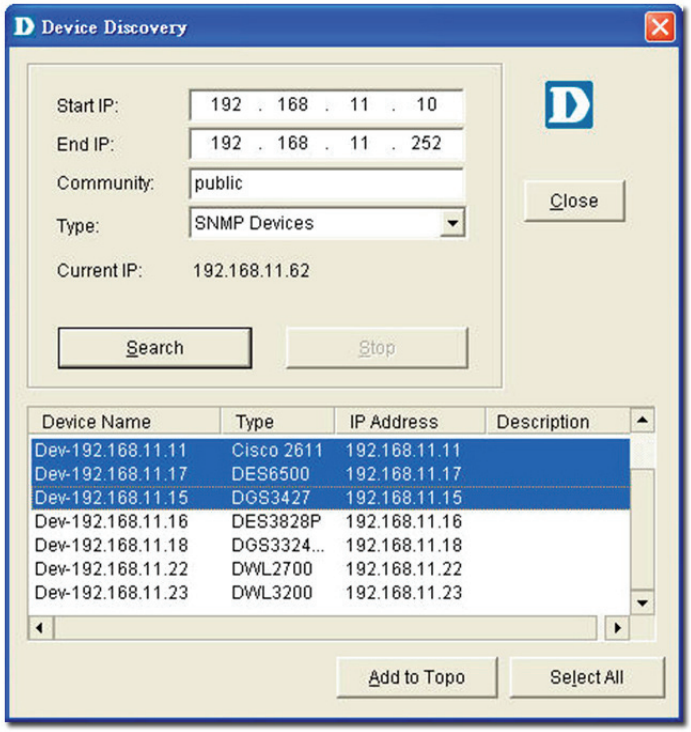


Figure 195: Device Discovery screen

2. Enter the IP address range to locate devices.
3. Enter the **Community** name.
4. Select the device **Type**.
5. Click **Search** to locate the devices based on the search criteria.
6. Select and click **Add Topo** to add devices to the topology.

Trace Route

The **Trace Route** utility enables you to view a network packet that is in transit and determine the number of hops necessary for that packet to reach its destination.

To Trace Routers:

Go to **NetTools** > **Trace Route** to open the Trace Route function.

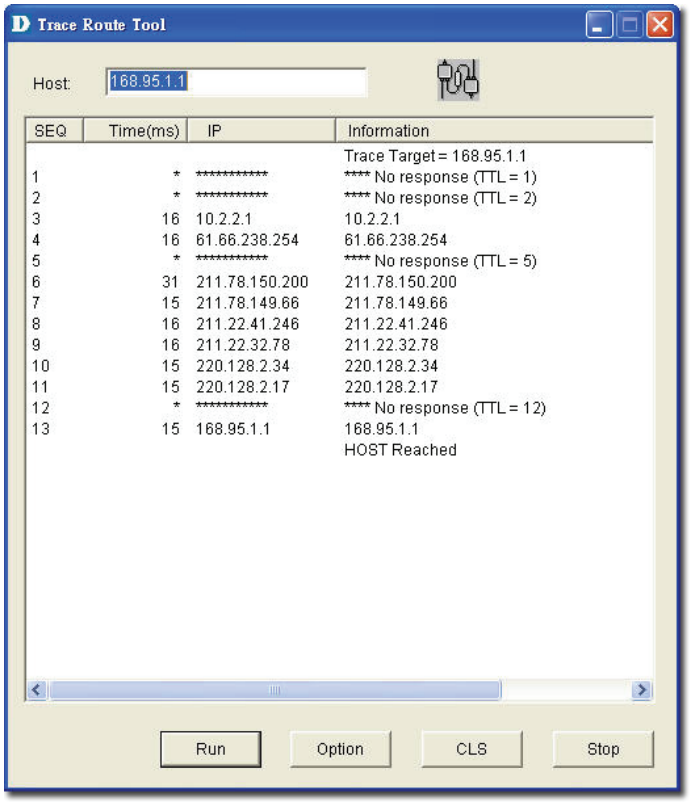


Figure 196: Trace Route Tool screen

1. Enter the host address and click **Run** to trace the routers.
2. Select **Option** to configure the ICMP parameters.

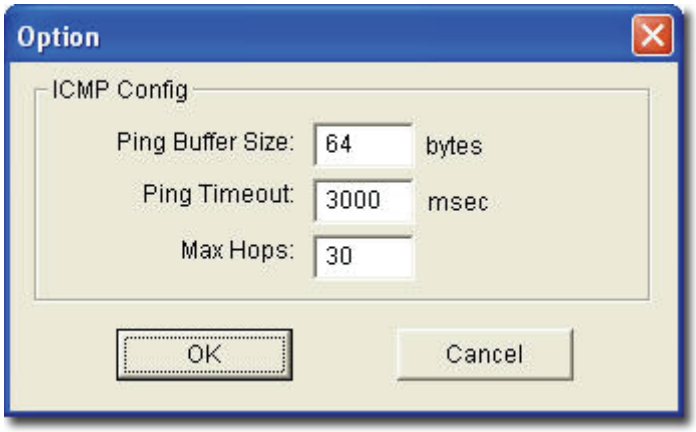


Figure 197: Option screen

3. Modify and customize the **Ping Buffer Size**, **Ping Timeout** and **Max Hops** parameters according to your requirements.
4. Click **CLS** to clear the list.
5. Click **Stop** to stop the search.

TFTP

The TFTP server enables the client to upload or download configuration files between the server and the client.

1. Go to **NetTools** > **TFTP** to call the TFTP Server tool.

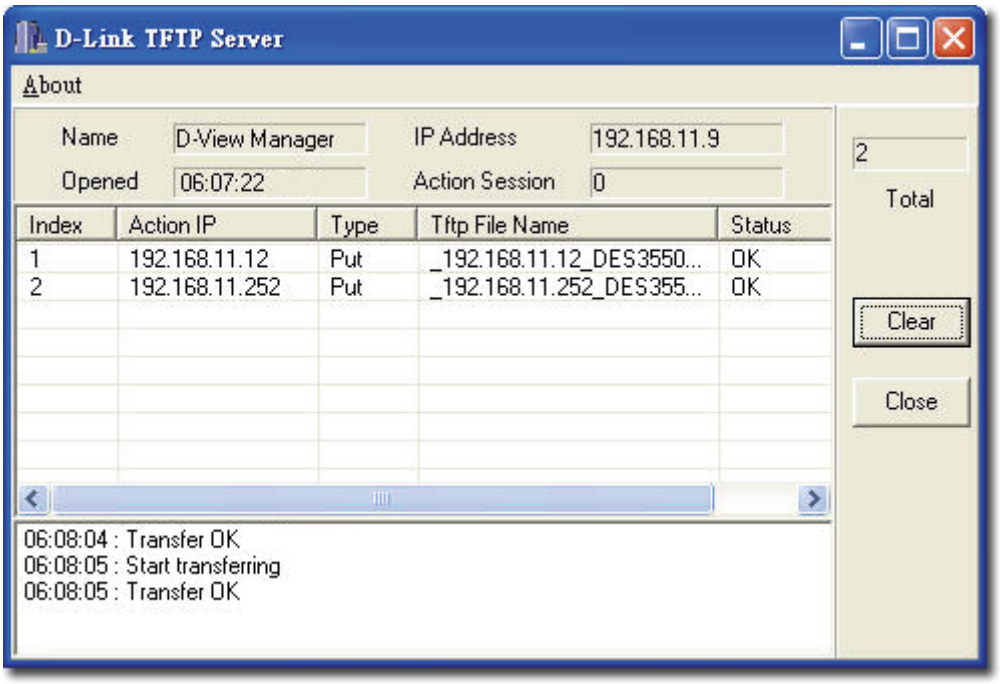


Figure 198: D-Link TFTP Server screen

- **Index:** Displays the number of connections between the devices and the TFTP server
- **Action IP:** Displays the device IP address.
- **Type:** Get/Put action of the configuration files.
- **TFTP File Name:** The uploaded or downloaded files through the TFTP server.
- **Status:** Displays the file transfer status.

2. Click **Clear** to erase the actions.

Retrieving ARP information

D-View provides a tool to retrieve the **ARP** (Address Resolution Protocol) information from devices and then create a table for the network. The table lists the IP and MAC addresses of all the devices in the topology.

To retrieve the ARP information:

1. Go to **Advanced** > **All of ARP Info**. The **ARP Information Retrieve** screen displays.

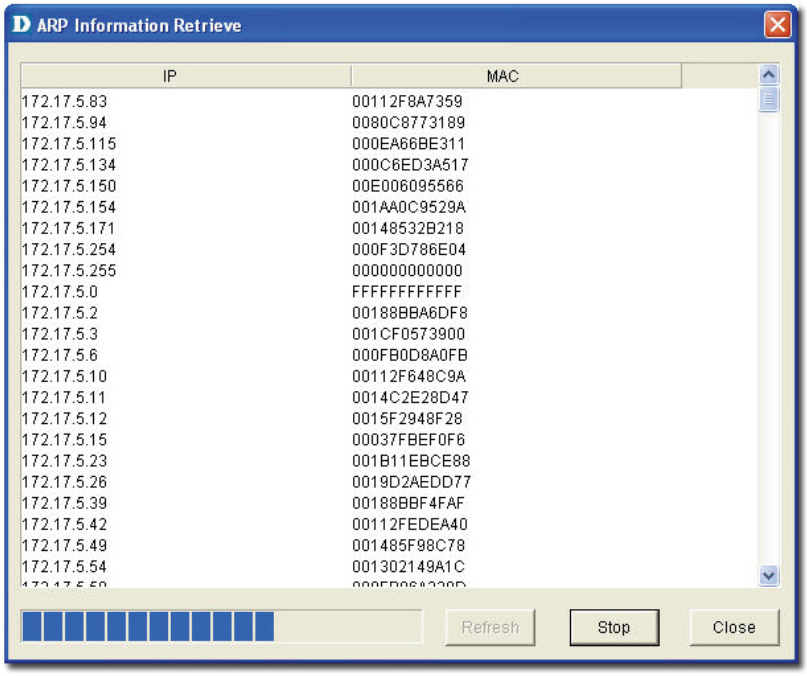


Figure 199: ARP Information Retrieve screen

2. Click **Refresh** to refresh the information. Click **Stop** to stop retrieving information.

Net Toolbox

D-View provides two ways to manage a device in the topology – Telnet and Web. Using **Net Toolbox**, administrators can configure the method of management for each device. **Net Toolbox** also allows administrators to ping device from the topology.

To select the management method:

1. Select the device you want to manage.
2. Go to **NetTools** > **Net Toolbox** to open the Toolbox

Figure 200: Net Toolbox screen

3. Enter the IP address of the device to manage.
4. Click **Telnet** or **Web.**

   You can also Ping the device from here.

Port Packet Monitor

D-View helps you monitor and troubleshoot Switch Ports for traffic, utilization and errors of a specific device. D-View pinpoints the port flow in real time and identifies their impact on the network.

Ensure the devices support RFC1213 to monitor the port flow in devices.

To monitor the Port Packet flow:

1. Go to **NetTools** > **Port Packet Monitor**. The **Port Monitor** screen displays.

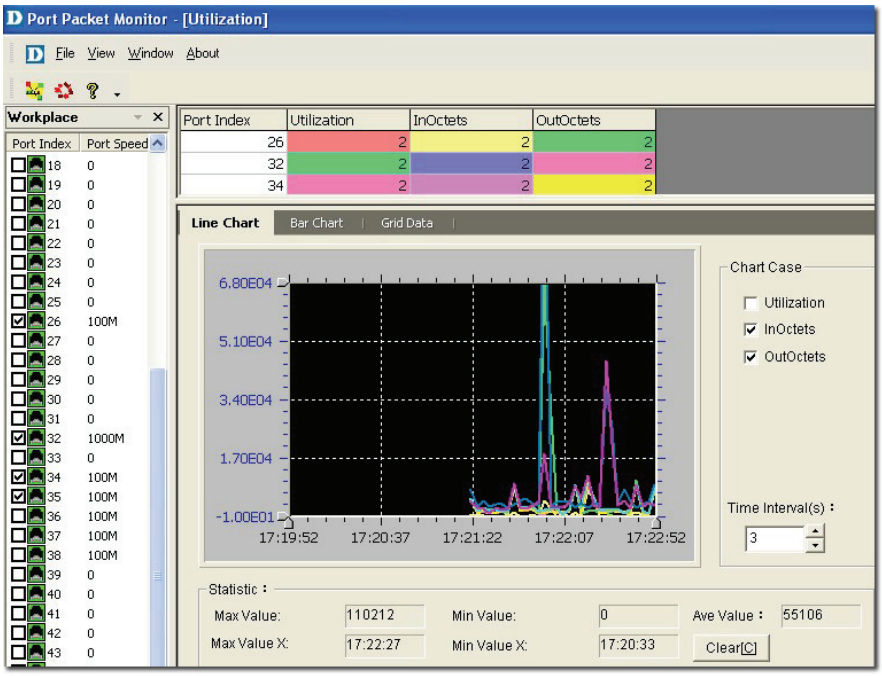


Figure 201: Port Packet Monitor: Line Chart screen

2. Select the ports and then click the **Utilization** button from the toolbar.

The formula to calculate the port percentage usage.

Utilization: *(InOctets + OutOctets)*8 / Port Speed / Time Interval*

- **InOctets:** The total number of octets received, including framing characters
- **OutOctets:** The total number of octets transmitted, including framing characters.

3. Set the **Port Packet** options. These values are calculated tracking the number of packets received and/or transmitted over a period of time.
   - **Port Index:** Represents the diameter of the network cable.
   - **Color:** Represents the different port packet types.
   - **InUcastPkts:** Number of subnetwork-unicast packets delivered to a higher-layer protocol.

- **InNUcastPkts:** Number of non-unicast packets delivered to a higher-layer protocol.
- **InDiscard:** Number of packets which are chosen to be discarded to prevent from entering the higher-layer protocol.
- **InErrors:** Number of error packets.
- **InUnknown Packets:** Number of unclassified/unknown packets discarded.
- **OutUcastPkts:** Number of out-going packets transmitted from higher-level protocols to a subnetwork-unicast address.
- **OutNUcastPkts:** Number of out-going packets transmitted from higher-level protocols to a non-unicast address.

4. Click **Clear[C]** to clear the current data on the graph.

Line Chart

The statistical graph (X-Y) shows the usage of packets of a specified device in real time.

- **Port Index:** Displays the number of ports of a specific device.
- **Port Speed:** Displays the link speed between devices.
- **Max/Min Value:** Displays the maximum/minimum number of packet flow in real time.
- **Max/Min Value X:** Displays the current time stamp of the packet flow graph.
- **Chart Case:** Filter options to monitor the packet flow.
- **Time Interval:** Enter the time period to refresh the packet flow.

Bar Chart

The **Bar Chart** displays the percentage of packet flow in real-time.

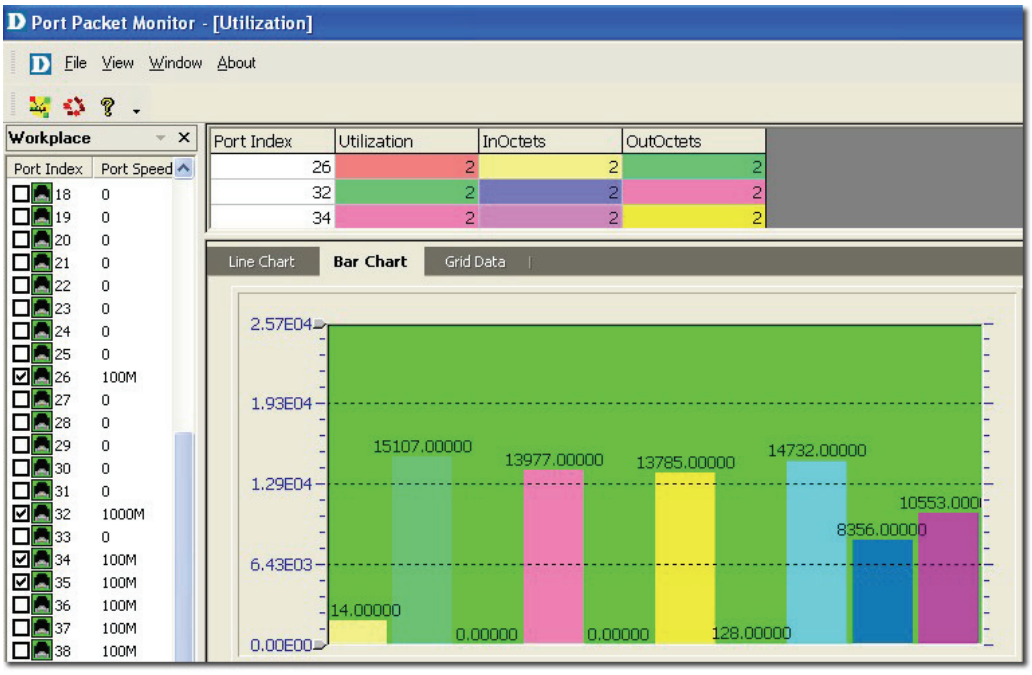


Figure 202: Port Packet Monitor: Bar Chart screen

Grid Data

The **Grid Data** shows the packet flow in a table format. Click **Packet Info** to view the packet type options.

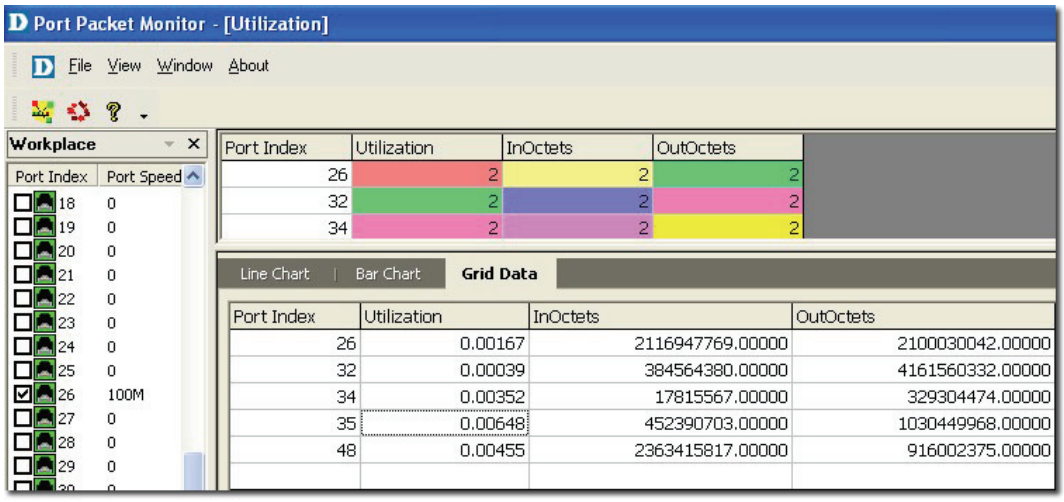


Figure 203: Port Packet Monitor: Grid Data screen

Performance Monitor

The **Performance Monitor** tool is a comprehensive bandwidth performance management application that allows you to directly view the real-time statistics of your network. D-View's **Performance Monitor** tool will monitor and collect data from routers, switches, servers, and any other SNMP-enabled device.

Ensure the RMON status of the devices is enabled to start monitoring devices.

To monitor the performance of devices:

1. Go to **NetTools > Performance Monitor**. The **Performance Monitor** screen displays.

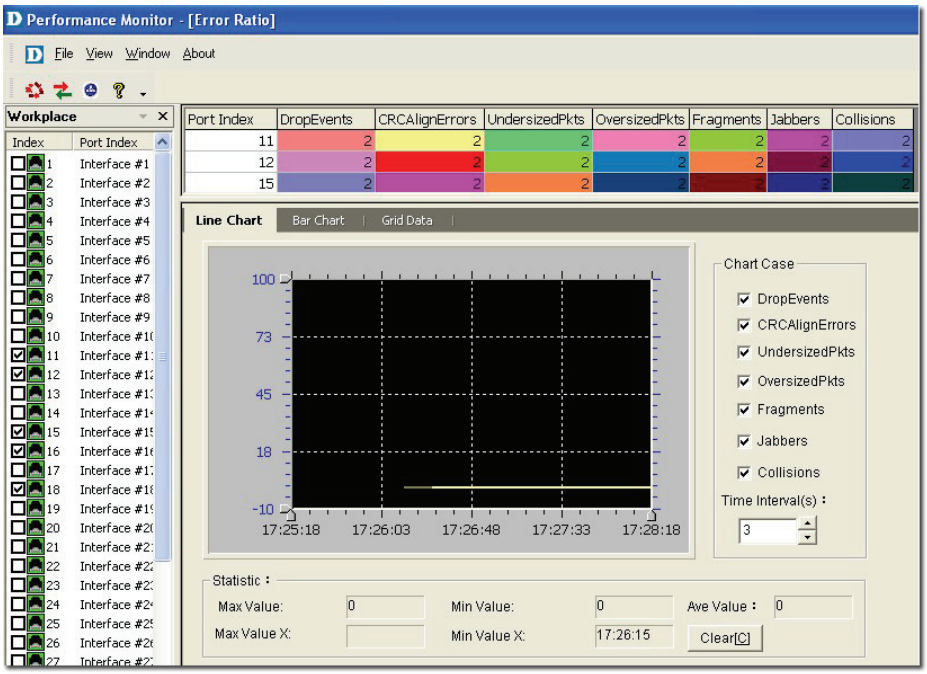


Figure 204: Performance Monitor screen

2. Select the ports and then click the **Errors Ratio** button from the toolbar.

   The graph displays a list of different types of error packets.
3. Set the **Port Packet** options. These values are calculated tracking the number of packets received over a period of time.
   - **Drop Events:** Represents the total number of events, when packets are dropped due to lack of resources.
   - **CRCAlignErrors:** Represents the total number of packets received that are between 64 and 1518 octets in length. These include packets of either a bad **Frame Check Sequence** (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
   - **UndersizePkts:** Represents the total number of packets received that are less than 64 octets in length.
   - **OversizePkts:** Represents the total number of packets received that are longer than 1518 octets in length.
   - **Segments:** Represents the total number of packets received that are less than 64 octets in length. These include packets of either a bad **Frame Check Sequence** (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
   - **Jabbers:** The total number of packets received that are longer than 1518 octets in length. These include packets of either a bad **Frame Check Sequence** (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
   - **Collisions:** An estimate of the total number of collisions on this Ethernet segment.
4. Click **Clear[C]** to clear the current data on the screen.

Line Chart

The Statistical graph (X-Y) shows the usage of packets of a specified device in real time.

- **Port Index:** Displays the number of ports of a specific device.
- **Port Speed:** Displays the link speed between devices.
- **Max/Min Value:** Displays the maximum/minimum number of packet flow in real time.
- **Max/Min Value X:** Displays the current time stamp of the packet flow graph.
- **Chart Case:** Filter options to monitor the packet flow.
- **Time Interval:** Enter the time period to refresh the packet flow.

Bar Chart

The **Bar Chart** displays the percentage of packet flow in real-time.

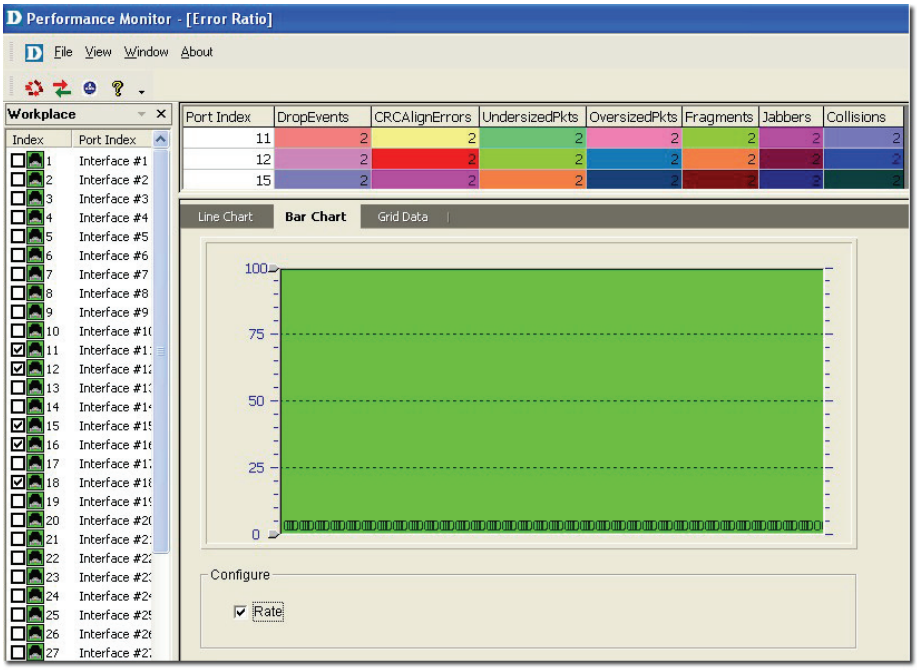


Figure 205: Performance Monitor: Bar Chart screen

Grid Data

The **Grid Data** shows the packet flow in a table format.

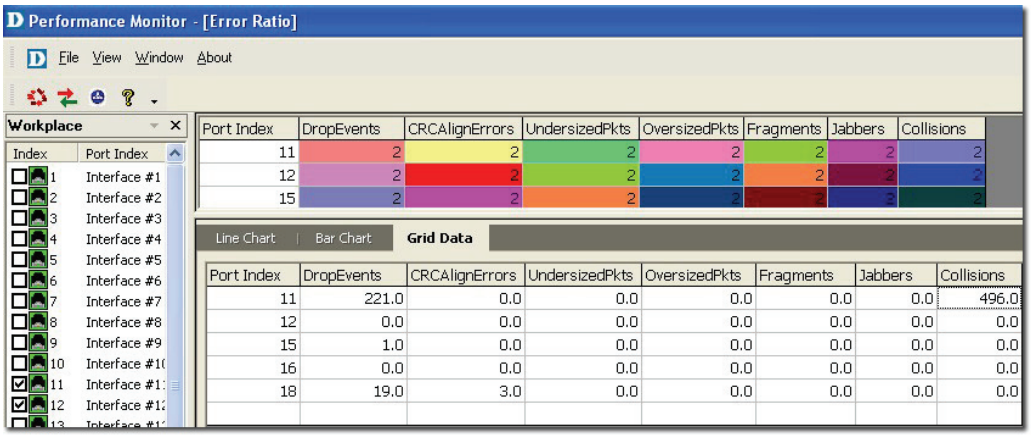


Figure 206: Performance Monitor: Grid Data screen

Data Distribution Chart

The **Data Distribution Chart** monitors packet types of different sizes received by their designated ports.

1. Click the **Data Distribution** button from the toolbar. The **Data Distribution Chart** screen displays.

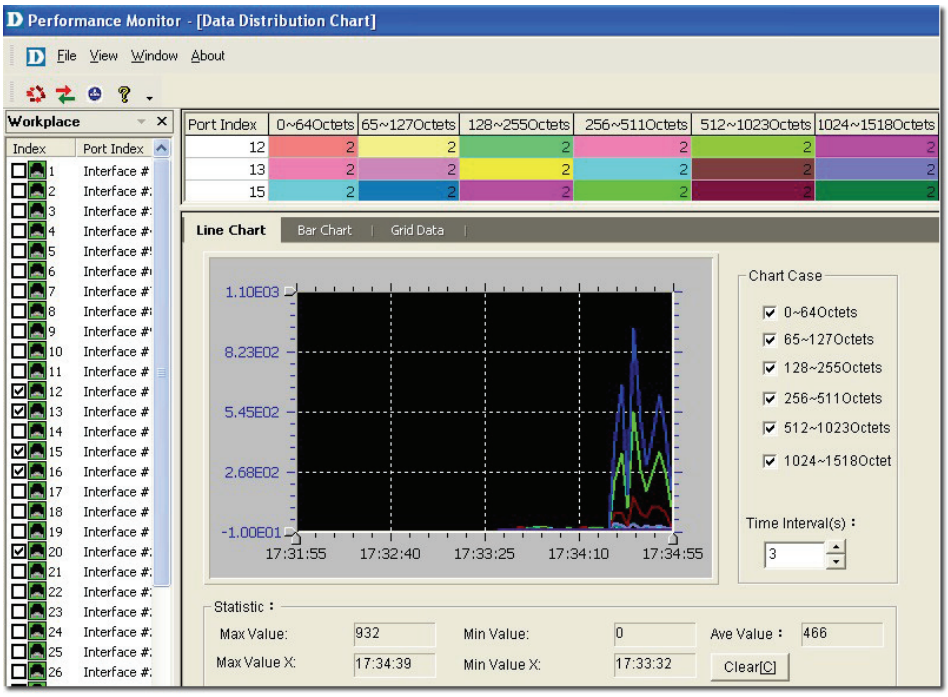


Figure 207: Performance Monitor: Data Distribution Chart screen

2. The packets are classified by its length:
   - **0~64Octets:** Total number of packets received that are 64 octets in length.
   - **65~127Octets:** Total number of packets received, between 65 and 127 octets in length.
   - **128~255Octets:** Total number of packets received, between 128 and 255 octets in length.

- **256~511Octets:** Total number of packets received, between 256 and 511 octets in length.
- **512~1023Octets:** Total number of packets received, between 512 and 1023 octets in length.
- **1024~1518Octets:** Total number of packets received, between 1024 and 1518 octets in length.

Port Flow Chart

The **Port Flow Chart** retrieves the statistical performance data to monitor the designated ports' performance status.

1. Click the **Port Flow** button from the toolbar. The **Port Flow** screen displays.

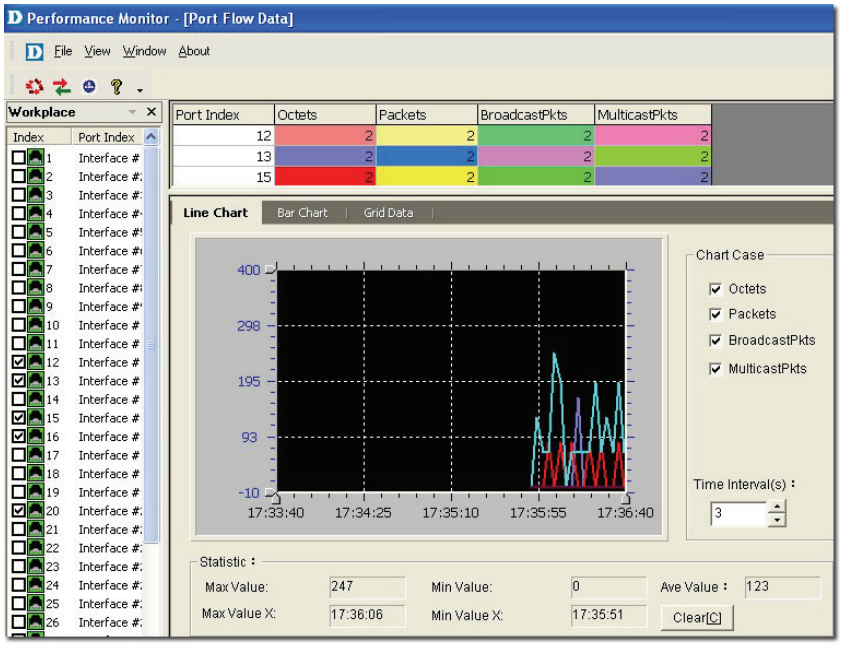


Figure 208: Performance Monitor: Port Flow Data screen

The different types of packets displayed in the graph are:

- **Octets:** Total number of octets received.
- **Packets:** Total number of packets received.
- **BroadcastPkts:** Total number of packets received and directed to the broadcast address.
- **MulticastPkts:** Total number of packets received and directed to a multicast address.

9 Index

INDEX

Activating, 43
Administrator Manager, 150
Advanced Option, 115
ARP Information Retrieve, 157
Batch Configuration, 115
Capacity Value, 139
Cold Start, 131
Config File Manager, 117
Device Collector, 141
Device Customization, 70
Device Discovery, 155
Device Event Config, 131
Device Event Log, 133
Device Group Manager, 128
Device Label, 122
Device Locator, 140
Device Statistics, 143
Device Type Check, 119
Devices Supported, 68
Domain Manager, 48
Edit link, 139
EGP Fail, 131
Enterprise OID, 136
Event Viewer by IP, 133
Features, 31
Firmware Update, 117
Functions, 32
Getting Started, 43
Link Down, 131
Link Label, 122
Link Status, 138
Lockup, 37
Mac Locator, 136
Mail Server Config, 132
Management Method, 124
MIB Compiler, 109
Modular Architecture, 30
Multi-vendor Support, 69
Net Toolbox, 158
NetTools, 155
OID Config, 116
Performance Monitor, 161
Poll Parameters, 126
Port Packet Monitor, 159
Port Status, 117
PORTSTATUS, 115
Query, 134
Radius Authentication, 47
Rearranging the Topology, 64
RMON, 115
Run Batch, 117
Safeguard Check, 120
Safeguard Engine, 121
SNMP v1/v2c, 125
SNMP v3, 125
SPANNING, 115
Spanning Tree, 117
Startup Wizard, 48
System Config, 47
System InfoGenSNMPDeviceModule, 114
System Log, 150
TELNET, 125
TFTP, 157
Threshold Event, 132
Topo Export/Import, 59
Topology Generator, 61
Topology Generator Principle, 60
Topology Rollback, 65
Trace Route, 155
Trap Editor, 135
Upper Layer, 147
User Locator, 142
User Statistics, 143
View Option, 146
Warm Start, 131
Zoom In / Out / Fit, 147