D-Link®

D-View 5.1

Network Management System

User's Guide

First Edition (July 2002)
651DS200.015
Printed In Taiwan

RECYCLABLE

Table of Contents

ABOUT THIS GUIDE

This User's guide provides brief descriptions of how to use the various menus and operations found in the D-View Network Management System. This guide does not discuss network design or management concepts, nor does it provide detailed explanation or definitions of SNMP, MIBs, RMON or associated concepts. It is assumed that the reader is familiar with these standardized networking concepts and protocols; hence variables presented in the D-View menus are self-explanatory. Variables such as MIB objects are listed exactly as they appear on the D-View GUI.

Overview of this User's Guide

Chapter 1, "*Introduction.*" Lists system requirements, gives installation procedures. Shows you how to get D-View 5.1 up and running.

Chapter 2, "*New Features."* Explains D-View 5.1's organization and highlights new features.

Chapter 3, "*How to Manage a Network.*" Describes how to manage a network with D-View 5.1. Topics: Discover, How to Monitor and Manage a network, Using Telnet, Changing Device Properties, Collect trap information to log file, Install Plug-in management module, Managing SNMP Devices without a management module (MIB Compiler/Browser), Topology.

Chapter 4, "MIB Utilities." Shows how to use D-View's user-friendly dialogs to manage without using plug-in modules. This chapter is organized according to the drop-down menu items under "MIBs" on the D-View 5.1 GUI.

Chapter 5, "*Internet Tools.*" Explains items in the "Tools" drop-down menu in the order of the descending menu items.

Chapter 6, "*Advanced Management.*" Explains how to use trap management functionalities.

Appendix, "*Troubleshooting.*" Provides solutions to different troubleshooting scenarios.

1

INTRODUCTION

This section gives systems requirements and explains installation procedures.

System Requirements

D-View 5.1 can be installed and operated on a computer that meets the following minimum requirements:

- CPU: 550 MHz
- DRAM: 256MB
- Hard Drive Available space: 100MB
- Ethernet Adapter: 10BASE-T
- Operating System: Windows 2000 or Windows XP
- Windows Component: Simple Network Management Protocol (SNMP)
- Access 2000

Installation

Note: ***To install D-View 5.1 you must use the Ethernet adapter provided with the software. If you do not use the Ethernet adapter provided with the software installation will fail.***

The following is a pictorial guide showing how to install D-View 5.1 and get it up and running:

Step1

Figure 1-1.

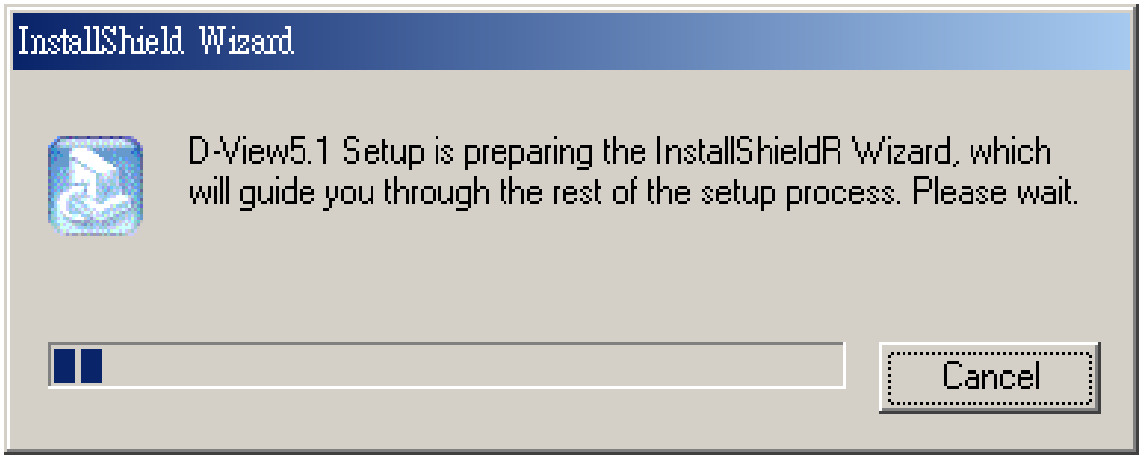

InstallShield Wizard
D-View5.1 Setup is preparing the InstallShieldR Wizard, which will guide you through the rest of the setup process. Please wait.
Cancel

Figure 1-2.

Step 2

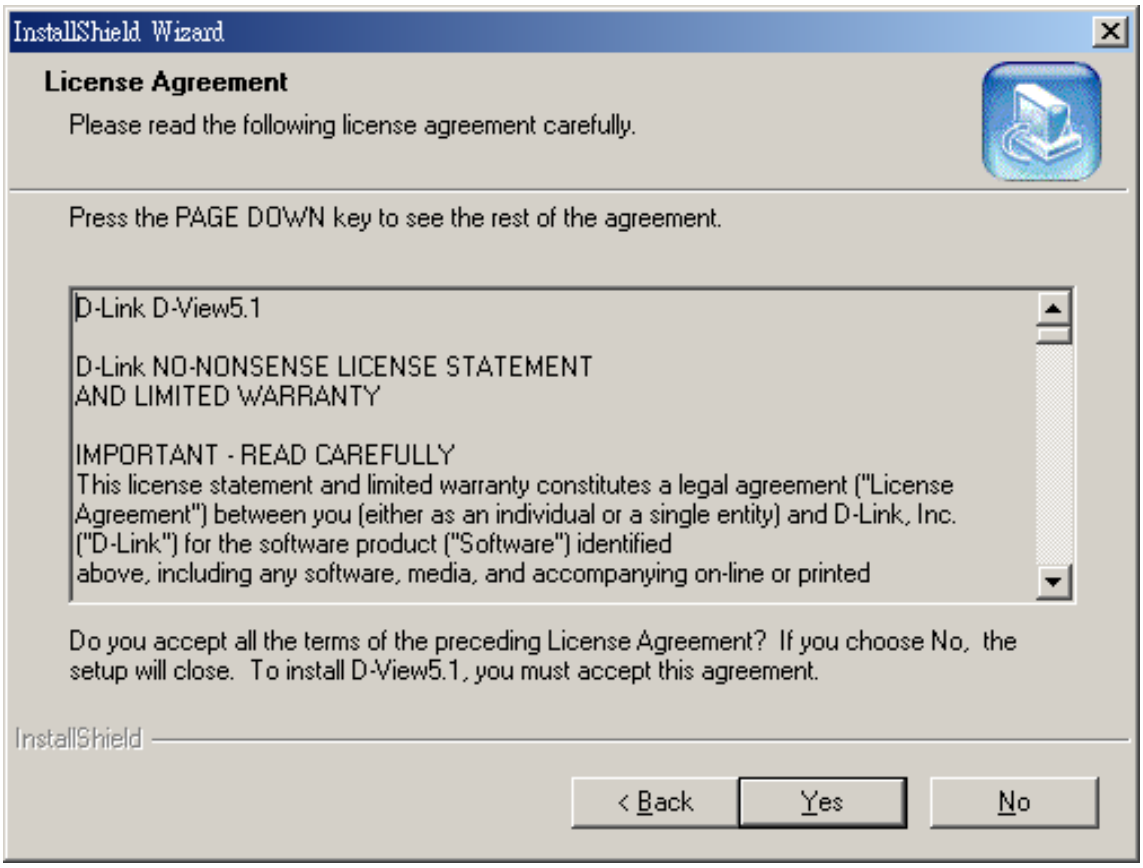


Figure 2.

Step 3

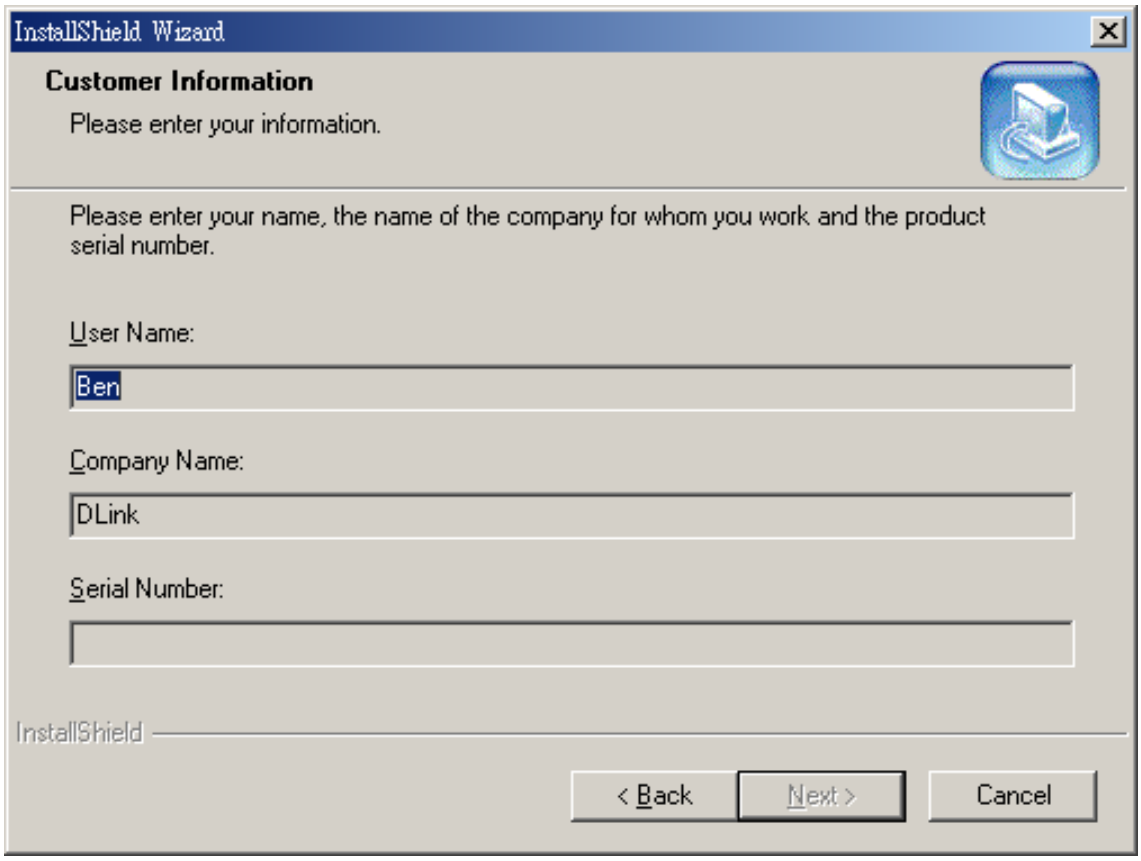


Figure 3.

Step 4

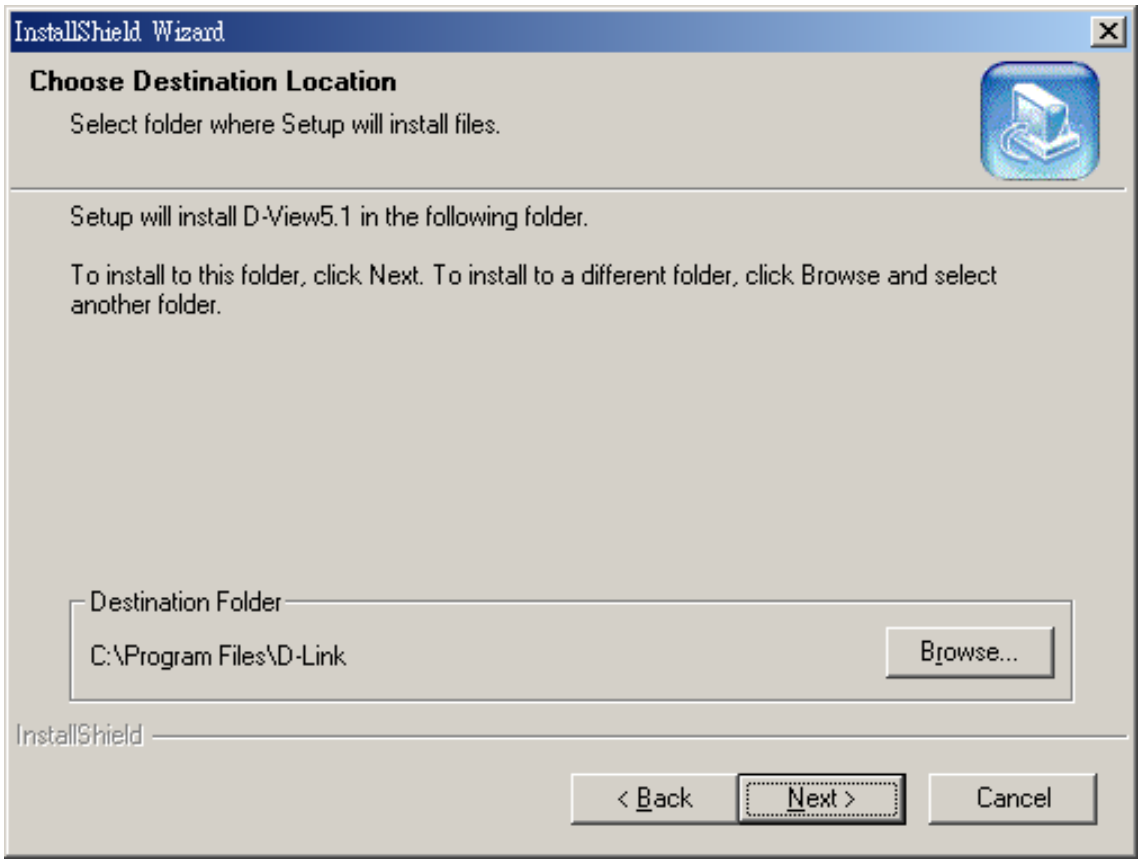


Figure 4.

Step 5

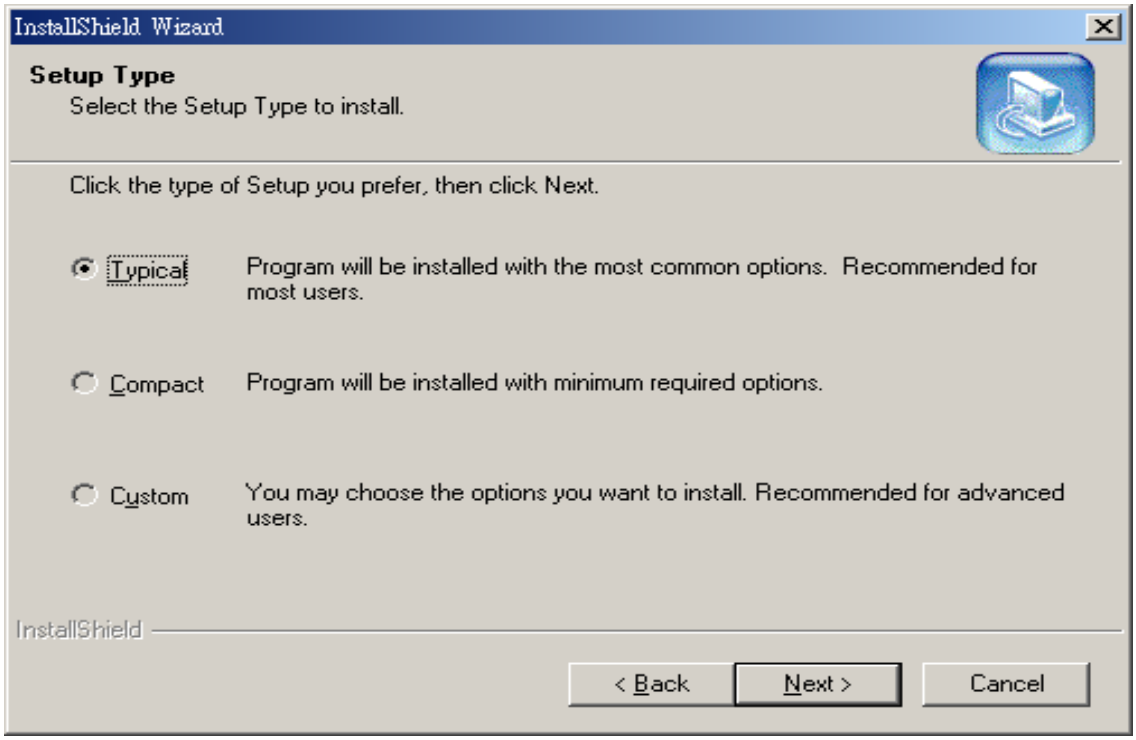


Figure 5.

Typical : Installs D-View 5.1 , D-Link SNMP Solutions Modules, DES-3225G, DES-3624I , DES-6000 , DGS-3208TG, DGS-3208F, DHS-3226, DHS-3218, DHS-3210, DES-3226, DHS-3224V, DGS-3224TG, DHS-102, Wireless AP

Compact: Installs D-View 5.1 , D-Link SNMP Solutions

Step 6

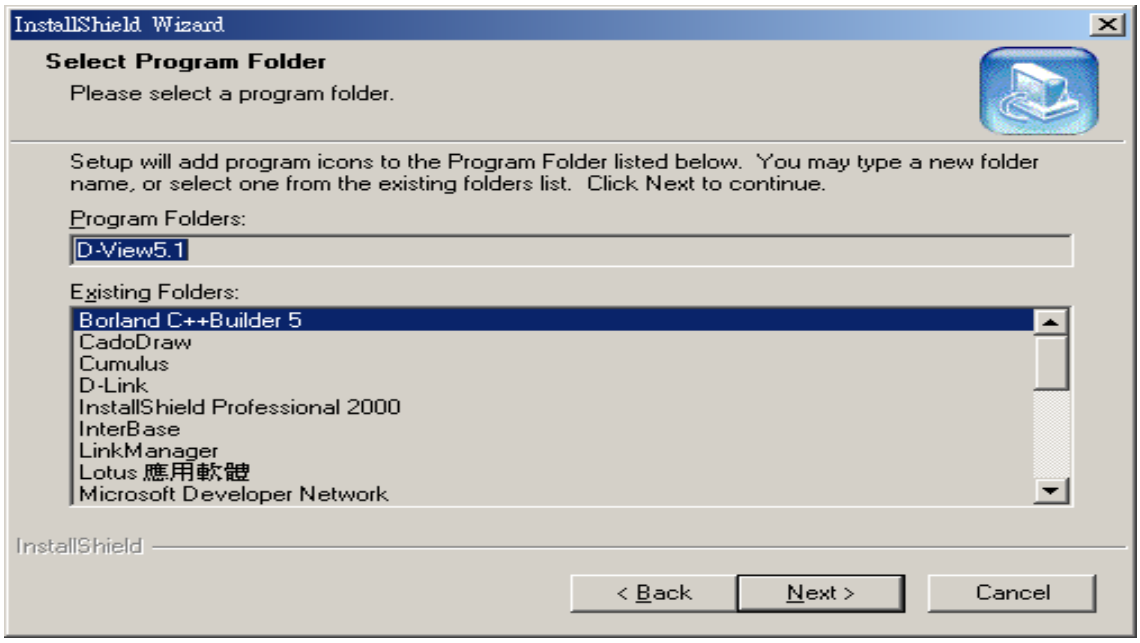


Figure 6.

Step 7

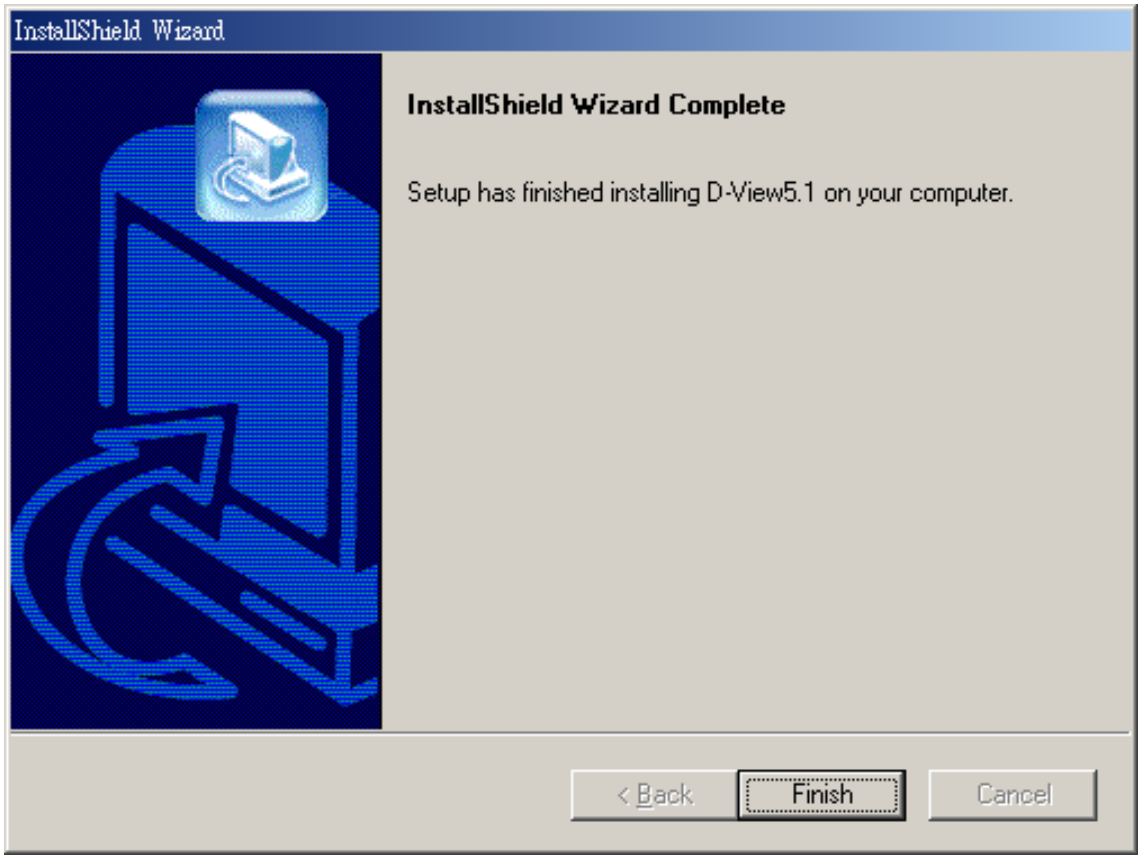


Figure 7.

Before you are Running

Note:. *If device can't be found under discovery, then you must enable SNMP service in Windows service before you run D-View 5.1, and remember to disable the SNMP trap service before you run the D-View*

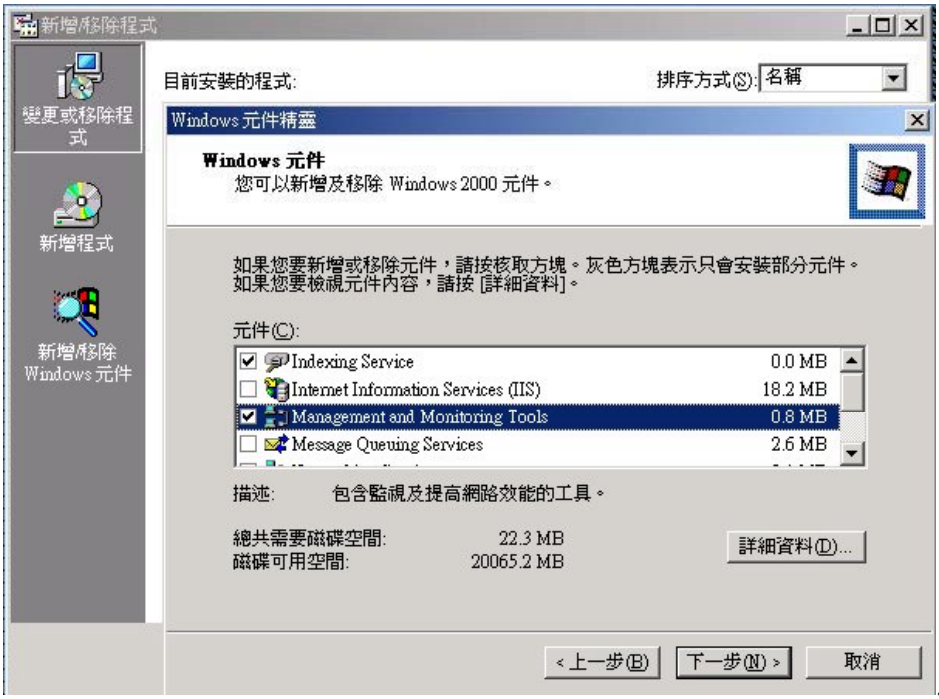


Figure 8-1.

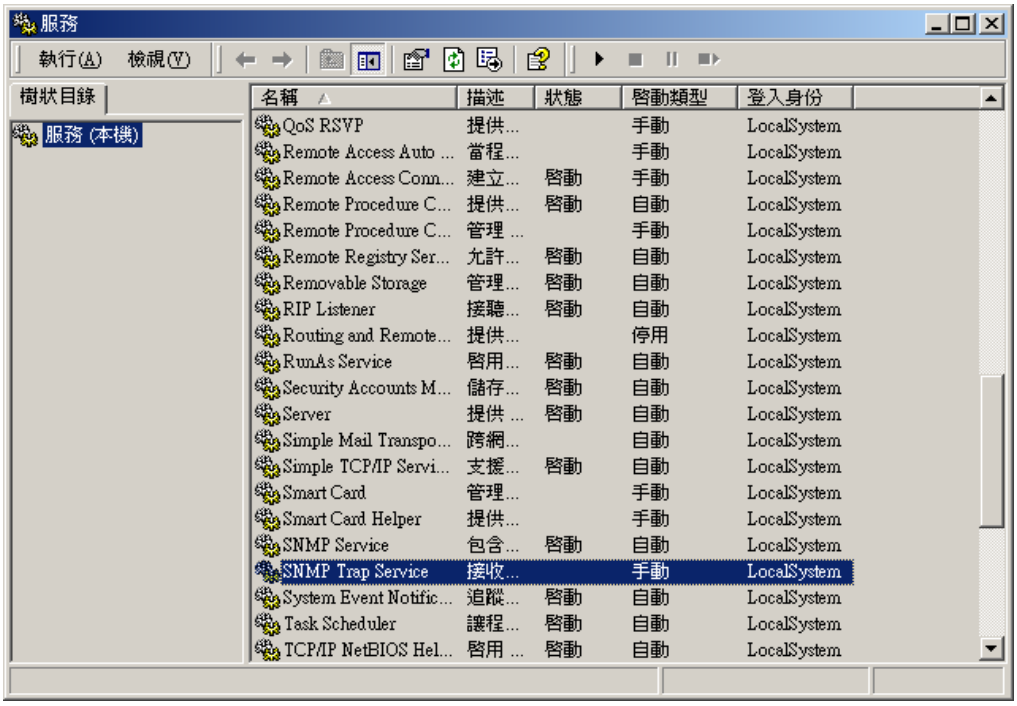

服務
執行(A)
檢視(V)
樹狀目錄
服務 (本機)
名稱
描述
狀態
啓動類型
登入身份
QoS RSVP 提供... 手動 LocalSystem
Remote Access Auto ... 當程... 手動 LocalSystem
Remote Access Conn... 建立... 啓動 手動 LocalSystem
Remote Procedure C... 提供... 啓動 自動 LocalSystem
Remote Procedure C... 管理 ... 手動 LocalSystem
Remote Registry Ser... 允許... 啓動 自動 LocalSystem
Removable Storage 管理... 啓動 自動 LocalSystem
RIP Listener 接聽... 啓動 自動 LocalSystem
Routing and Remote... 提供... 停用 LocalSystem
RunAs Service 啓用... 啓動 自動 LocalSystem
Security Accounts M... 儲存... 啓動 自動 LocalSystem
Server 提供 ... 啓動 自動 LocalSystem
Simple Mail Transpo... 跨網... 自動 LocalSystem
Simple TCP/IP Servi... 支援... 啓動 自動 LocalSystem
Smart Card 管理... 手動 LocalSystem
Smart Card Helper 提供... 手動 LocalSystem
SNMP Service 包含... 啓動 自動 LocalSystem
SNMP Trap Service 接收... 手動 LocalSystem
System Event Notific... 追蹤... 啓動 自動 LocalSystem
Task Scheduler 讓程... 啓動 自動 LocalSystem
TCP/IP NetBIOS Hel... 啓用 ... 啓動 自動 LocalSystem

Figure 8-2.

Step 1

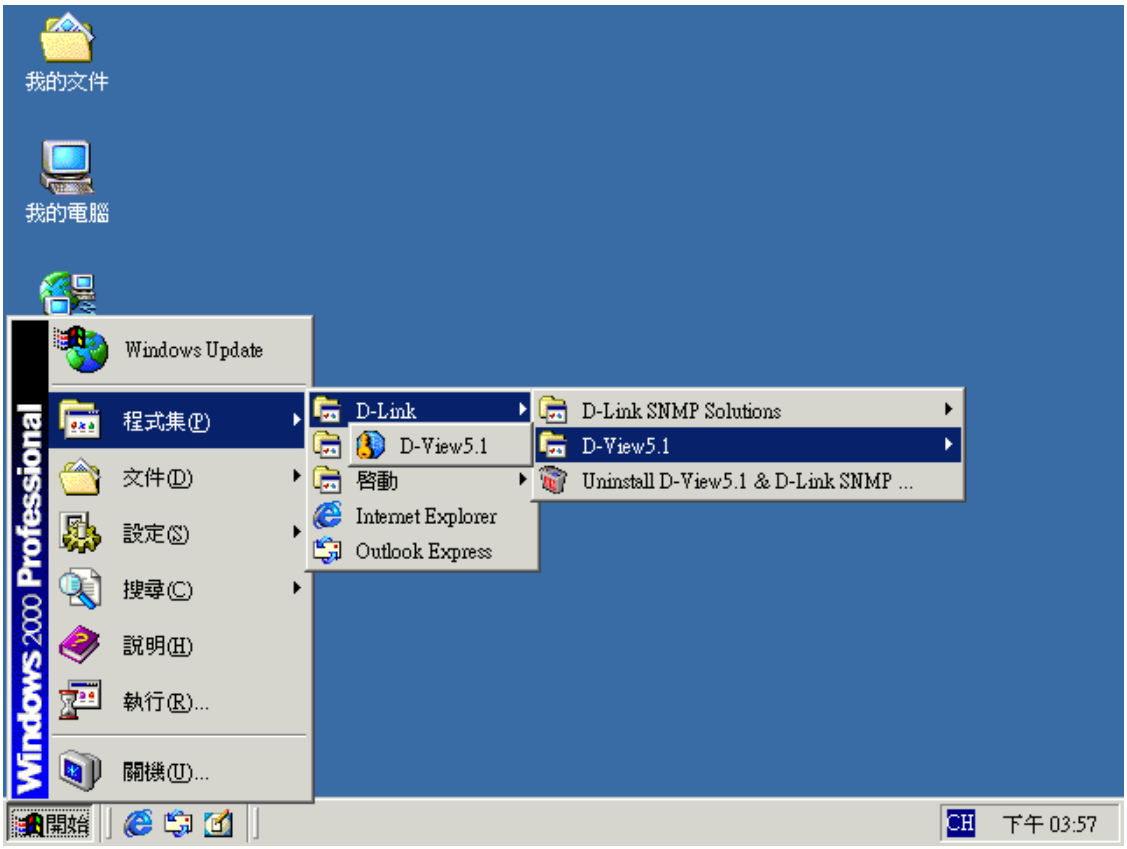


Figure 9.

Step 2

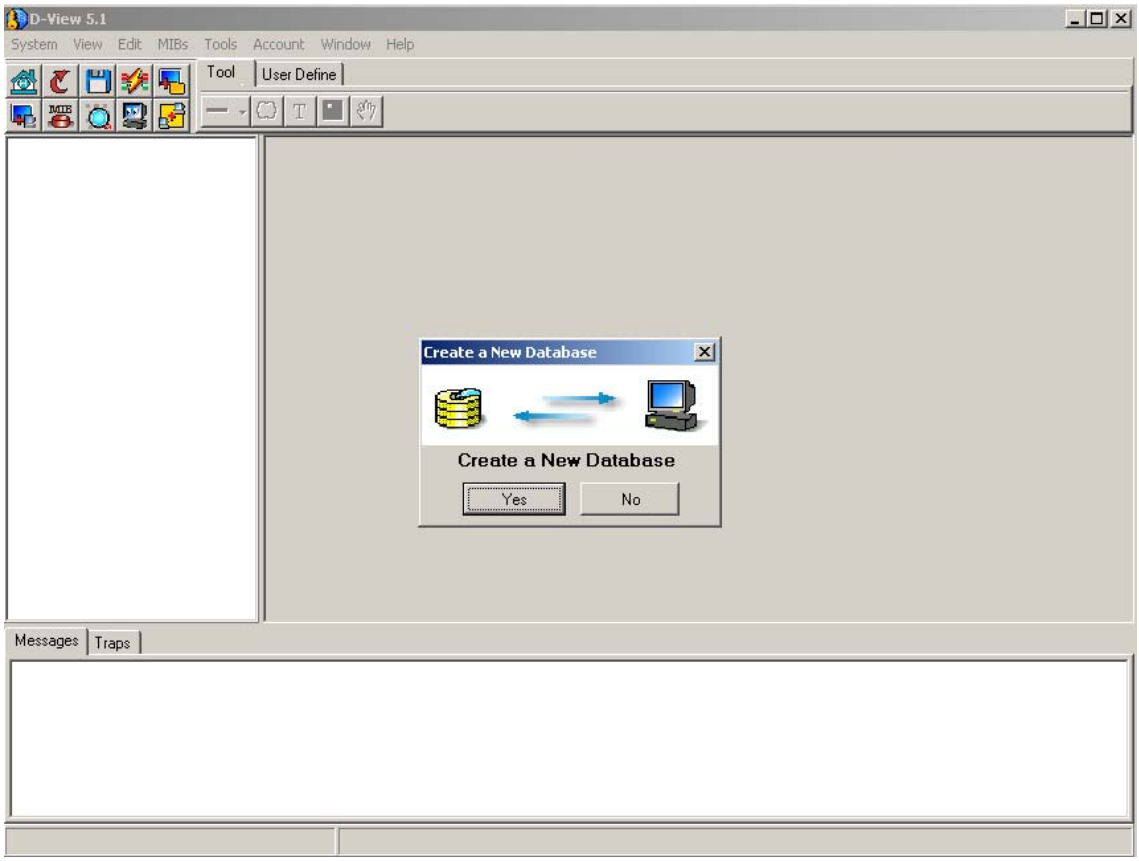


Figure 10.

Step 3

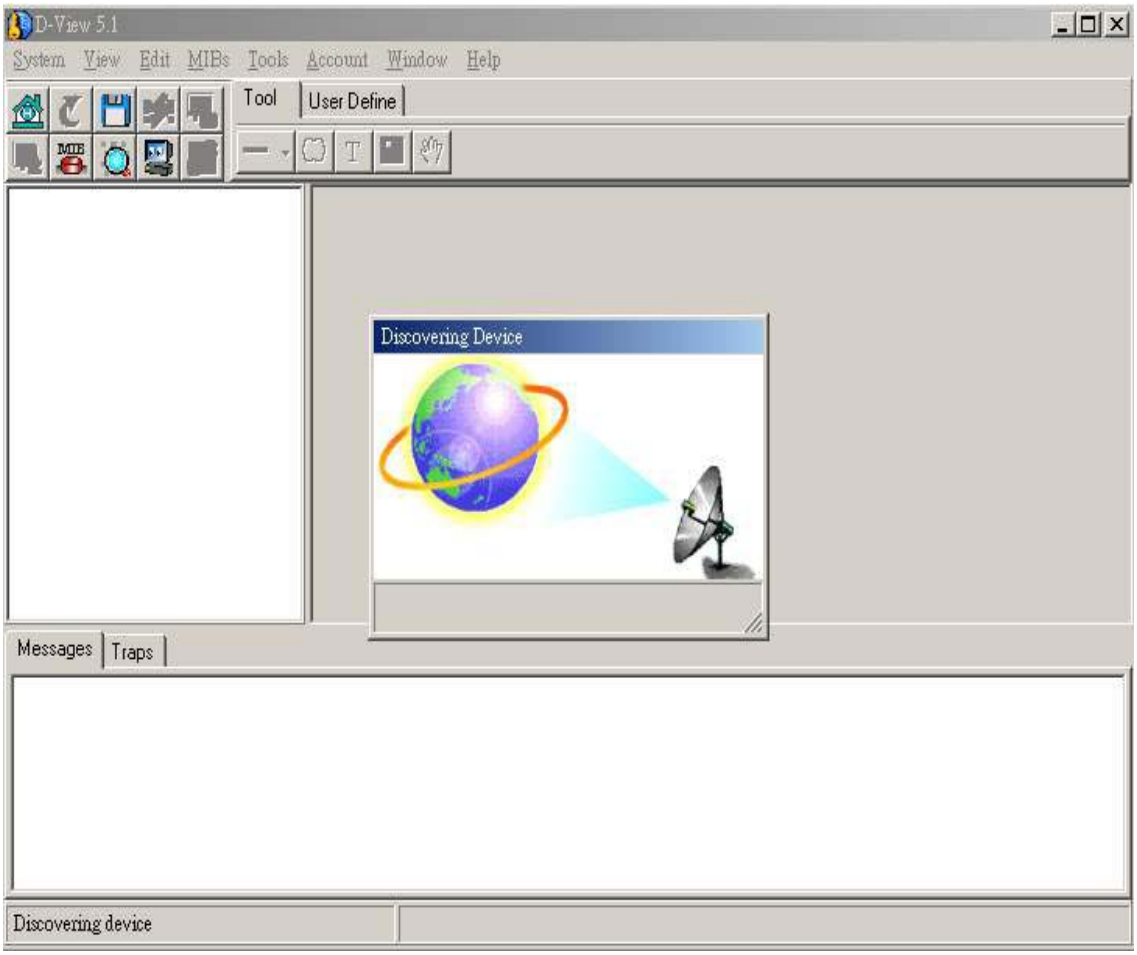


Figure 11.

2

NEW FEATURES

This chapter explains the organization and highlights new features of D-View 5.1.

Organization

D-View is organized into five main components

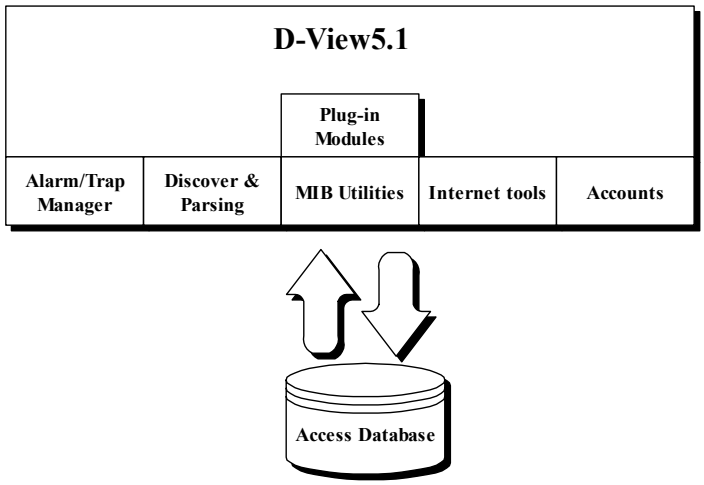


Figure 12.

New Features

Some significant additions are new to this generation of D-View software:

- A number of powerful **Layer 3 utilities** including IP Forwarding, RIP 2, OSPF, IP MRoute, DVMRP and PIM functions have been added to accommodate the increasing presence of Layer 3 switches and advanced routers in enterprise networks.

- The **DIAP proprietary administrative protocol** used in D-Link SOHO broadband routers has been added so you do not need any additional utility to administer these devices.
- An array of **Accounts information functions** has been added for client record maintenance.

- A **topology creation program** is an embedded function of D-View. This can be used to create diagrams and schematics useful for network design and layout planning.

- **SNMP V3 for major MIBs**

  MIB II, IF-MIB(RFC2233), Entity MIB(RFC2737),
  Bridge 802.1D(RFC1493), RMON,802.1P(RFC2674), 802.1Q(RFC2674).

- **Trap/Alarm notification** by using e-mail

- **Multiple views for platform:**

  After Auto Discover is complete you can view objects in the Ethernet domain by tree view. At the same time you can have a list view display open. Additionally you can create a topology domain in the same workspace to make network management more convenient.

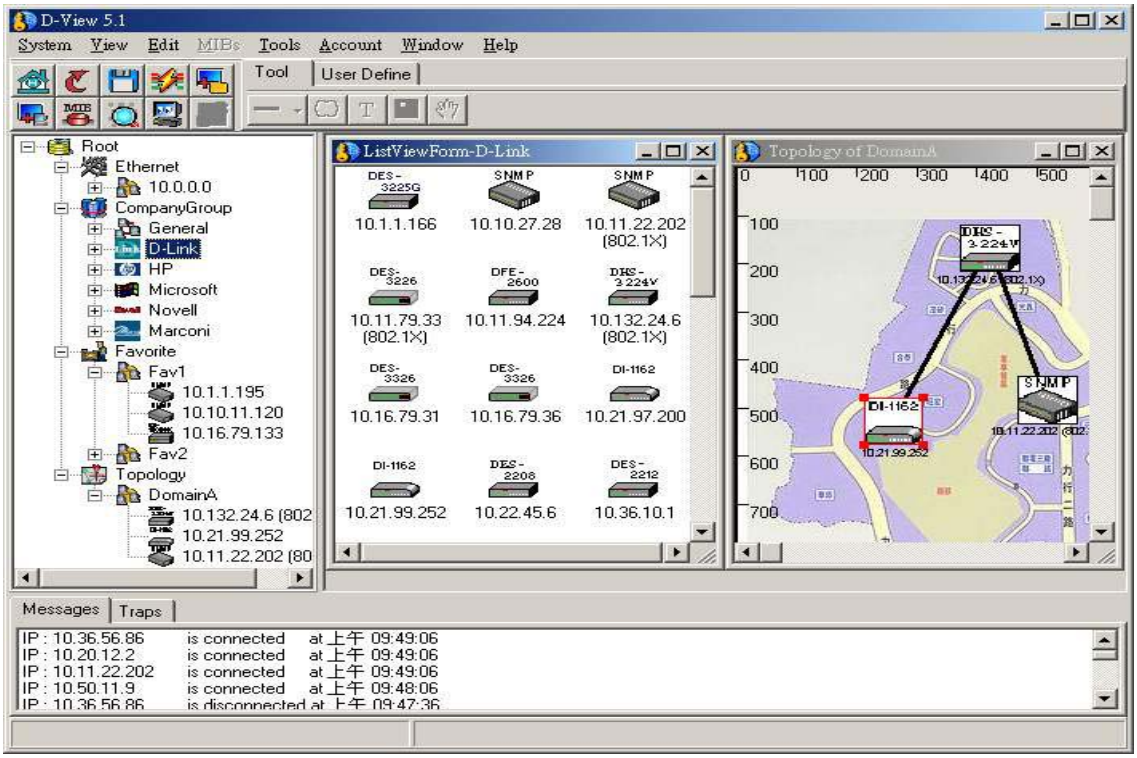


Figure 13.

- **Powerful MIB Compiler and Browser:**

  With an easy to use GUI, MIB Compiler and Browser can be used independent of D-View or can be used with the D-View software. This makes network management more effective and efficient.

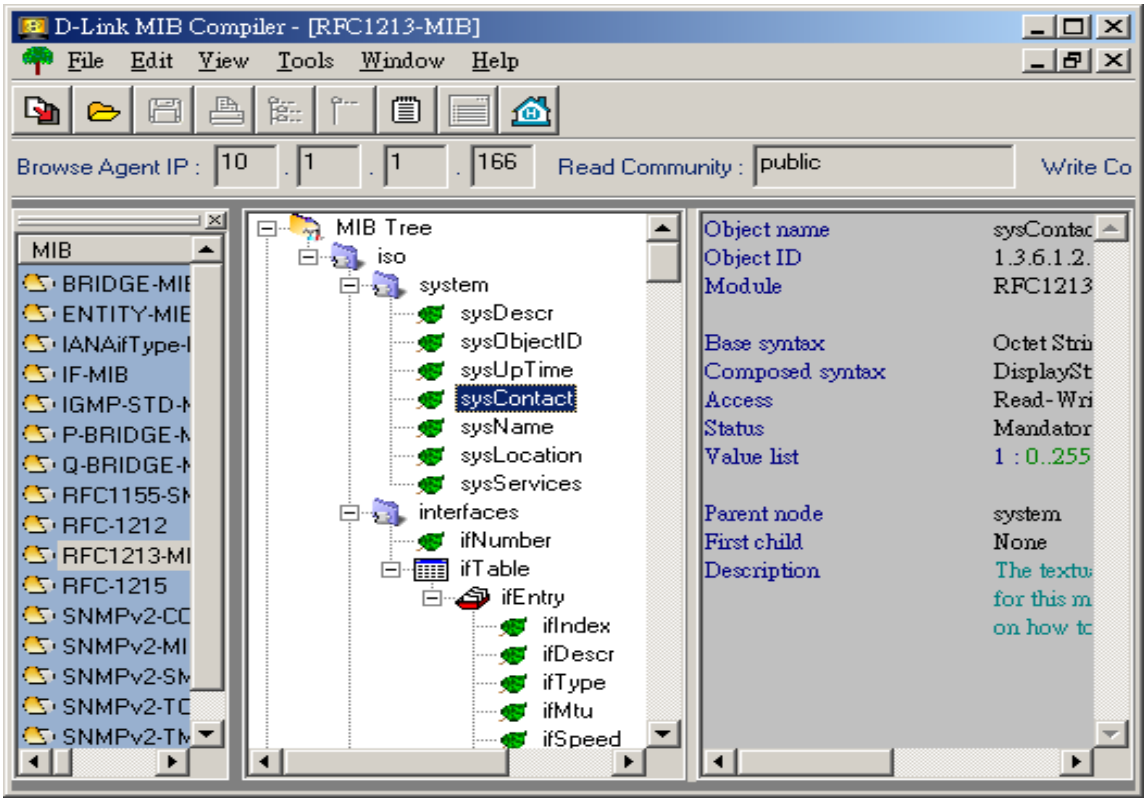


Figure 14. MIB Compiler

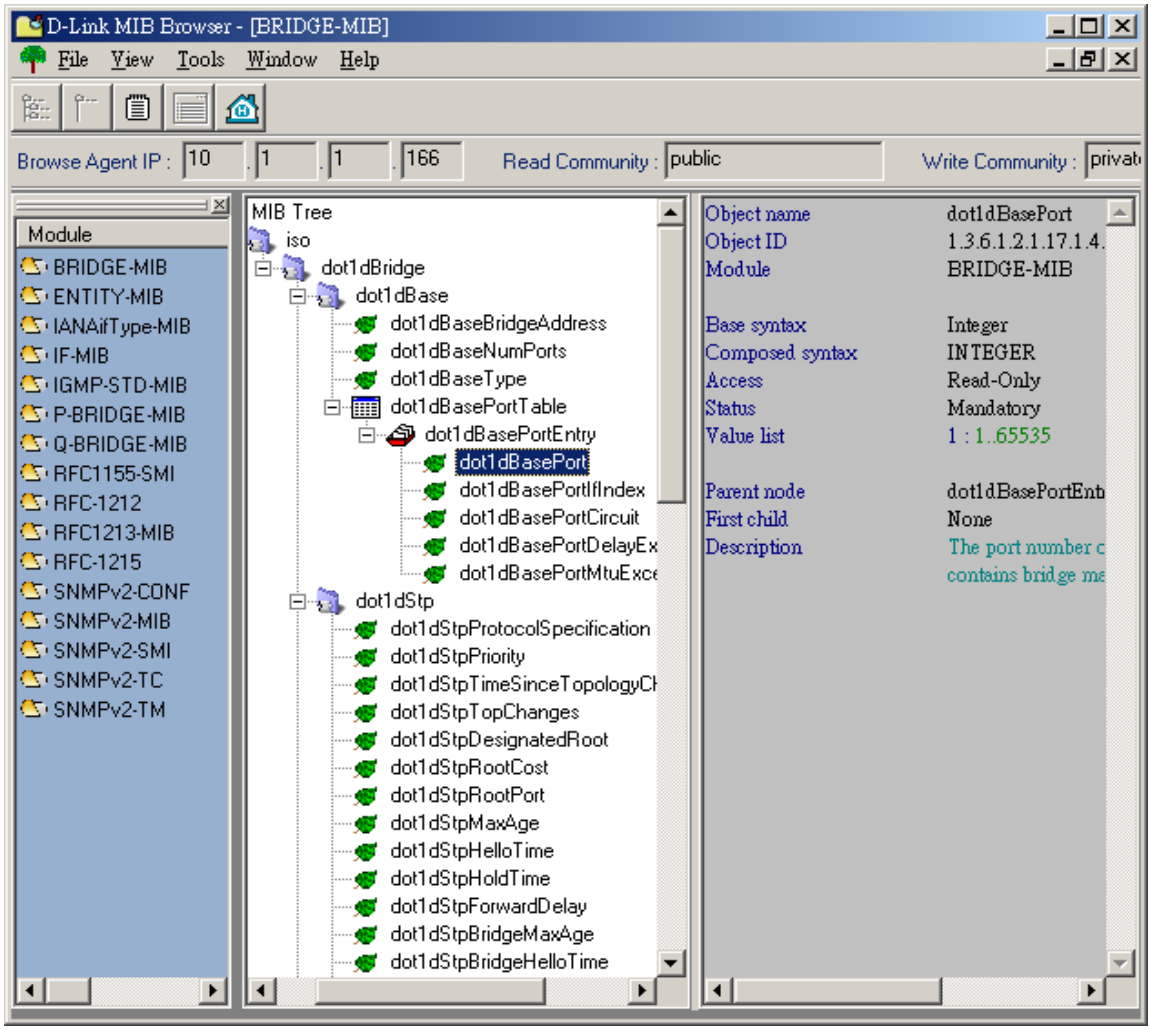


Figure 15. MIB Browser

- **User Account management:**

  Account is a simple account management system to keep track of the bills.

  It has the following features:

  1. Each client assigned an account with personal authorization IP Address
  2. Different groups of clients can generate statements with different schedules
  3. Detects abnormal usage for clients
  4. Assigns custom taxes to service charges
  5. Credit adjust function allow you to insert credit records manually and give credit for wrong or misdialed work.
  6. Late fee assessment function
  7. Real-time reporting

3

HOW TO MANAGE A NETWORK USING D-VIEW 5.1

This chapter describes how to use the various menus and operations found in the D-View Network Management System with different example scenarios.

Orientation

Using D-View

D-View uses the same conventions as other Windows-based programs in its GUI. Left-click to select a device or domain, left-click to carry out a function from the drop-down menu, and so on. If you double-click on an SNMP device, this will launch the device-specific module if it is installed. If it is not installed, you will be offered an opportunity to download the module from the D-Link website.

The three display panels of the D-View Main Menu:

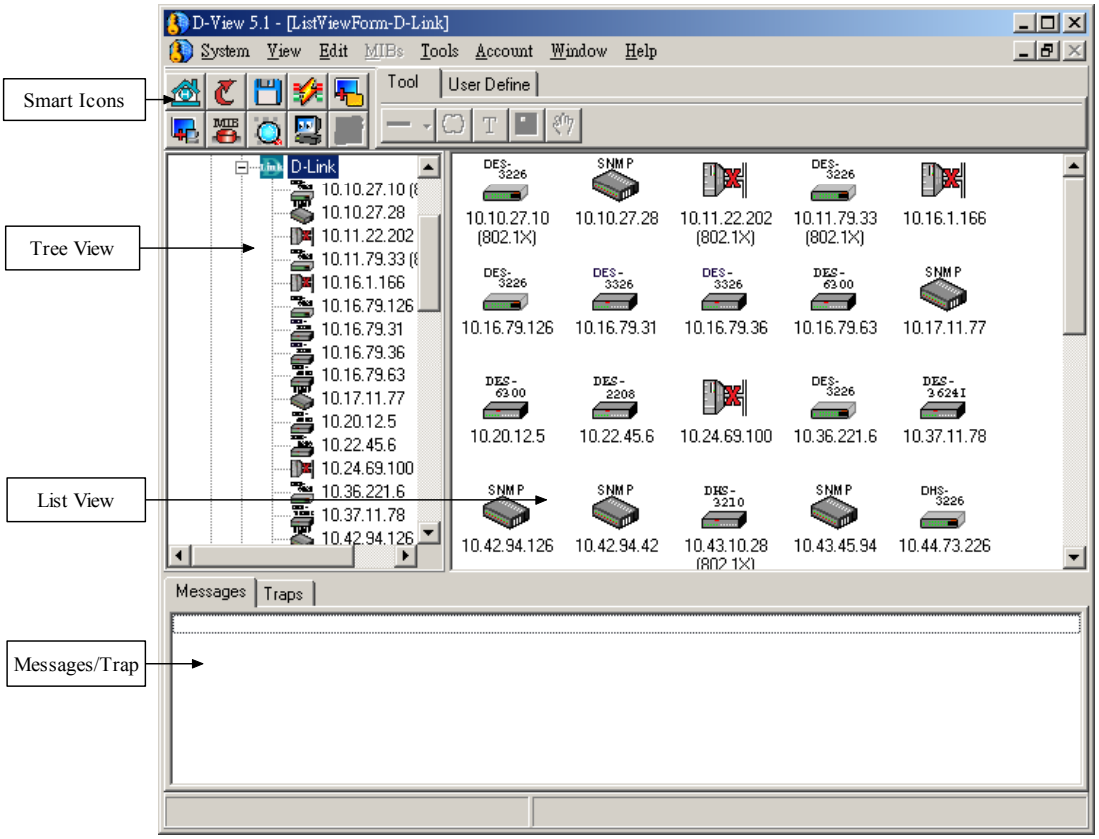


Figure 16.

Tree View:

Presents the entire network grouped into major domains extending from Root. The major domains for the default setup are Ethernet, CompanyGroup, Favorites and Topology. The Favorites group is a vacant domain available as a convenient means of tracing devices that require frequent monitoring. It can contain any or all devices and can be arranged into sub-

domains as needed. The Company group is divided into sub-domains according to the device manufacturer. The "tree" in this panel or any domain can be expanded or contracted to view the contents of any group.

List View:

Displays the contents of whatever group is highlighted in the tree view. Large icons are used by default; however, you may choose to use small icons, a simple list or a list that includes device details.

Traps/Messages:

Displays Trap and connect/disconnect messages.

Use the View drop-down menu to customize the display panels.

Topology:

Right-click on Topology under Root in the Tree View display to launch new topology diagram. Use the "Tool" pad and "User Define" pad to modify the topology.

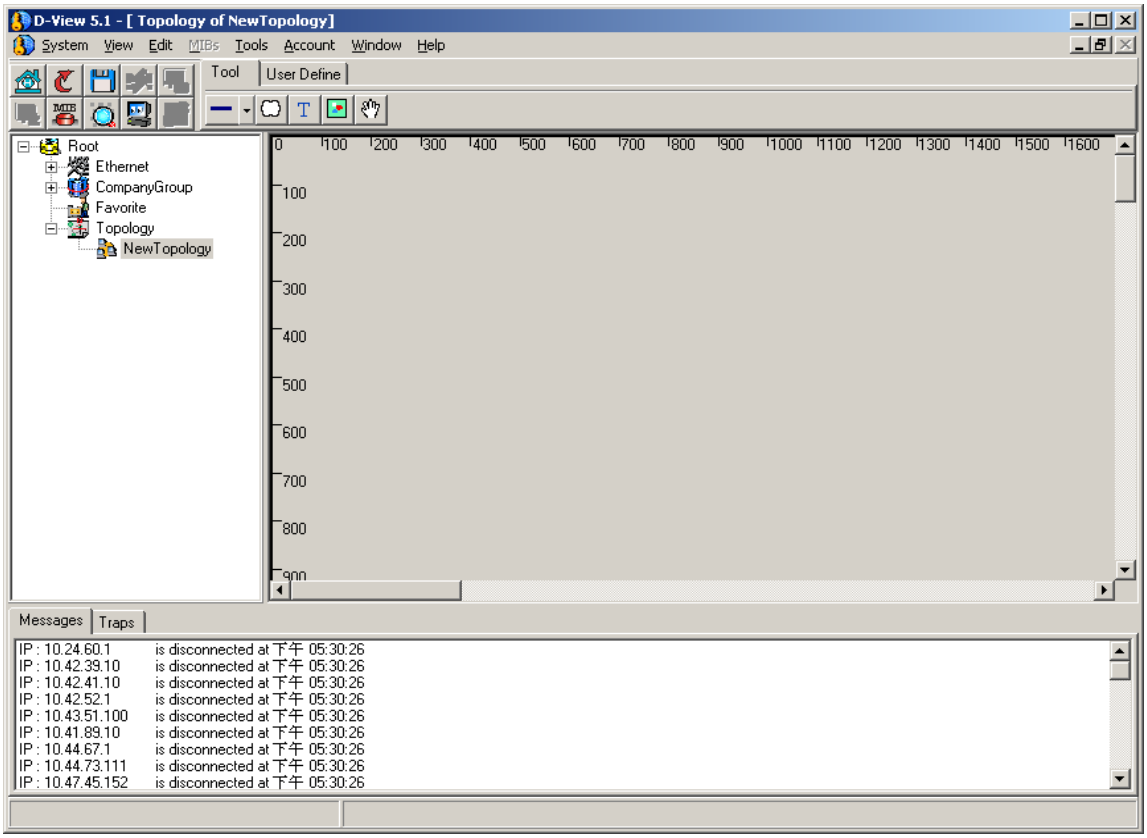


Figure 17.

Smart Icons: The five main icons that appear in D-View 5.1 GUI are summarized below.

Icon	Description
	Unknown device, device type and function not known.
	RADIUS server.
	Device off line or disconnected.
	SNMP device with SNMP agents.
	Wireless Access Point

Table 1. General Device Icon Summary

Basic Operations

Network Basic Information

The basic information available under System provides graphical and numerical information about device type and role distribution. The information represents the sum total of the basic information communicated by every device including non-SNMP devices. The graphical representation can be viewed as a color-coded pie chart (default) or bar graph. Network make up is broken down by type and role. Select your preference of graph style by clicking the graph icon of choice in the middle of the menu. View network role or type distribution by selecting the appropriate tab. The reference key explains the colors used for the graphs and displays the number of devices in each category.

System→All Basic Information

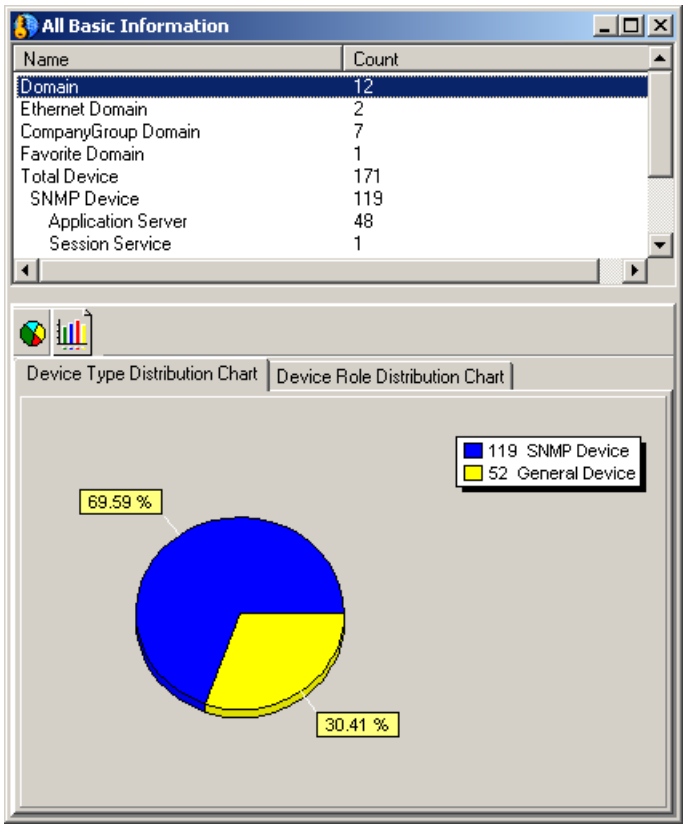


Figure 18.

Repolling Configuration

By default D-View polls the network for status updates every 30 seconds. This repolling configuration can be changed or turned off using the Repolling Configuration menu under System. Adjust the polling interval from 10 to 60 and the time out (1-10 seconds) and click the Set button to put the settings into effect. Turn off repolling by checking the Don't Repoll box and clicking Set. Default repolling configuration = 30 sec Interval, 3 sec Time Out.

System→Repolling Configuration

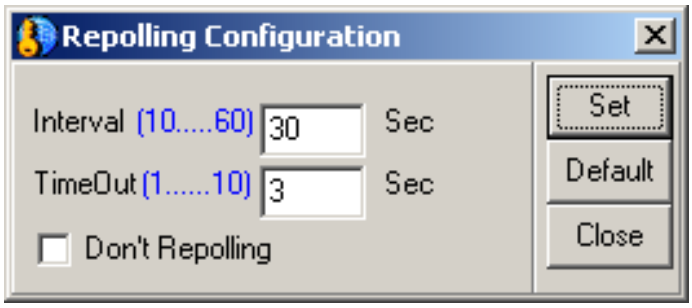


Figure 19.

Community String Configuration

Set the Read and Write Community String to allow D-View management access to SNMP devices.

System→Community String Configuration

- Read Community String: input read community string
- Write Community String: input write community string
- OK: click to put settings into effect

Figure 20.

Note: ***Read/Write Community String settings must be correct otherwise you will not be able to find devices.***

Saving D-View Database

Save the current settings arrangement for D-View using the Save Database function located under System. This will save any domains that have been created.

System→Save To Database

Clear Database

To delete the saved arrangements and settings, use the Clear Database function under system.

System→Clear Database

Note: ***Make sure that the database is one you wish to clear otherwise you will lose your settings (Topology and Favorites).***

Find Object

This option allows the user to quickly find a particular device in the system by entering Alias Name, IP Address, or Module Name.

Edit→Find Object

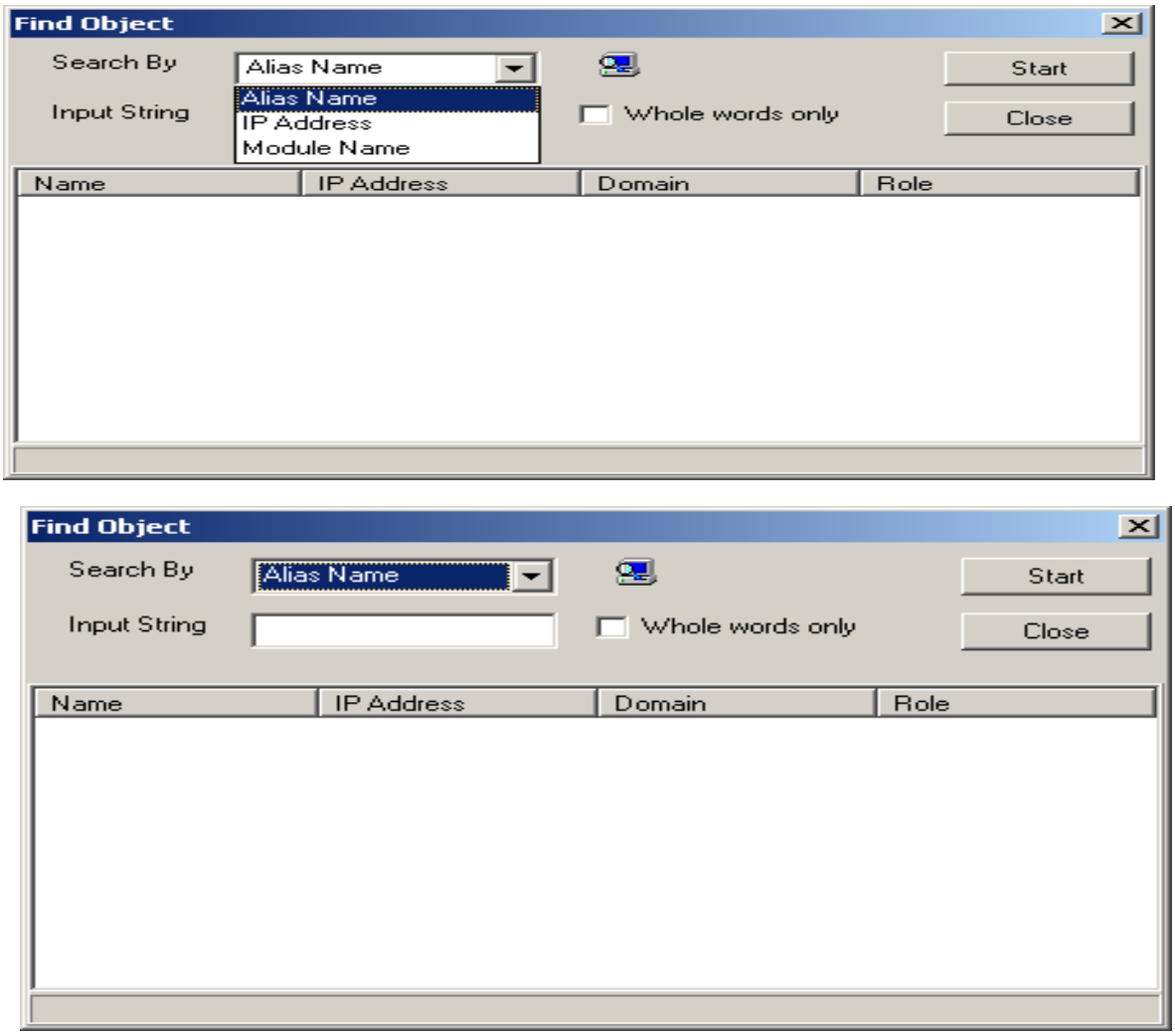


Figure 21.

- Input **Search By**: select Alias Name, IP Address or Module Name
- **Input String**: enter Alias Name, IP Address or Module Name

Domain Control

Select a domain or sub-domain in D-View to add or create a new sub-domain. This can be done under the Edit drop-down menu or right click on the selected domain to view the New Sub-domain Form.

Edit→Domain

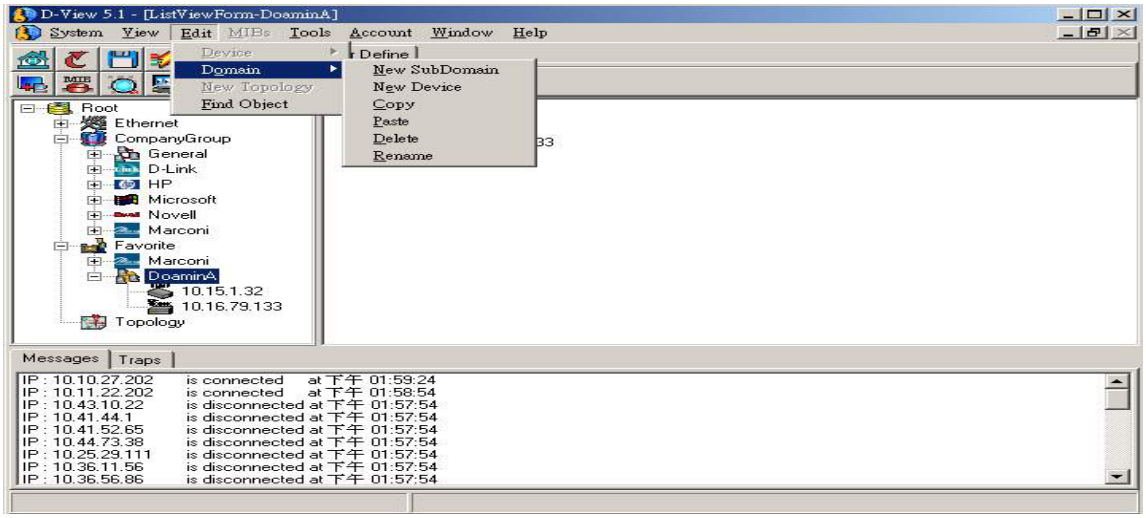


Figure 22. Create a New Sub-Domain

For example, the Company Group domain can be expanded using a list of companies. Select the company you wish to add from the pull-down menu and click OK. Alternatively, you may select a specific company group and create a new sub-domain within that group. Highlight the company group from the main menu and pull up the New Sub-domain Form. A list of the devices within that group appears listed in the left panel.

Select the devices you want in the new sub-domain and add them to the new group by clicking the arrow

The selected device now appears in the Device List on the right side panel. Type in a name for the new sub-domain and click OK to create it. Large Ethernet domains may be divided into smaller work groups and are more easily managed using this function.

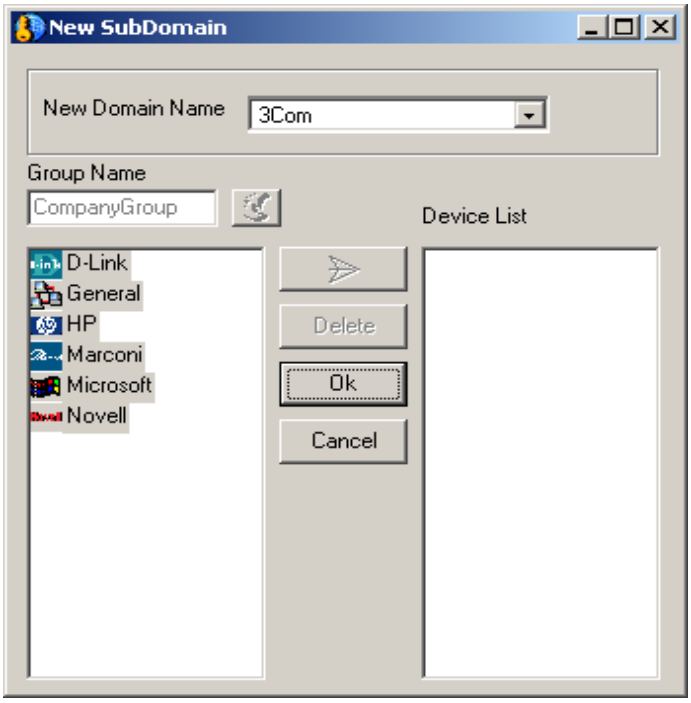


Figure 23.

Edit→New Device

You may create a new device to be managed along with the other domains that already exist via the New Device option. Enter the Device name, IP Address, Read/Write Community Strings, Module Type, and check appropriate boxes in the MIB Database.

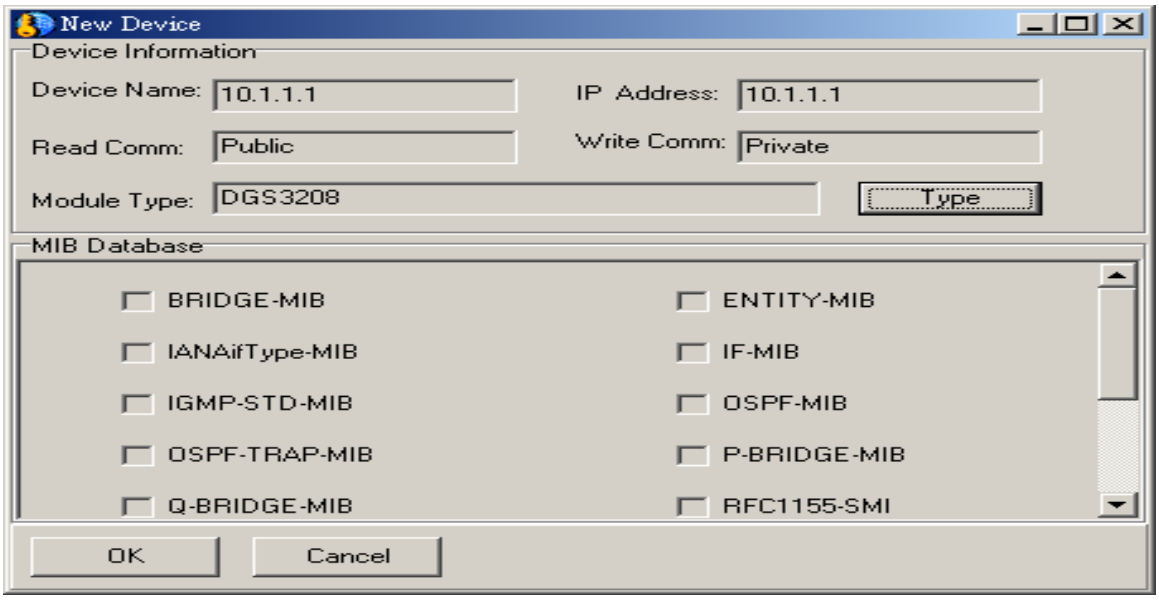


Figure 24.

Input Device Name: name of the device

IP Address: IP address of the device

Read Comm: Read Community string of device

Write Comm: Write Community string of device

Module Type: Module type of new device

MIB Database: Check MIBs that comprise new device

Device Control

Edit→Device

Through the Device menu item under the Edit drop-down menu you may keep inventory and edit the devices in your management database.

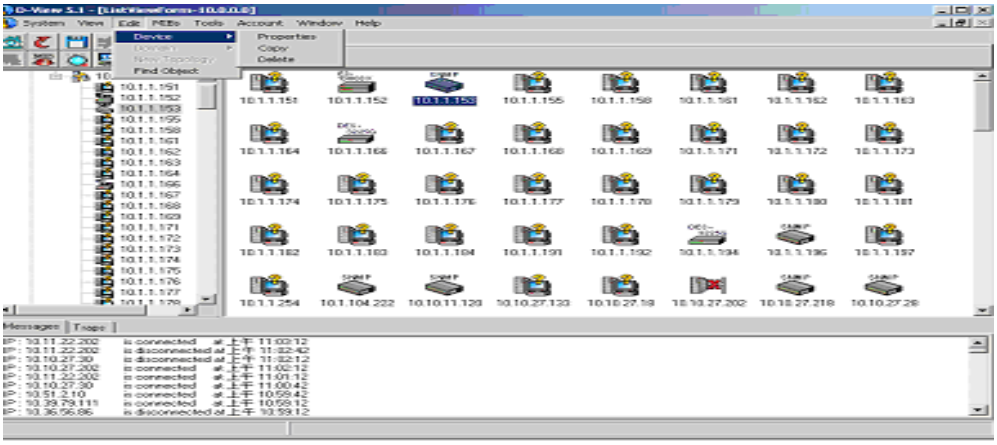


Figure 25.

Edit→Device→Properties allows you to control the settings of a particular device by entering

- Device Name: Name of device usually in the form of numbers separated by periods.
- IP Address: The IP address of the device.
- Read Comm: The Read Community String setting of the device.
- Write Comm: The Write Community String setting of the device.
- Module Type: The Module type of the device.
- MIB Database: Check boxes of MIBs of which device are comprised.

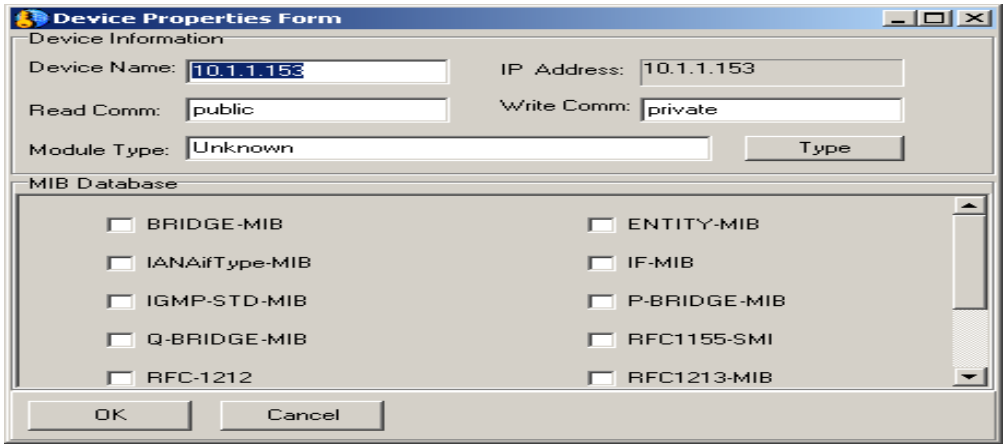


Figure 26.

Press OK to execute property settings or Cancel to cancel.

Multiple View Settings in D-View

1. **View→Topology View**→*50 % , 75% , 100% , 125% , 150% , Custom*

Allows you to have different views of the topology

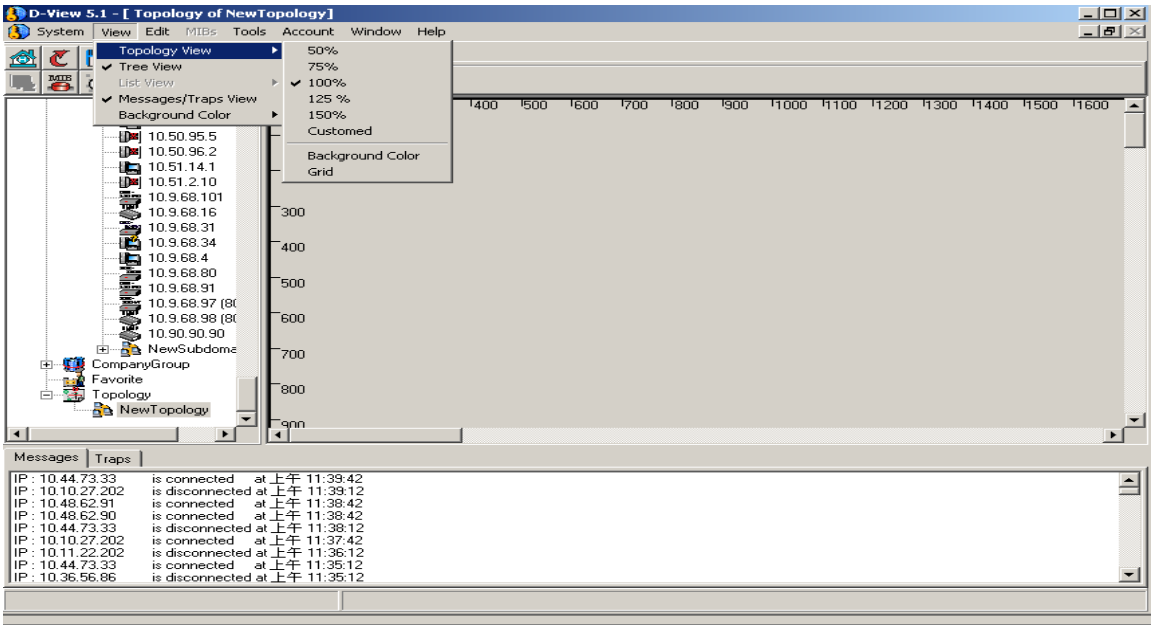


Figure 27.

View→Topology View→Background Color

Allows you to set background color of the topology

View→Topology View→Grid

Gives you the option of having a grid on the topology

2. View→Tree View

Allows you to see devices in the management network displayed in a tree on the left panel.

3. View→List View

Allows you to view devices in different ways: Icon, Small Icon, List, Report

4. View→Messages/Traps View

Allows you to view messages and traps on the bottom panel of the display screen

5. View→ Background Color

Allow you to set the background color for the Tree View, List View, Messages, and Traps displays.

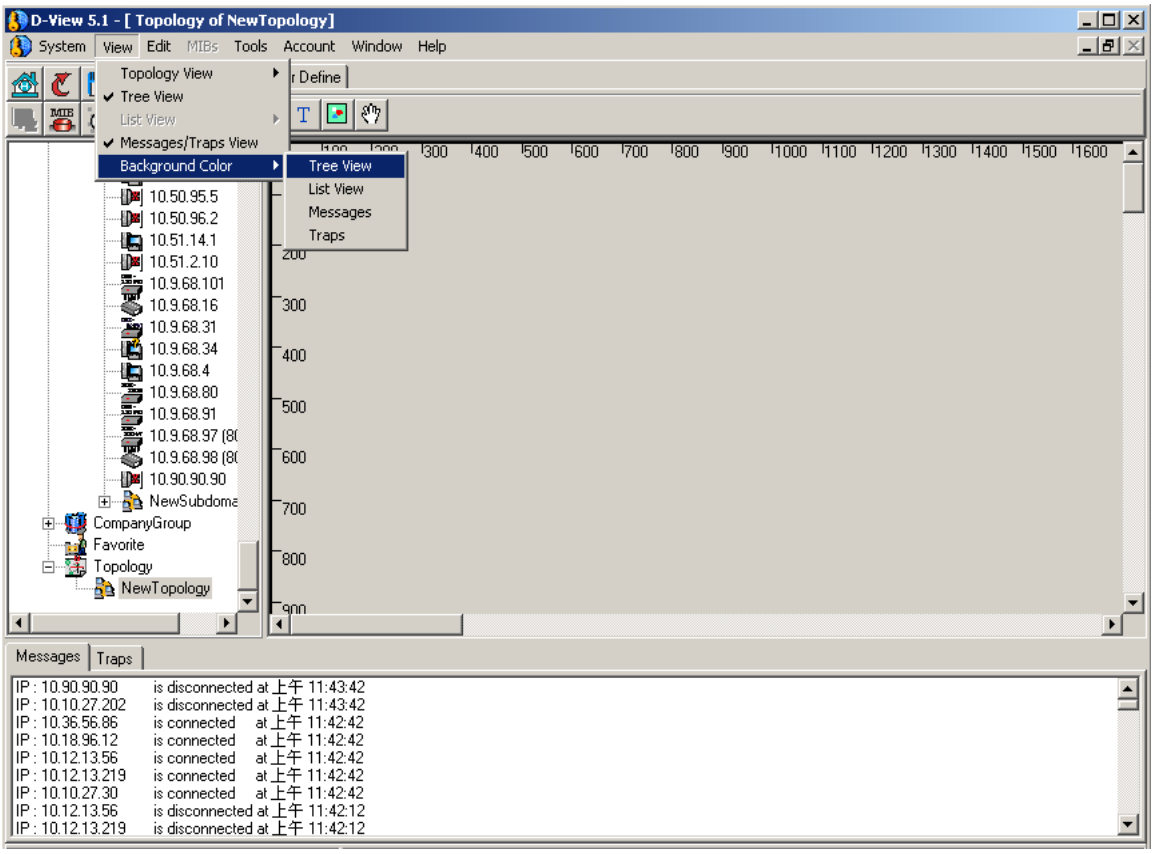

D-View 5.1 - [Topology of NewTopology]
System
View
Edit
MIBs
Tools
Account
Window
Help
Topology View
Tree View
List View
Messages/Traps View
Background Color
Tree View
List View
Messages
Traps
10.50.95.5
10.50.96.2
10.51.14.1
10.51.2.10
10.9.68.101
10.9.68.16
10.9.68.31
10.9.68.34
10.9.68.4
10.9.68.80
10.9.68.91
10.9.68.97 (8
10.9.68.98 (8
10.90.90.90
NewSubdoma
CompanyGroup
Favorite
Topology
NewTopology
Messages
Traps
IP : 10.90.90.90 is disconnected at 上午 11:43:42
IP : 10.10.27.202 is disconnected at 上午 11:43:42
IP : 10.36.56.86 is connected at 上午 11:42:42
IP : 10.18.96.12 is connected at 上午 11:42:42
IP : 10.12.13.56 is connected at 上午 11:42:42
IP : 10.12.13.219 is connected at 上午 11:42:42
IP : 10.10.27.30 is connected at 上午 11:42:42
IP : 10.12.13.56 is disconnected at 上午 11:42:12
IP : 10.12.13.219 is disconnected at 上午 11:42:12

Figure 28.

Starting off in D-View 5.1

When D-View is run the first time it will automatically search all around the net domain and parse the contents in the network. It then creates a database to store the data and creates tree lists, icon lists and the like in its work area.

Since this default search is just a rough search with quick response time it usually loses some hosts. Hosts not discovered the first time could be found using the Discover functionality by giving it a net domain and using unicast SNMP rule. You can search more thoroughly using Discover but this search will be slower than the initial one.

Discover

Use this menu to search for a single device or several devices using the IP address or a selected range of IP addresses.

In the Discover window define the following variables:

- **IP Address** Type in a range of IP addresses or a single IP address (in both "From" and "To" spaces). Keep in mind that the time needed to do the search increases as the range of addresses searched becomes larger.
- **SNMP Read** Type in the read community string.
- **Time Out** Range variable from 1000 to 10,000 milliseconds
- **Search Approach** Select Unicast (default) or Broadcast. A Broadcast request is not IP address specific and will cause every device connected at the moment of broadcast to reply.
- **Discover Scheme** Select SNMP or ICMP. ICMP will only report the IP address of connected devices. SNMP discoveries reply with available device information.

- **Search Method** Choose to find a single SNMP agent defined below by the Enterprise ID or all agents in the previously refined search field.

Click on the Start button to begin the discover process. Unicast discovery will send Ping packets to the selected range of IP addresses in ascending consecutive order and repost each reply as it is received. Use the Save & Exit button to insert the device into the Tree View.

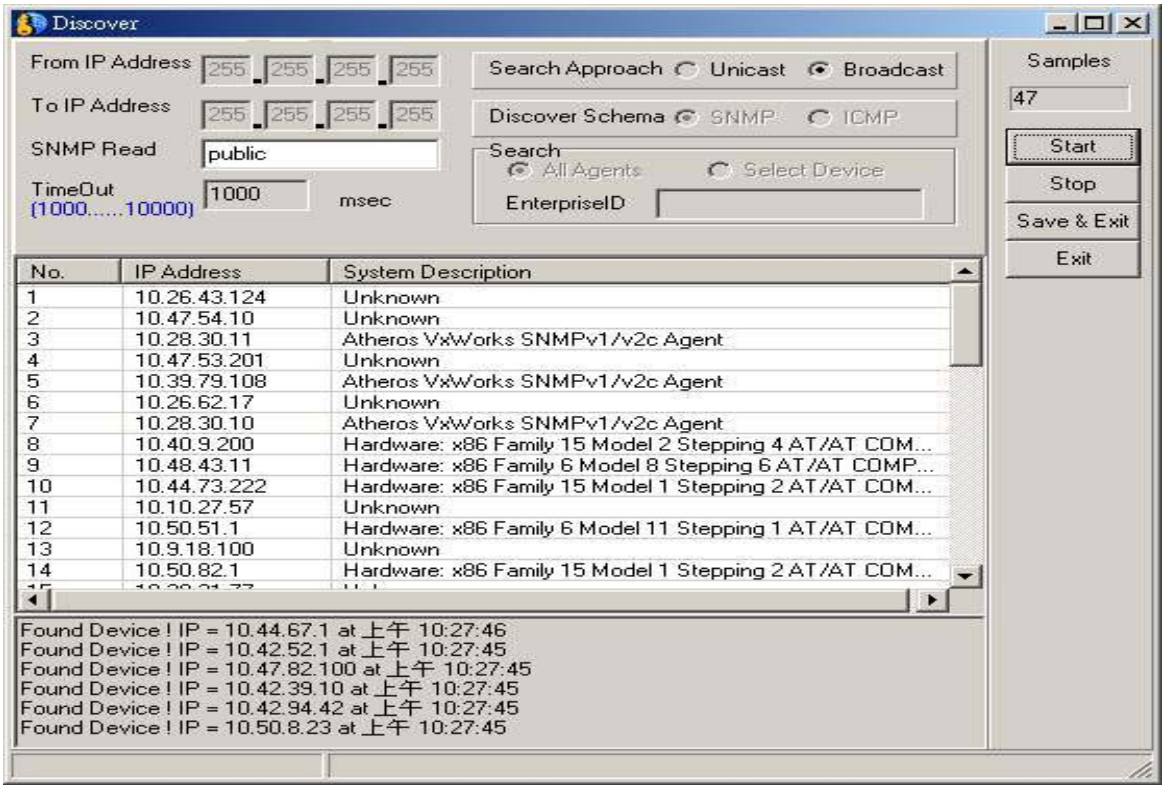


Figure 29.

How to Monitor and Manage a Network

D-View polls all devices automatically. If a device is disconnected, D-View will display a disconnected icon in the work area. Otherwise, it will show a device icon.

The D-View platform allows users to set up special cases to monitor and manage and supports multiple ways of doing so.

Scenario 1:

Monitoring Device 10.1.1.194 DES3225G (shows both connected status and disconnected status)

Connected

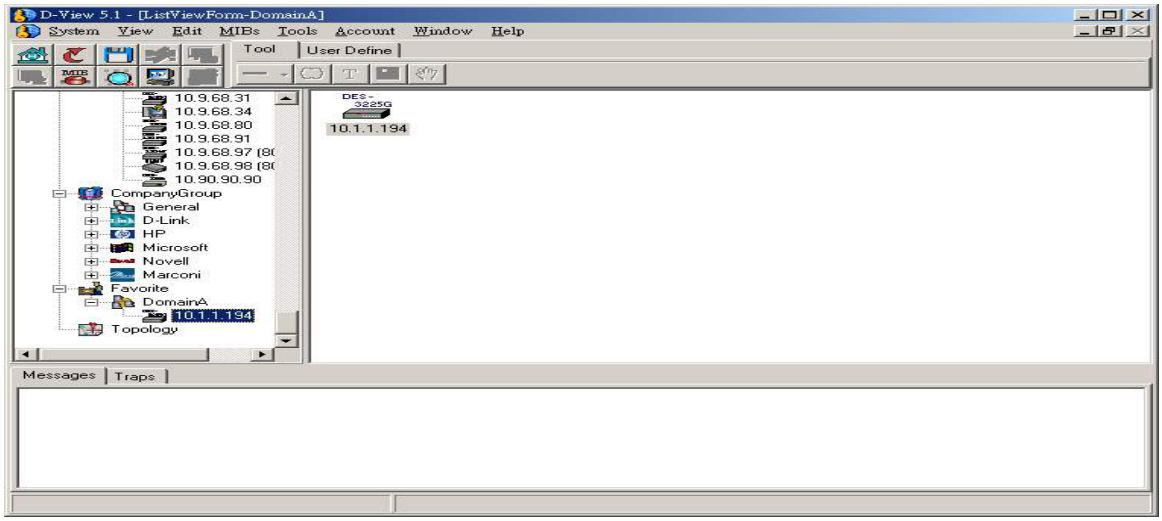


Figure 30.

Disconnected (When device does not respond during Repelling)

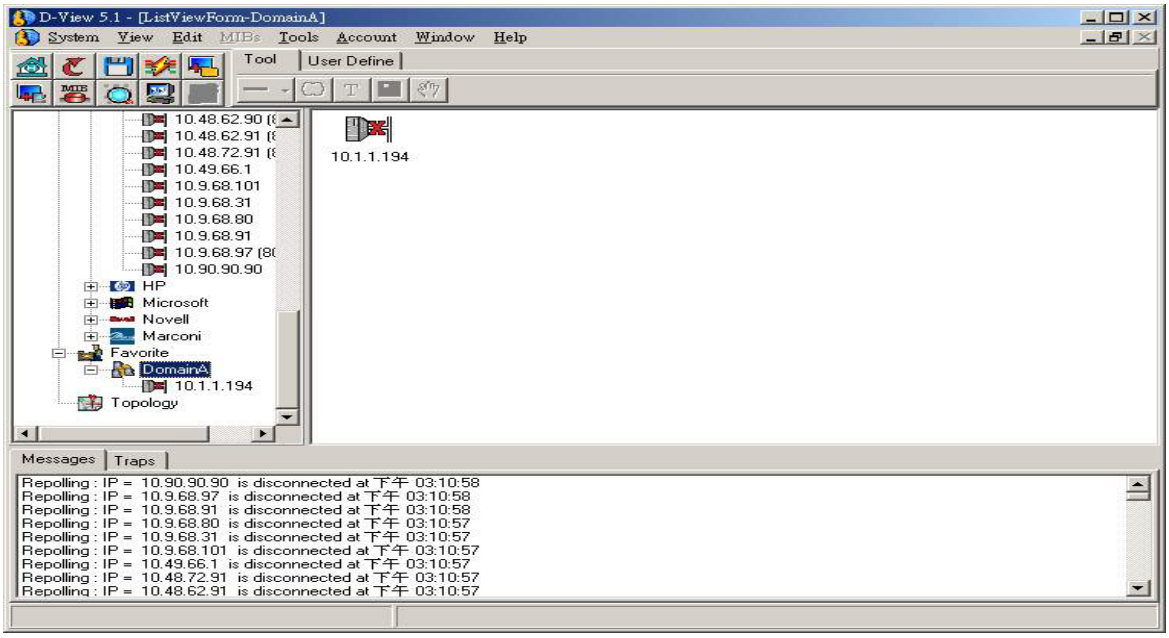

D-View 5.1 - [ListViewForm-DomainA]
System View Edit MIBs Tools Account Window Help
Tool User Define
10.48.62.90
10.48.62.91
10.48.72.91
10.49.66.1
10.9.68.101
10.9.68.31
10.9.68.80
10.9.68.91
10.9.68.97
10.90.90.90
HP
Microsoft
Novell
Marconi
Favorite
DomainA
10.1.1.194
Topology
10.1.1.194
Messages Traps
Repolling : IP = 10.90.90.90 is disconnected at 下午 03:10:58
Repolling : IP = 10.9.68.97 is disconnected at 下午 03:10:58
Repolling : IP = 10.9.68.91 is disconnected at 下午 03:10:58
Repolling : IP = 10.9.68.80 is disconnected at 下午 03:10:57
Repolling : IP = 10.9.68.31 is disconnected at 下午 03:10:57
Repolling : IP = 10.9.68.101 is disconnected at 下午 03:10:57
Repolling : IP = 10.49.66.1 is disconnected at 下午 03:10:57
Repolling : IP = 10.48.72.91 is disconnected at 下午 03:10:57
Repolling : IP = 10.48.62.91 is disconnected at 下午 03:10:57

Figure 31.

Scenario 2: Managing device 10.1.1.194

Using "Web Configure"

Step 1: Right click on mouse to execute "Web Configure"

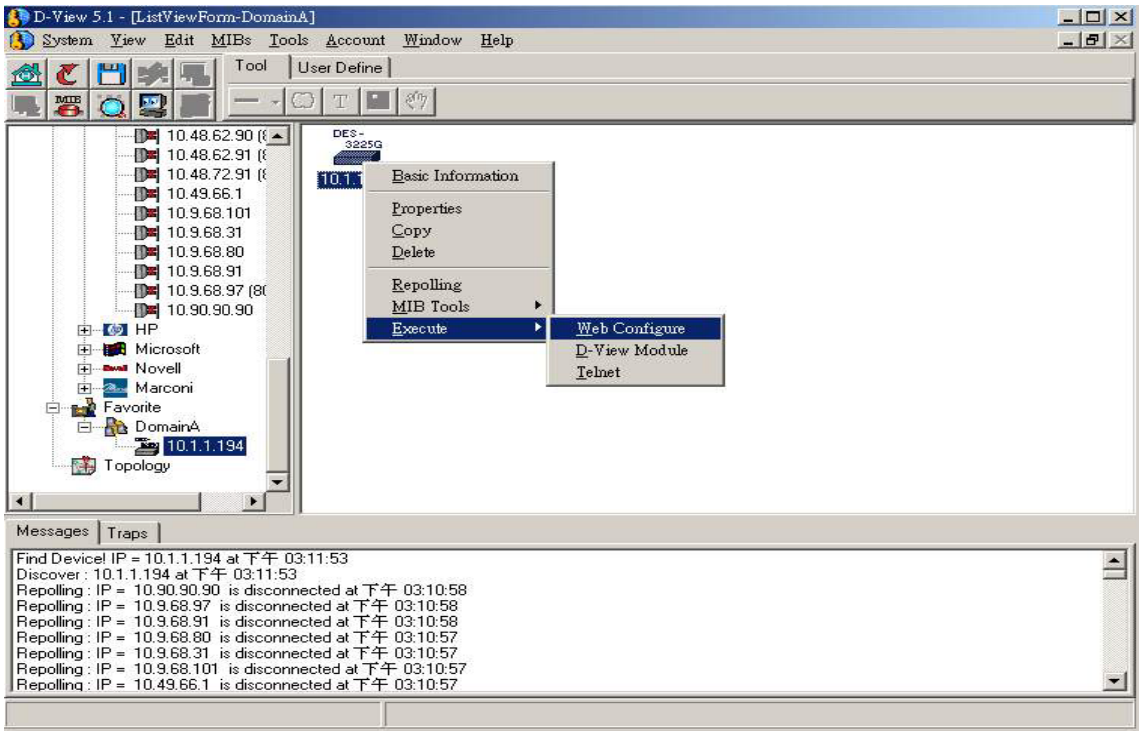


Figure 32.

Step 2:

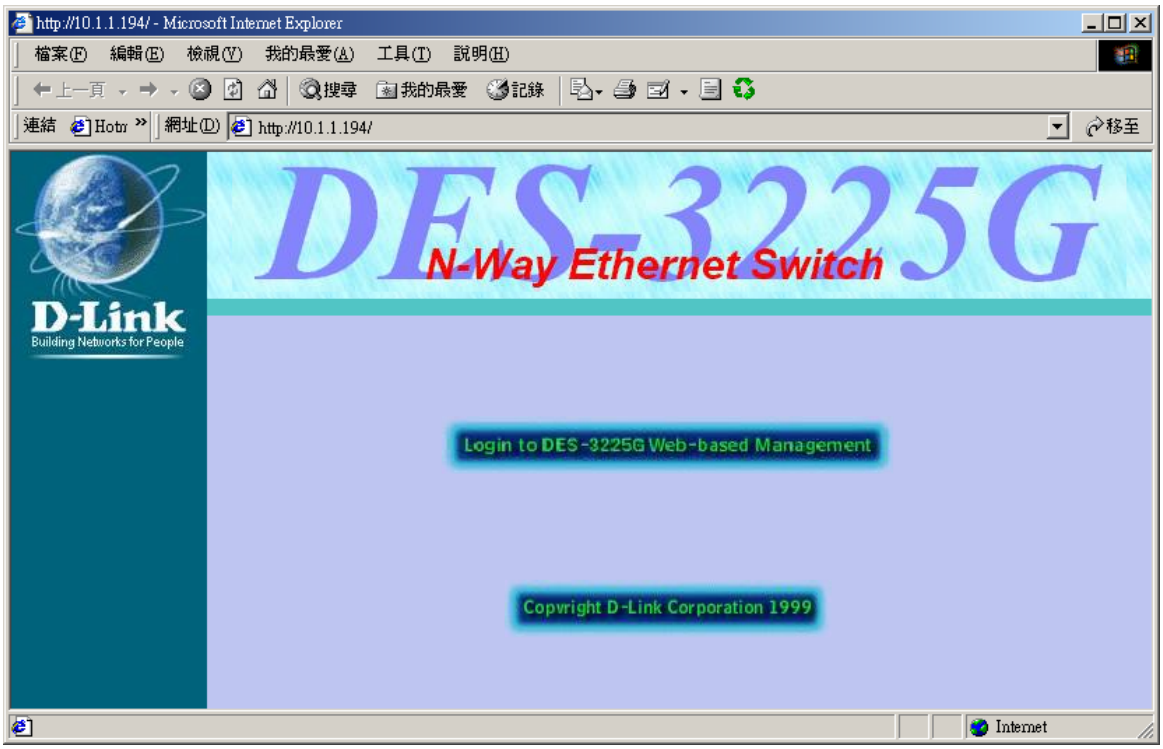


Figure 33.

Using the "D-View Module"

Double-click on the device Icon or right-click on "D-View Module" to execute:

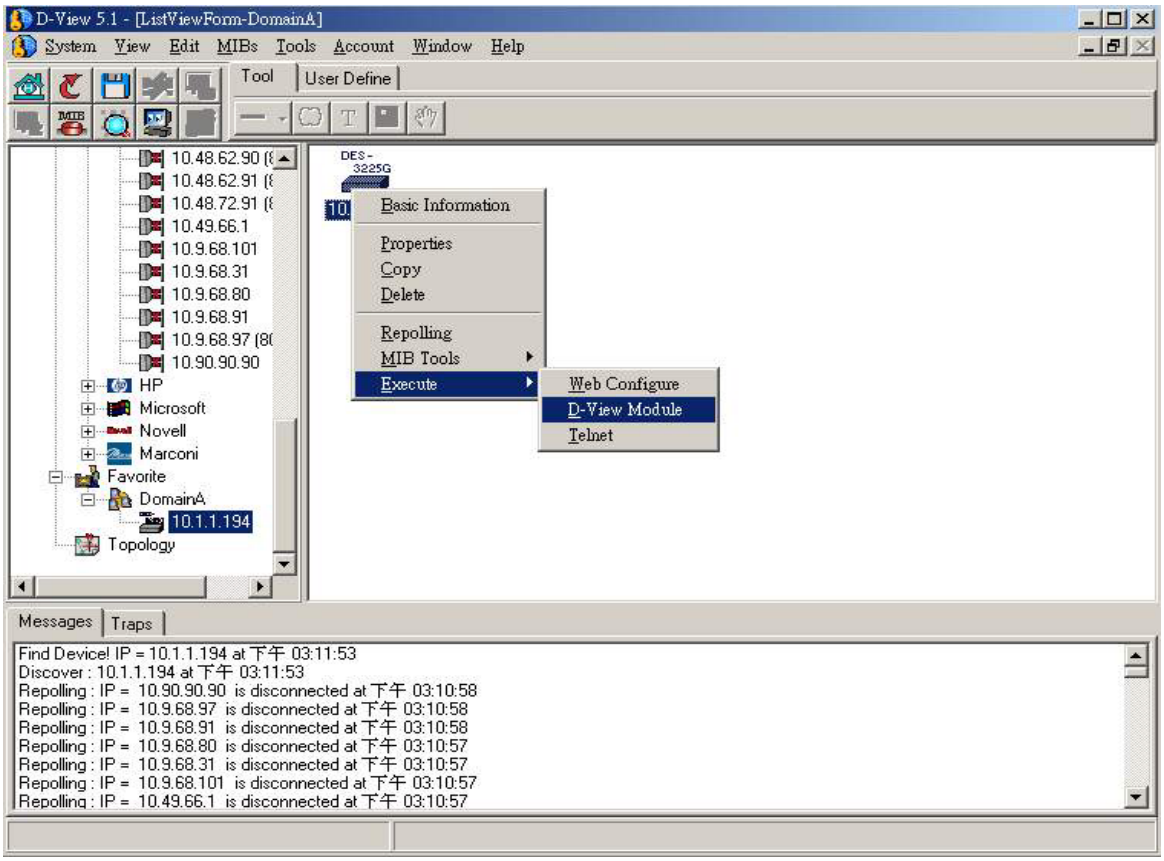


Figure 34.

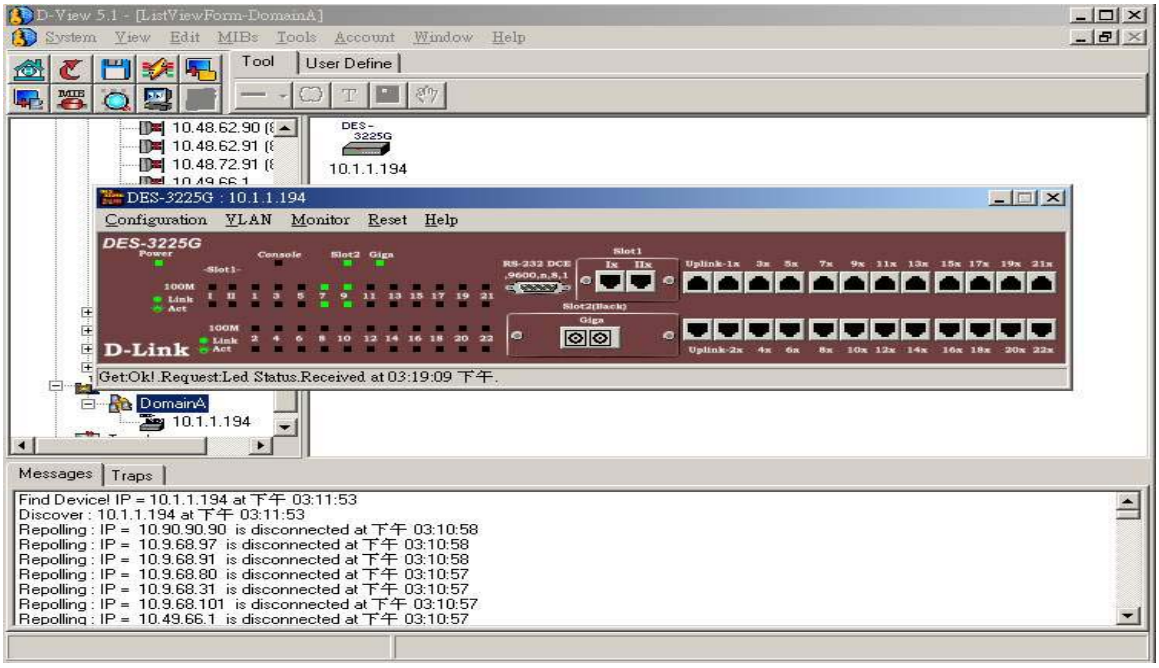

D-View 5.1 - [ListViewForm-DomainA]
System View Edit MIBs Tools Account Window Help
Tool User Define
10.48.62.90
10.48.62.91
10.48.72.91
10.1.1.194
DES-3225G : 10.1.1.194
Configuration VLAN Monitor Reset Help
DES-3225G
D-Link
Get:Ok! Request:Led Status.Received at 03:19:09 下午.
DomainA
10.1.1.194
Messages Traps
Find Device! IP = 10.1.1.194 at 下午 03:11:53
Discover : 10.1.1.194 at 下午 03:11:53
Repolling : IP = 10.90.90.90 is disconnected at 下午 03:10:58
Repolling : IP = 10.9.68.97 is disconnected at 下午 03:10:58
Repolling : IP = 10.9.68.91 is disconnected at 下午 03:10:58
Repolling : IP = 10.9.68.80 is disconnected at 下午 03:10:57
Repolling : IP = 10.9.68.31 is disconnected at 下午 03:10:57
Repolling : IP = 10.9.68.101 is disconnected at 下午 03:10:57
Repolling : IP = 10.49.66.1 is disconnected at 下午 03:10:57

Figure 35.

Using Telnet

Right-click on mouse to execute telnet.

Step 1

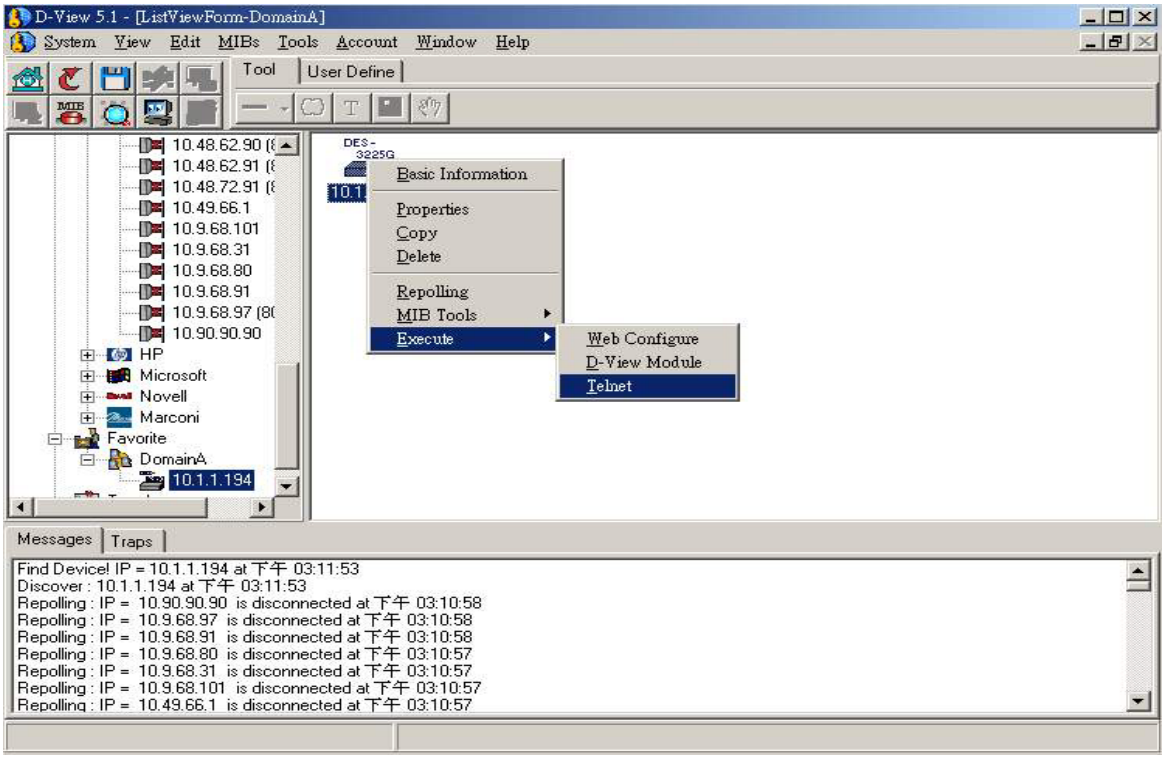


Figure 36.

Step 2

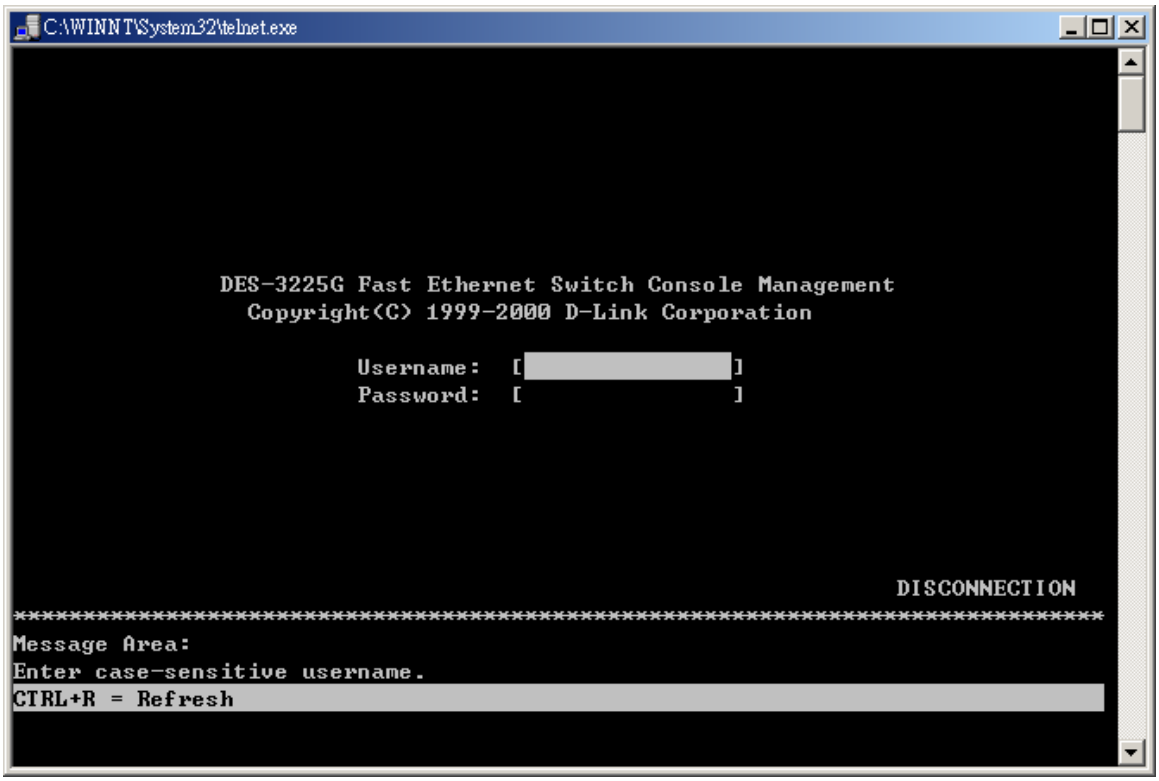


Figure 37.

Changing device properties

When you need to modify an IP address for a device use the "Properties" menu item on the device pop-up menu to change its identity.

Scenario 1: Changing the device 10.1.1.194 from DES-3225G to DES-3226

Step1: Right-click with mouse on "Properties"

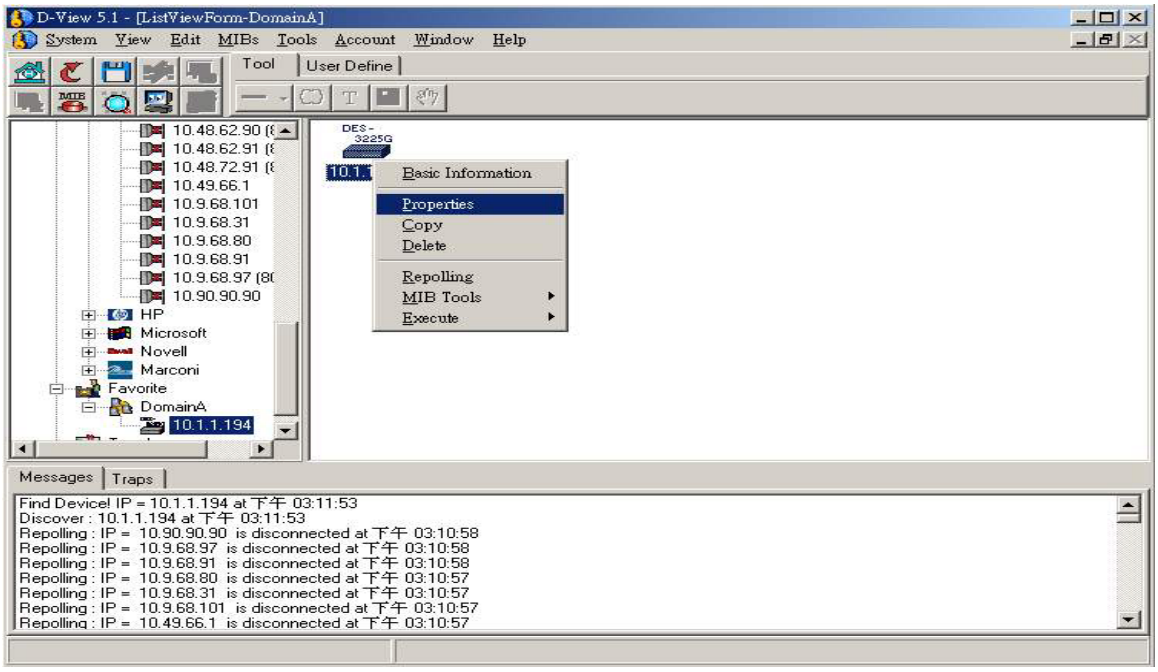


Figure 38.

Step2: Press the "Type" Button

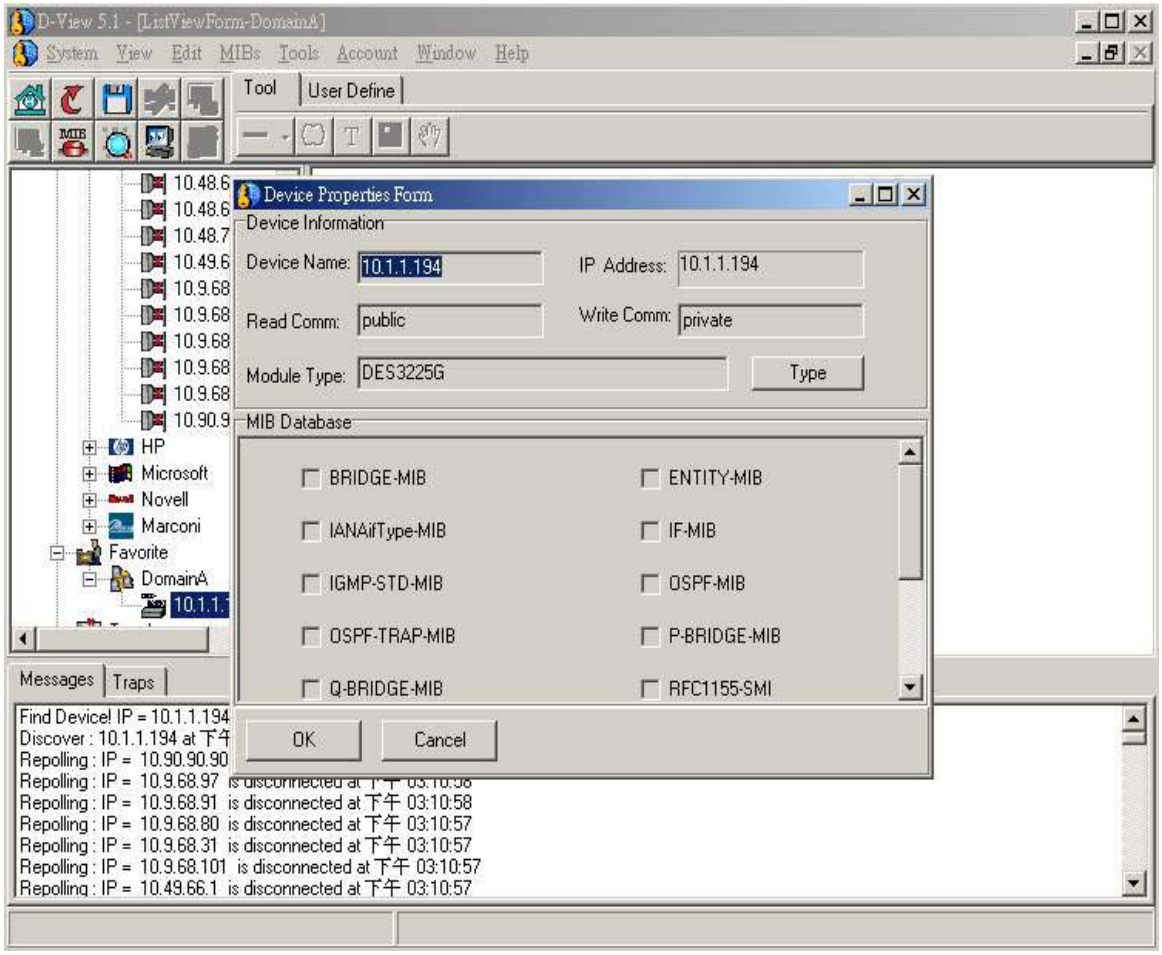


Figure 39.

Step3: Select D-Link and DES 3226. Then Press OK.

Figure 40.

Step 4: Properties have been changed.

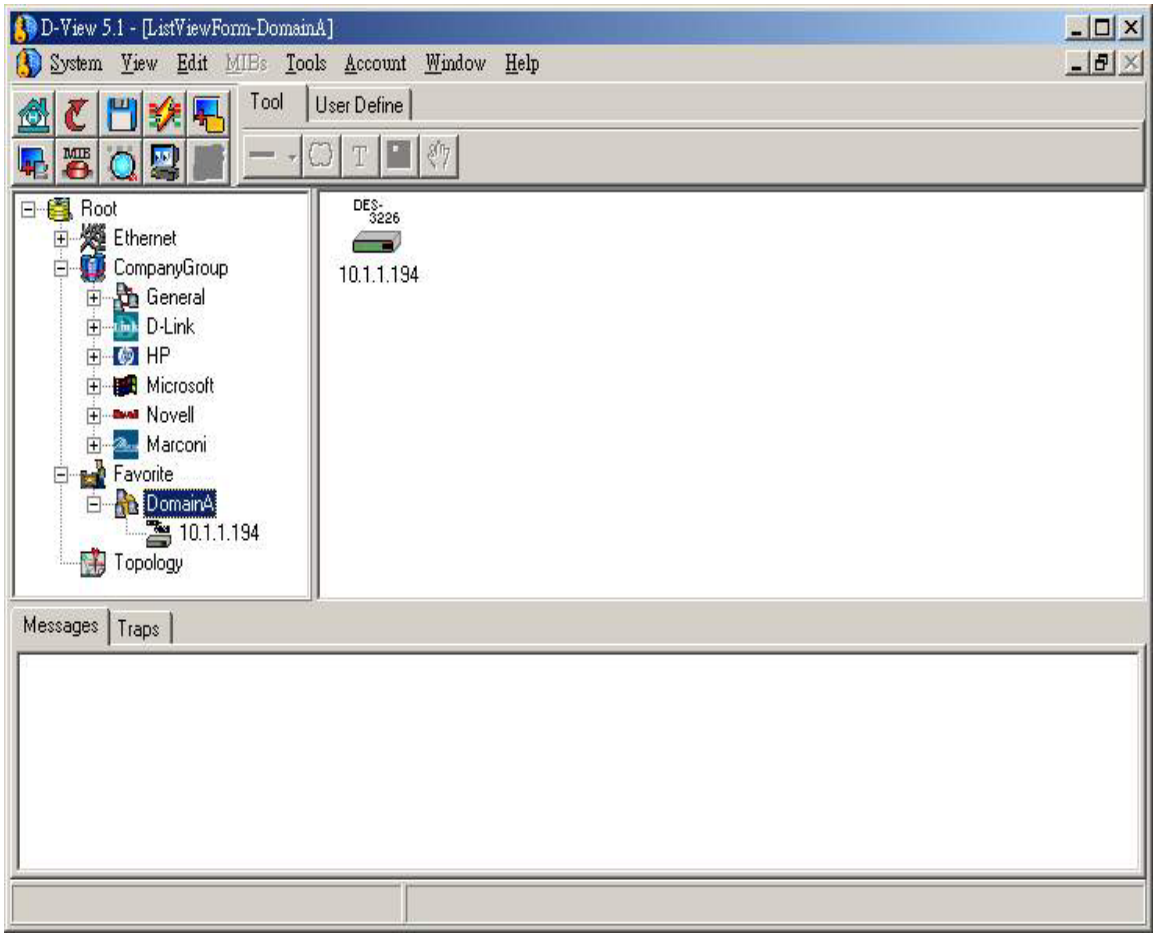


Figure 41.

Collect trap information to log file

The user can log the trap history. The trap filename and path is /DLINK_INSTALL_PATH/var/log/trap.log. The user can clear it by using any editor to view and clear it.

Log On Trap:

System→Trap Management→Log→Log On

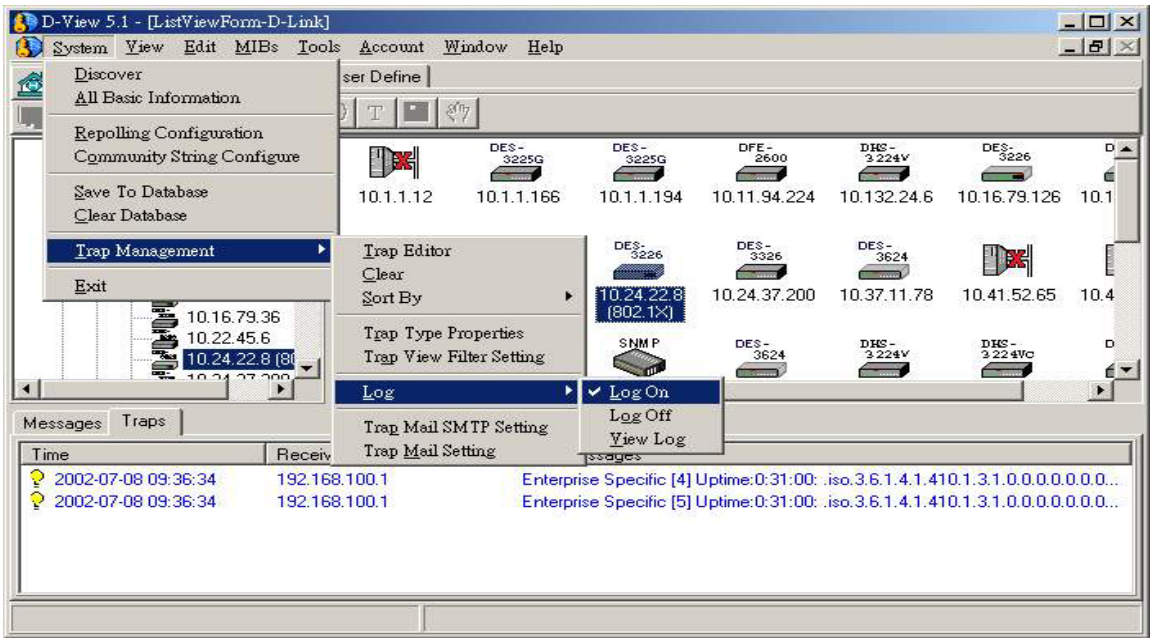


Figure 42.

Log Off Trap:

System→Trap Management→Log→Log Off

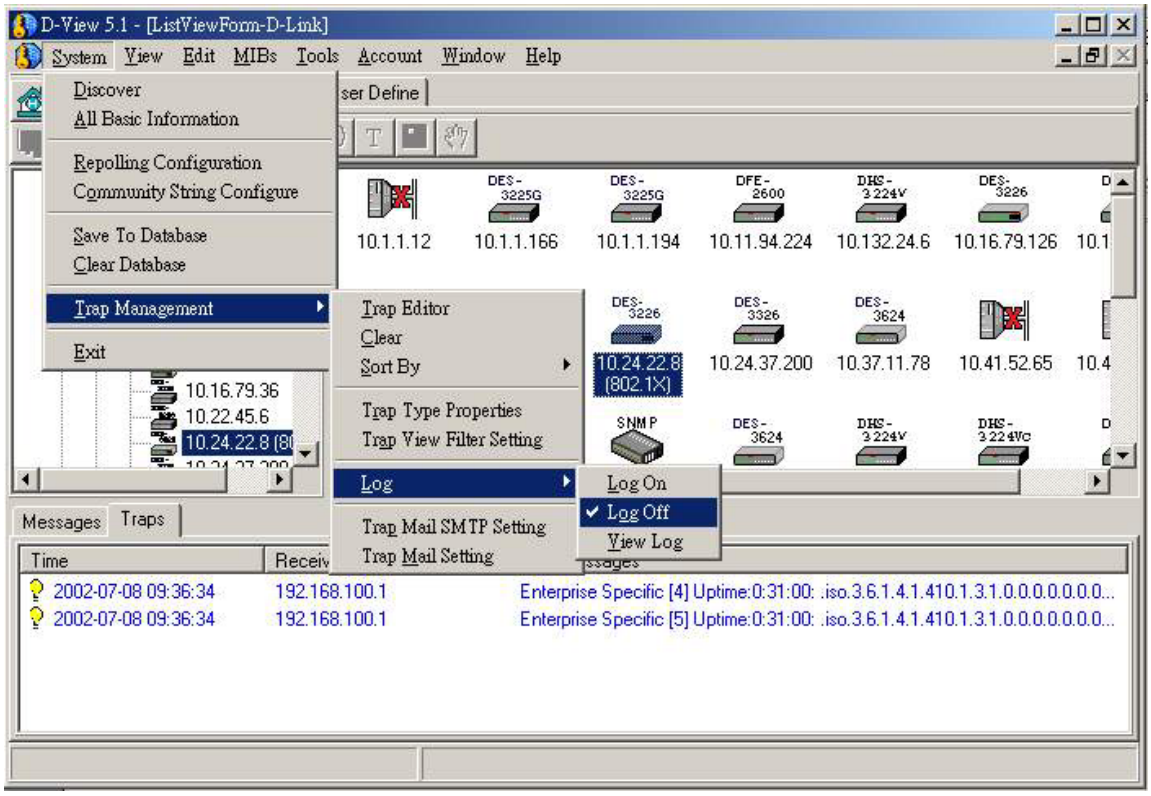


Figure 43.

View Trap and Edit:

System→Trap Management→Log→View Log

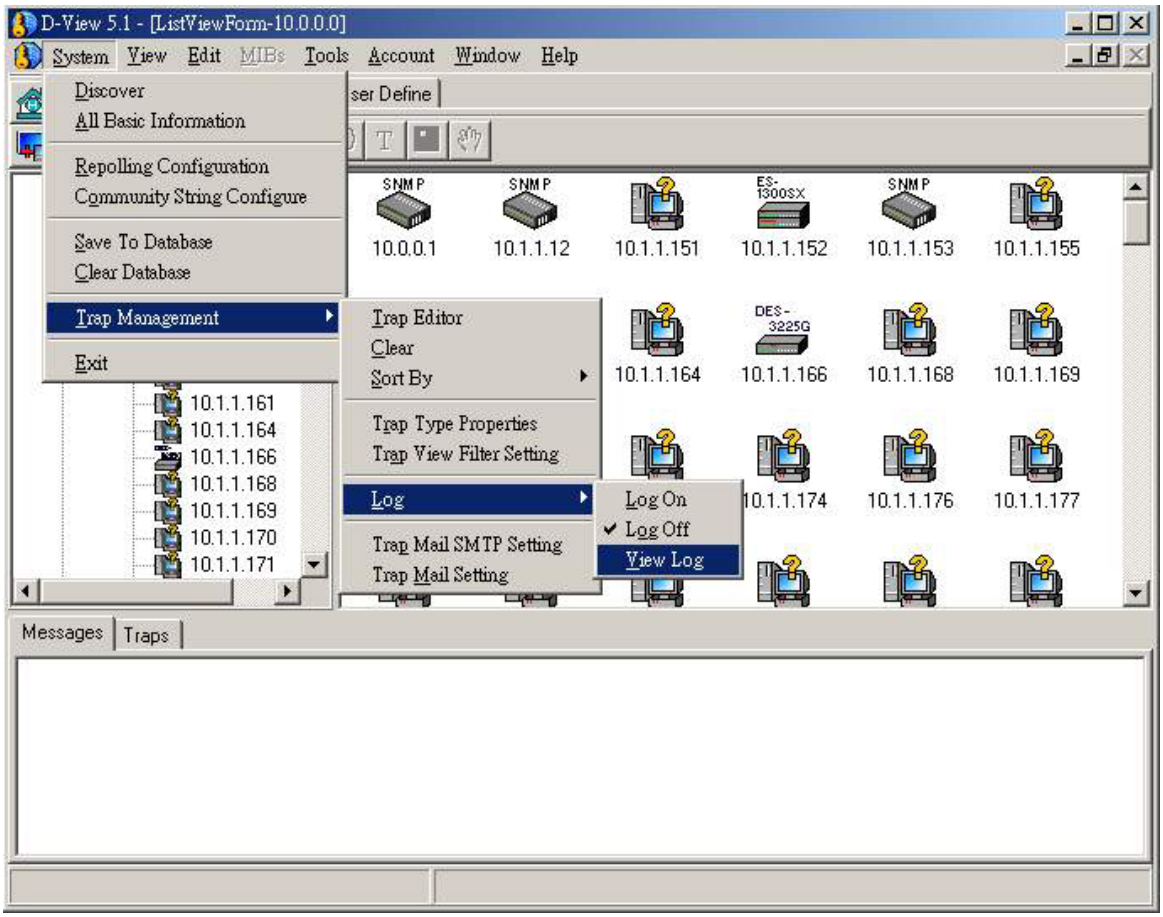


Figure 44.

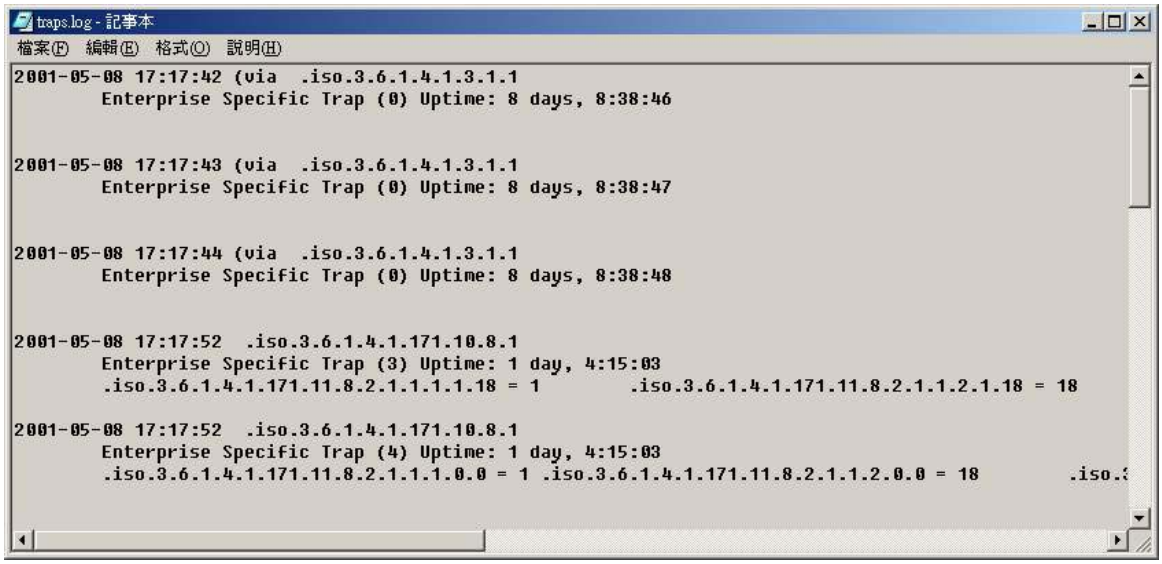


Figure 45.

Note: ***For more on trap management functions please refer to Chapter 6: Advanced Management.***

Install Plug-in management module

If you need more management modules for devices, install the plug-in management module. You can get modules from http://www.dlink.com.tw where all D-View supported modules can be found. You can download all of these modules. When the module has been installed, double-click on your chosen icon and a device panel will appear. To date D-View supports many kinds of D-Link SNMP products. You are welcome to visit the D-Link web page for more information.

Scenario: Installing Plug-in DES3326 Device Module

Step 1

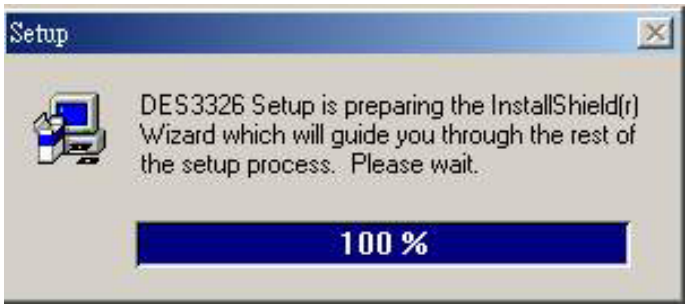


Figure 46.

Step 2

Figure 47.

Step 3

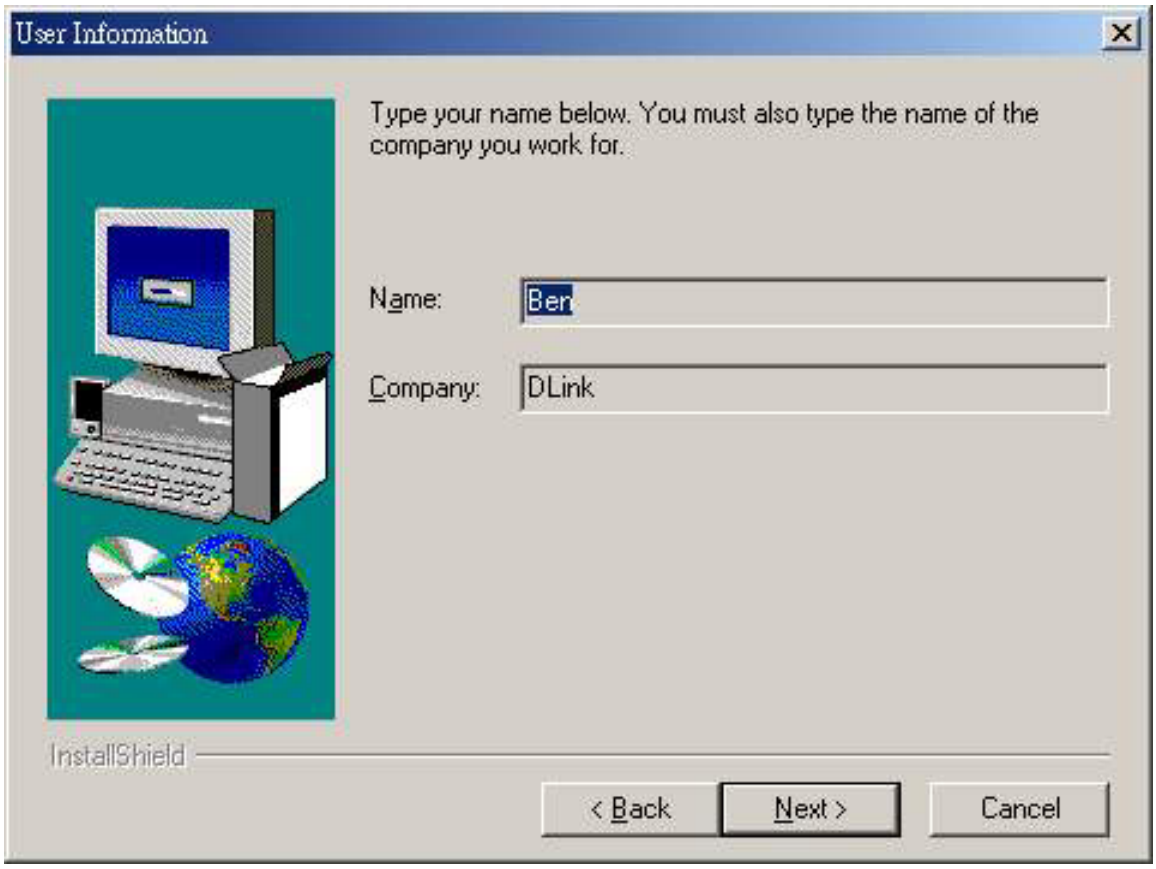


Figure 48.

Step 4

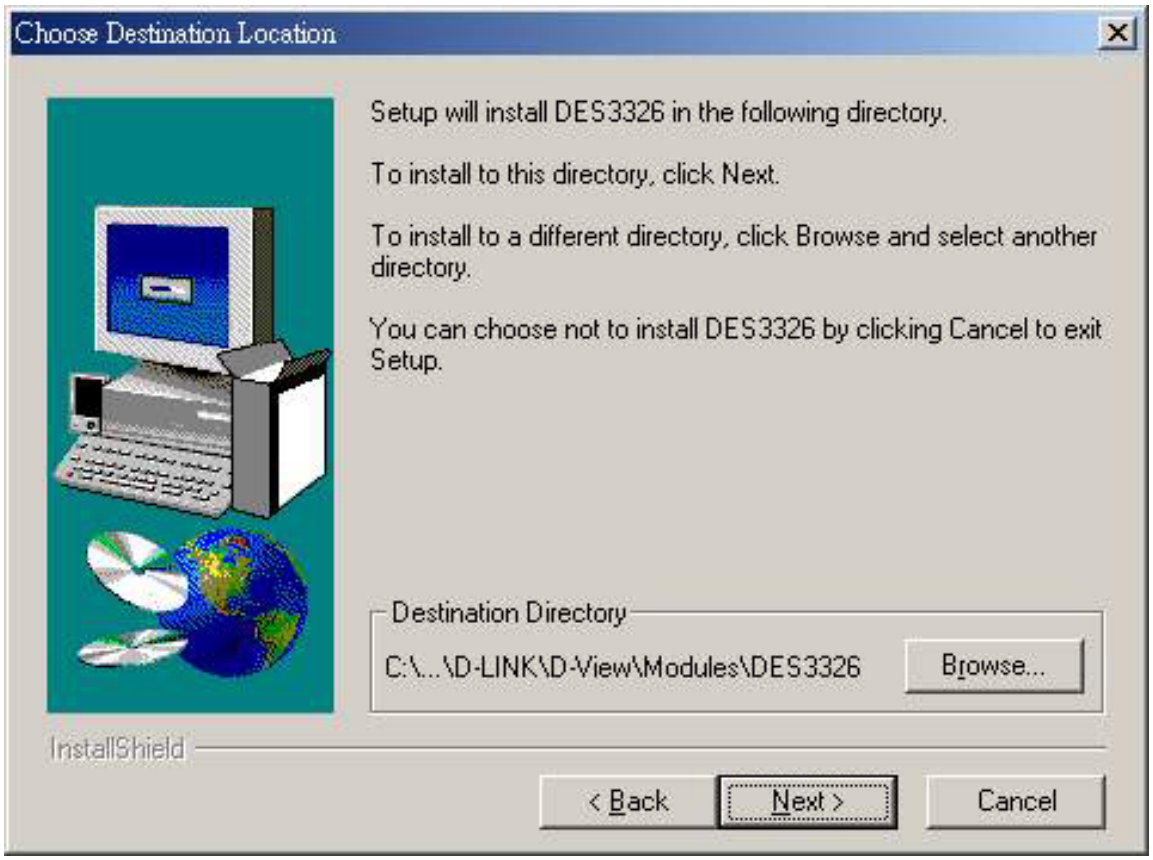


Figure 49.

Step 5

Figure 50.

Step 6

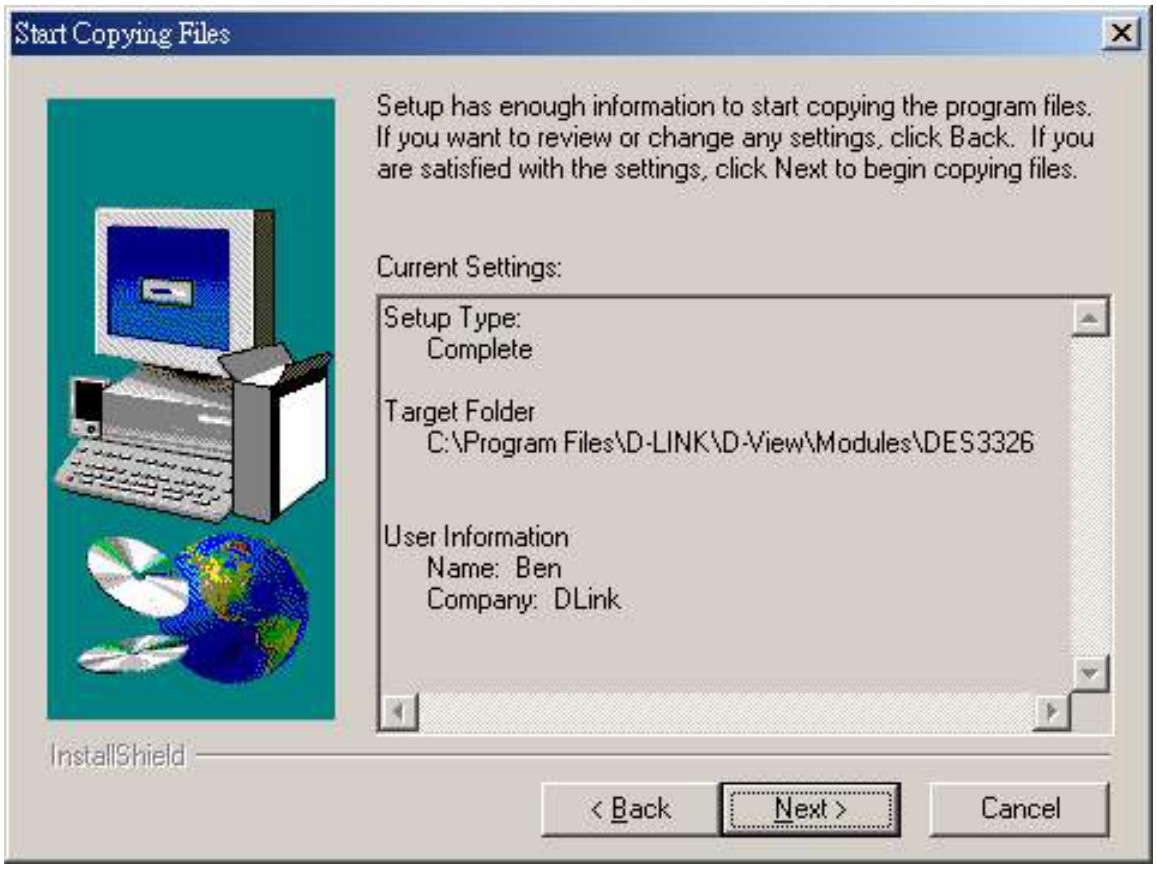


Figure 51.

Step 7

Figure 52.

Managing SNMP Devices without a management module

MIB Browser

When you need to manage a SNMP device without a plug-in module in the D-View platform use a D-View supported MIB browser with the associated MIBs. Right-click on the chosen icon and you will see a "Properties" item on the pop-up menu. Click it and a dialog box will appear with an area listing many MIBs with checkboxes. Select which MIBs the device supports. Then click OK. Go back to the work area, right-click on the icon again. Select "MIB browser." This will invoke the MIB browser with the MIBs that you selected. Now you can use the MIB browser to manage devices.

Note: ***Before using MIB browser, you have to retrieve MIB files from a vendor who develops SNMP devices. You can then use the MIB compiler to compile MIBs. If compilation is successful, then the MIB compiler will store MIBs to database, and you will see the entire MIBs list under device properties.***

How to Use MIB Browser

Step 1: Choose the device you wish to browse, right-click to bring up a menu and left-click on "Properties"

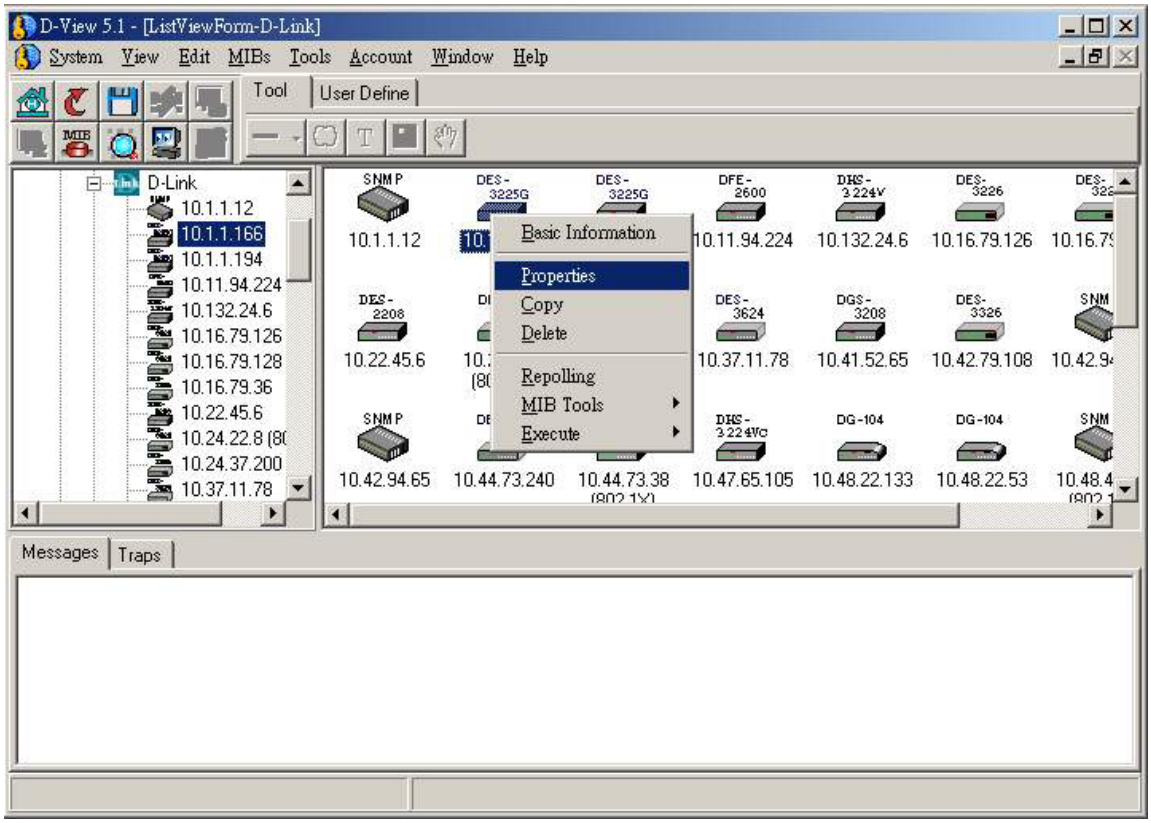


Figure 53.

Step 2: Enter settings and press OK.

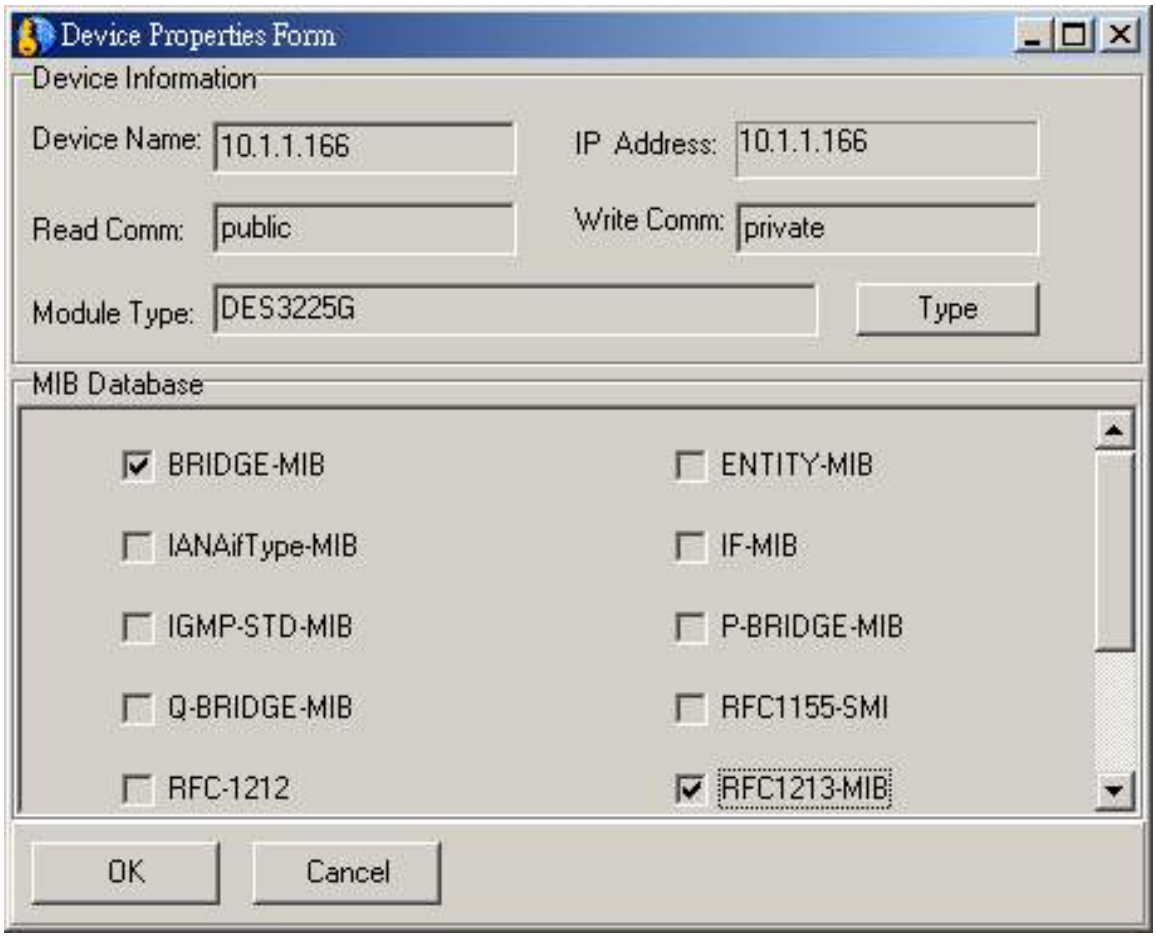


Figure 54.

Step 3: Open "MIB Browser"

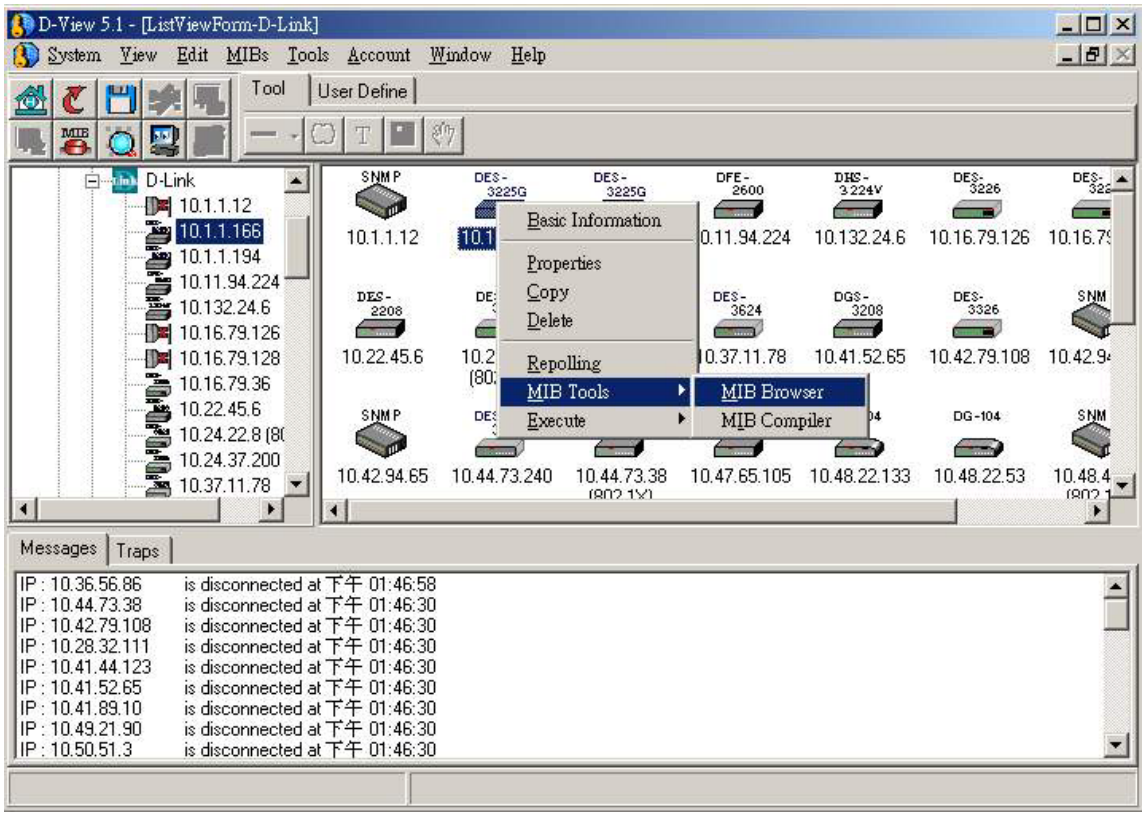


Figure 55.

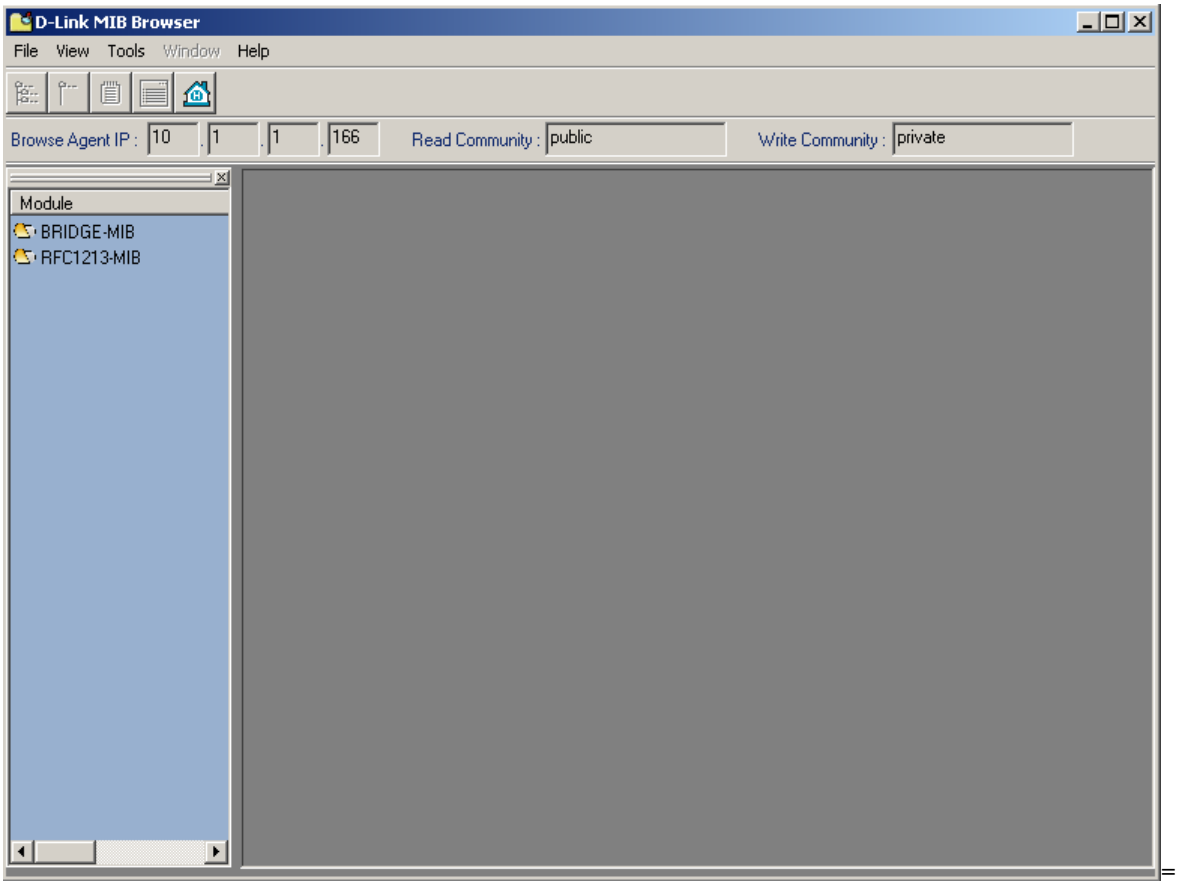

D-Link MIB Browser
File View Tools Window Help
Browse Agent IP : 10 . 1 . 1 . 166
Read Community : public
Write Community : private
Module
BRIDGE-MIB
RFC1213-MIB

Figure 56.

Step 4: Double-click on RFC1213-MIB

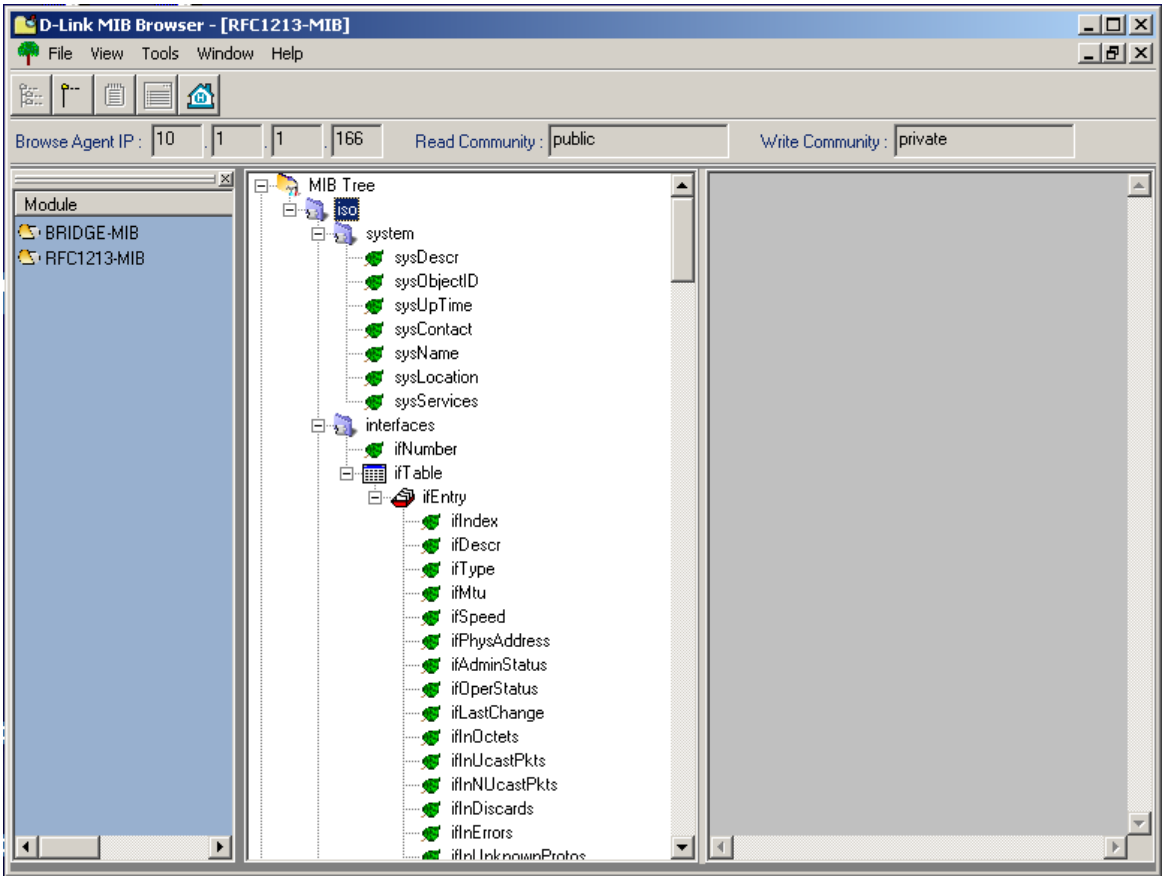


Figure 57.

Step 5: Use MIB Browser to manage these entities

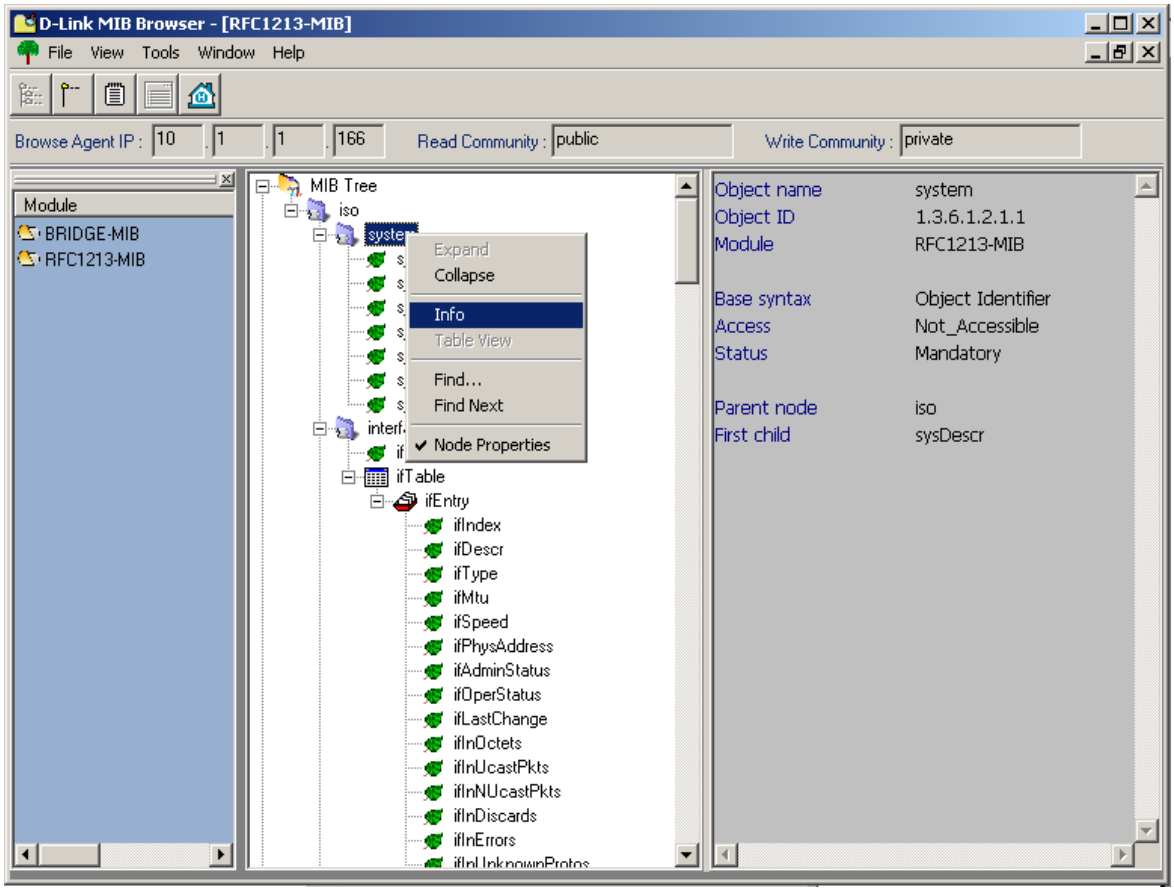


Figure 58.

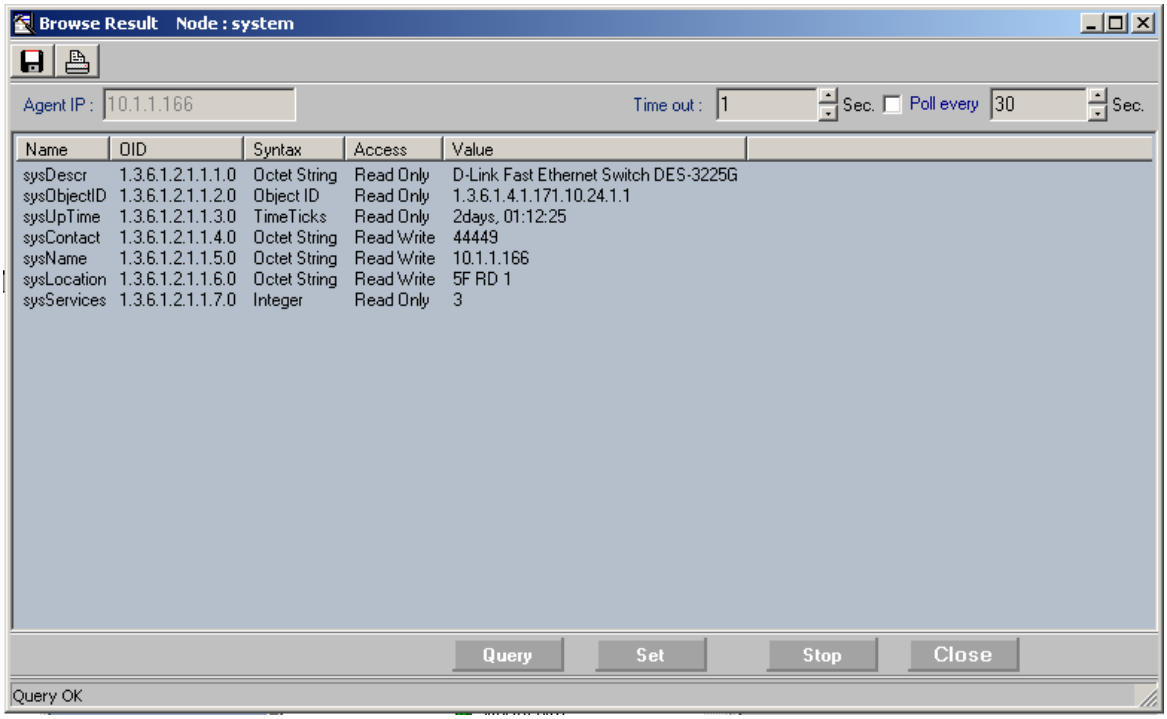


Figure 59.

MIB Compiler

The MIB Compiler provides another way to manage SNMP devices without a management module. It compiles an original Management Information Base (MIB) textual file into a system recognized format and loads it into a database. It converts a MIB into a graphic tree view. A node of the tree represents an object in the MIB. The relationship between nodes of the tree reflects OIDs of corresponding objects in the MIB.

The compiler shows detailed definitions of each object in the MIB:

- Object name
- OID
- Module to which the object belongs
- Syntax
- Access limit
- Status
- Description, and so on.

The compiler can communicate with a remote device (bridge, switch, or router) to get the current value or to set a new value for the MIB object of interest. This is achieved by sending SNMP requests and receiving SNMP responses to get/set the value of the object of the MIB, which resides in an SNMP enabled device.

Note: ***Not every MIB is needed to be implemented in any SNMP enabled device***

The current values of the MIB objects of a specific device can be obtained in two ways: "Info" or "Table View." "Info" shows more detailed information for objects, both definitions and values. "Table view" shows only the values of objects.

How to Use the MIB Complier:

Step 1: Invoke the MIB Compiler

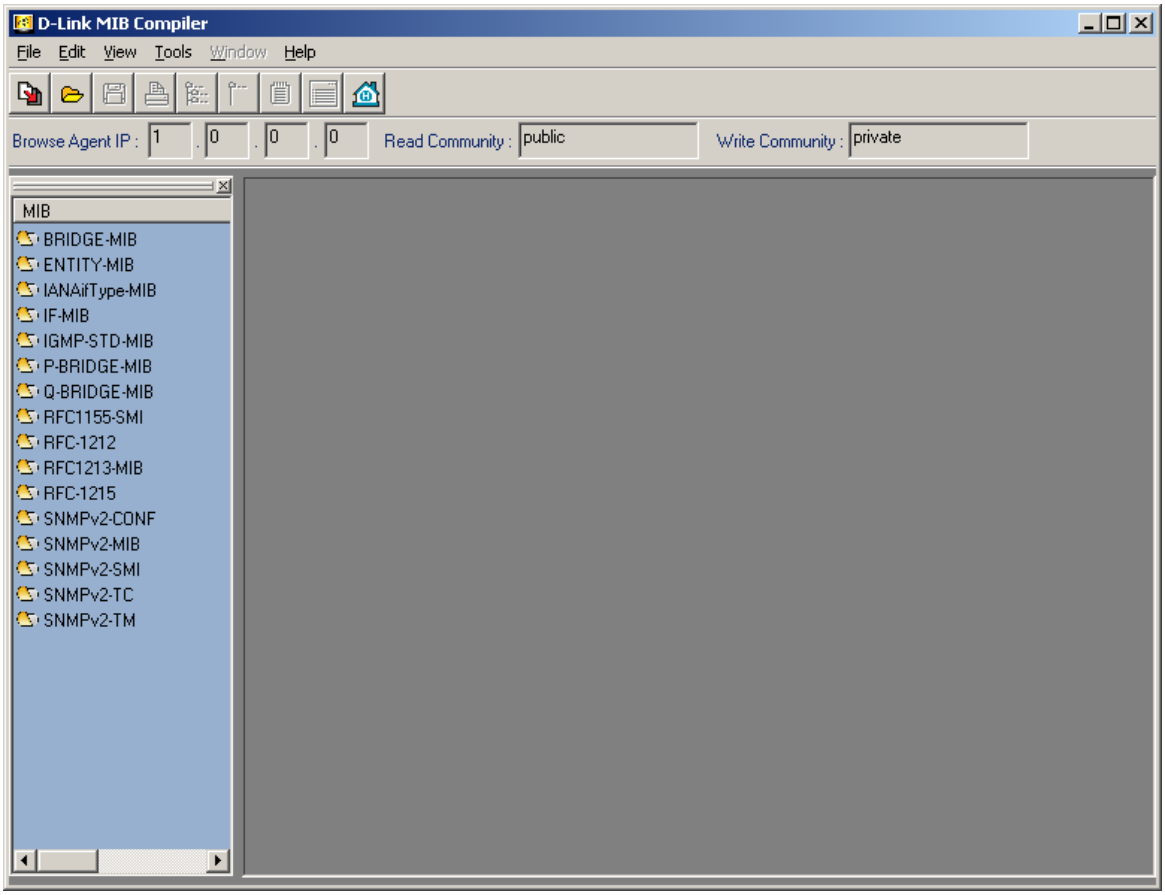


Figure 60.

Step 2: Open up MIB File

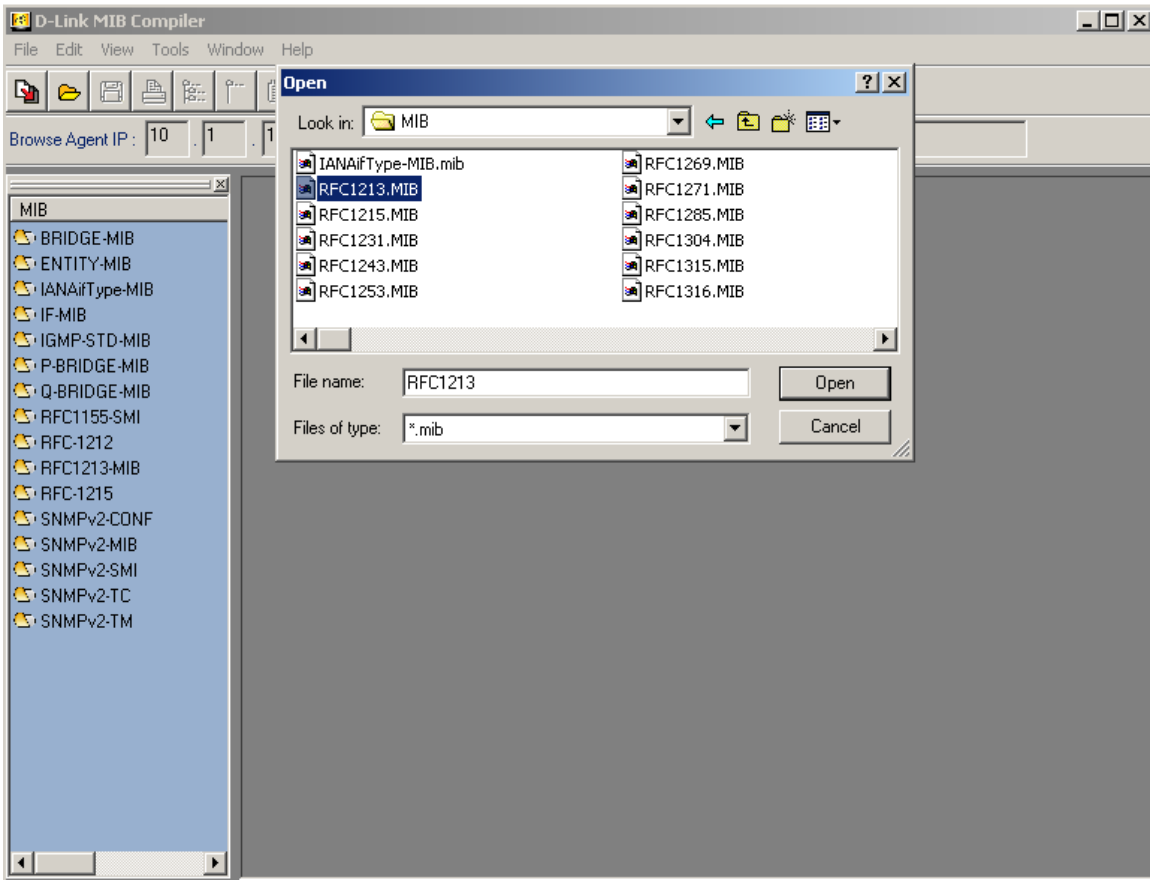


Figure 61.

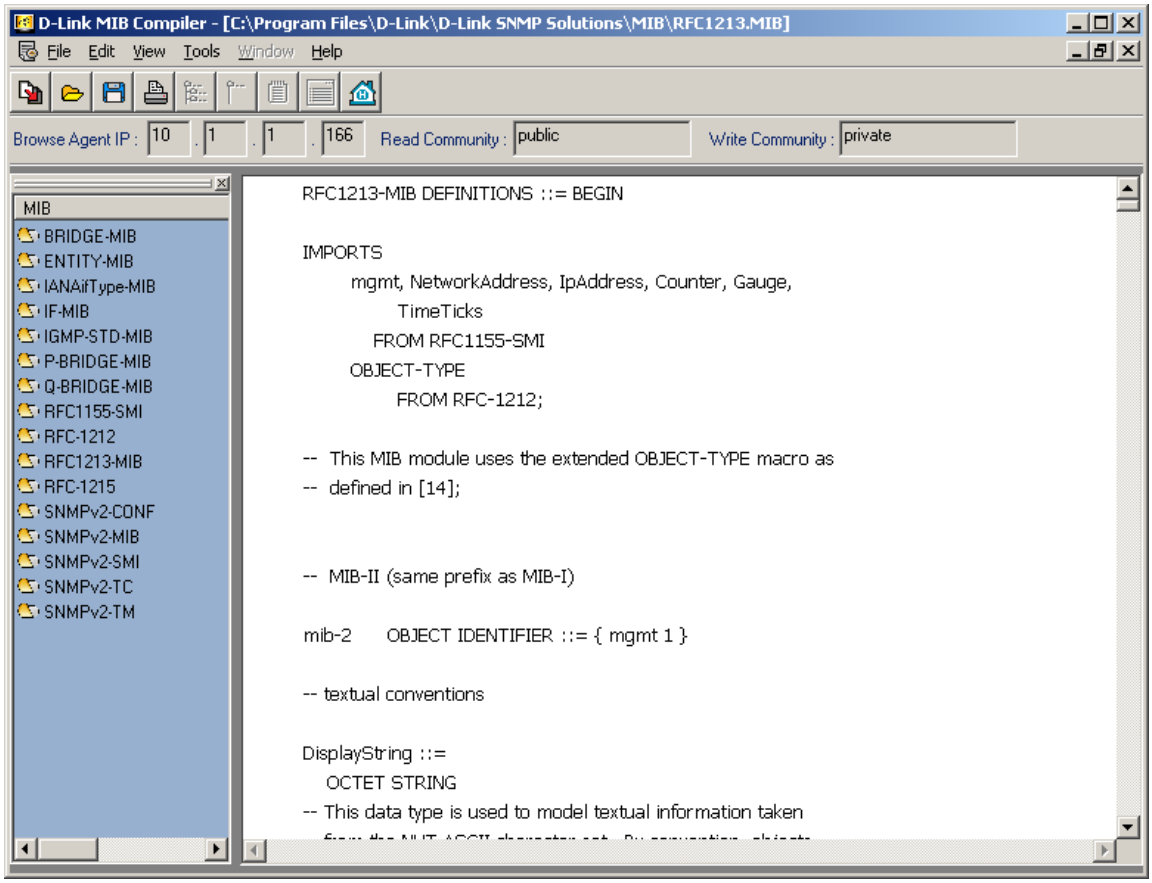

D-Link MIB Compiler - [C:\Program Files\D-Link\D-Link SNMP Solutions\MIB\RFC1213.MIB]
File Edit View Tools Window Help
Browse Agent IP : 10 . 1 . 1 . 166
Read Community : public
Write Community : private
MIB
BRIDGE-MIB
ENTITY-MIB
IANAifType-MIB
IF-MIB
IGMP-STD-MIB
P-BRIDGE-MIB
Q-BRIDGE-MIB
RFC1155-SMI
RFC-1212
RFC1213-MIB
RFC-1215
SNMPv2-CONF
SNMPv2-MIB
SNMPv2-SMI
SNMPv2-TC
SNMPv2-TM
RFC1213-MIB DEFINITIONS ::= BEGIN
IMPORTS
mgmt, NetworkAddress, IpAddress, Counter, Gauge,
TimeTicks
FROM RFC1155-SMI
OBJECT-TYPE
FROM RFC-1212;
-- This MIB module uses the extended OBJECT-TYPE macro as
-- defined in [14];
-- MIB-II (same prefix as MIB-I)
mib-2 OBJECT IDENTIFIER ::= { mgmt 1 }
-- textual conventions
DisplayString ::=
OCTET STRING
-- This data type is used to model textual information taken

Figure 62.

Step 3: Compile the MIB file

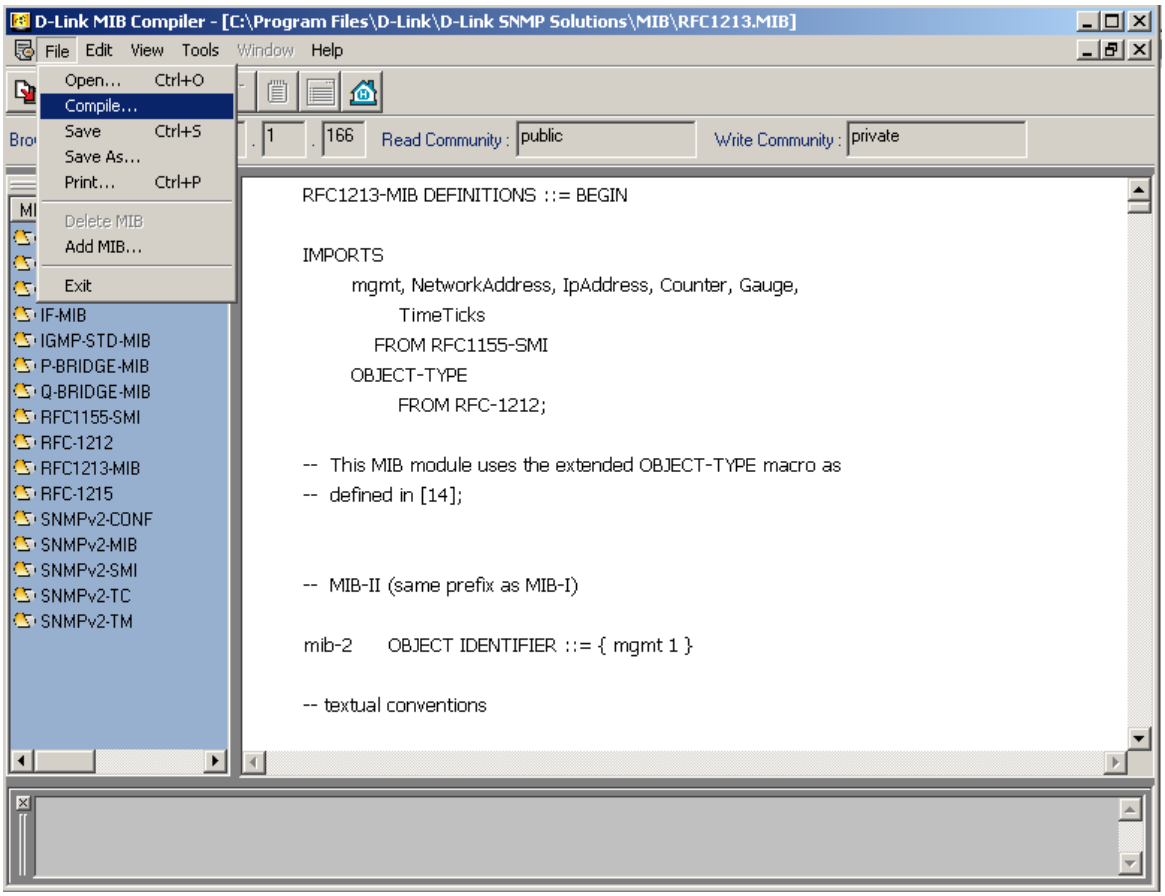


Figure 63.

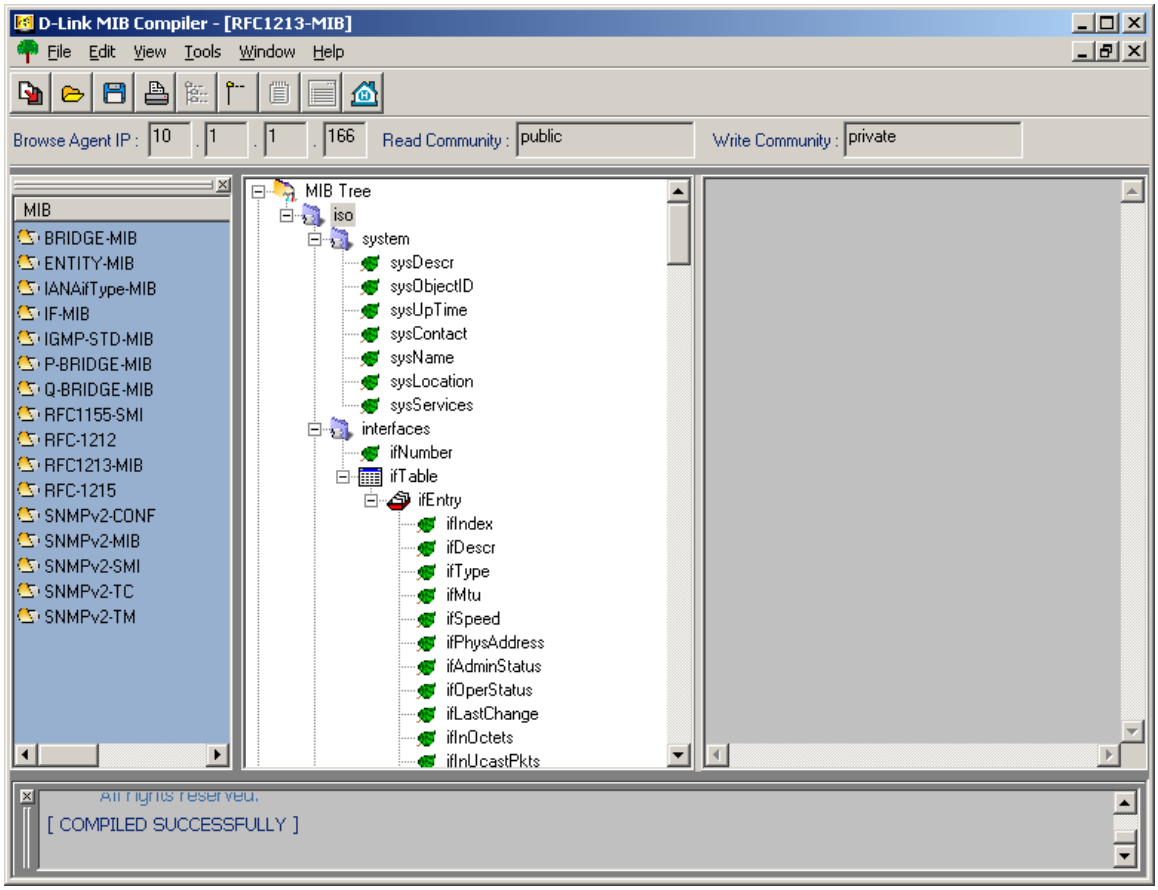

D-Link MIB Compiler - [RFC1213-MIB]
File Edit View Tools Window Help
Browse Agent IP : 10 . 1 . 1 . 166
Read Community : public
Write Community : private
MIB
BRIDGE-MIB
ENTITY-MIB
IANAifType-MIB
IF-MIB
IGMP-STD-MIB
P-BRIDGE-MIB
Q-BRIDGE-MIB
RFC1155-SMI
RFC-1212
RFC1213-MIB
RFC-1215
SNMPv2-CONF
SNMPv2-MIB
SNMPv2-SMI
SNMPv2-TC
SNMPv2-TM
MIB Tree
iso
system
sysDescr
sysObjectID
sysUpTime
sysContact
sysName
sysLocation
sysServices
interfaces
ifNumber
ifTable
ifEntry
ifIndex
ifDescr
ifType
ifMtu
ifSpeed
ifPhysAddress
ifAdminStatus
ifOperStatus
ifLastChange
ifInOctets
ifInUcastPkts
[COMPILED SUCCESSFULLY]

Figure 64.

More on the MIB Compiler

1. How to find the MIB values of a device.

Step 1: Enter Device IP Address by entering the Browser Agent IP address, Read and Write Community settings. Then left-click on the MIB module you wish to view.

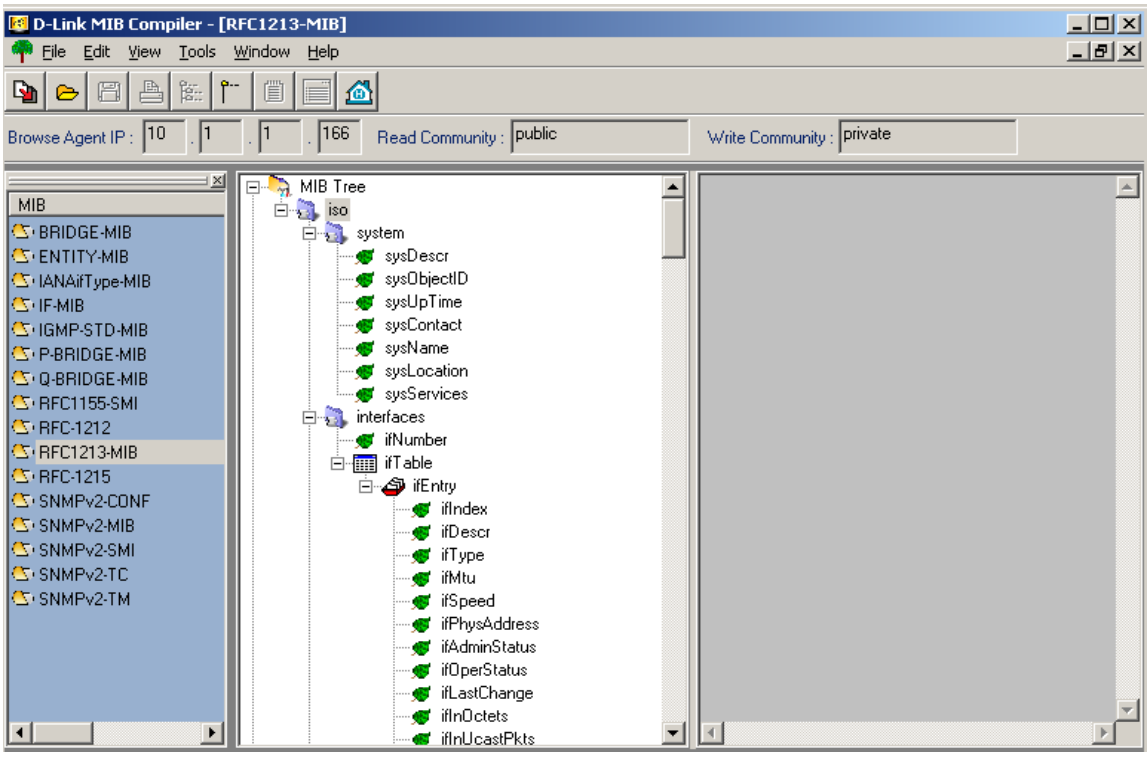


Figure 65.

Step 2: Right-click on object and execute "Info."

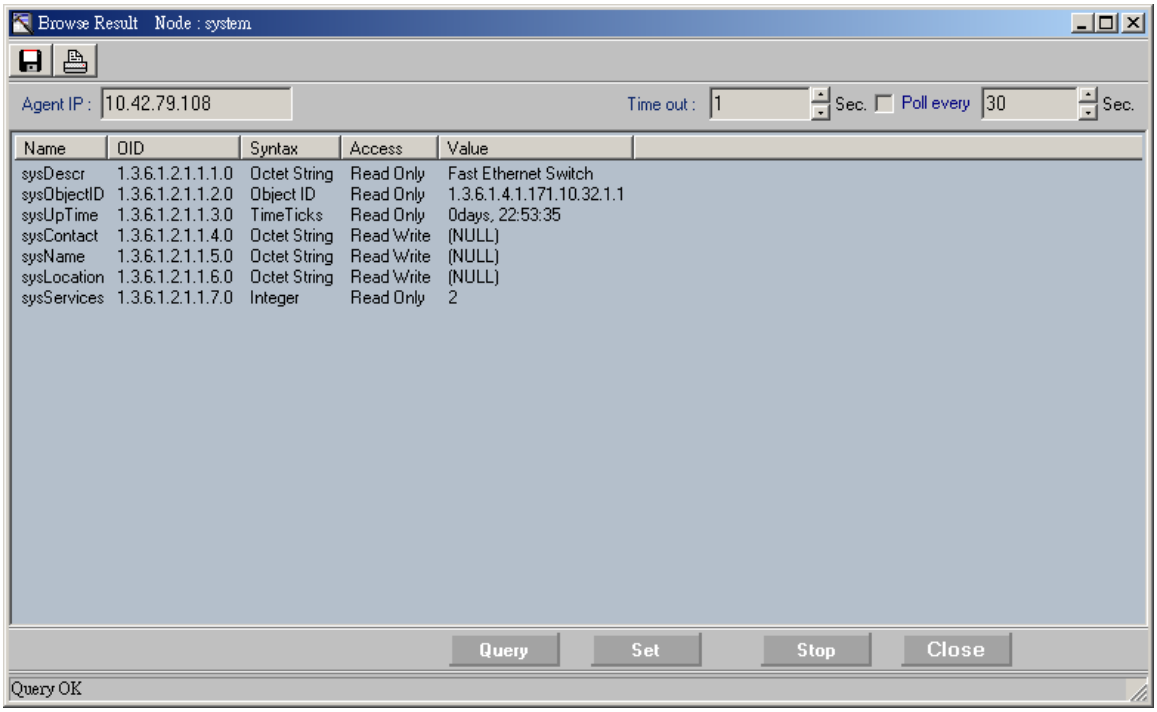
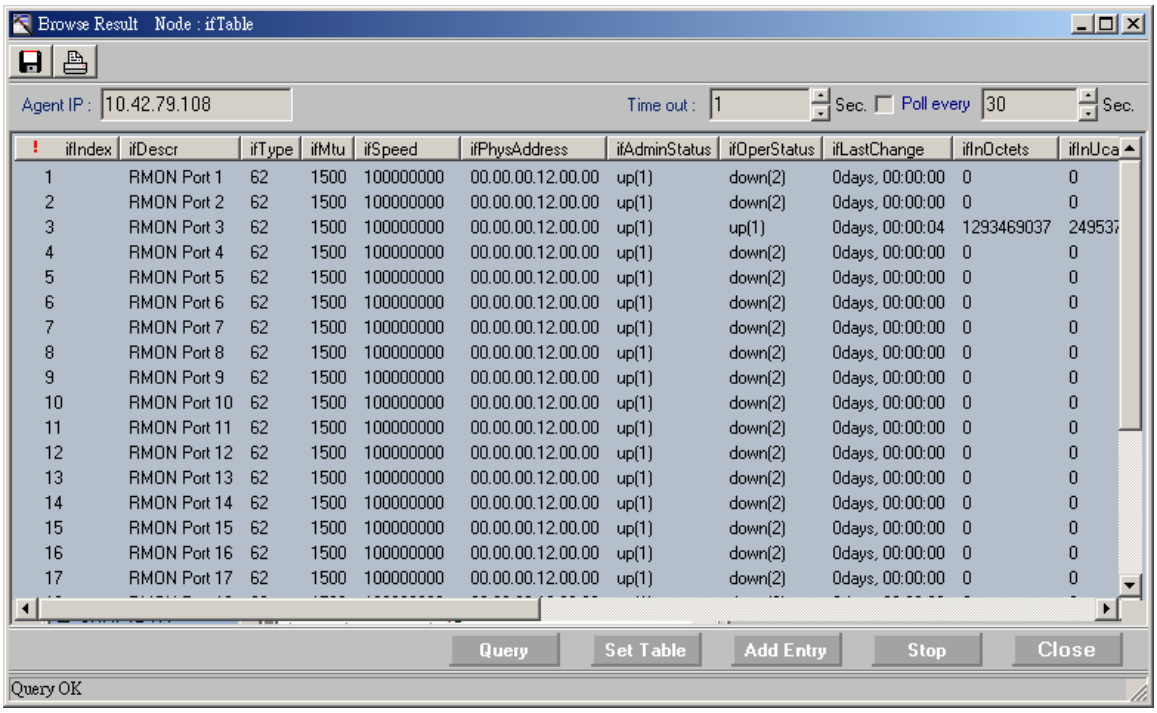


Figure 66.

Left-click on "If Table." Then left-click on "Table View" to display values.



ifIndex	ifDescr	ifType	ifMtu	ifSpeed	ifPhysAddress	ifAdminStatus	ifOperStatus	ifLastChange	ifInOctets	ifInUca
1	RMON Port 1	62	1500	100000000	00.00.00.12.00.00	up(1)	down(2)	0days, 00:00:00	0	0
2	RMON Port 2	62	1500	100000000	00.00.00.12.00.00	up(1)	down(2)	0days, 00:00:00	0	0
3	RMON Port 3	62	1500	100000000	00.00.00.12.00.00	up(1)	up(1)	0days, 00:00:04	1293469037	249537
4	RMON Port 4	62	1500	100000000	00.00.00.12.00.00	up(1)	down(2)	0days, 00:00:00	0	0
5	RMON Port 5	62	1500	100000000	00.00.00.12.00.00	up(1)	down(2)	0days, 00:00:00	0	0
6	RMON Port 6	62	1500	100000000	00.00.00.12.00.00	up(1)	down(2)	0days, 00:00:00	0	0
7	RMON Port 7	62	1500	100000000	00.00.00.12.00.00	up(1)	down(2)	0days, 00:00:00	0	0
8	RMON Port 8	62	1500	100000000	00.00.00.12.00.00	up(1)	down(2)	0days, 00:00:00	0	0
9	RMON Port 9	62	1500	100000000	00.00.00.12.00.00	up(1)	down(2)	0days, 00:00:00	0	0
10	RMON Port 10	62	1500	100000000	00.00.00.12.00.00	up(1)	down(2)	0days, 00:00:00	0	0
11	RMON Port 11	62	1500	100000000	00.00.00.12.00.00	up(1)	down(2)	0days, 00:00:00	0	0
12	RMON Port 12	62	1500	100000000	00.00.00.12.00.00	up(1)	down(2)	0days, 00:00:00	0	0
13	RMON Port 13	62	1500	100000000	00.00.00.12.00.00	up(1)	down(2)	0days, 00:00:00	0	0
14	RMON Port 14	62	1500	100000000	00.00.00.12.00.00	up(1)	down(2)	0days, 00:00:00	0	0
15	RMON Port 15	62	1500	100000000	00.00.00.12.00.00	up(1)	down(2)	0days, 00:00:00	0	0
16	RMON Port 16	62	1500	100000000	00.00.00.12.00.00	up(1)	down(2)	0days, 00:00:00	0	0
17	RMON Port 17	62	1500	100000000	00.00.00.12.00.00	up(1)	down(2)	0days, 00:00:00	0	0

Figure 67.

2. How to set Device MIB values.

After completing 1. , left-click on "MIB Entry." Execute "Set" or "Set Table" to set MIB values. Or double click on "Entry."

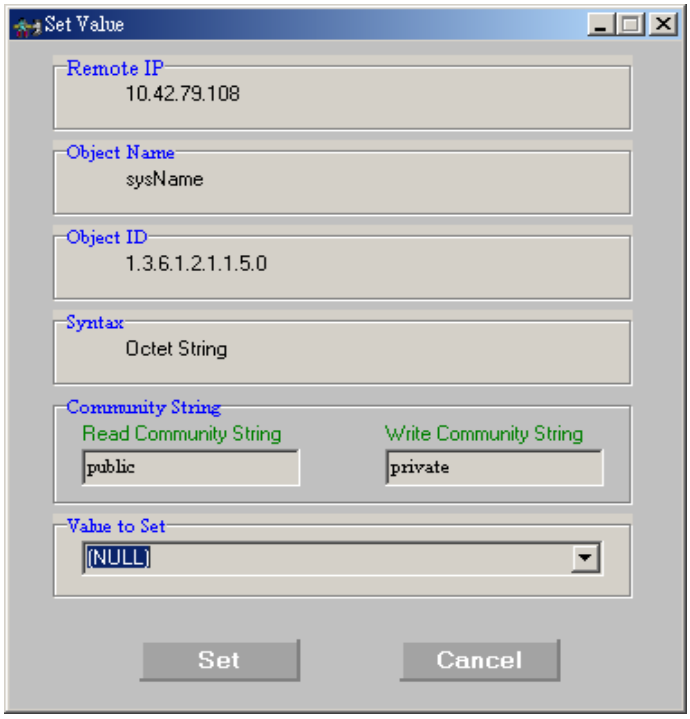


Figure 68.

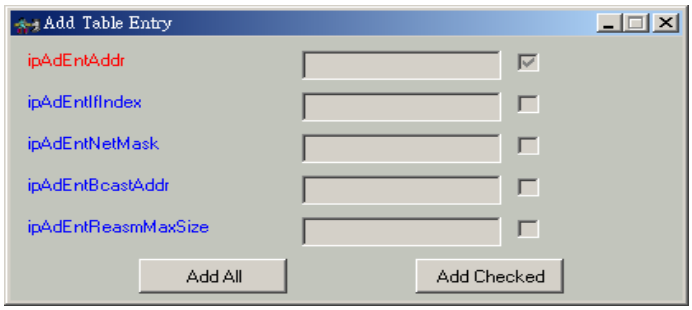


Figure 69

3. How to edit the MIB Source file:

Double-click on a MIB Module bring up a tree-view. Under "View" left-click on "MIB Source" and proceed to edit the source file for the compiled MIB.

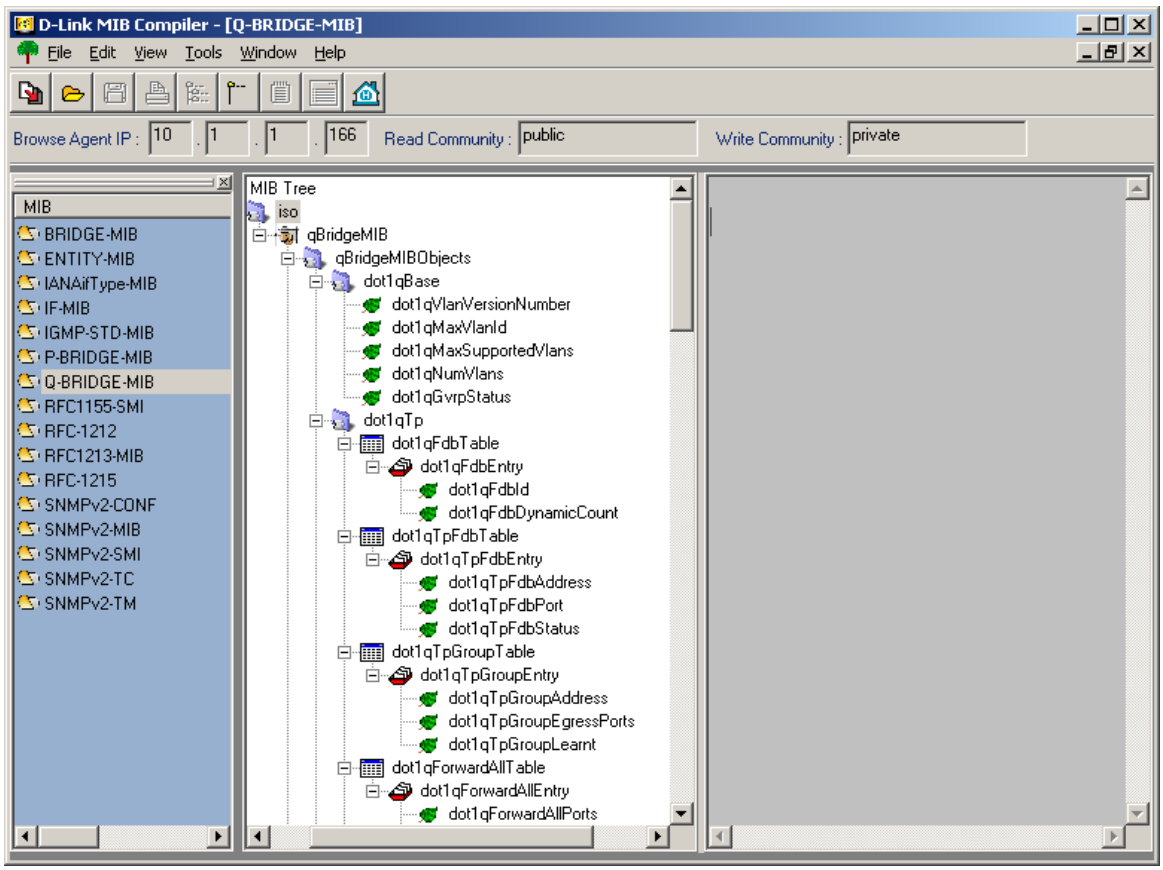


Figure 70

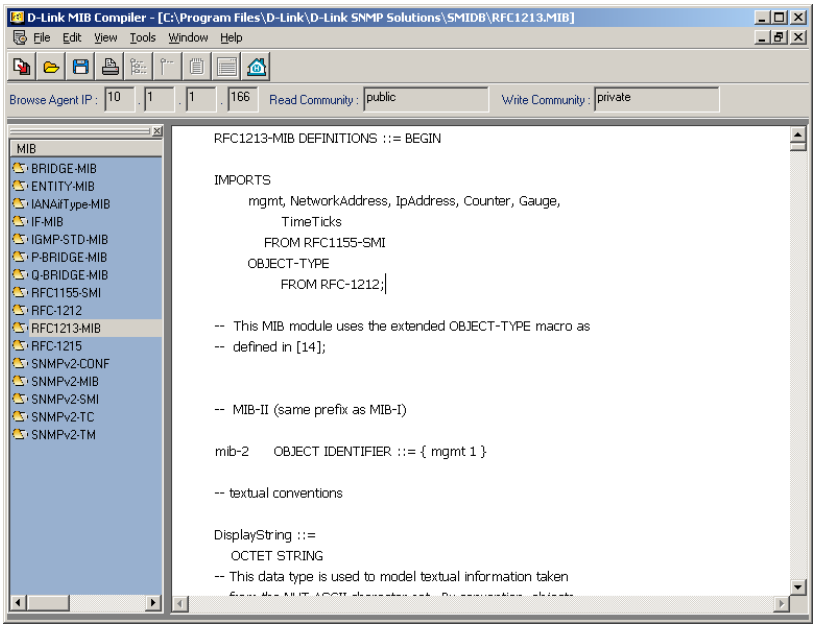


Figure 71

4. How to print an MIB Source file:

After opening the MIB Source file by left-clicking "MIB Source" under File left-click on "Print."

5. How to save an MIB Source file:

Under "File" left-click on "Save" or "Save As"

6. How to delete an MIB Module:

Highlight MIB Module. Under "File" left-click on "Delete MIB" or right-click on MIB Module and left-click on "Delete MIB."

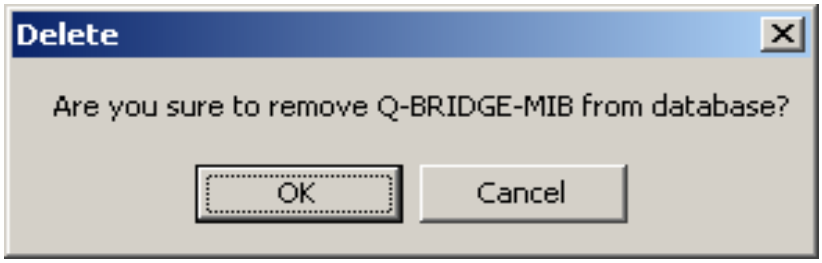


Figure 72

7. How to set MIB Module font:

Under "View" left-click on "Set Module Font."

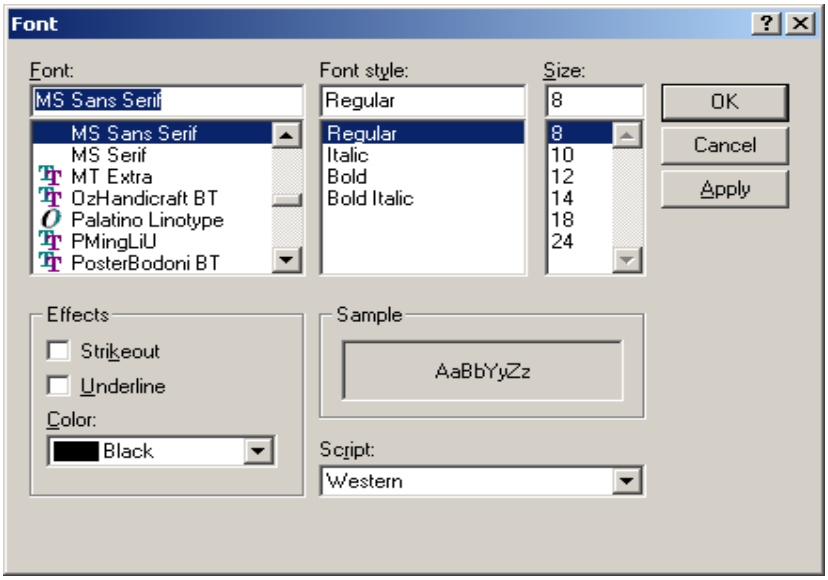


Figure 73

8. How to set MIB Module background color:

Under "View" left-click on "Set Module Color."

Figure 74

9. How to set the MIB Module tree-view display font:

Under "View" left-click on "Set MIB Tree Font."

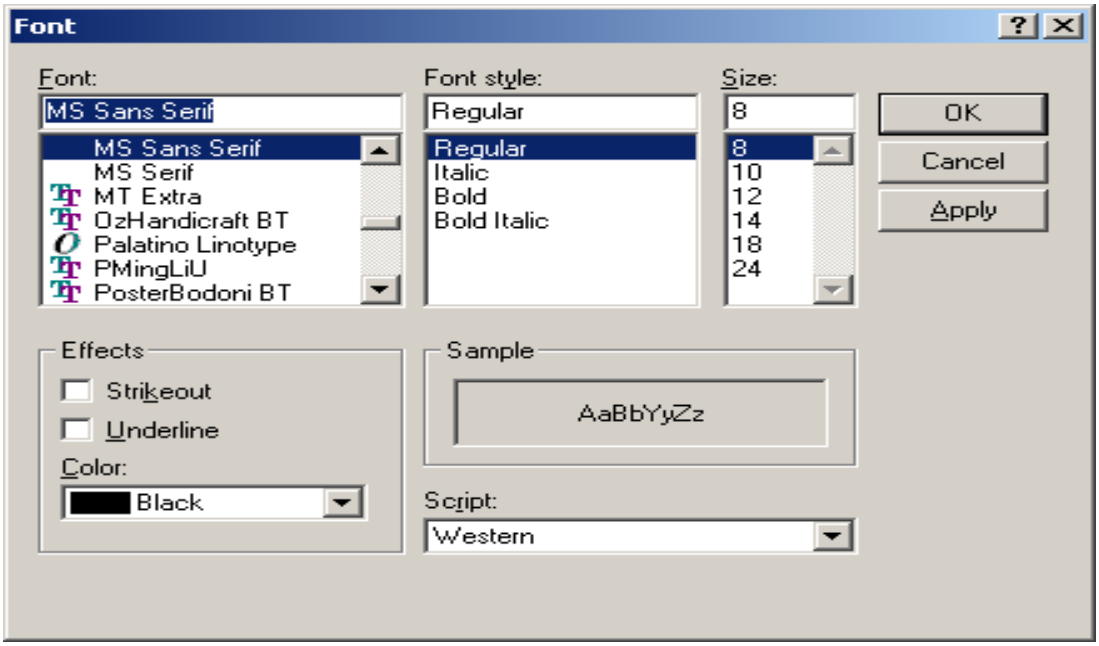

Font
Font:
MS Sans Serif
MS Sans Serif
MS Serif
MT Extra
OzHandicraft BT
Palatino Linotype
PMingLiU
PosterBodoni BT
Font style:
Regular
Regular
Italic
Bold
Bold Italic
Size:
8
8
10
12
14
18
24
OK
Cancel
Apply
Effects
Strikeout
Underline
Color:
Black
Sample
AaBbYyZz
Script:
Western

Figure 75

10. How to set the MIB Module tree-view display color:

Under "View" left-click on "Set MIB Tree Color."

Figure 76.

Creating a topology

The Topology diagram creation program included with D-View 5.1 is used to graphically represent planned or existing networks to aid network design. This program is designed to be flexible and easy to use. The primary tool for this application is the mouse. Topology diagrams can incorporate user created symbols. You can also use live device icons copied from any domain in the network. The diagrams may be further customized with user selected icons and bitmap files used for the background.

Create a New Topology

To create a new topology right-click on the Topology icon in the Tree View display panel.

Step 1: Right-click on "Topology"

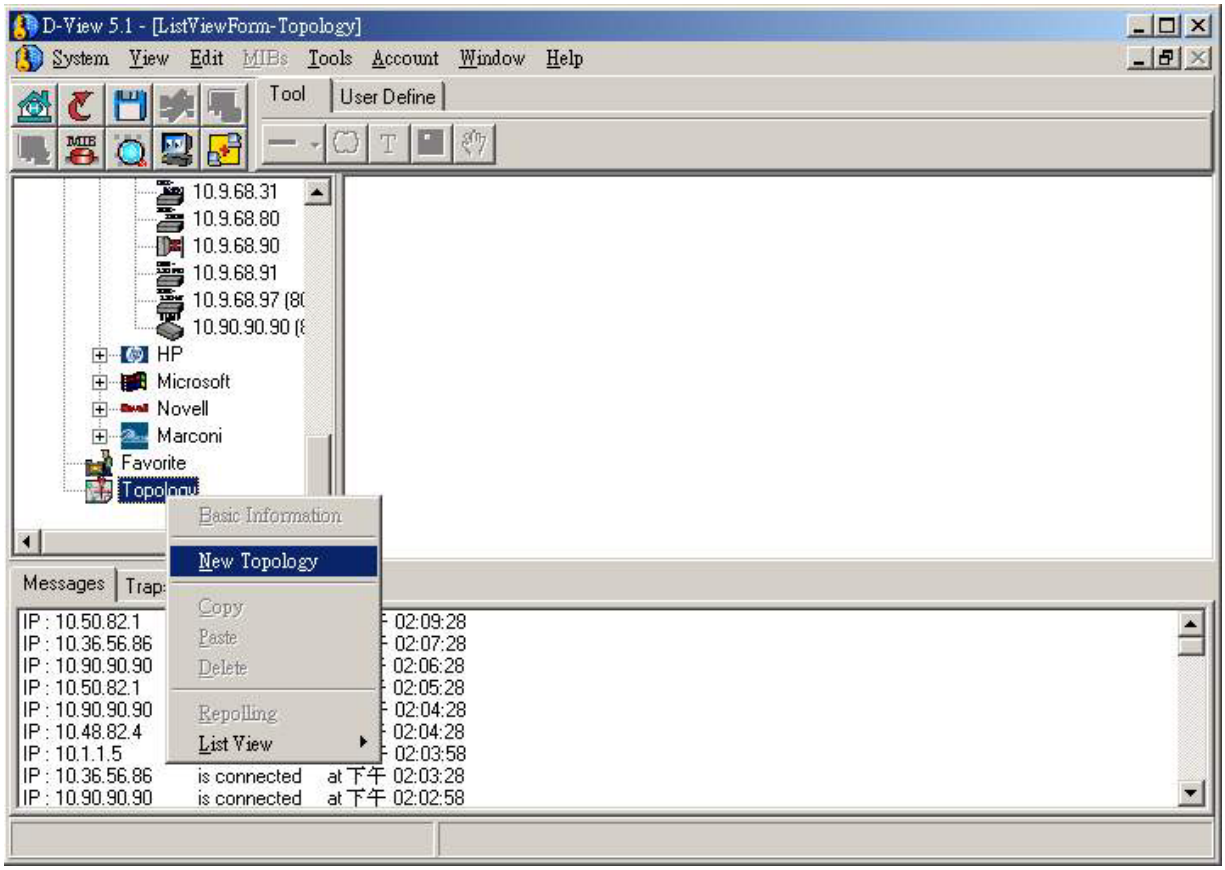

D-View 5.1 - [ListViewForm-Topology]
System View Edit MIBs Tools Account Window Help
Tool
User Define
10.9.68.31
10.9.68.80
10.9.68.90
10.9.68.91
10.9.68.97 (8(
10.90.90.90 (
HP
Microsoft
Novell
Marconi
Favorite
Topology
Basic Information
New Topology
Copy
Paste
Delete
Repolling
List View
Messages
Trap
IP : 10.50.82.1 02:09:28
IP : 10.36.56.86 02:07:28
IP : 10.90.90.90 02:06:28
IP : 10.50.82.1 02:05:28
IP : 10.90.90.90 02:04:28
IP : 10.48.82.4 02:04:28
IP : 10.1.1.5 02:03:58
IP : 10.36.56.86 is connected at 下午 02:03:28
IP : 10.90.90.90 is connected at 下午 02:02:58

Figure 77.

Step 2: Name New Topology

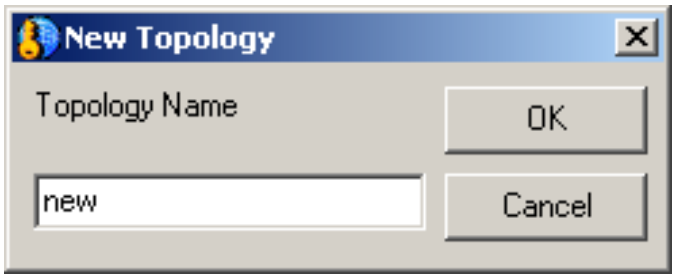


Figure 78.

Step 3: "New" Topology Established

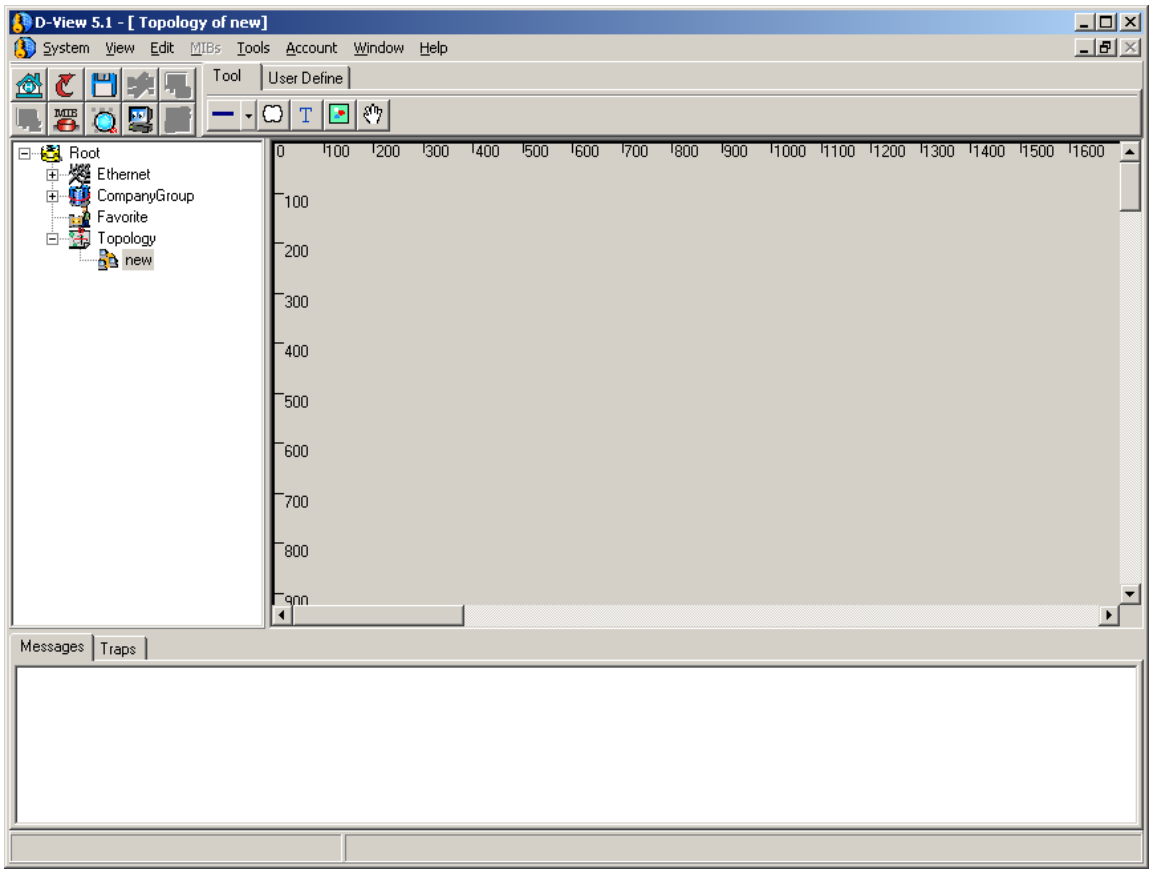


Figure 79.

Manipulating Icons and Images

Use the **"Tool"** pad and **"User Define"** pad under the tool bar to manipulate icons and images in your new topology.

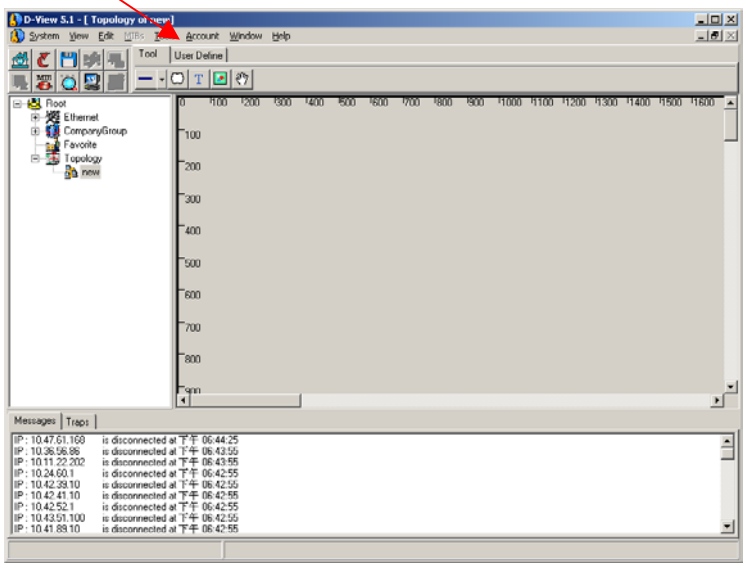


Figure 80.

1. Tool tab

The Tool tab presents a number of tools used to select and move items in the diagram. This guide discusses its functions from left to right order on the tab.

Left-click on "Tool" icon to bring up Tool tab:

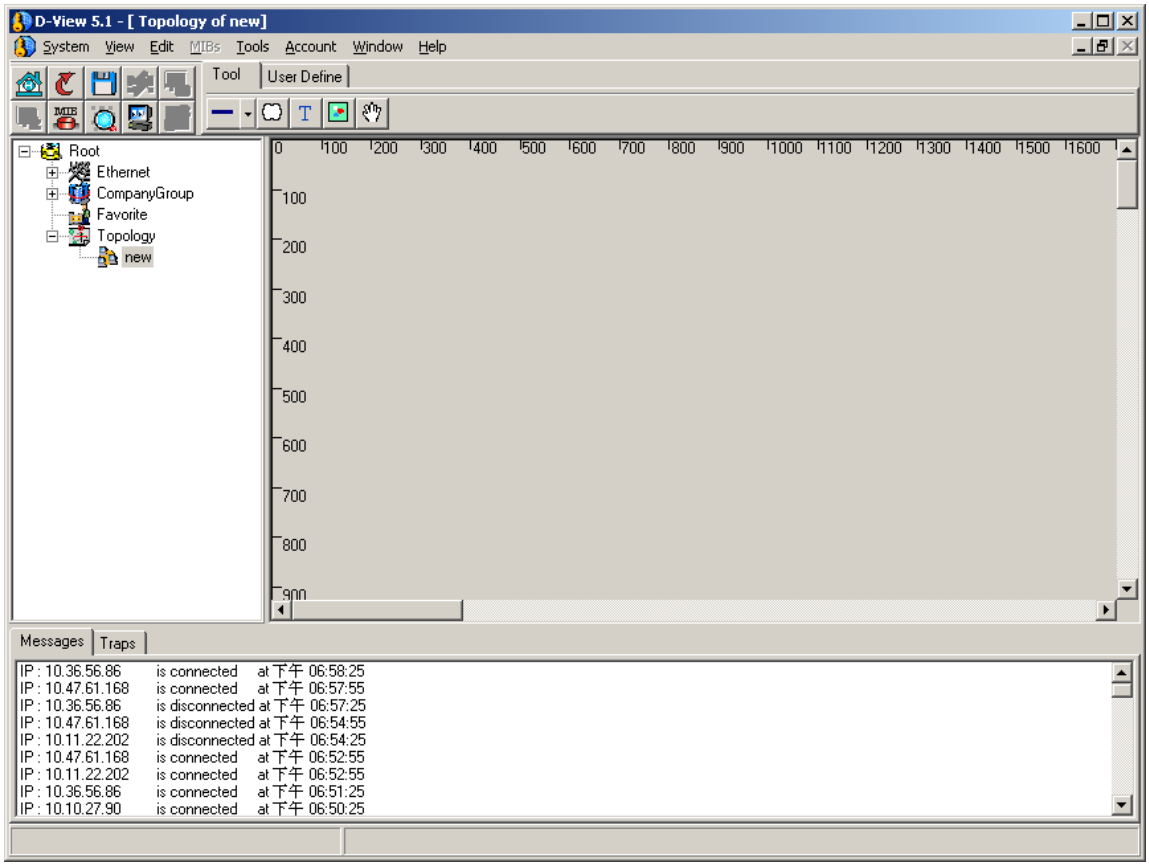


Figure 81.

a. Connecting Objects

Objects can be connected using a choice of visually distinct lines, solid lines, dotted lines etc. These lines will remain attached to the connected objects if the object is moved around the diagram.

To connect objects first click on the "line" icon in the toolbar. Clicking on the "down" arrow to the right of the line icon gives you a choice of lines to use in your drawing.

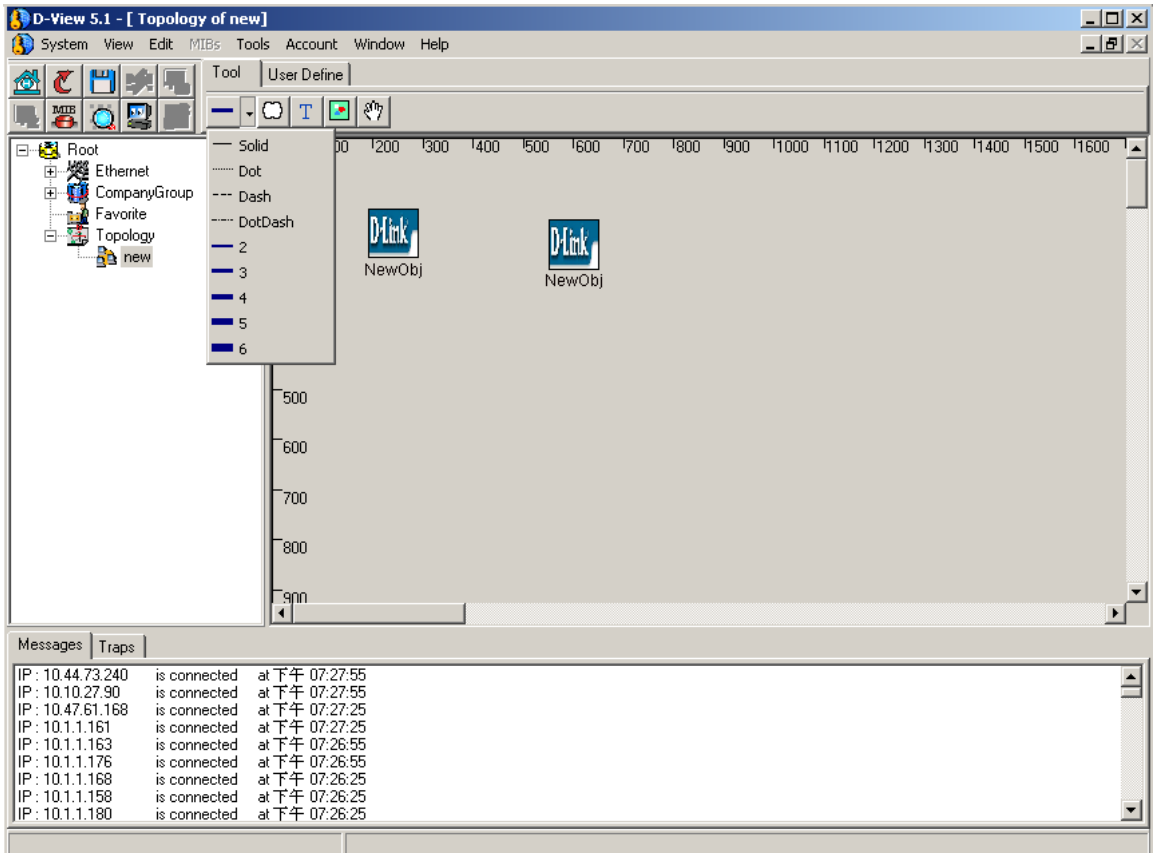


Figure 82.

Left-click on origin object.

Release.

Drag line from point of origin to destination object.

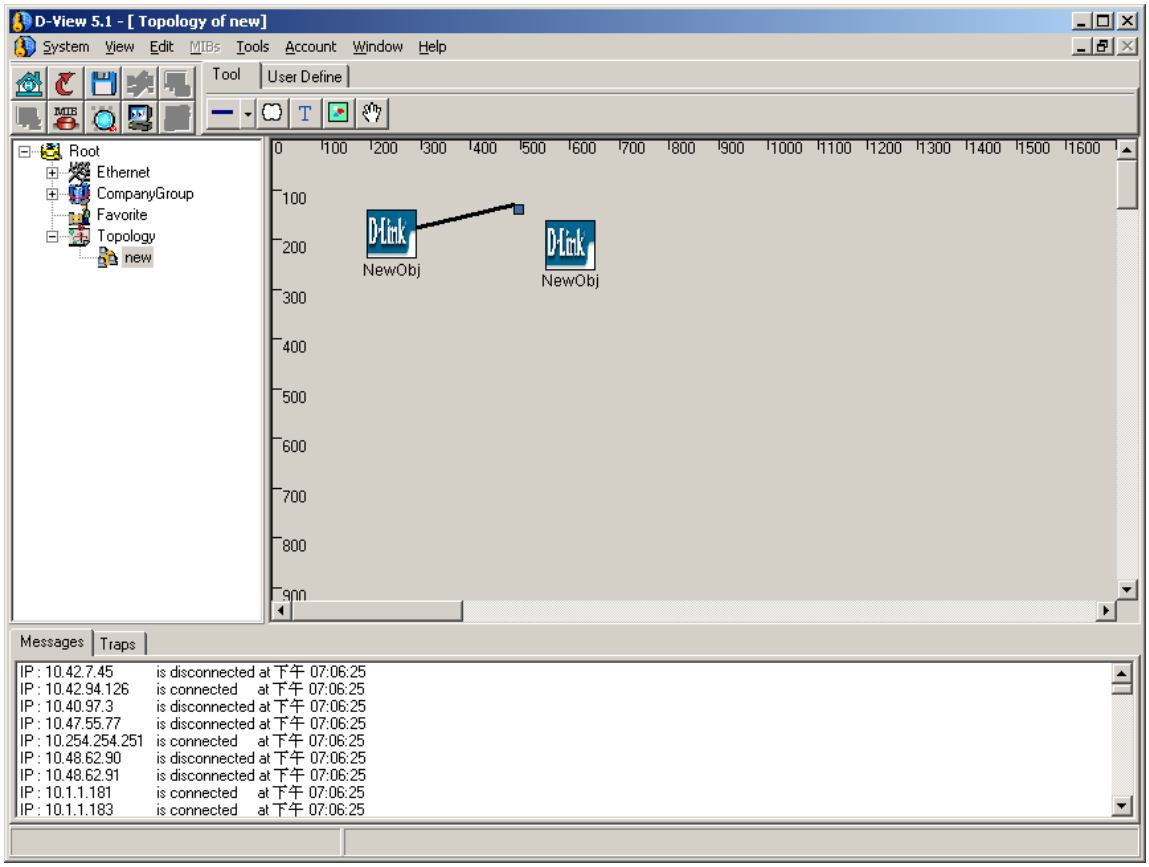


Figure 83.

Left-click on destination object.

A line should appear connecting both objects.

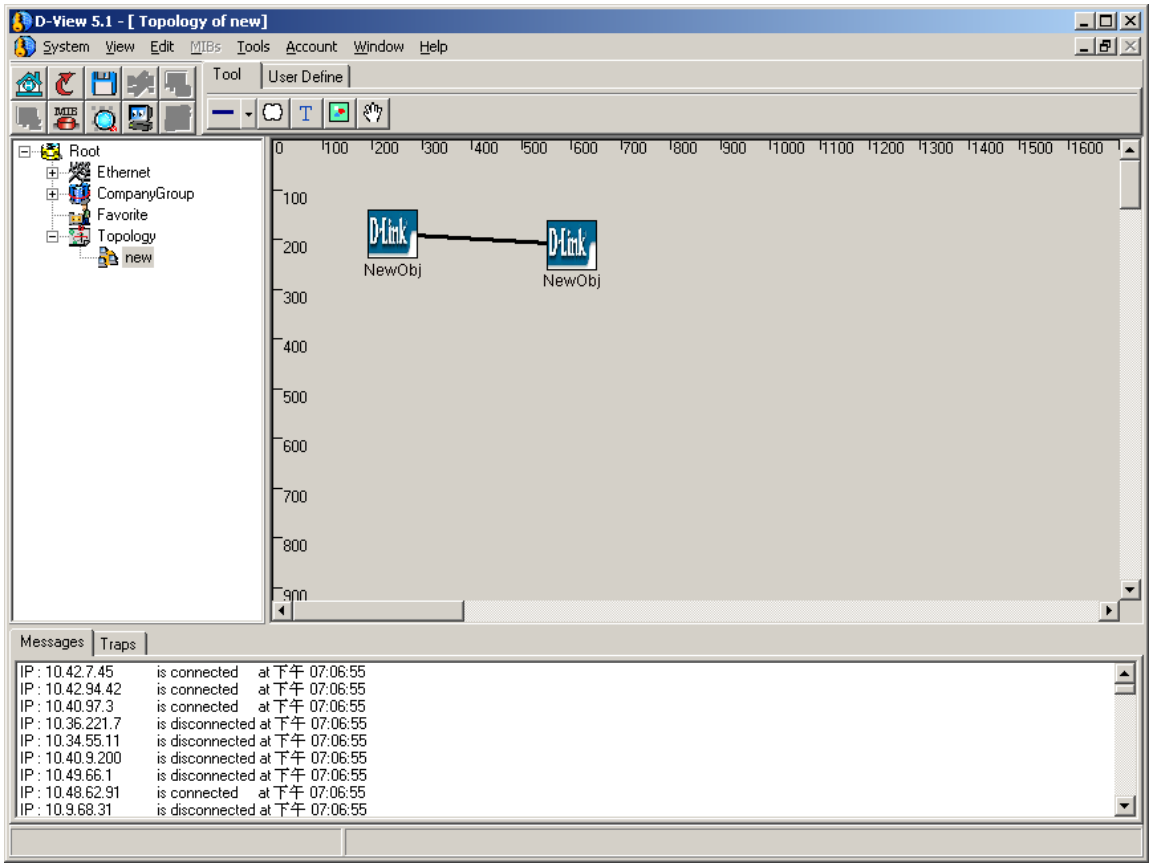


Figure 84.

Note: ***You need to click on open space to discontinue drawing. Otherwise you will continue to be in drawing mode. You can also double-click on the line drawn to undo.***

b. Creating a new domain

You can click on the white bubble to place a new domain on the topology.

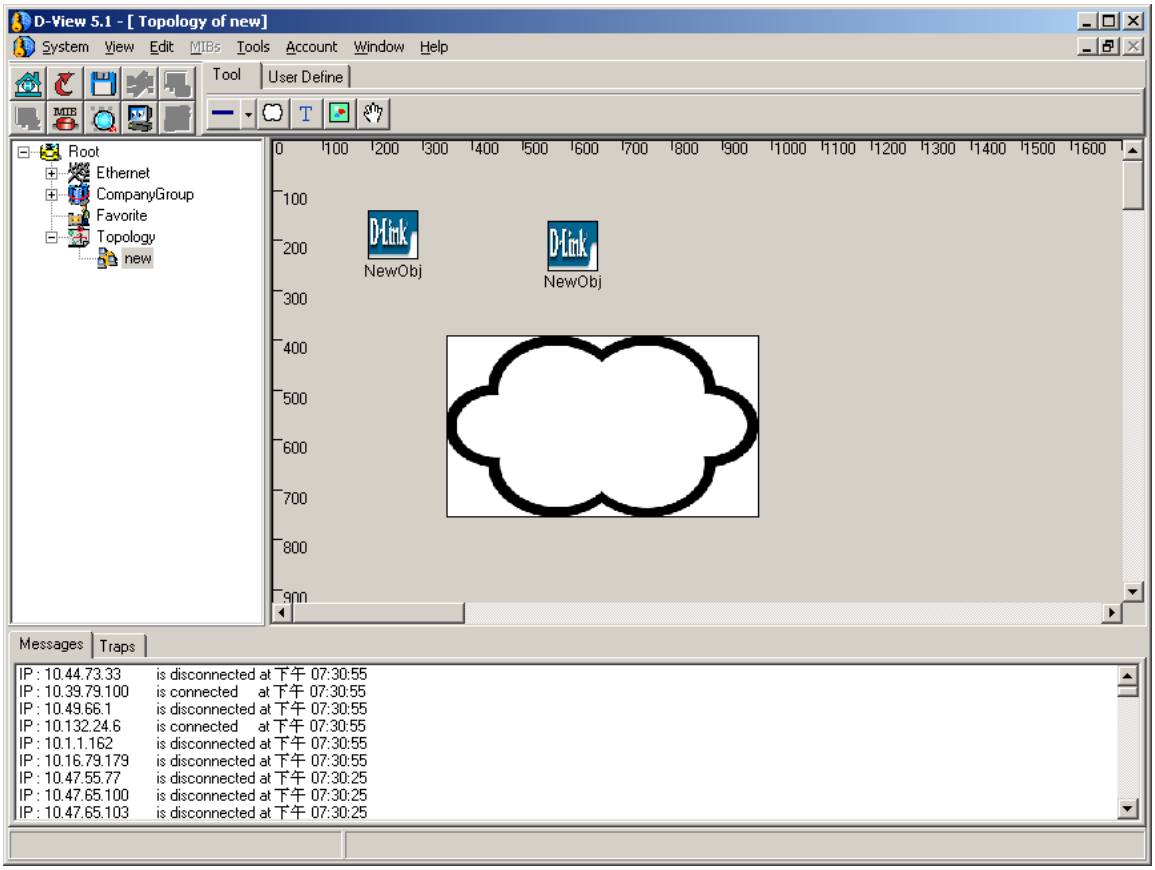


Figure 85.

c. Writing text

Left-click on the text tool "T" to select the text option then left-click again on diagram to place a text box on the diagram.

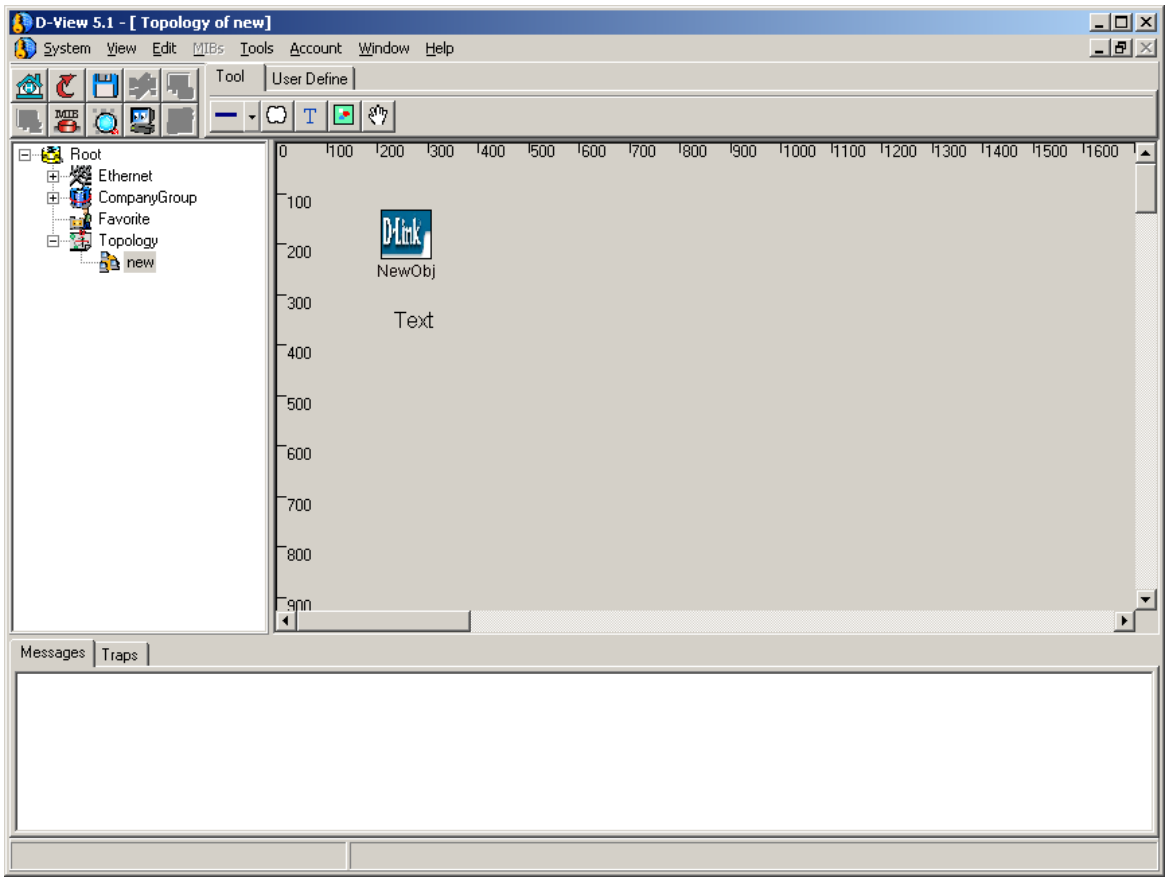


Figure 86.

Left-click once on the text to move text around. Text will be highlighted in red rectangle.

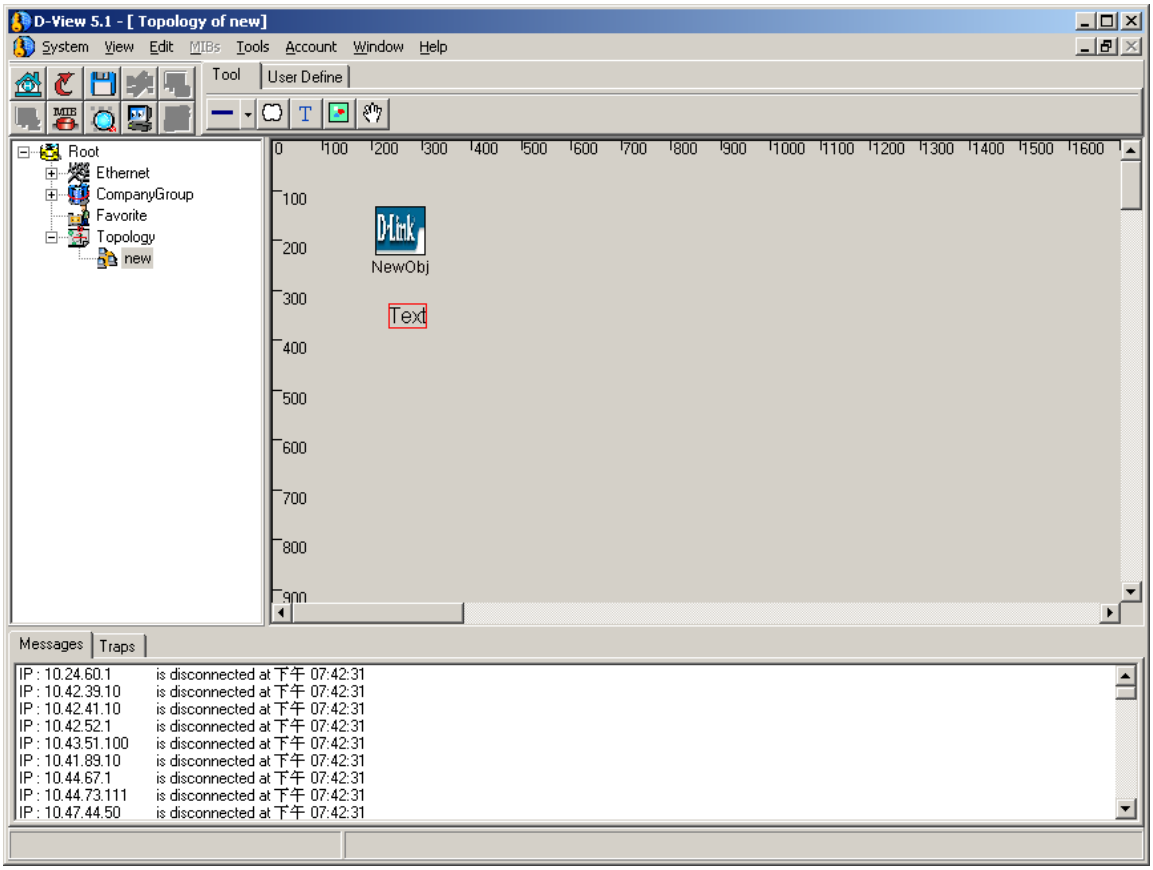


Figure 87.

Left-click twice on the mouse to edit the text.

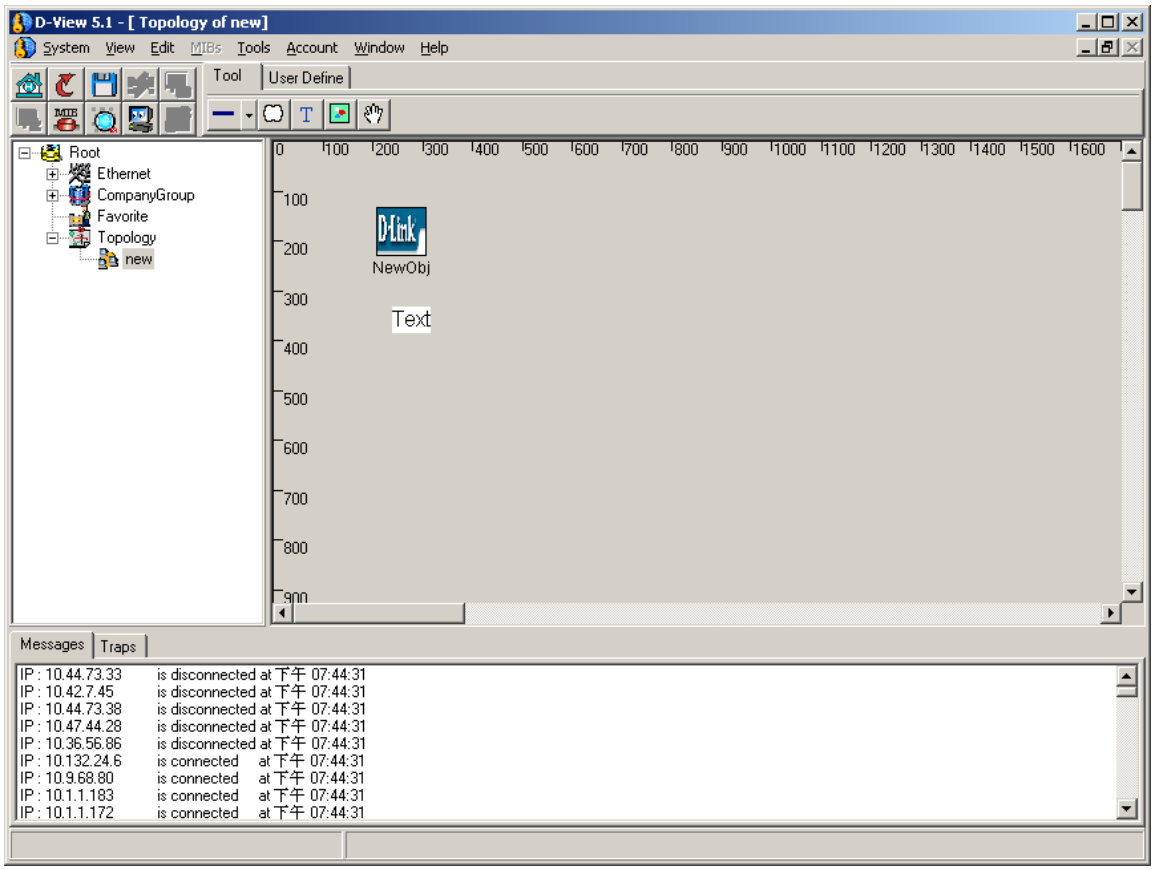


Figure 88.

To delete text left-click once then right-click on text to bring up "Delete" option.

d. Selecting multiple items

The multi-select tool (rectangular-shaped icon on tool pad) enables you to select a number of items (holding the left button down to select) and move these items as a unit.

e. Selecting individual items

You can click on the "hand" icon to select individual items.

2. User Define Tab

Importing Icons

Icons from any of the domains may be used in the diagram simply by selecting and copying them and pasting it into the new diagram.

Step 1: Left-click on "New" under "User Define"

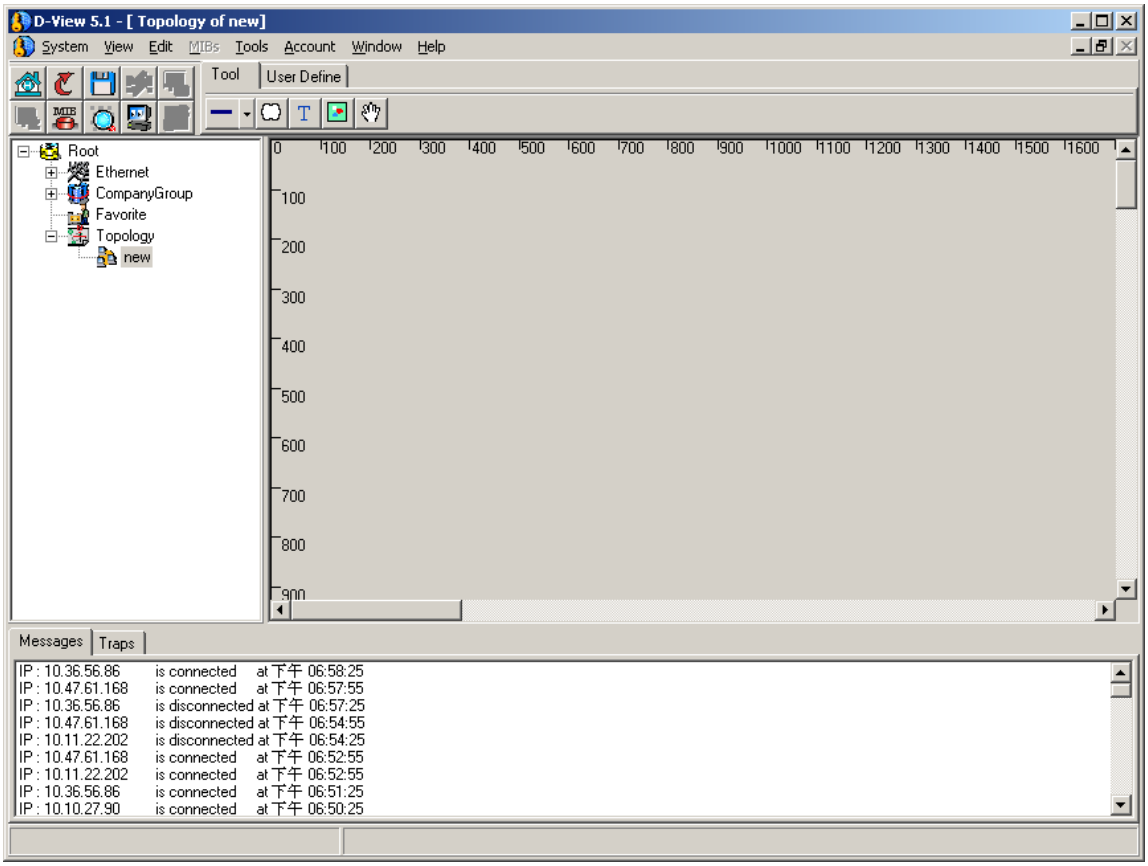

D-View 5.1 - [Topology of new]
System View Edit MIBs Tools Account Window Help
Tool User Define
Root
Ethernet
CompanyGroup
Favorite
Topology
new
Messages Traps
IP : 10.36.56.86 is connected at 下午 06:58:25
IP : 10.47.61.168 is connected at 下午 06:57:55
IP : 10.36.56.86 is disconnected at 下午 06:57:25
IP : 10.47.61.168 is disconnected at 下午 06:54:55
IP : 10.11.22.202 is disconnected at 下午 06:54:25
IP : 10.47.61.168 is connected at 下午 06:52:55
IP : 10.11.22.202 is connected at 下午 06:52:55
IP : 10.36.56.86 is connected at 下午 06:51:25
IP : 10.10.27.90 is connected at 下午 06:50:25

Figure 89.

Step 2: Allows you to bring up icon to be imported

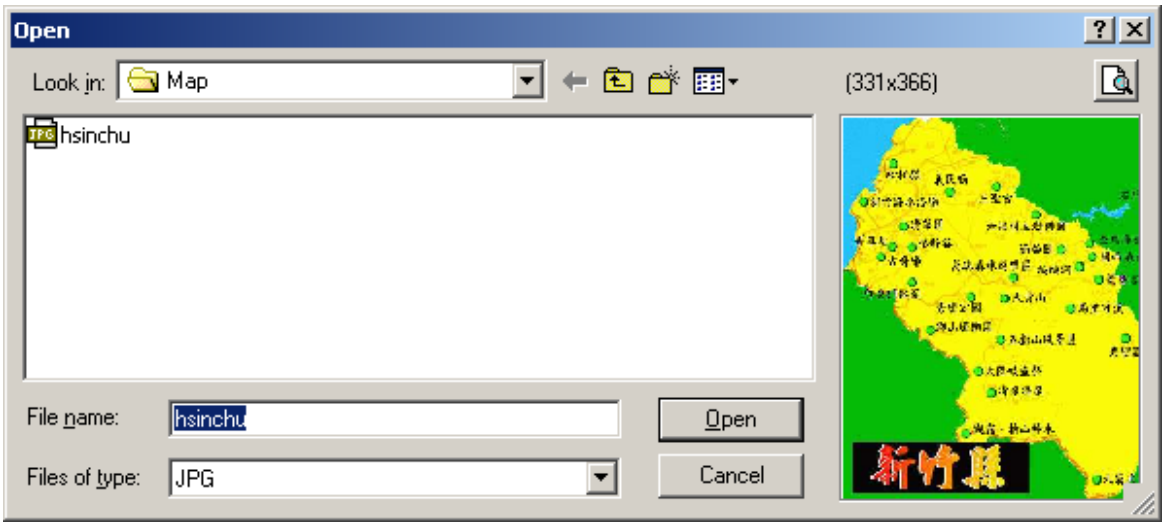


Figure 90.

Step 3: Drag domain icon into workspace. Pictured below is the default D-Link "New Object" icon

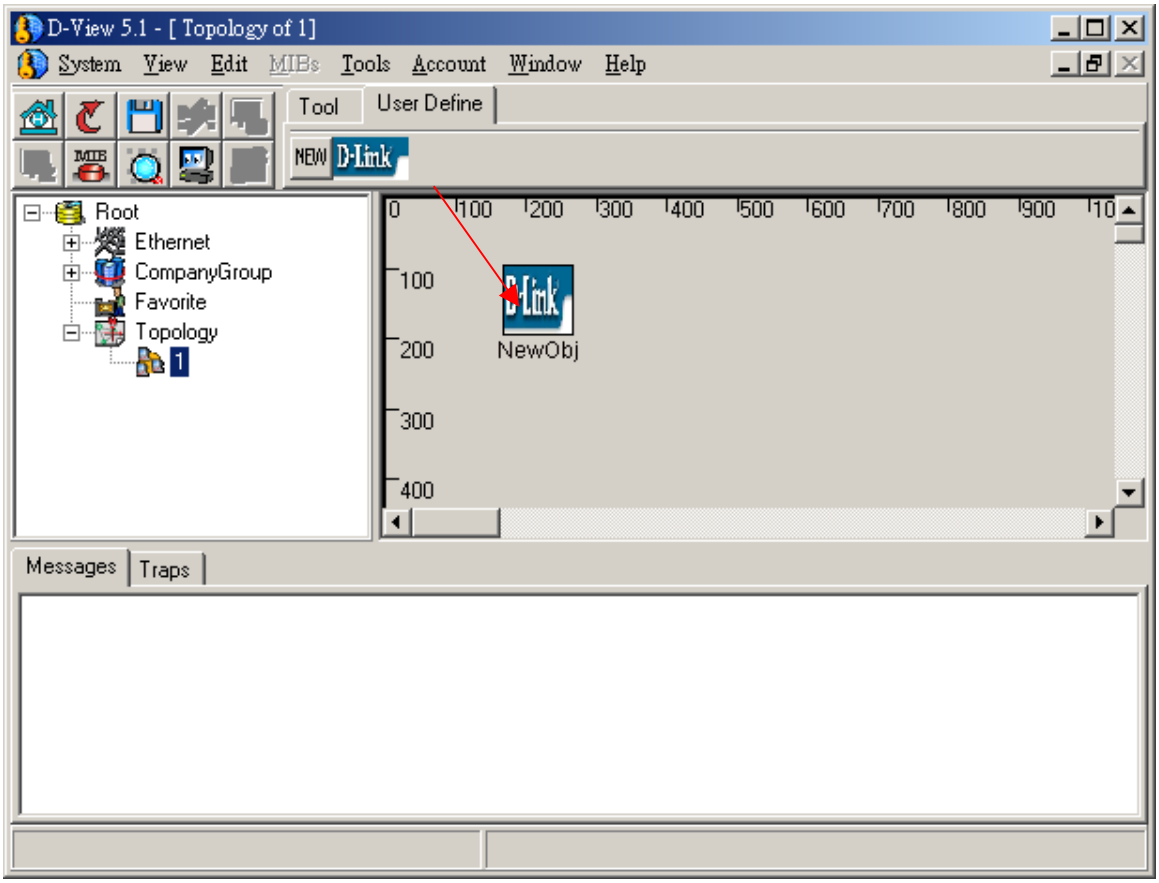

D-View 5.1 - [Topology of 1]
System View Edit MIBs Tools Account Window Help
Tool
User Define
NEW D-Link
Root
Ethernet
CompanyGroup
Favorite
Topology
1
NewObj
Messages
Traps

Figure 91.

An Example: Creating a Topology Diagram

Step1: Click on New Topology

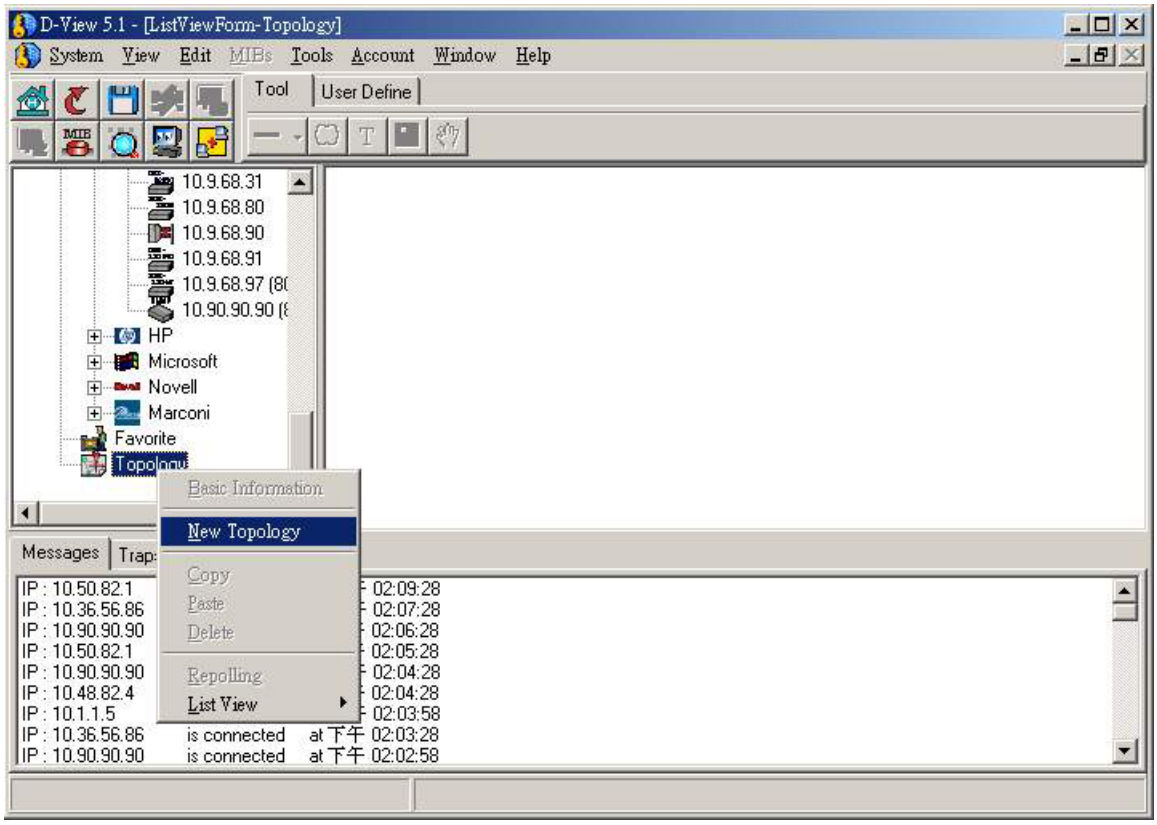


Figure 92.

Step 2: Name new topology and press OK.

Figure 93.

Step3: New Topology created:

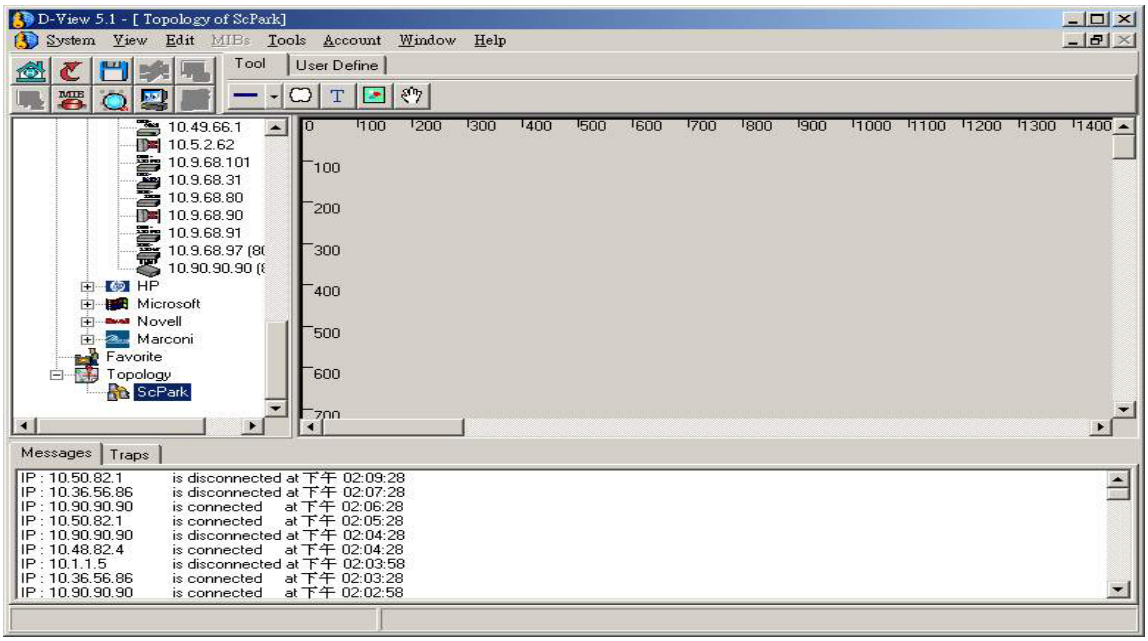


Figure 94.

Step 4: Import background picture by clicking on "New Background Picture."

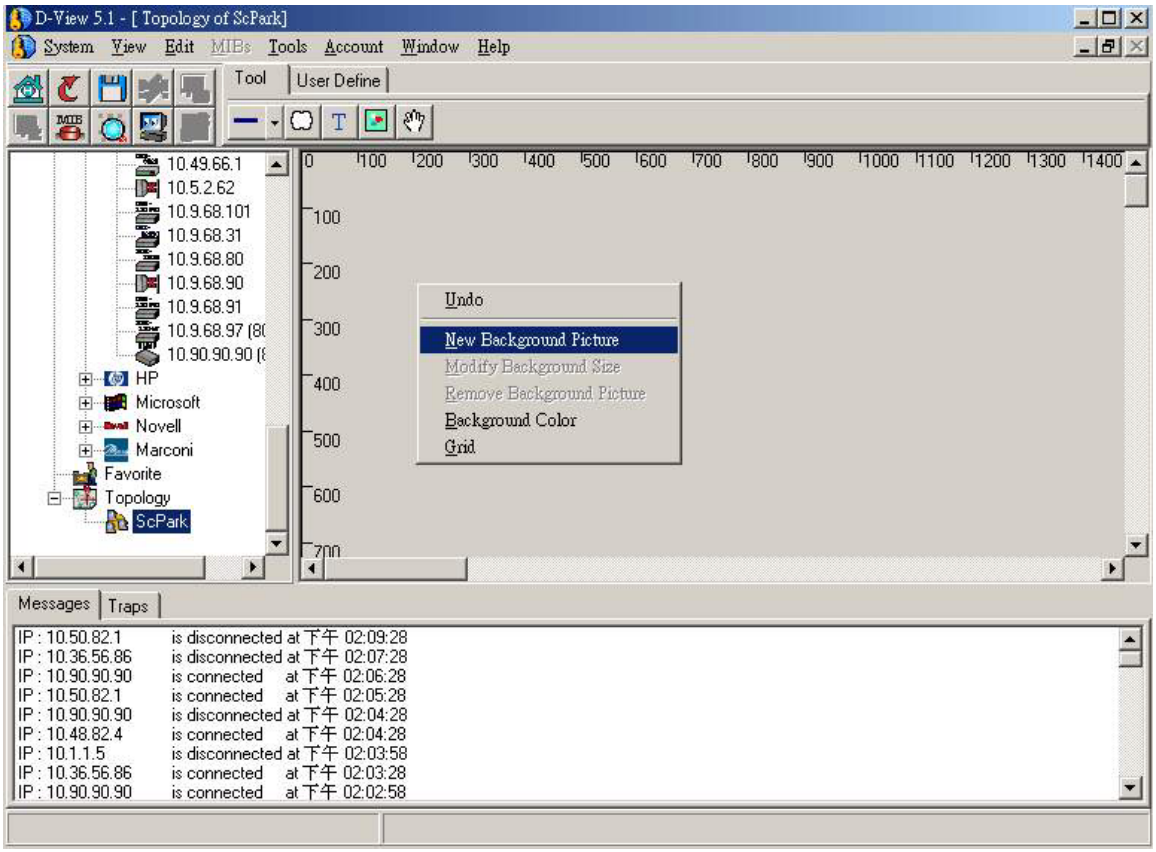


Figure 95.

Step 5: Import .jpg or .bmp file

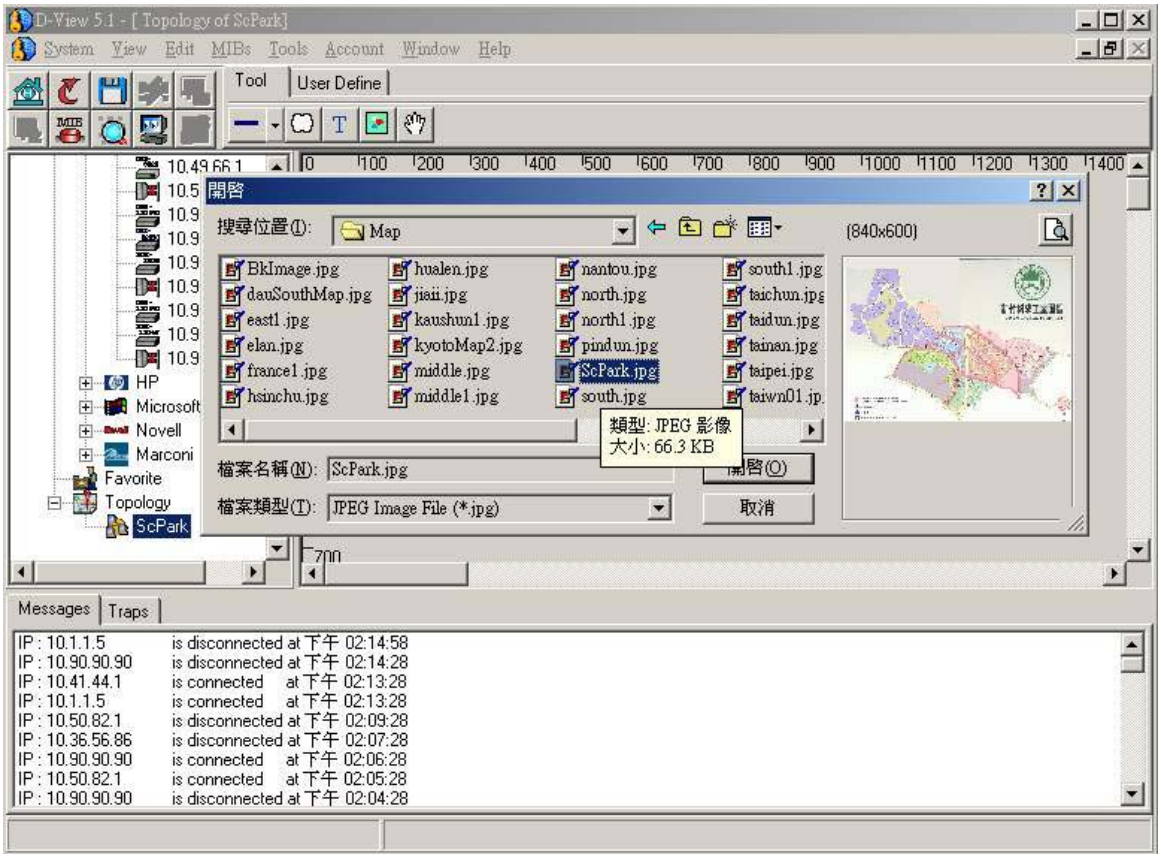


Figure 96.

Step 6: Set background size and press OK.

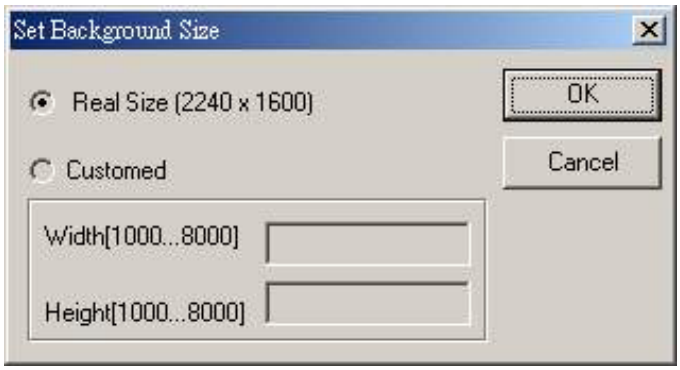


Figure 97.

Step 7: Background picture imported

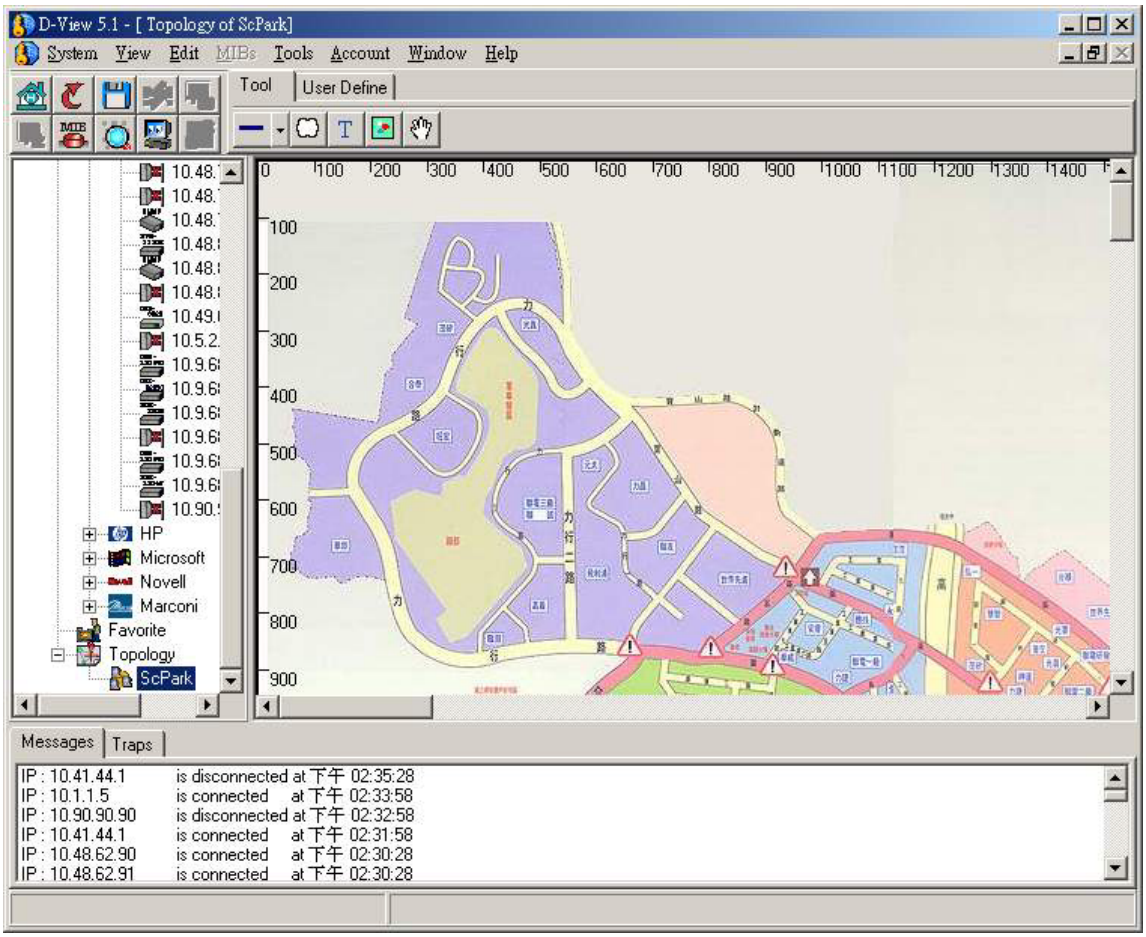


Figure 98.

Step 8: You can drag devices directly from Tree View onto the Topology diagram or copy and paste.

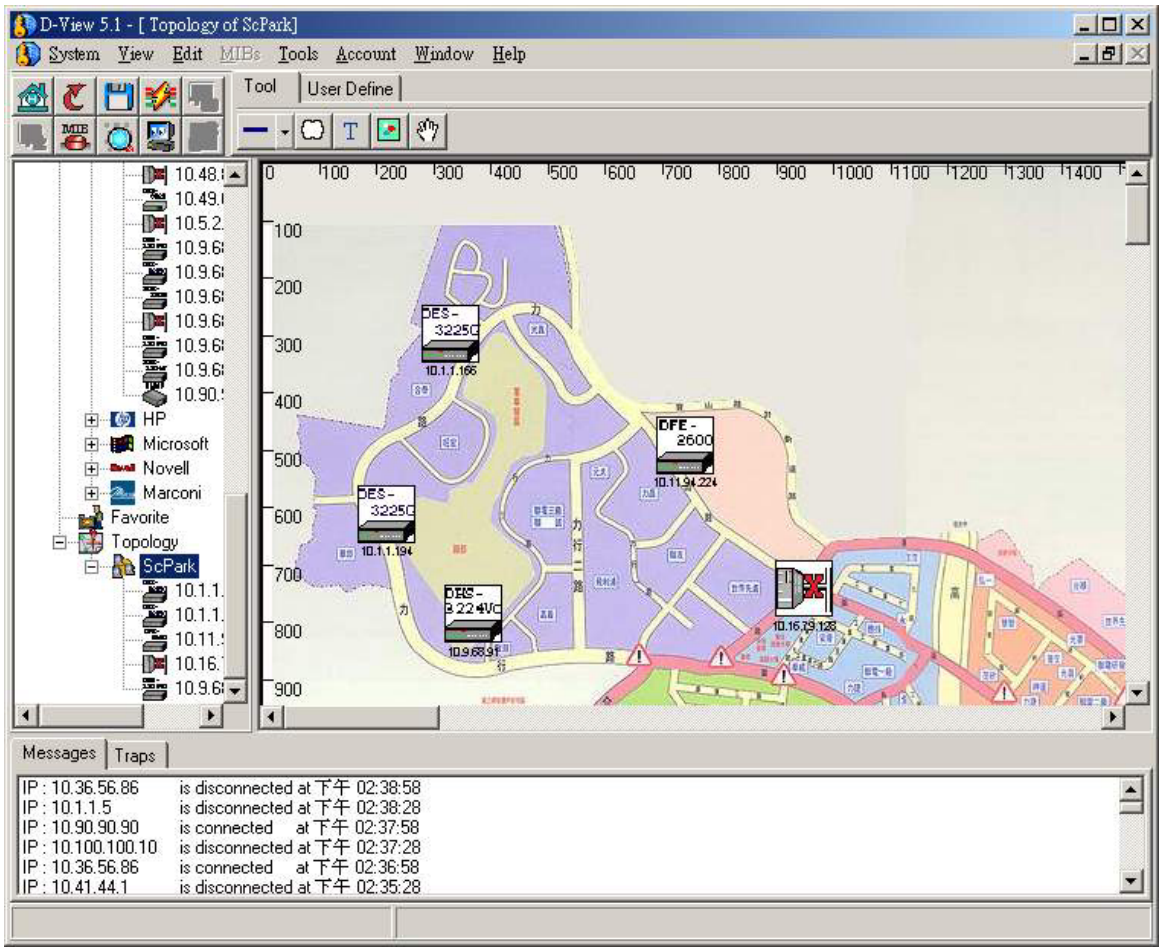


Figure 99.

Step 9: Use the line function on the tool pad to connect devices in the topology drawing and set colors.

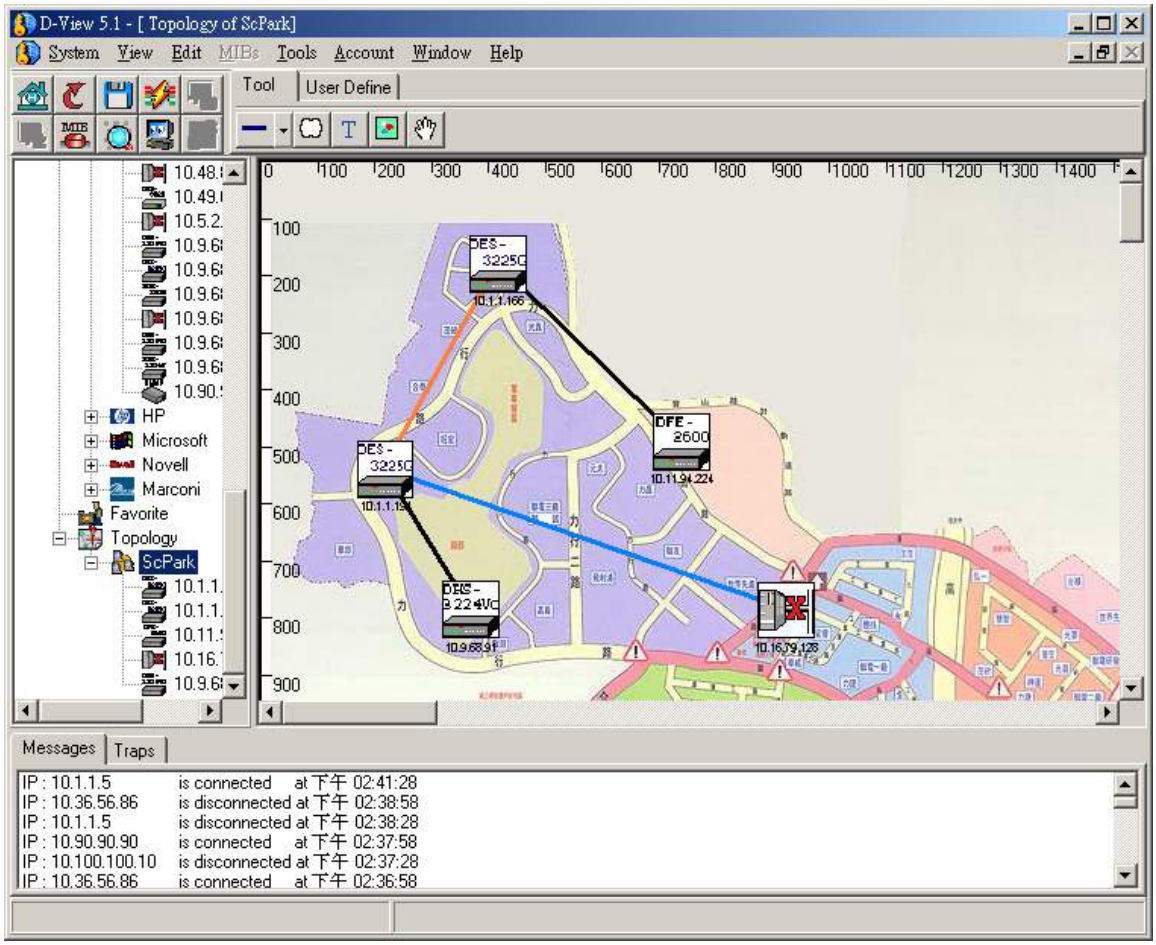


Figure 100.

Step 10: Save to Database

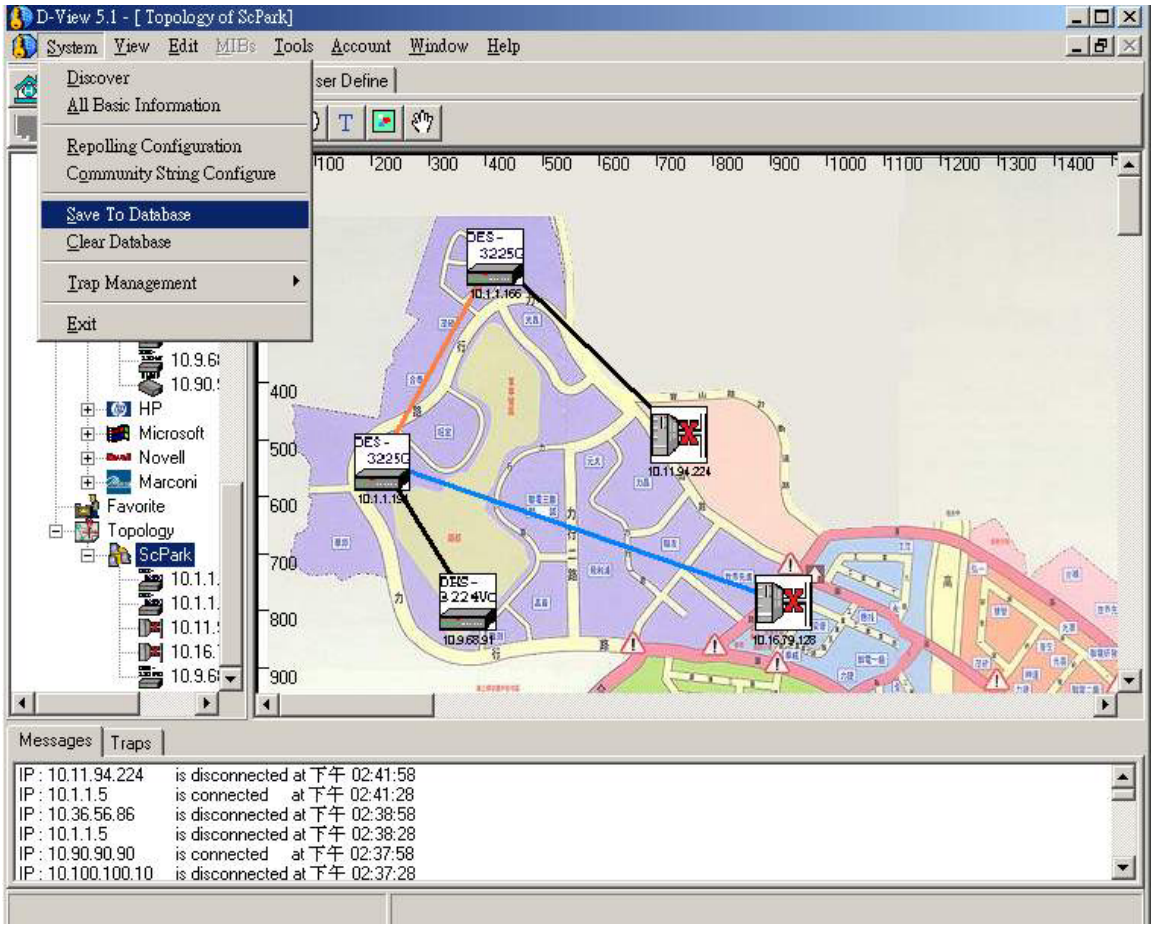


Figure 101.

4

MIB UTILITIES

This chapter explains how to use MIBs tools and other utilities located under the MIBs drop-down menu. It is organized according to the top to bottom, left to right order of the menu items. These menus will allow you to view statistics and to configure Layer 2 and Layer 3 functions. For many of the menu items an information table (RFCs—technical reports called Internet Requests for Comments) is presented along with a path diagram to illustrate how to utilize the particular functionality.

Note: ***In order to use MIB Utilities you need to first select an SNMP-enabled device.***

The menus in this group include:

- Device SNMP Configuration
- MIB II Information and Statistics Windows
- IF MIB Information Tables
- Entity MIB Information Tables
- Bridge 802.1d Information and Port Configuration Table
- Spanning Tree Information and Port Configuration Table

- Transparent Bridge Forwarding and Static Filter Tables and Port Counter
- RMON Statistics, History and Event Windows
- 802.1p Priority Configuration Including GMRP and GARP
- 802.1Q VLAN Information and Configuration Including Forwarding/Filtering and Unicast/Multicast Configuration
- Port VLAN Traffic Statistics
- Layer 3 Utilities Including IP Forwarding, RIP2, OSPF, IP Multicast, DVMRP and PIM Configuration
- SNMP Configuration

Device SNMP Configuration

You can change the SNMP configuration of the device. Otherwise you will use the default settings.

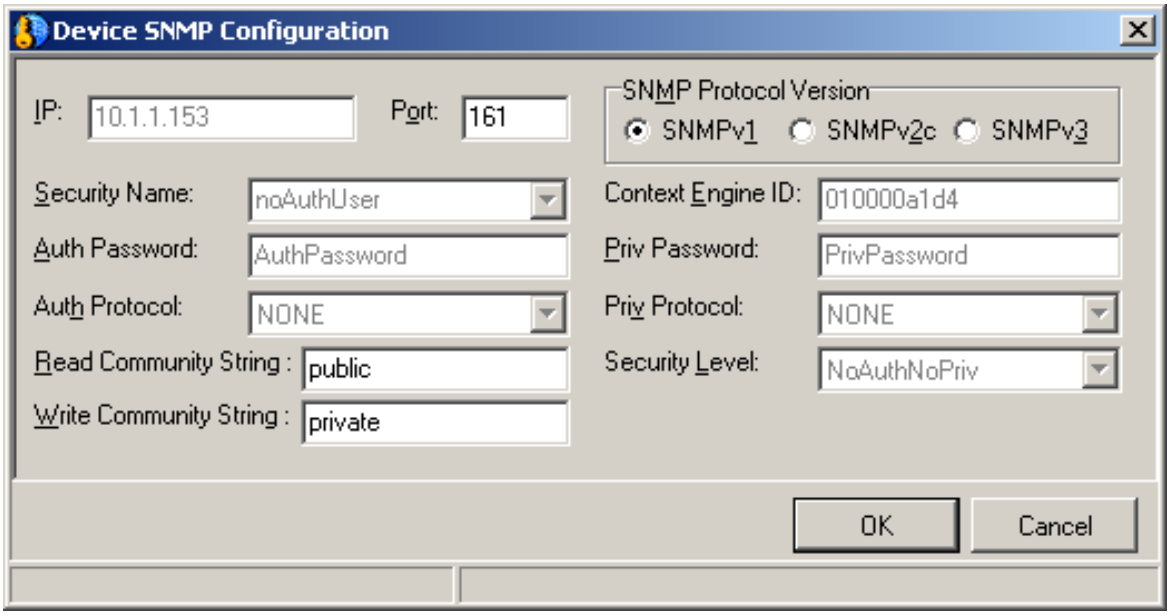


Figure 102.

MIB II Menus

MIB II pop-up menus are accessed as side (client) menus and can be viewed alone. You can also have multiple windows opened simultaneously.

Information

Use the MIB II Information window to view and write basic device SNMP information.
Enter the following:

- **System Contact,**
- **System Name**

- **System Location**

Type in the new text and click on set to make these change effective.

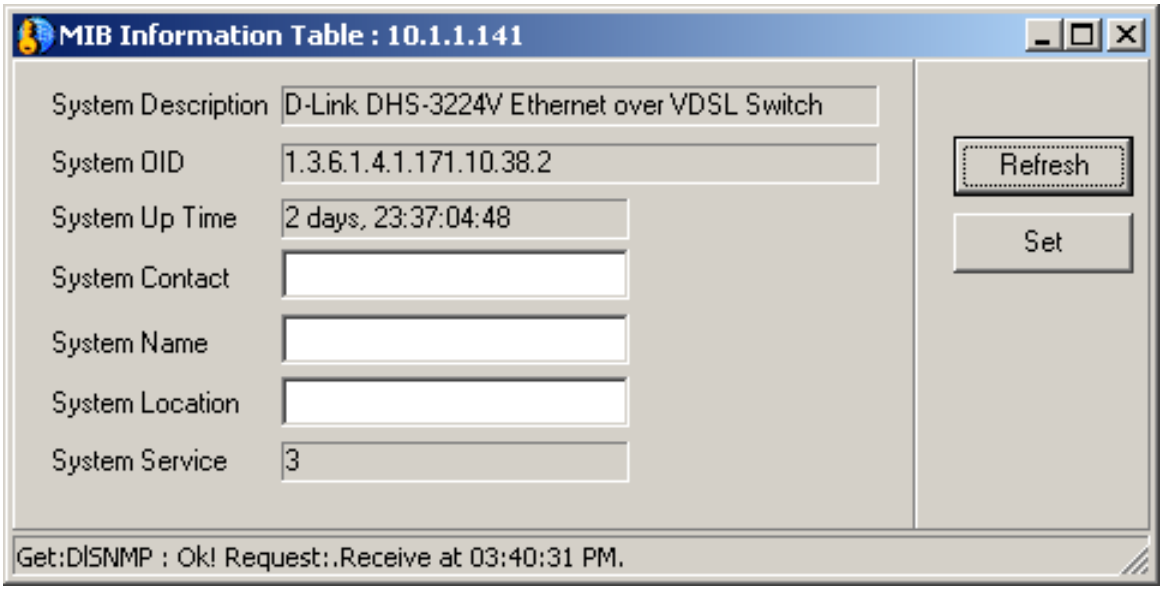


Figure 103.

The remaining menus under MIB II are the following read-only table and counter windows (examples pictured on next page):

- **IF Table**
- **IF Counters**
- **IP Counters**
- **IP Routing**
- **IP Address Table**
- **ICMP Counters**
- **UDP Counters**
- **SNMP Counters**

MIB II Read-only Windows

Read-only menus can be refreshed, reset and paused; you may adjust the poll interval for the counters. A few examples screen captures are pictured here:

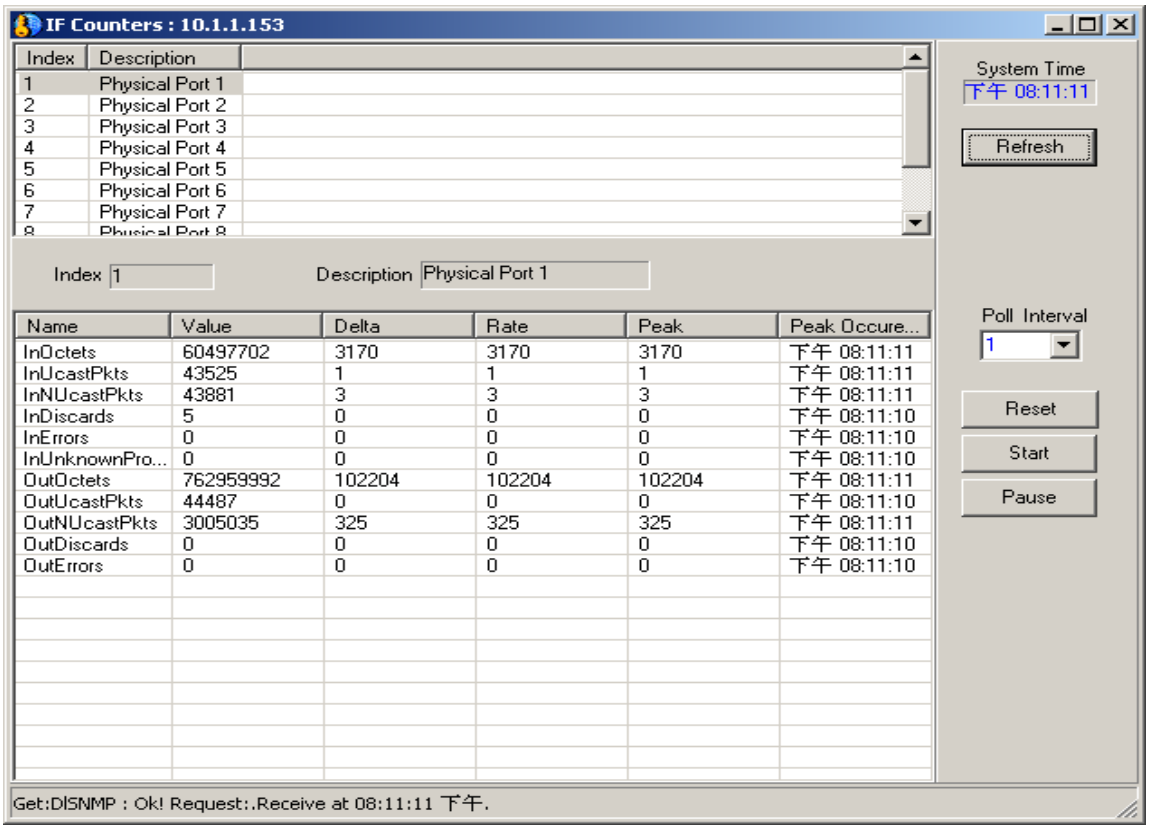


Figure 104. Example of MIB II Read-Only Menus

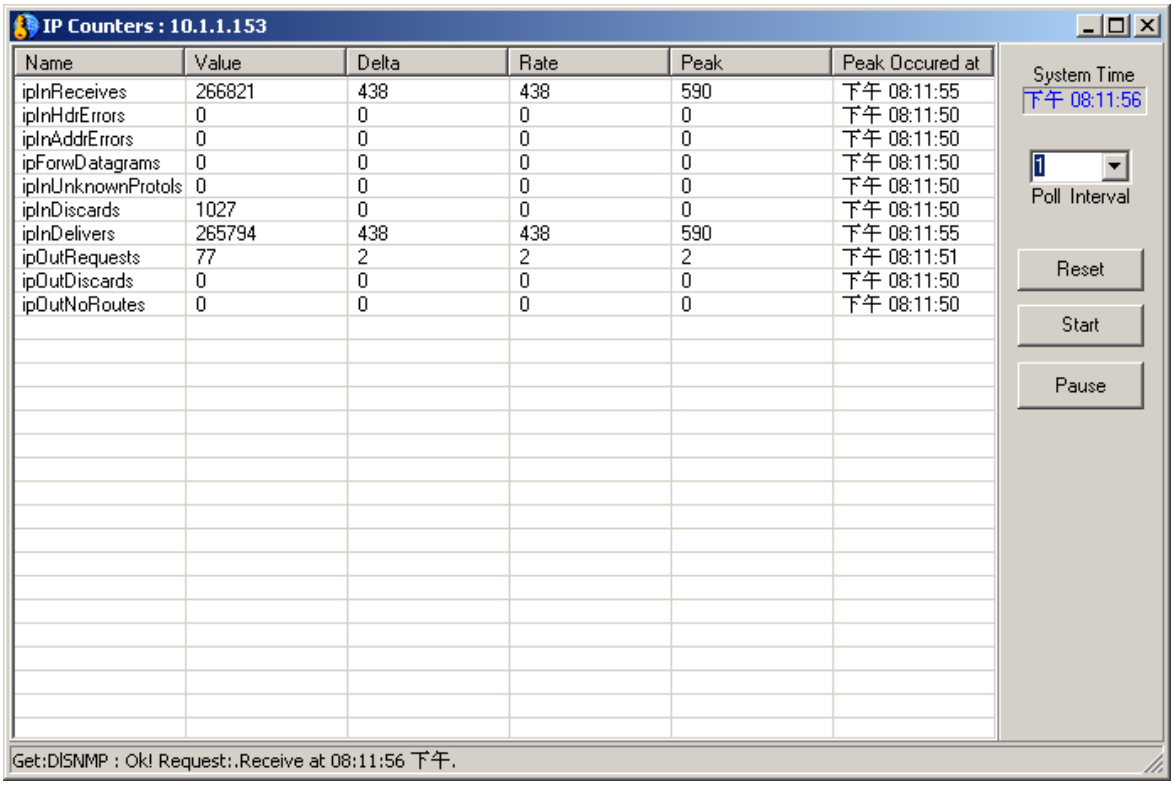

IP Counters : 10.1.1.153
Name
Value
Delta
Rate
Peak
Peak Occured at
ipInReceives 266821 438 438 590 下午 08:11:55
ipInHdrErrors 0 0 0 0 下午 08:11:50
ipInAddrErrors 0 0 0 0 下午 08:11:50
ipForwDatagrams 0 0 0 0 下午 08:11:50
ipInUnknownProtols 0 0 0 0 下午 08:11:50
ipInDiscards 1027 0 0 0 下午 08:11:50
ipInDelivers 265794 438 438 590 下午 08:11:55
ipOutRequests 77 2 2 2 下午 08:11:51
ipOutDiscards 0 0 0 0 下午 08:11:50
ipOutNoRoutes 0 0 0 0 下午 08:11:50
System Time
下午 08:11:56
1
Poll Interval
Reset
Start
Pause
Get:DISNMP : Ok! Request:.Receive at 08:11:56 下午.

Figure 105.

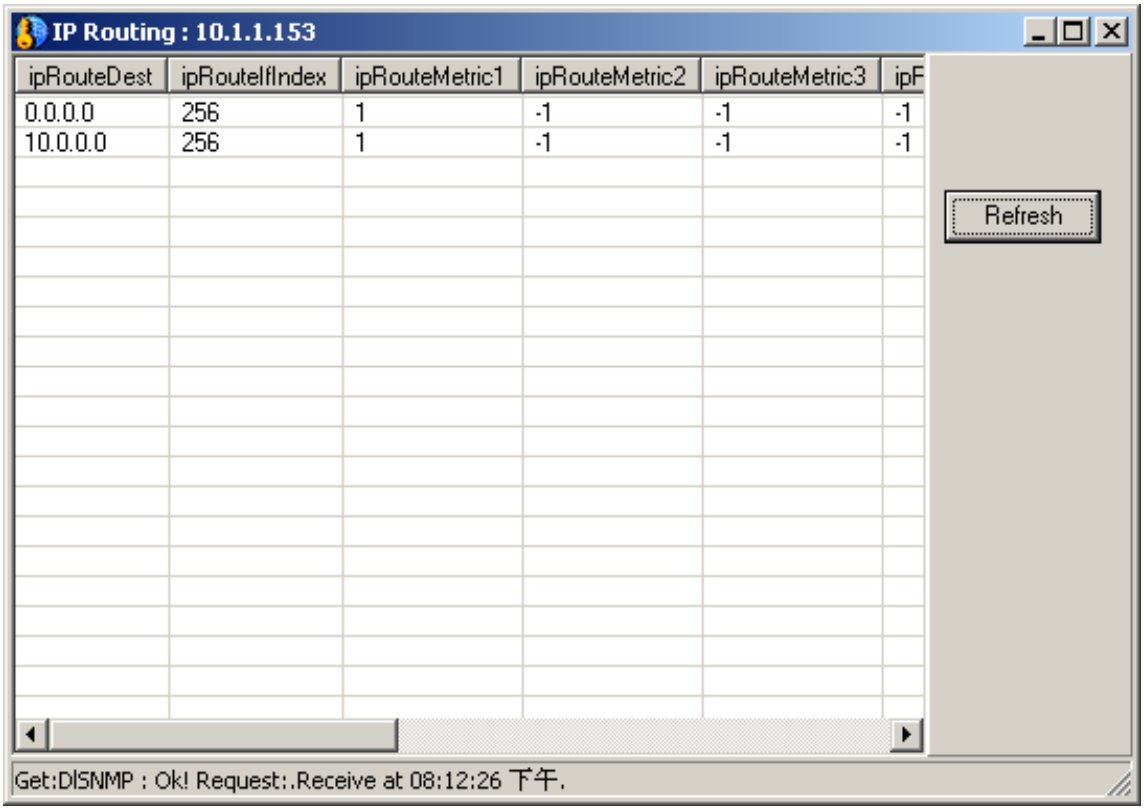

IP Routing : 10.1.1.153
ipRouteDest
ipRouteIfIndex
ipRouteMetric1
ipRouteMetric2
ipRouteMetric3
ipF
0.0.0.0
256
1
-1
-1
-1
10.0.0.0
256
1
-1
-1
-1
Refresh
Get:DISNMP : Ok! Request:.Receive at 08:12:26 下午.

Figure 106.

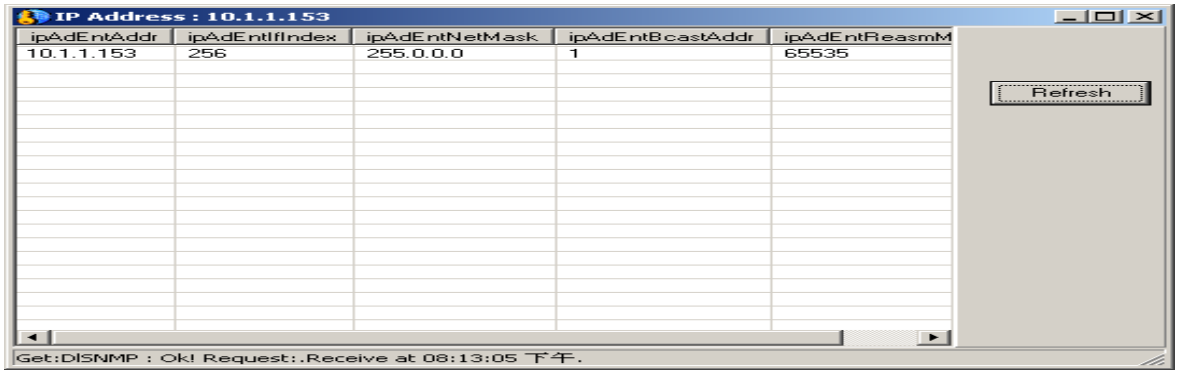


Figure 107. Figure Examples of MIB II Read-only Menus

IF MIB Tables

The following table gives a brief description of the IF MIB:

IF-MIB (RFC 2233)
1. The ifGeneralInformationGroup. This group contains those objects applicable to all types of network interfaces, including bit-oriented interfaces. 2. The ifPacketGroup. This group contains those objects applicable to packet-oriented network interfaces. 3. The ifFixedLengthGroup. This group contains the objects applicable not only to character-oriented interfaces, such as RS-232, but also to those subnetwork technologies, such as cell-relay/ATM, which transmit data in fixed length transmission units. As well as the octet counters, there are also a few other counters (e.g., the error counters) which are useful for this type of interface, but are currently defined as being packet-oriented. To accommodate this, the definitions of these counters are generalized to apply to character-oriented interfaces and fixed-length-transmission interfaces.

It should be noted that the octet counters in the if Table aggregate octet counts for unicast and non-unicast packets into a single octet counter per direction (received/transmitted). Thus, with the above definition of fixed-length-transmission interfaces, where such interfaces which support non-unicast packets, separate counts of unicast and multicast/broadcast transmissions can only be maintained in a media-specific MIB module.

Table 2.

The IF MIB General Information and IF Stack tables:

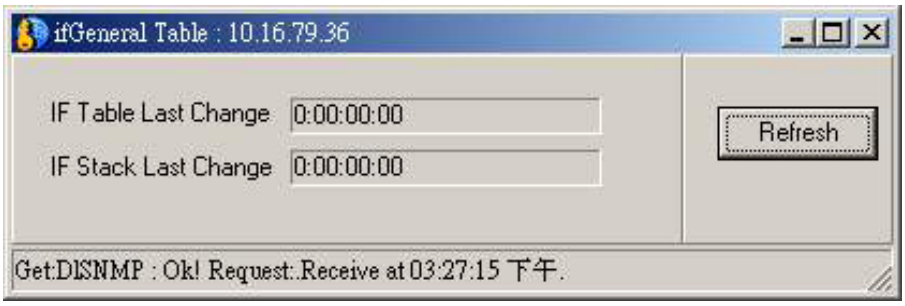


Figure 108

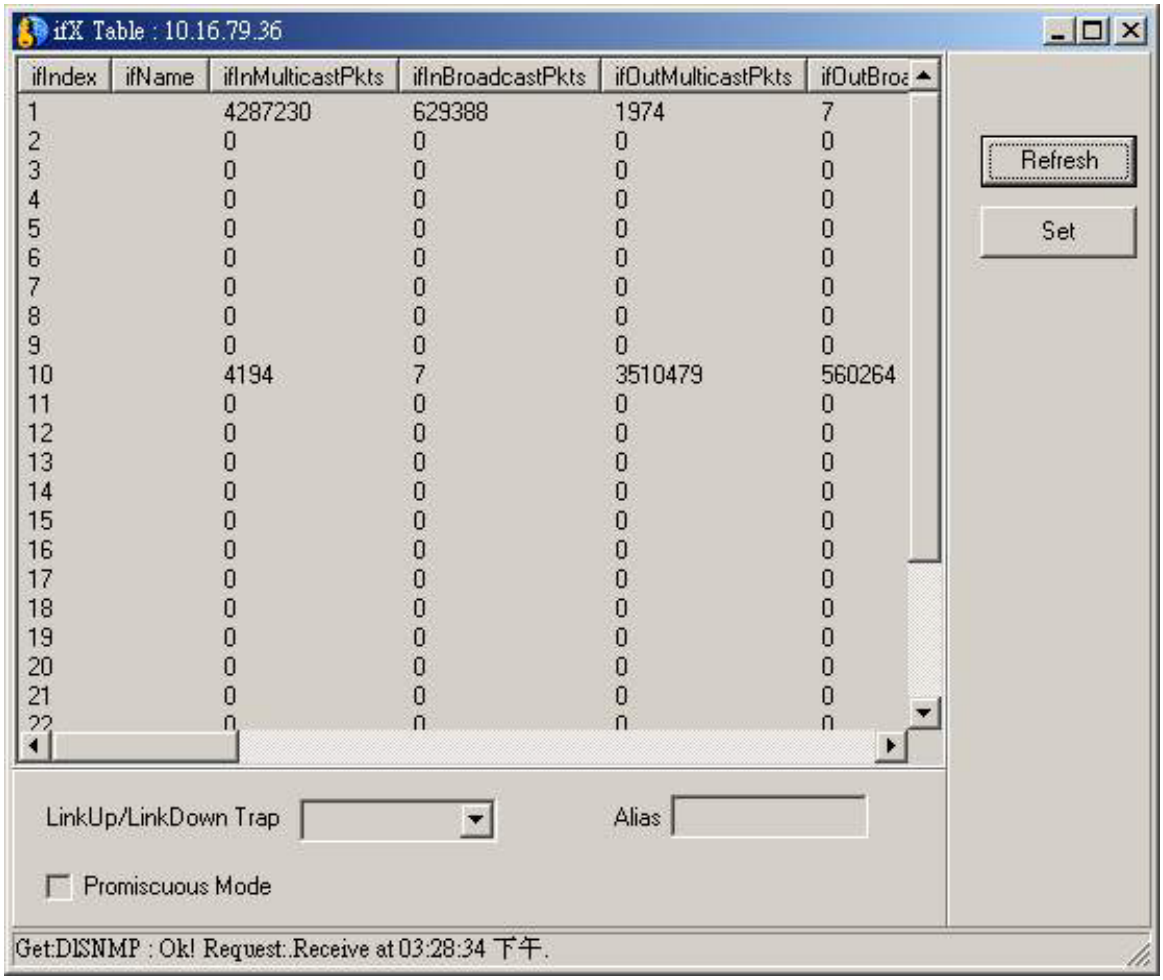


Figure 109.

To enable Link Up/Link Down Trap, assign an Alias or enable Promiscuous Mode highlight the appropriate index and supply the information at the bottom of the menu.

Entity

The following table gives information about the Entity MIB:

Entity MIB (RFC 2737)
- Logical Entity A managed system contains one or more logical entities, each represented by at most one instantiation of each of a particular set of MIB objects. A set of management functions is associated with each logical entity. Examples of logical entities include routers, bridges, print-servers, etc. - Physical Entity A "physical entity" or "physical component" represents an identifiable physical resource within a managed system. Zero or more logical entities may utilize a physical resource at any given time. It is an implementation-specific manner as to which physical components are represented by an agent in the EntPhysicalTable. Typically, physical resources (e.g., communications ports, back planes, sensors, daughter-cards, power supplies, the overall chassis) which can be managed via Functions associated with one or more logical entities are included in the MIB. - Containment Tree Each physical component may be modeled as 'contained' within another physical component. A "containment-tree" is the conceptual sequence of entPhysicalIndex values which uniquely specifies the exact physical location of a physical component within the managed system. It is generated by 'following and recording' each 'entPhysicalContainedIn' instance 'up the tree towards the root', until a value of zero indicating no further containment is found.

Table 3.

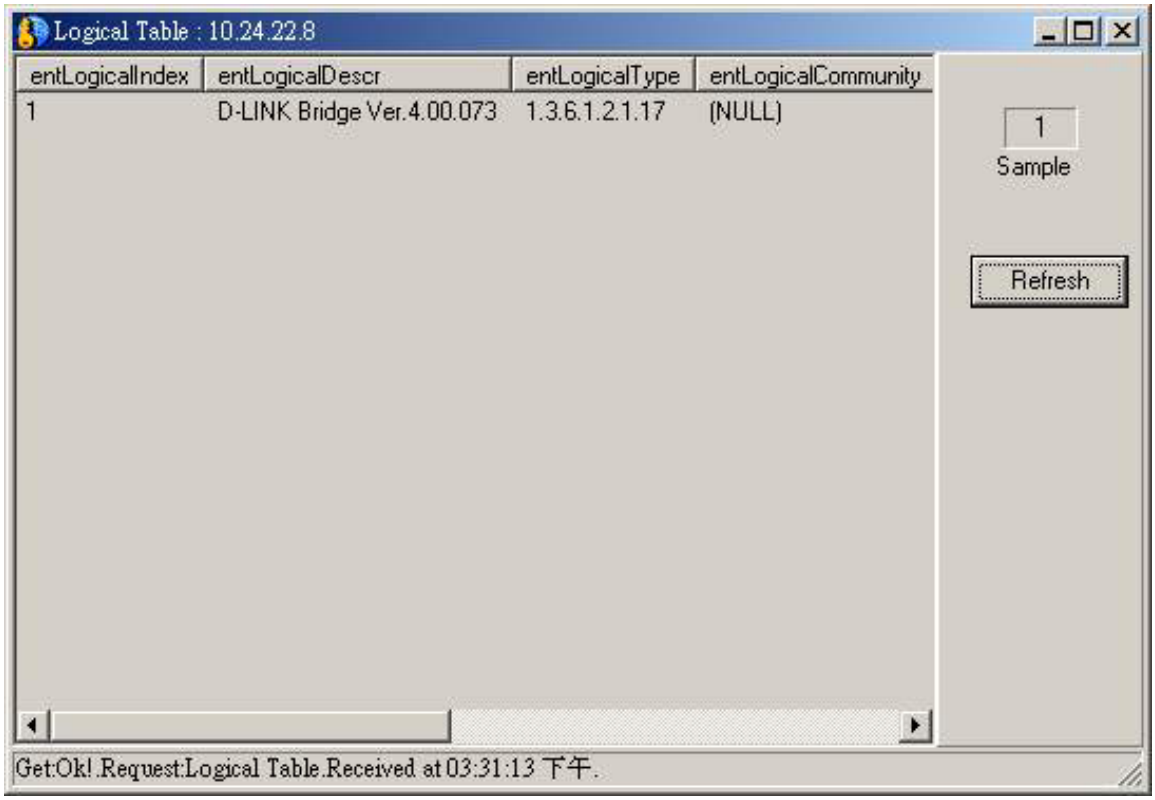


Figure 110. Entity Logical Table

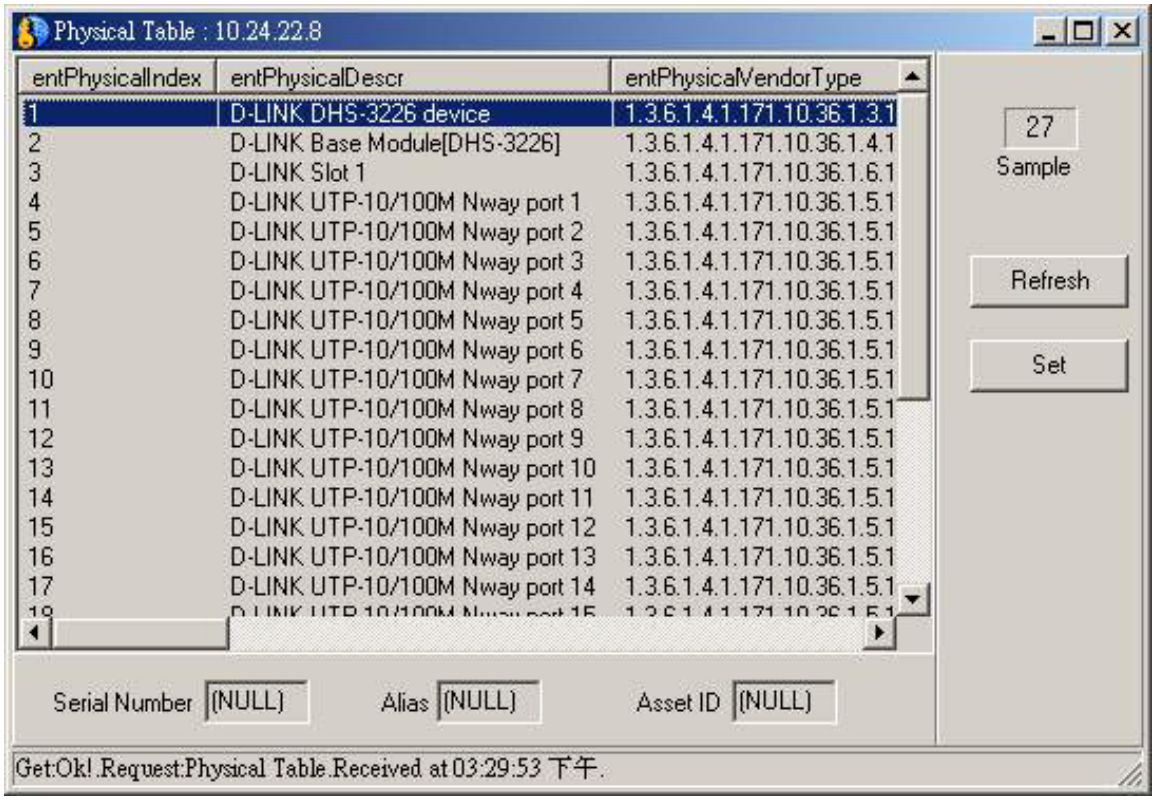


Figure 111. Entity Physical Table

Bridge 802.1d

Bridge 802.1d Information and Port Table

First some Bridge 802.1D (RFC 1493) MIB Group Definitions:

Bridge 802.1D (RFC 1493) MIB Groups
The dot1dBase Group
This mandatory group contains the objects, which are applicable to all types of bridges.
The dot1dStp Group
This group contains the objects that denote the bridge's state with respect to the Spanning Tree Protocol. If a node does not implemented the Spanning Tree Protocol, this group will not be implemented.
The dot1dSr Group
This group contains the objects that describe the entity's state with respect to source route bridging. If source routing is not supported this group will not be implemented. This group is applicable to source route only, and SRT bridges. This group will be described in a separate document applicable only to source route bridging.
The dot1dTp Group
This group contains objects that describe the entity's state with respect to transparent bridging. If transparent bridging is not supported this group will not be implemented. This group is applicable to transparent only and SRT bridges.
The dot1dStatic Group
This group contains objects that describe the entity's state with respect to destination-address filtering. If destination-address filtering is not supported this group will not be implemented. This group is applicable to any type of bridge which performs destination-address filtering.
Relationship to Other MIBs

As described above, some IEEE 802.1d management objects have not been included in this MIB because they overlap with objects in other MIBs applicable to a bridge implementing this MIB. In particular, it is assumed that a bridge implementing this MIB will also implement (at least) the 'system' group and the 'interfaces' group defined in MIB-II.
Relationship to the 'system' group
In MIB-II, the 'system' group is defined as being mandatory for all systems such that each managed entity contains one instance of each.

Table 4. Bridge 802.1D (RFC 1493) MIB Group Definitions

Bridge aging time can be adjusted in the Information window; otherwise Bridge 802.1 windows are read-only.

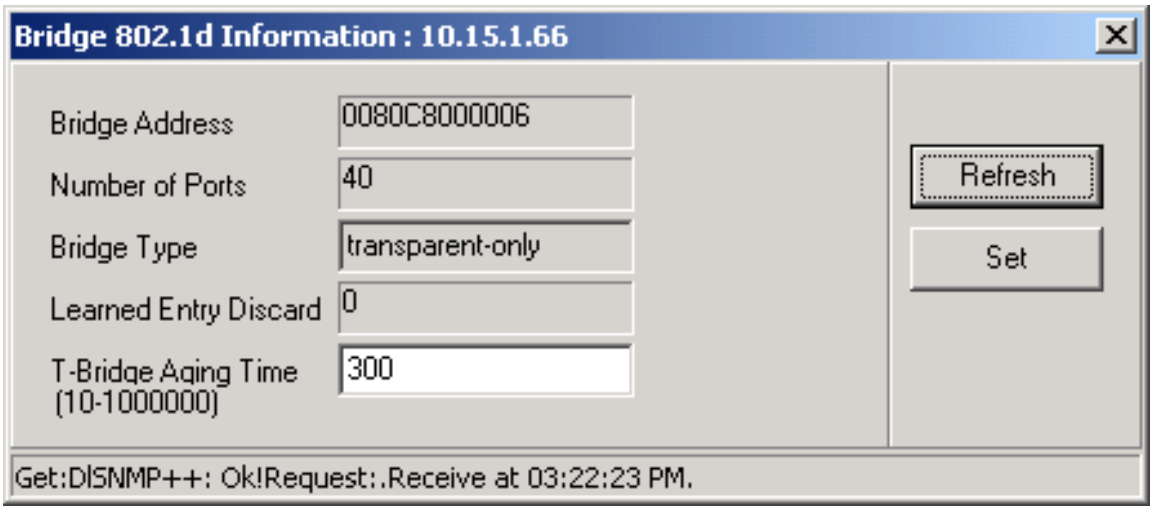


Figure 112. Bridge 802.1d Information

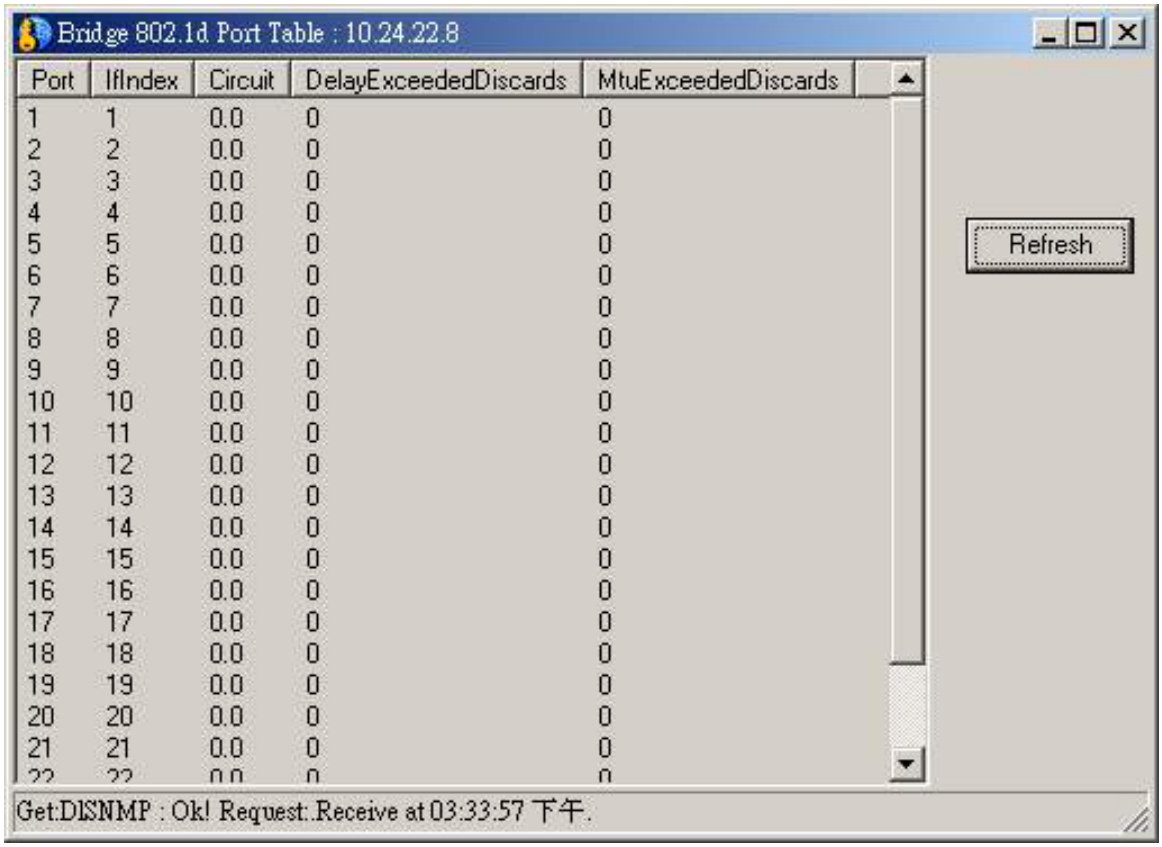


Figure 113. Bridge 802.1d Port Table

Path: MIBs → 802.1D Information/Port Table	
Bridge 802.1D Information	Bridge Address, Number of Ports, Bridge Type, Learned Entry Discard
Port Table Information	Port, IfIndex, Circuit, DelayExceededDiscards, MtuExceededDiscards

Table 5. Bridge 802.1D Information/Port Table

Spanning Tree

Spanning Tree Information

Use the STP Information window for global changes to the selected device. User configurable global STP settings include **Priority**, **Maximum Aging Time**, **Hello Time** and **Forward Delay**.

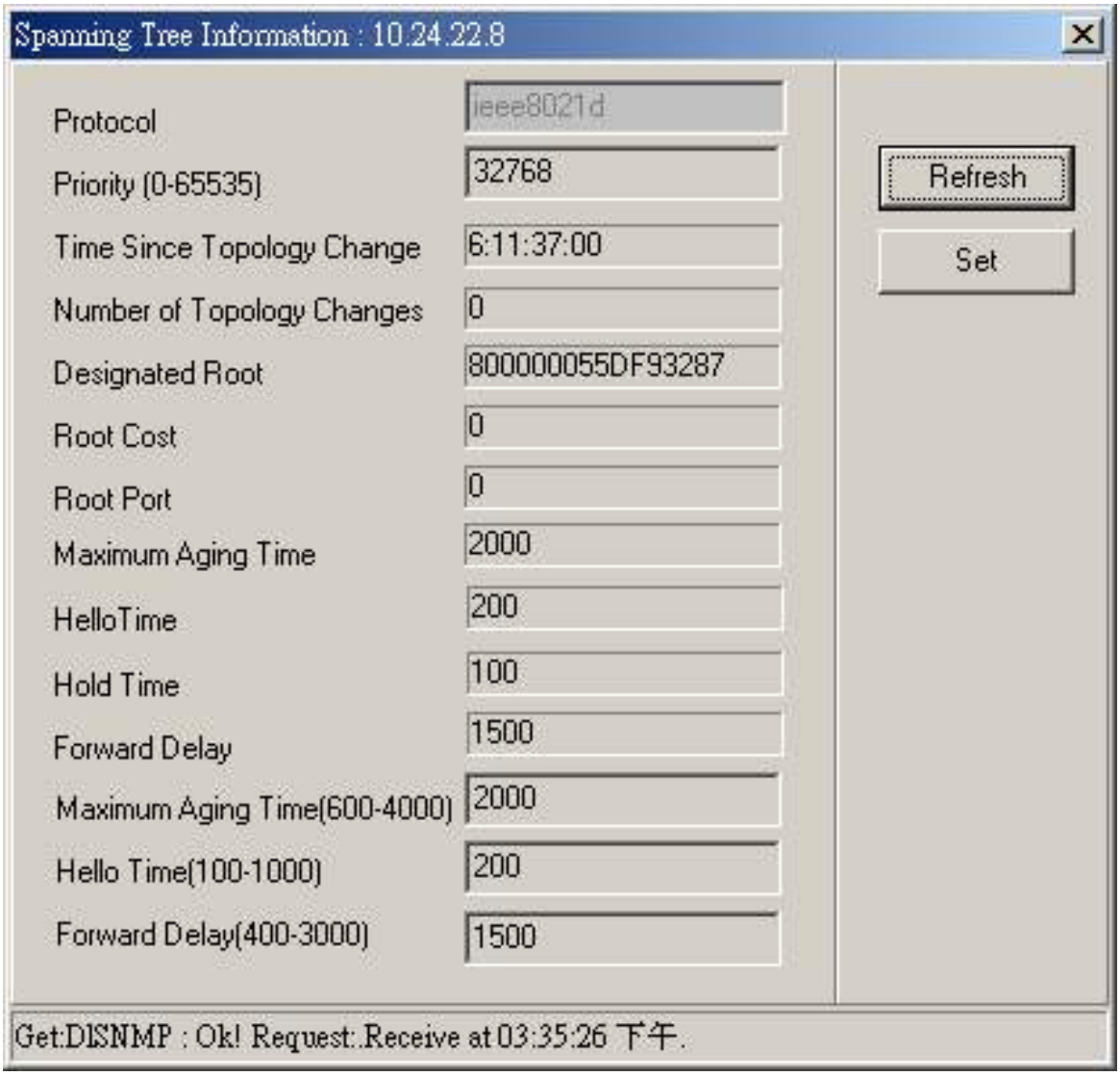


Figure 114. Figure 2. Spanning Tree Information

Path: MIBs → Spanning Tree → Information	
Read-only Information	Protocol, Time Since Topology Change, Number of Topology Changes, Designated Root, Root Cost, Root Port, Maximum Aging Time, Hello Time, Forward Delay
Set Variables	Maximum Aging Time(600-4000), Hello Time(100-1000), Forward Delay(400-3000)

Table 6. Spanning Tree Information

Spanning Tree Port Table

The STP Port Table allows you to configure STP port settings. Select the port you wish to configure and type in the desired Priority and Path Cost for the port. The Status pull-down menu is used to enable or disable the STP settings for the port.

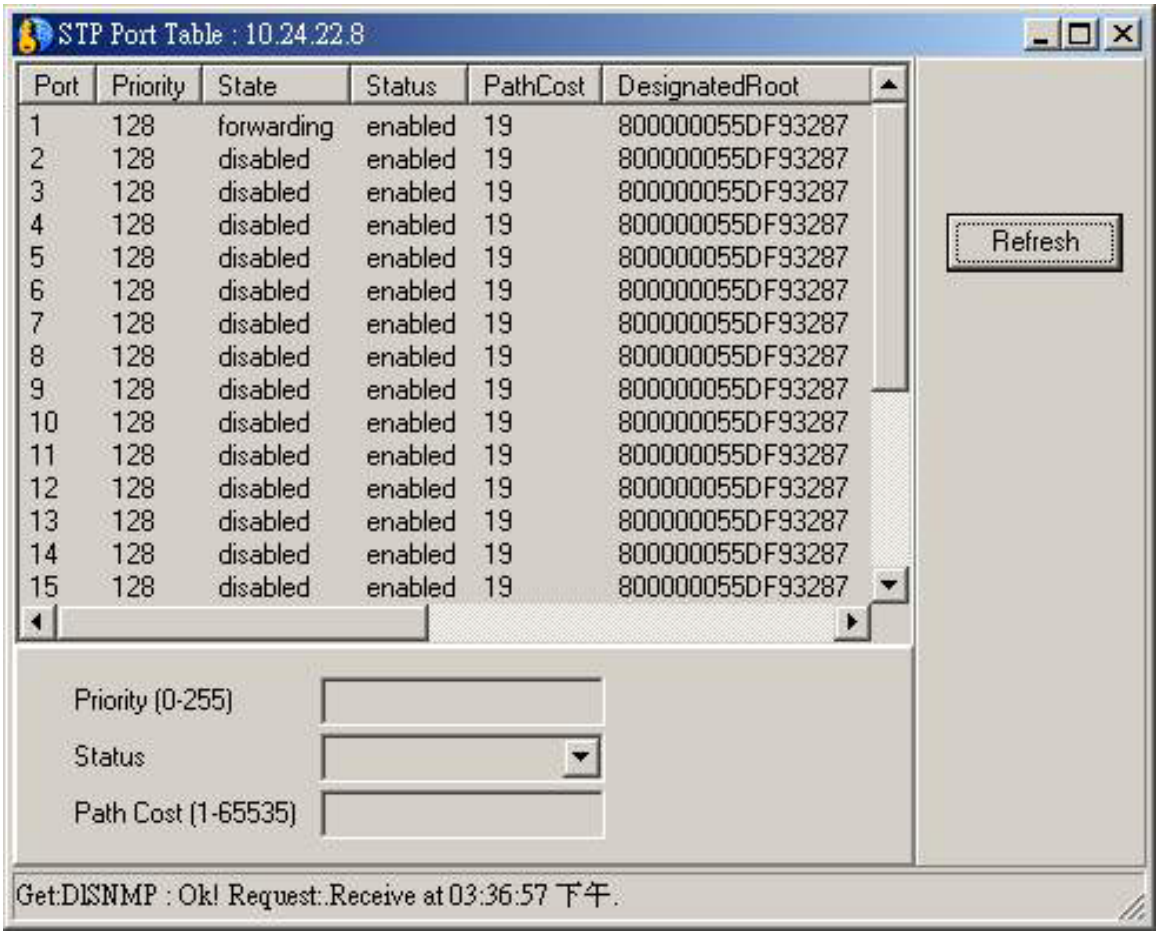


Figure 115. STP Port Table

Path: MIBs → Spanning Tree → Port Table	
Read-only Information	Port, Port Priority, State, Status, Path Cost, DesignatedRoot, DesignatedCost, DesignatedBridge, DesignatedPort, Forwarding Transitions
Set Variables	Priority, Status, Path Cost

Table 7. Spanning Tree Port Table

Transparent Bridge

Transparent Bridge Forwarding & Static Filtering Tables

Highlight to select the device and access these read-only menus from the Transparent Bridge side menu.

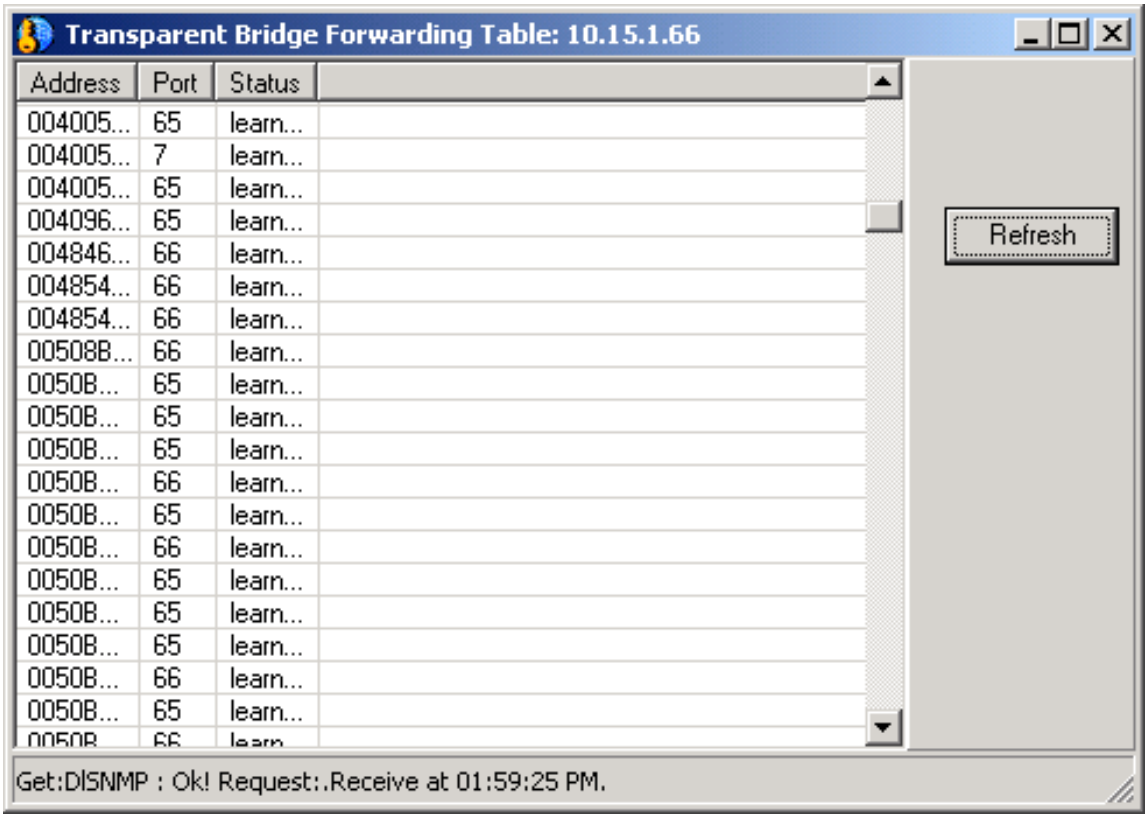


Figure 116. Transparent Bridge Forwarding Table

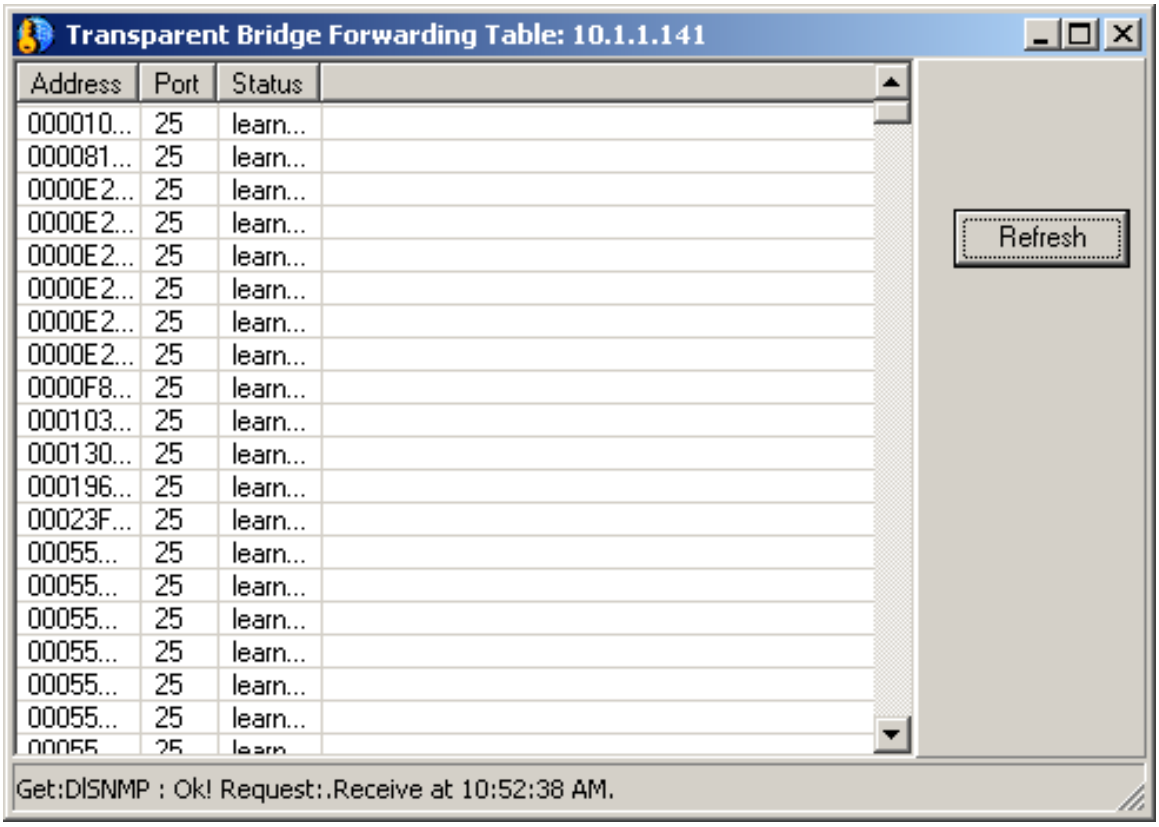


Figure 117. Transparent Bridge Static Filtering Table

Path: MIBs → Transparent Bridge →Forwarding Table/Static Table	
Transparent Bridge Forwarding Table Information	Address, Port, Status
Transparent Bridge Static Filtering Table Information	Address, ReceivePort, AllowedtoGoTo, Status

Table 8. Transparent Bridge Forwarding/Static Filtering Table

Transparent Bridge Port Counter Table & Port Traffic Graph

Counter tables and traffic graphs can be paused or reset as desired. The user can change the Poll Interval and Count, graphs may use a three dimensional line by checking the 3D Line box.

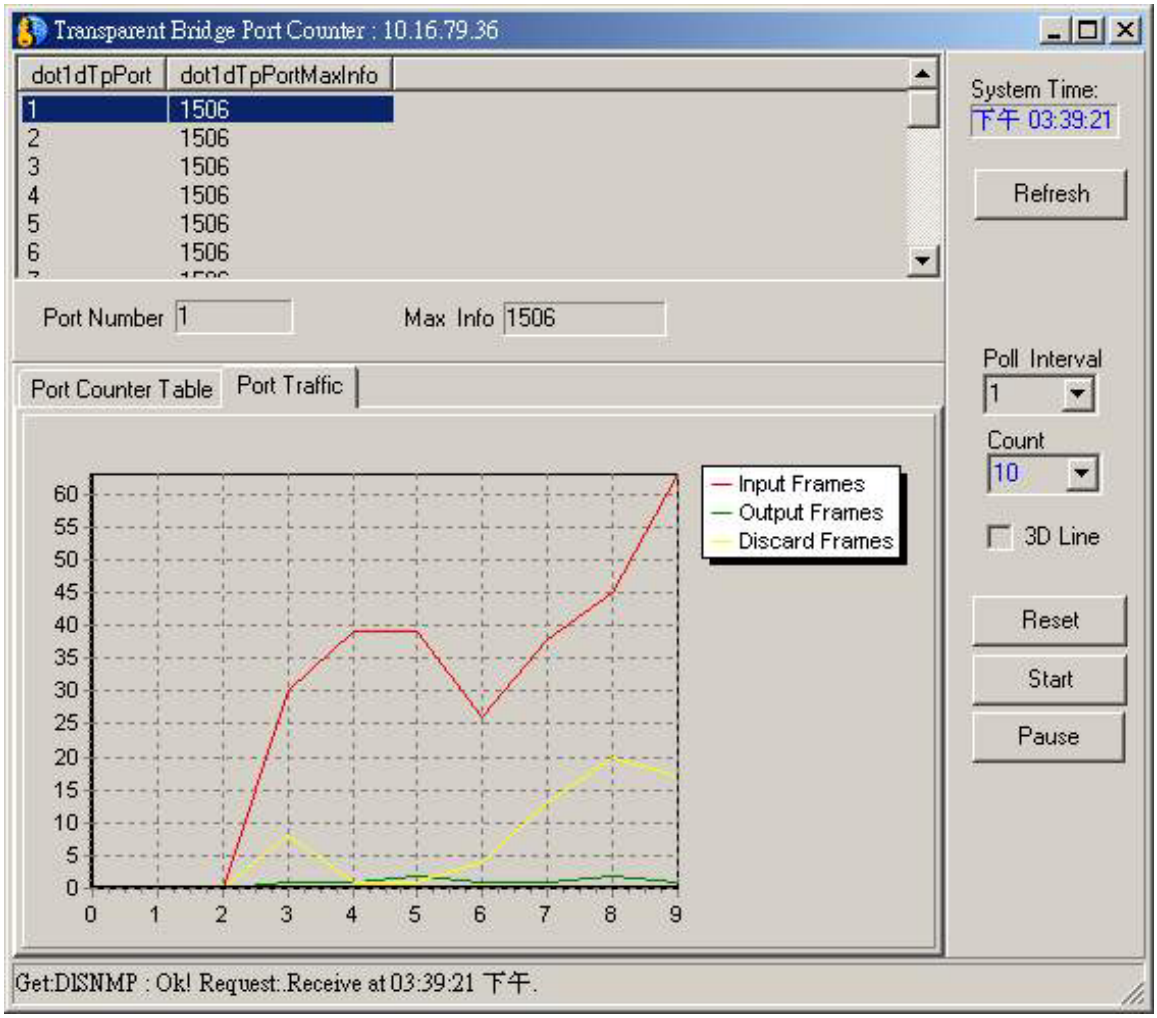


Figure 118. Transparent Bridge Port Counter

Path: MIBs → Transparent Bridge → Port Counter	
Transparent Bridge Port Counter Table	dot1dTpPort, dot1dTpPortMaxInfo, Port Number, Max Info Name, Value, Delta, Rate, Peak, Peak Occ.

Table 9. Transparent Bridge Port Counter

RMON

View RMON statistics for any port on the selected device by clicking the index (port) number. By default the **Statistics Table** is displayed for index 1. **Port Utilization**, **Error** and **Packet Distribution** are displayed graphically. Check the 3D Line for more readily visible graph lines.

Remote Network Monitoring Object Groups
The Ethernet Statistics Group
The Ethernet statistics group contains statistics measured by the probe for each monitored Ethernet interface on this device. This group consists of the etherStatsTable. In the future other groups will be defined for other media types including Token Ring and FDDI. These groups should follow the same model as the Ethernet statistics group.
The History Control Group
The history control group controls the periodic statistical sampling of data from various types of networks. This group consists of the historyControlTable.
The Alarm Group
The alarm group periodically takes statistical samples from variables in the probe and compares them to previously configured thresholds. If the monitored variable crosses a threshold, an event is generated. A hysteresis mechanism is implemented to limit the generation of alarms. This group consists of the alarmTable and requires the implementation of the event group.
The Event Group

The event group controls the generation and notification of events from this device. This group consists of the event Table and the log Table.

Table 10. RMON Statistics

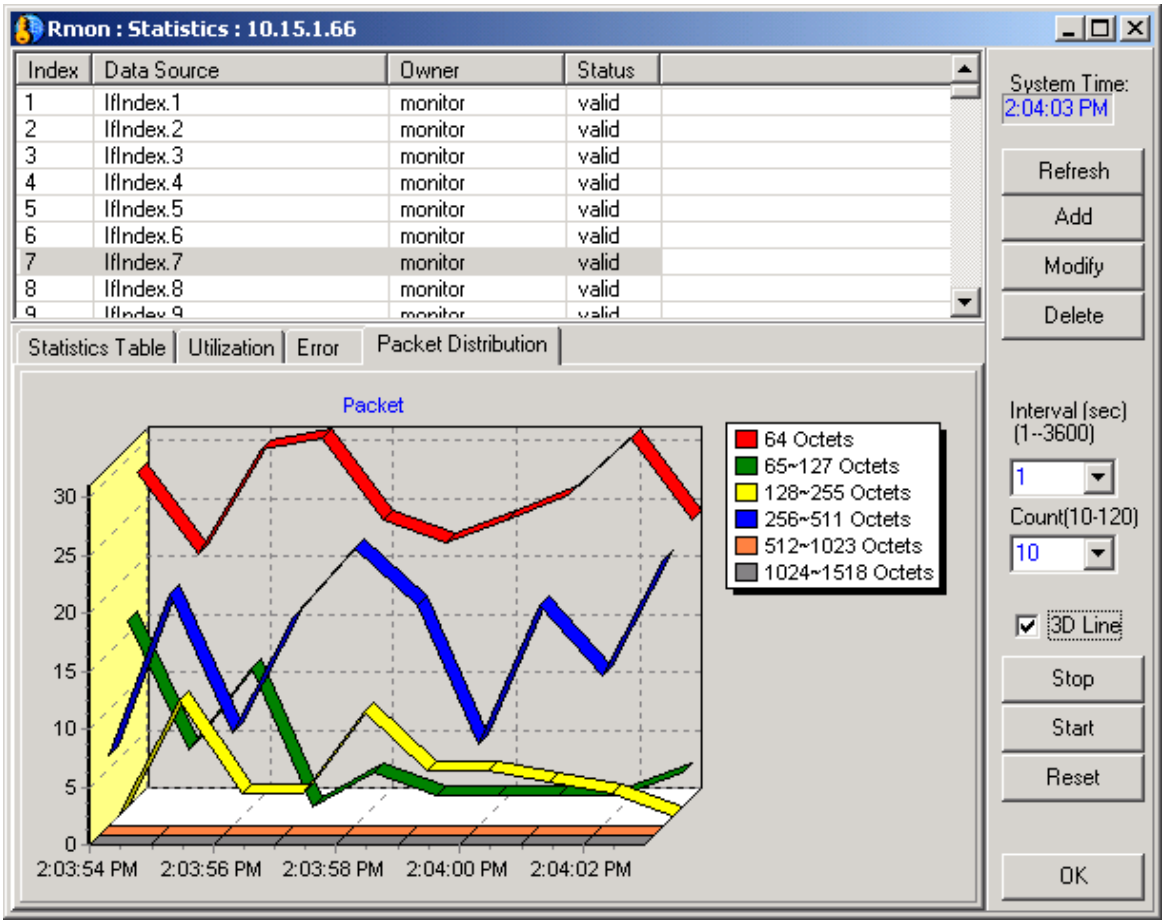


Figure 119. RMON Statistic (Packet Distribution Graph)

Use the Add and Modify function to add an index or change a selected index's variables. Clicking the Add or Modify button will bring up the Control Table pop-up menu. The Control Table pop-up screen is used to input index variables. Statistics information displayed may be frozen at any point and resumed using the Start and Stop buttons.

Path: MIBs → RMON → Statistics	
RMON Statistics Table Information	Index, Data source, Owner, Ststus, Name, Value, Delta, Rate, Pea, Peak Occurred At

Table 11. RMON Statistics

RMON History

View the history table and graphs including Utilization, Error and Packet Distribution. Add or modify and index with the Control Table.

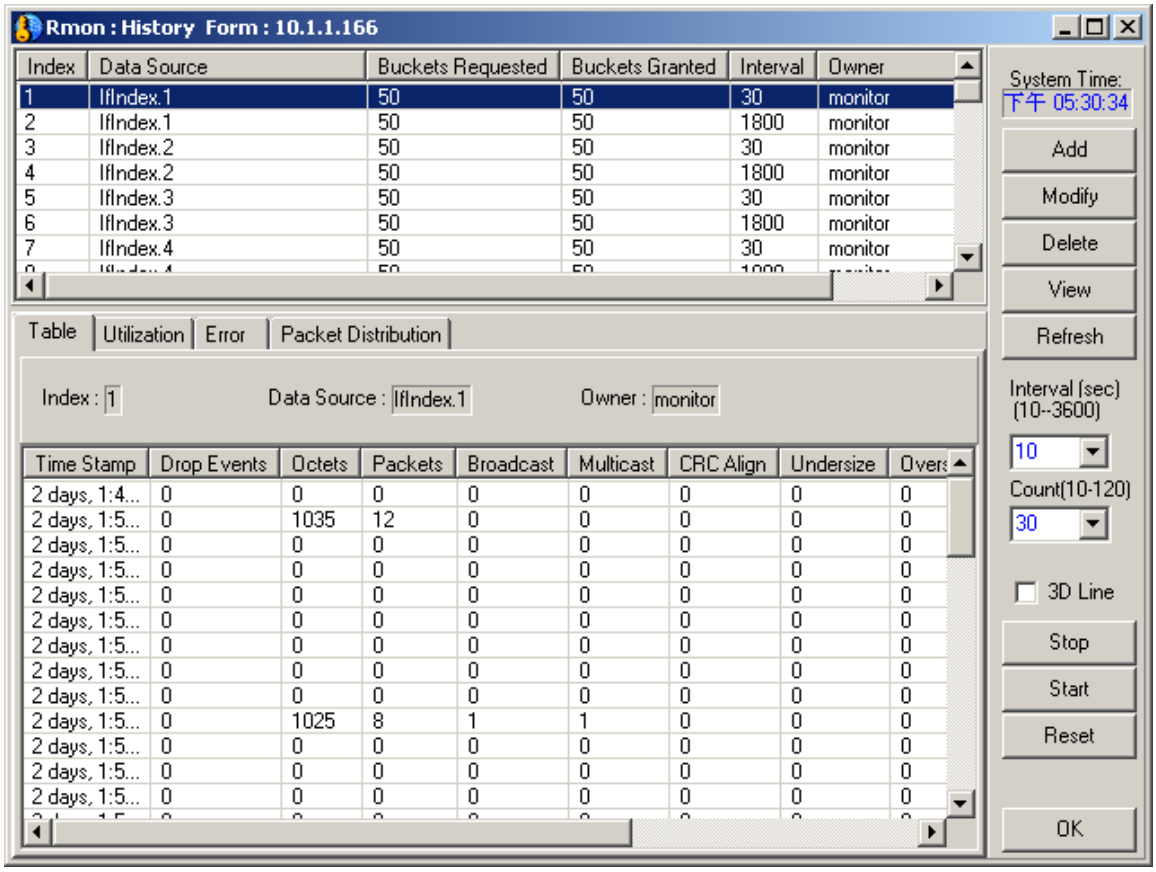


Figure 120. RMON History Table

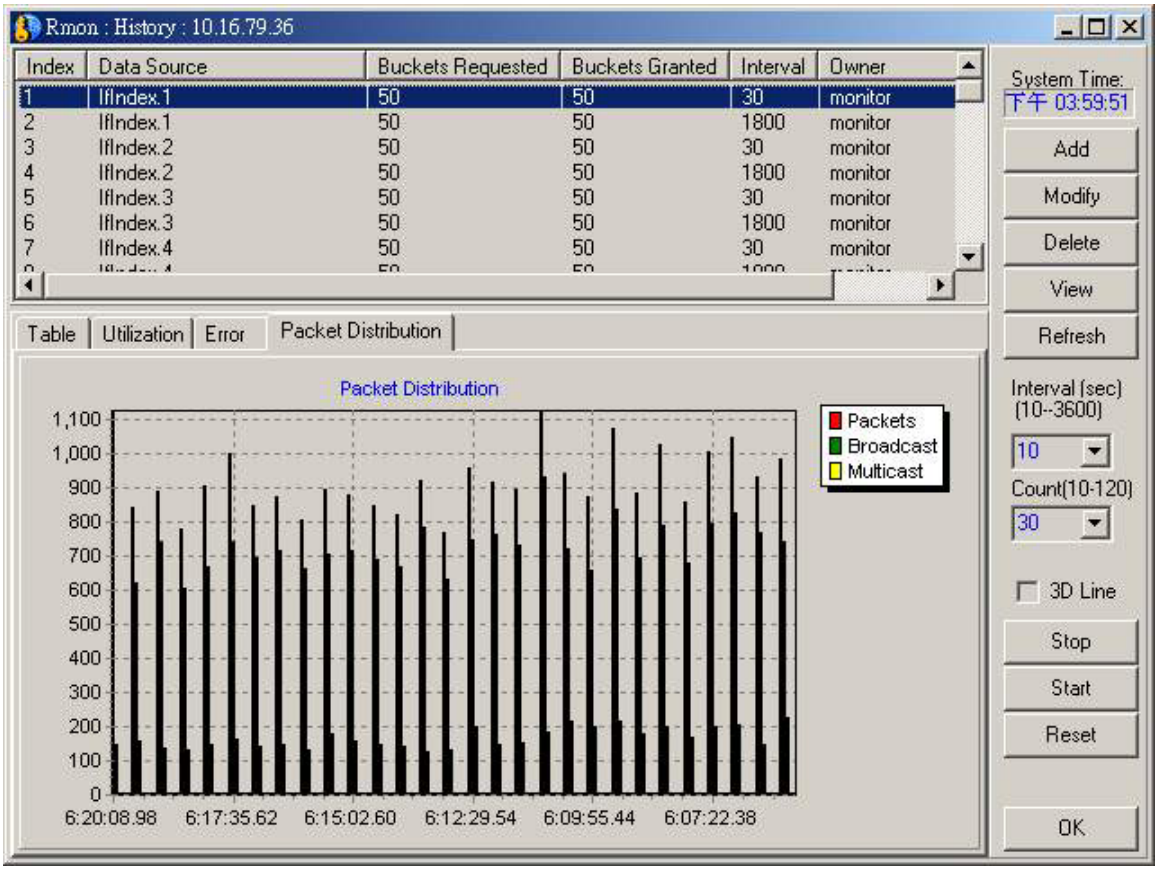


Figure 121. RMON History Graph

Path: MIBs → RMON → History	
RMON History Table Information	Index, Data source, Buckets Requested, Buckets Granted, Interval, Owner, Status, Time Stamp, Drop Events, Octets, Packets, Broadcast, Multicast, CRCAlign, Umndersize, Oversize, Fragments, Jabbers, Collisions, Utilizations

Table 12. RMON History

RMON Alarm

To add an alarm and define parameters for it click the Add button. The Alarm Table pop-up will accept a user-defined index number or you can use the index automatically generated.

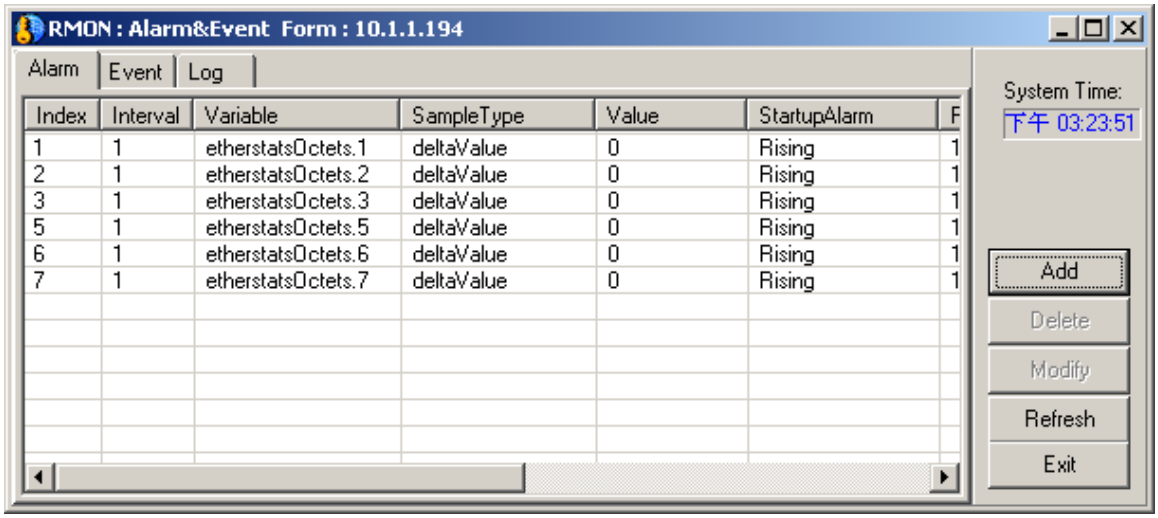


Figure 122. RMON Alarm Table

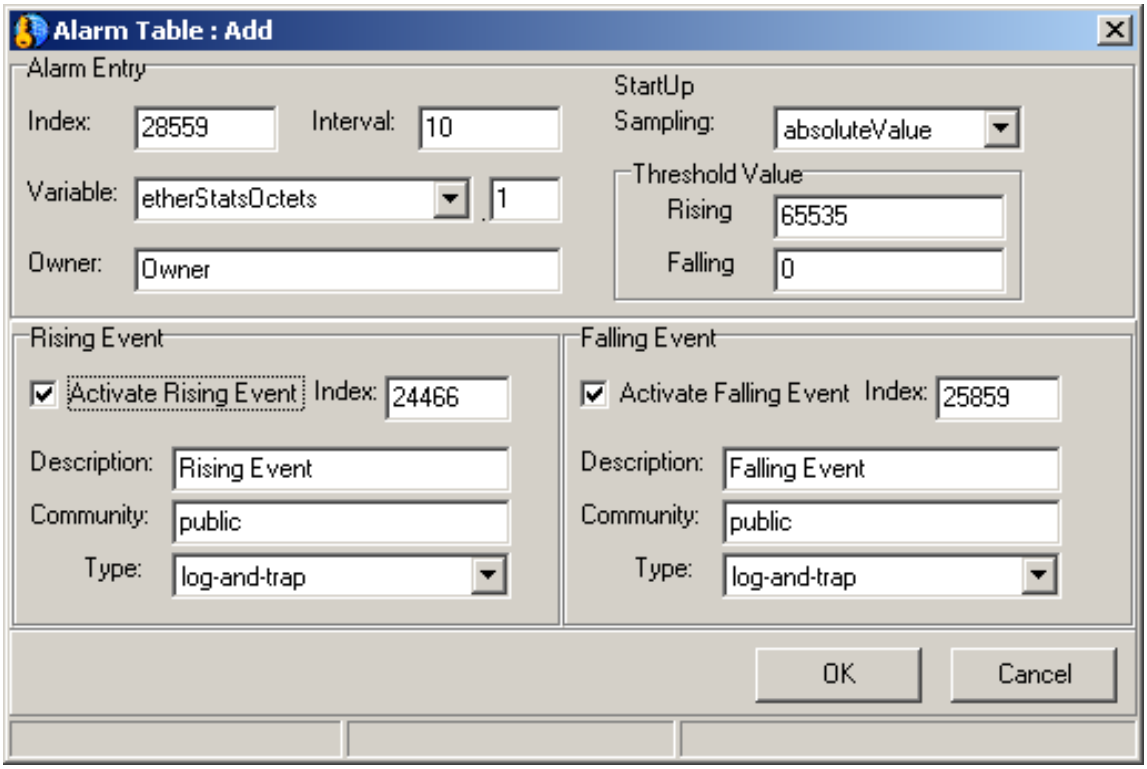


Figure 123. RMON Alarm Table: Add

Path: MIBs → RMON → Alarm/Event	
RMON Alarm Table Information	Index, Interval, Variable, SampleType, Value, StartupAlarm, RisingThreshold, FallingThreshold, RisingEvent, FallingEvent, Owner, Status
RMON Alarm : Add/Modify Parameters	Index, Interval, Variable, Owner, StartUp Sampling, Threshold Value: Rising/Falling, Rising Event: Activate/Index/Description/Community/Type Falling Event: Activate/Index/Description/Community/Type

Table 13. RMON Alarm Table

RMON Event

The Event controls work in a similar fashion. Add or modify an Event control and define its parameters by clicking the Add or Modify button, the Event Control pop-up menu appears.

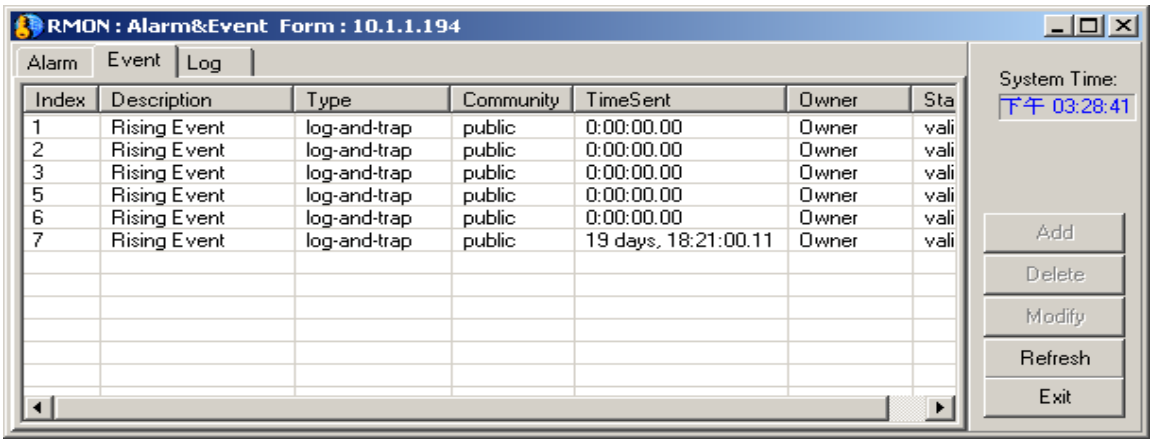
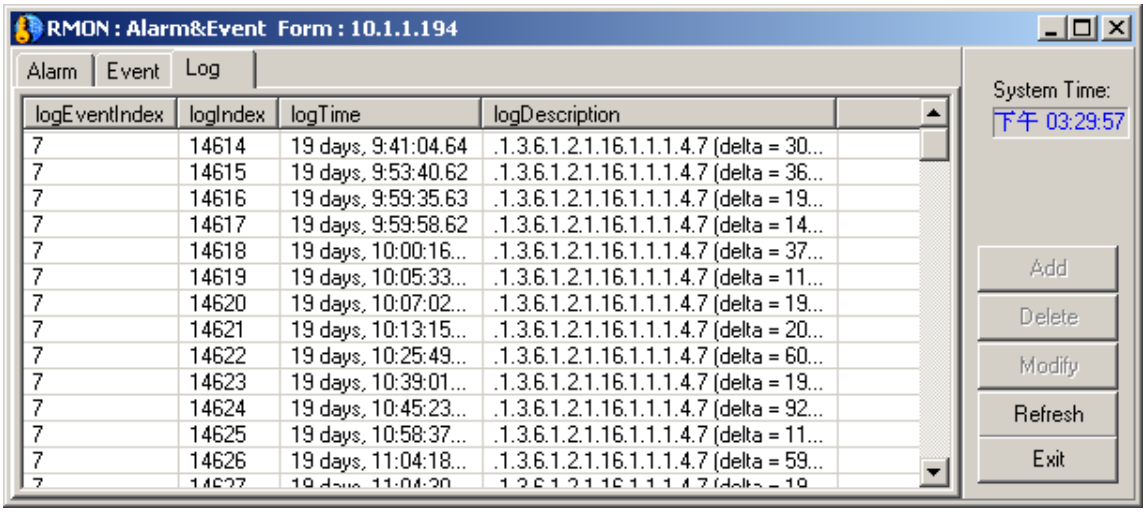


Figure 124. RMON Event



logEventIndex	logIndex	logTime	logDescription
7	14614	19 days, 9:41:04.64	.1.3.6.1.2.1.16.1.1.1.4.7 (delta = 30...
7	14615	19 days, 9:53:40.62	.1.3.6.1.2.1.16.1.1.1.4.7 (delta = 36...
7	14616	19 days, 9:59:35.63	.1.3.6.1.2.1.16.1.1.1.4.7 (delta = 19...
7	14617	19 days, 9:59:58.62	.1.3.6.1.2.1.16.1.1.1.4.7 (delta = 14...
7	14618	19 days, 10:00:16...	.1.3.6.1.2.1.16.1.1.1.4.7 (delta = 37...
7	14619	19 days, 10:05:33...	.1.3.6.1.2.1.16.1.1.1.4.7 (delta = 11...
7	14620	19 days, 10:07:02...	.1.3.6.1.2.1.16.1.1.1.4.7 (delta = 19...
7	14621	19 days, 10:13:15...	.1.3.6.1.2.1.16.1.1.1.4.7 (delta = 20...
7	14622	19 days, 10:25:49...	.1.3.6.1.2.1.16.1.1.1.4.7 (delta = 60...
7	14623	19 days, 10:39:01...	.1.3.6.1.2.1.16.1.1.1.4.7 (delta = 19...
7	14624	19 days, 10:45:23...	.1.3.6.1.2.1.16.1.1.1.4.7 (delta = 92...
7	14625	19 days, 10:58:37...	.1.3.6.1.2.1.16.1.1.1.4.7 (delta = 11...
7	14626	19 days, 11:04:18...	.1.3.6.1.2.1.16.1.1.1.4.7 (delta = 59...

Figure 125. RMON Log

Path: MIBs → RMON → Alarm/Event	
RMON Alarm Event Table Information	Index, Description, Type, Community, TimeSent, Owner, Status
	LogEventIndex, logIndex, logTime, logDescription

Table 14. RMON Alarm Event Table

802.1P & 802.1Q

802.1P

802.1P Priority Settings

Use the 802.1P side menus to view and set 802.1P port priority as well as **GMRP** and **GARP** settings. The read-only **Port Capability Form** is accessed as a side menu.

802.1P / 802.1Q (RFC2674) MIBs
1pPriority Group
This group contains the objects for configuring and reporting status of priority-based queuing mechanisms in a bridge. This includes per-port user priority treatment, mapping of user priority in frames into internal traffic classes and outbound user priority and access priority.
1pGarp Group
This group contains the objects for configuring and reporting on operation of the Generic Attribute Registration Protocol (GARP).
1pGmrp Group
This group contains the objects for configuring and reporting on operation of the GARP Multicast Registration Protocol (GMRP).
Dot1qBase Group
This mandatory group contains the objects, which are applicable to all bridges implementing IEEE 802.1Q virtual LANs.
The dot1qTp Group
This group contains objects that control the operation and report the status of transparent bridging. This includes management of the dynamic Filtering Databases for both unicast and multicast forwarding. This group will be implemented by all bridges that perform destination-address filtering.
The dot1qStatic Group

This group contains objects that control static configuration information for transparent bridging. This includes management of the static entries in the Filtering Databases for both unicast and multicast forwarding.
The dot1qVlan Group
This group contains objects that control configuration and report status of the Virtual LANs known to a bridge. This includes management of the statically configured VLANs as well as reporting VLANs discovered by other means e.g. GVRP. It also controls configuration and reports status of per-port objects relating to VLANs and reports traffic statistics. It also provides for management of the VLAN Learning Constraints.

Table 15.

802.1P Basic Configuration

Set the Traffic Class State (true, false) and GMRP Status.

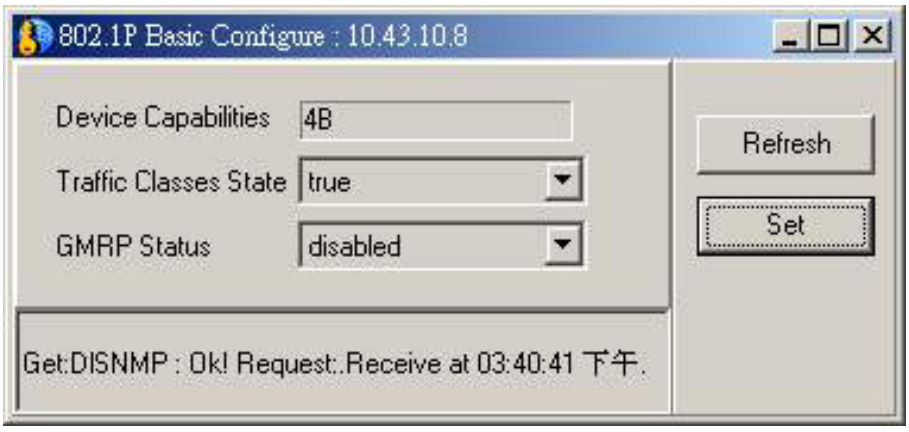


Figure 126. 802.1P Basic Configuration

Path: MIBs → 802.1P → Basic Configuration		
802.1P Basic Configuration	**Read-only**	Device Capabilties
	Set	Traffic Class Status, GMRP Status

Table 16. 802.1P Basic Configuration

Priority Information Form

Choose the appropriate tab to view information listed by port number:

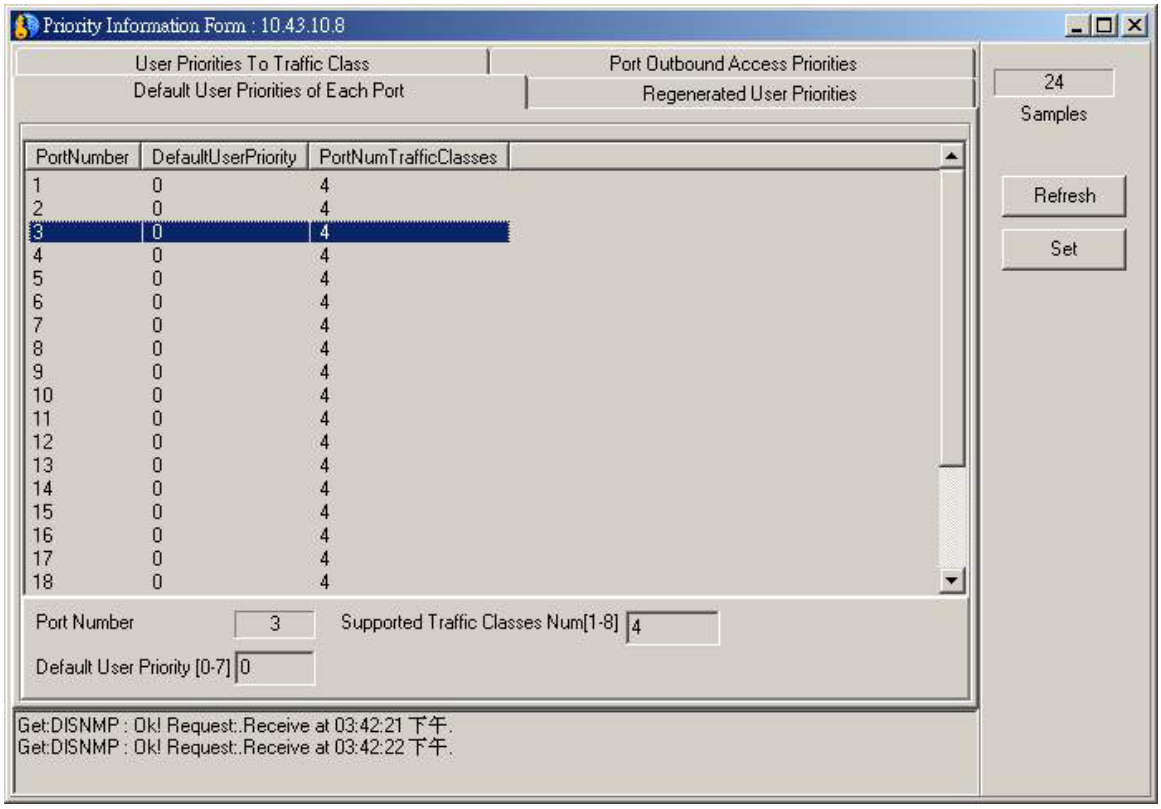


Figure 127. Priority Information Form

Select the port number and type in the appropriate priority values; click Set to effect the change.

Path: MIBs → 802.1P → Priority Information Form		
Default User Priorities of Each Port	**Table Information**	PortNumber, DefaultUserPriority, PortNumTrafficClasses
	Set	SupportedTrafficClassesNum, DefaultUserPriority
Regenerated User Priorities	**Table Information**	PortNumber, UserPriority, RegeneratedUserPriority
	Set	UserPriority
User Priority To Traffic Class	**Table Information**	PortNumber, TrafficClassPriority, MappedTrafficClass
	Set	MappedTrafficClass
Port Outbound Access Priority	**Table Information**	PortNumber, RegenerateUserPriority

Table 17. Priority Information Form

Port Capability

The Port Capability window (accessed as a side menu from 802.1P submenu) is read-only and lists Port Capabilities Entry Messages listed by port number.

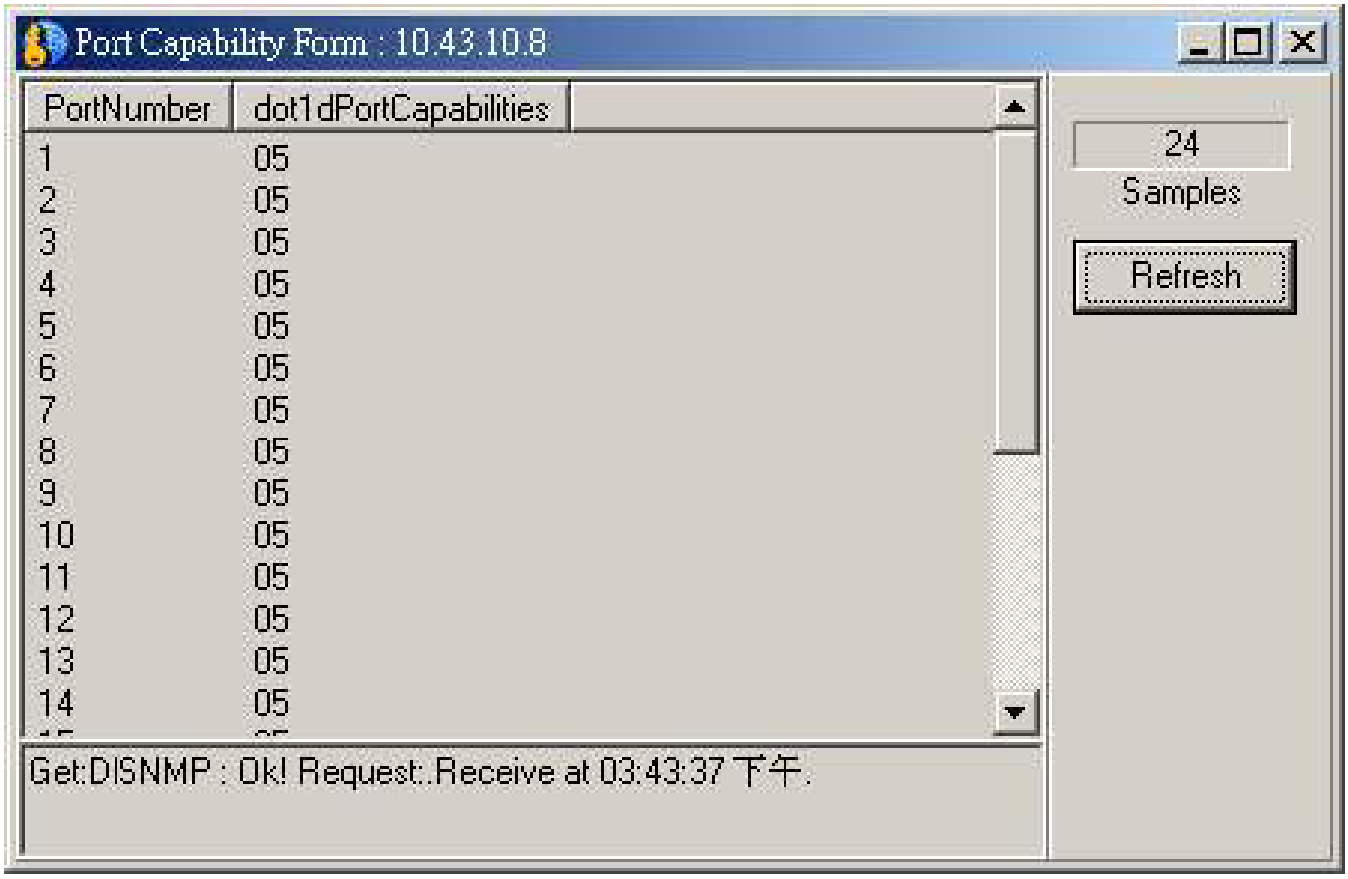


Figure 128. Ports Capability

Path: MIBs → 802.1P → Ports Capability	
Table Information	PortNumber, dot1dPortCapabilities

Table 18. Ports Capability

GMRP

The GMRP Form allows you to enable GMRP for a selected port. To enable GMRP for a given port, highlight to select, choose Enable from the pull-down menu and click Set.

Path: MIBs → 802.1P → GMRP	
GMRP Table Information	PortNumber, Status, GmrpFailed, GmrpLastPduOrign

Table 19. GMRP Table

GARP

GARP settings are expressed in Centi-seconds (hundredths of a second) for each port.

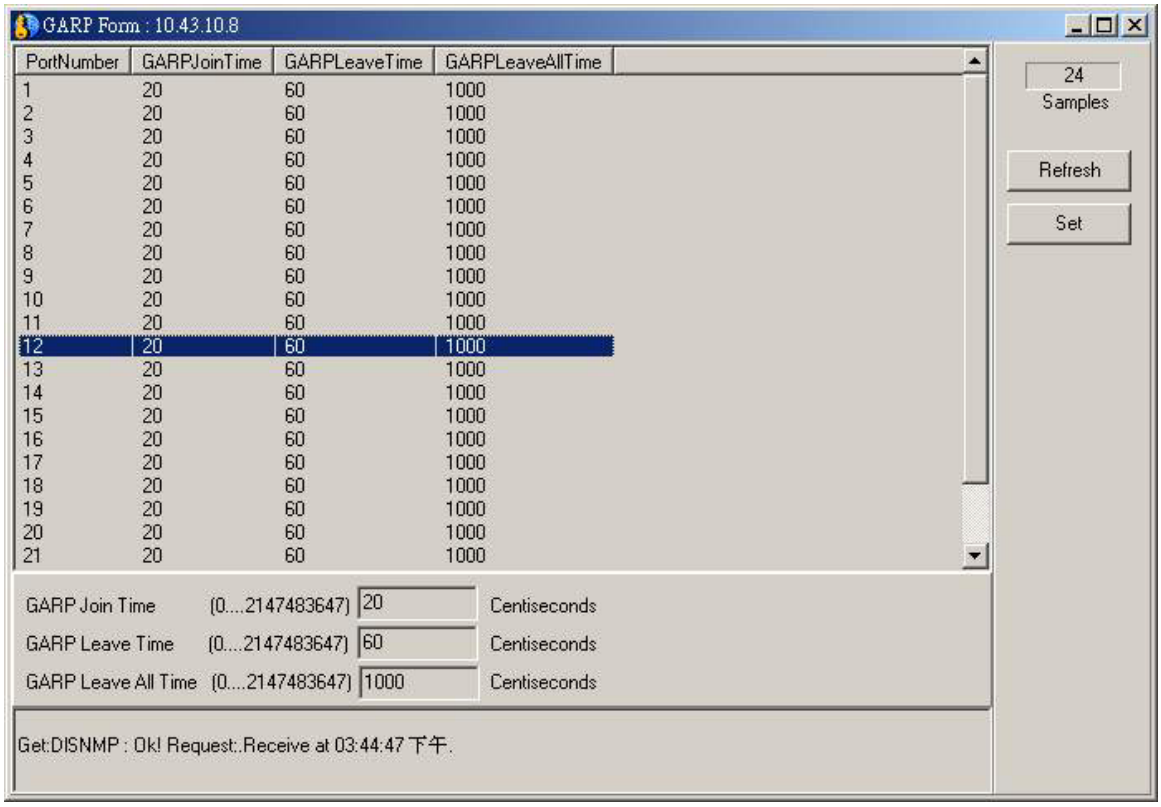


Figure 129. GARP Form

Path: MIBs → 802.1P → GARP	
GARP Table Information	PortNumber, GarpJoinTime, GarpLeaveTime, GarpLeaveAllTime
Set	GarpJoinTime, GarpLeaveTime, GarpLeaveAllTime

Table 20. GARP Table

802.1Q

802.1Q Ports Information

Configure VLANs settings for the selected device in the VLAN Ports Information side menu.

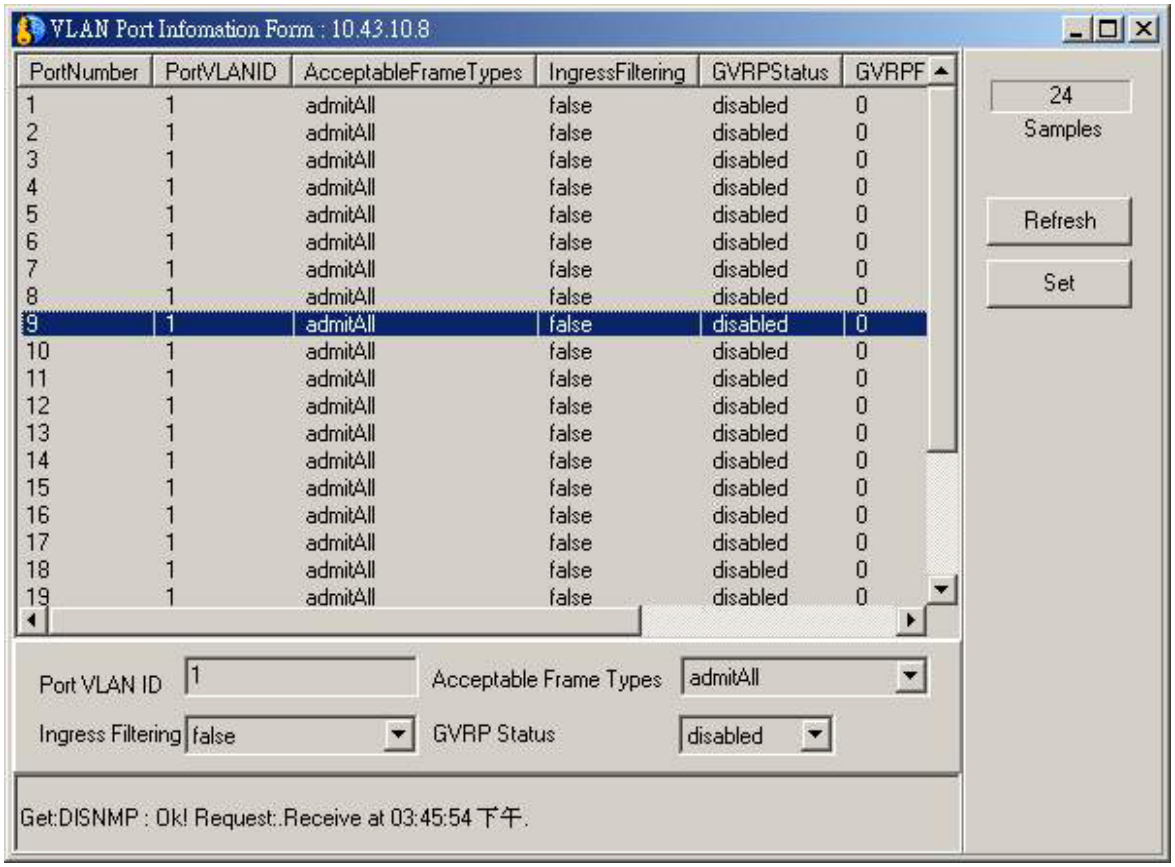


Figure 130. 802.1Q VLAN Port Information Form

Path: MIBs → 802.1Q → 802.1Q Bridge → Ports Information		
VLAN Ports Information Form	**Table Information**	PortNumber, PortVlanID, AcceptableFrameTypes, IngressFiltering, GvrpStatus, GvrpFailedRegistrations, GvrpLastPduOrigin
	Set	PortVlanID, AcceptableFrameTypes, IngressFiltering, GvrpStatus

Table 21. Ports Information

802.1Q Learning Constraint Table

Set Default VLAN Constraint Value and Default Constraint Type.

To add a new listing to the Constraint Table or Modify and existing one, highlight it and select Status and Type from the pull-down menus. Click the Add/Update button effect the changes.

Path: MIBs → 802.1Q → 802.1Q Bridge → Learning Constraint Table		
Learning Constraint Table	**Table Information**	ConstraintVlanID, ConstraintSet, Type, Status
	Set	DefaultVlanConstraintSet, DefaultVlanConstraintType
	Configure	ConstraintVlanID, Type, ConstraintSet, Status

Table 22. Learning Constraint Table

802.1Q VLAN

The Basic VLAN Configuration Form presents in two tables to display VLAN Static and VLAN Current information.

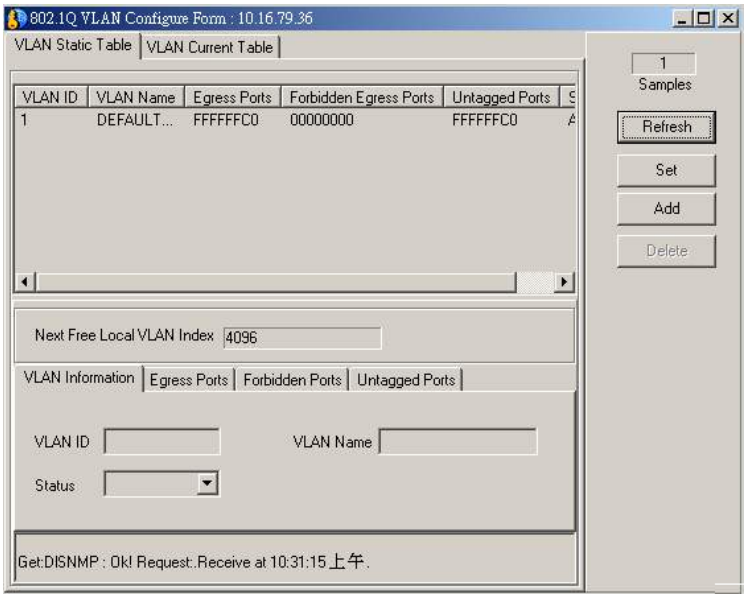


Figure 131. 802.1Q VLAN

Path: MIBs → 802.1Q → 802.1Q VLAN		
VLAN Static Table	**Table Information**	VLAN ID, VLAN Name, Egress Ports, Forbidden Egress Ports
	Set	VLAN Information, Egress Ports, Forbidden Ports, Untagged Ports
VLAN Current Table	**Table information**	VLAN ID, VLAN Name, Egress Ports, Forbidden Egress Ports, Untagged Ports, Status
	Set	Egress Ports, Untagged Ports

Table 23. 802.1Q VLAN

802.1Q Forwarding/Filtering

Forwarding and Filtering information is presented in four separate menus. The menus listed here appear as tabs in the Forwarding/Filtering Form.

Path: MIBs → 802.1Q → Forwarding/Filtering Form		
Unicast Forwarding Info	**Table Information**	Fdb Id, FdbMacAddress, PortNumber, Status
Tp Group Destination Forwarded	**Table Information**	VLAN ID, GroupAddres, EgressPorts, GMRPLearntPorts
	Configure	EgressPorts, GMRPLearntPorts
Multcast Forwarding Info	**Table information**	VLAN ID, AllPorts, StaticPorts, ForbiddenPorts
	Configure	AllForwardedPorts, AllStaticPorts, AllForbiddenPorts
Forward Unregistered Info	**Table Information**	VLAN ID, UnregisteredPorts, Unregistered,StaticPorts
	Configure	UnregisteredPorts, UnregisteredStaticPorts, UnregisteredForbiddenPorts

Table 24. Forwarding/Filtering Form

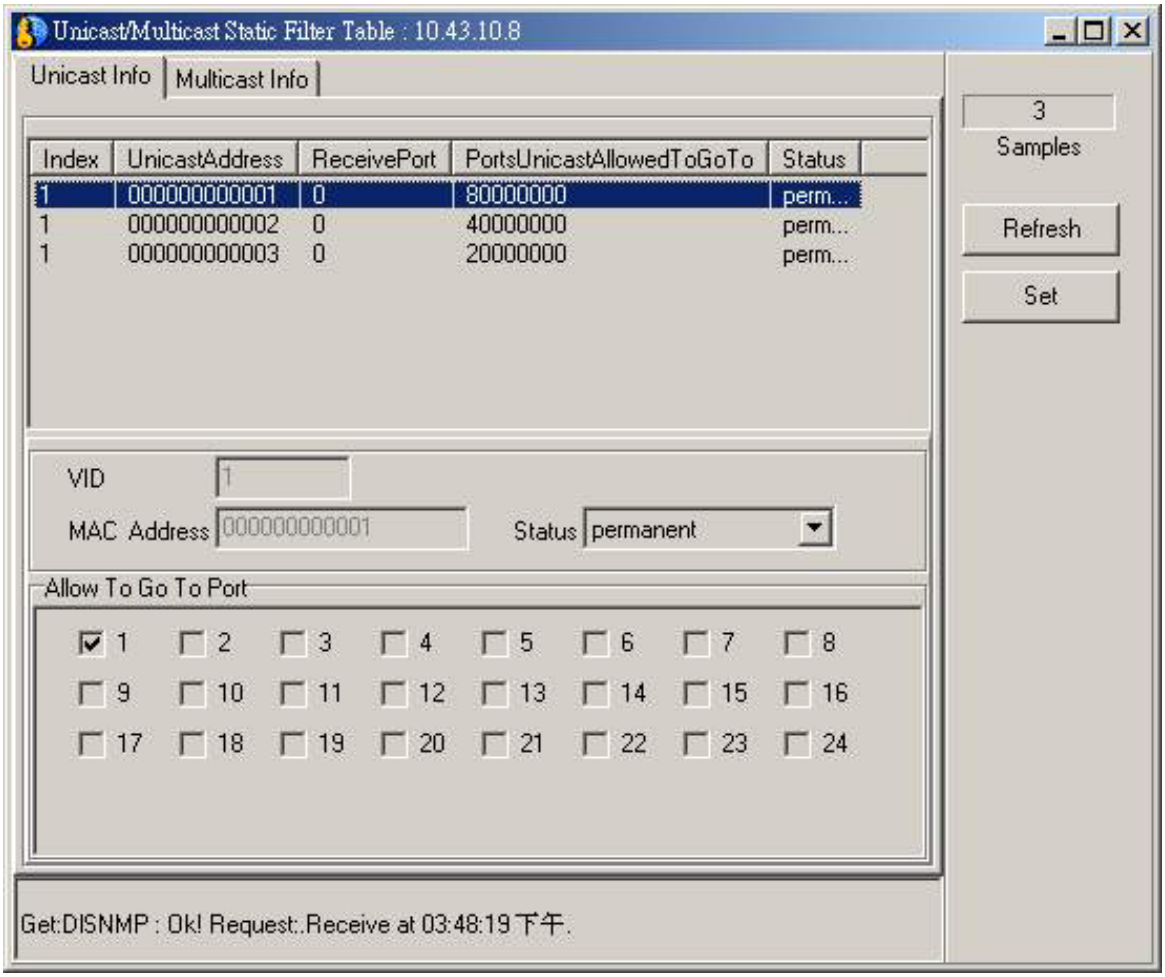


Figure 132. Unicast Multicast Static Filter Table

Path: MIBs → 802.1Q → Unicast/Multicast Static Filter Table		
Unicast Info	**Table Information**	UnicastAddress, ReceivePort, PortsUnicastAllowedToGoTo, Status
	Configure	VID, MAC Address, Status, Allow To Go To Ports (select ports)
VLAN Current Table	**Table information**	MAC Address, Receive Port, Egress Port, Forbidden Ports, Status
	Configure	VID, MAC Address, Status, Egress Ports, Forbidden Ports (select ports)

Table 25. Unicast/Multicast Static Filter Table

Traffic Statistics

Traffic Statistics

Port traffic statistics for selected devices are viewed by highlighting the chosen port and clicking on the Statistics Info button. A new menu pops up displaying port statistics in line graph form.

Port VLAN Statistics

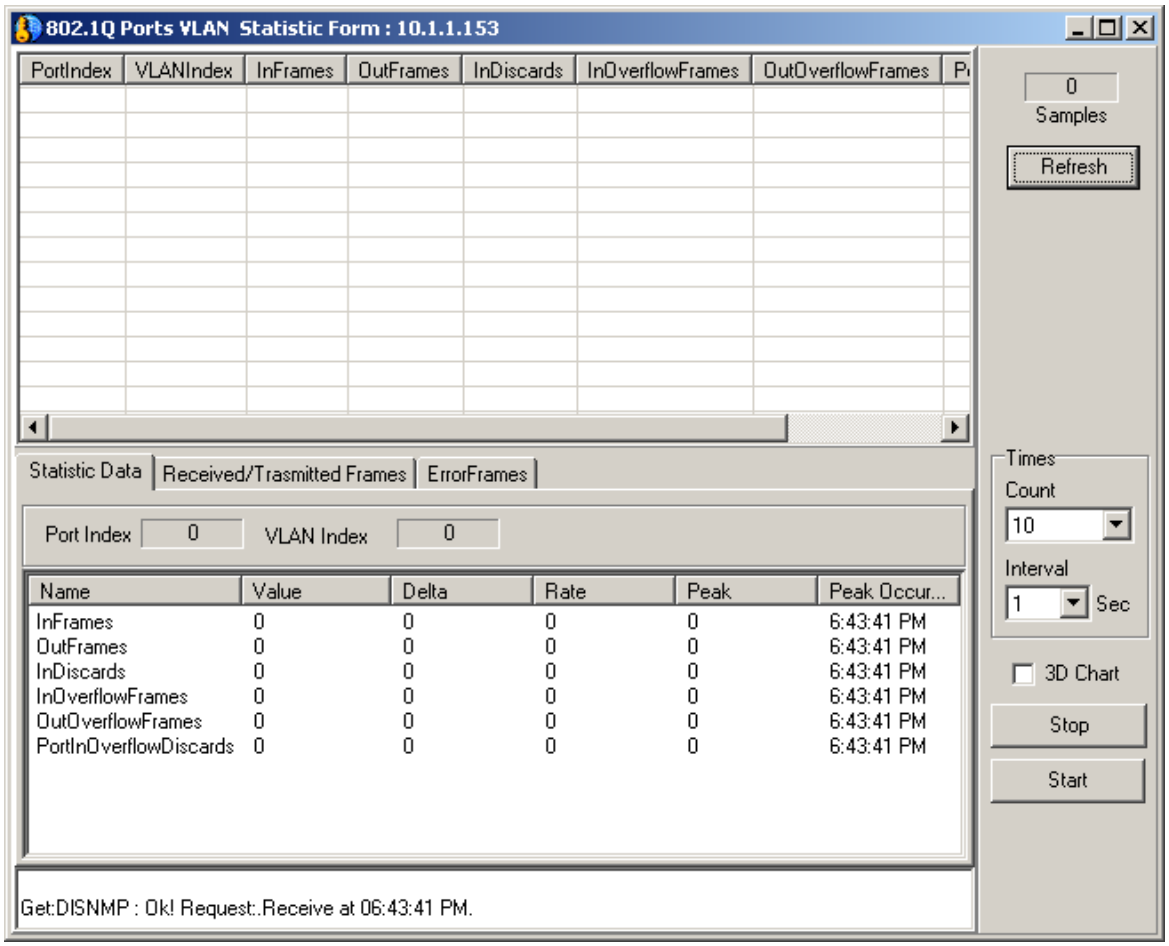


Figure 133.

Layer 3 Utilities

Layer 3 Utilities

To access Layer 3 utilities located under the MIBs proceed as follows: MIBs → 802.1Q → Layer 3 Utilities.

IP Forwarding

IP Forward (RFC 2096) MIB
The MIB consists of two tables and two global objects. 1. The object ipForwardNumber indicates the number of current routes. This is primarily to avoid having to read the table in order to determine this number. 2. The ipForwardTable updates the RFC 1213 ipRouteTable to display multipath IP Routes. This is in turn obsoleted by the ipCidrRouteTable. 3. The ipCidrRouteTable updates the RFC 1213 ipRouteTable to display multipath IP Routes having the same network number but differing network masks.

Table 26.

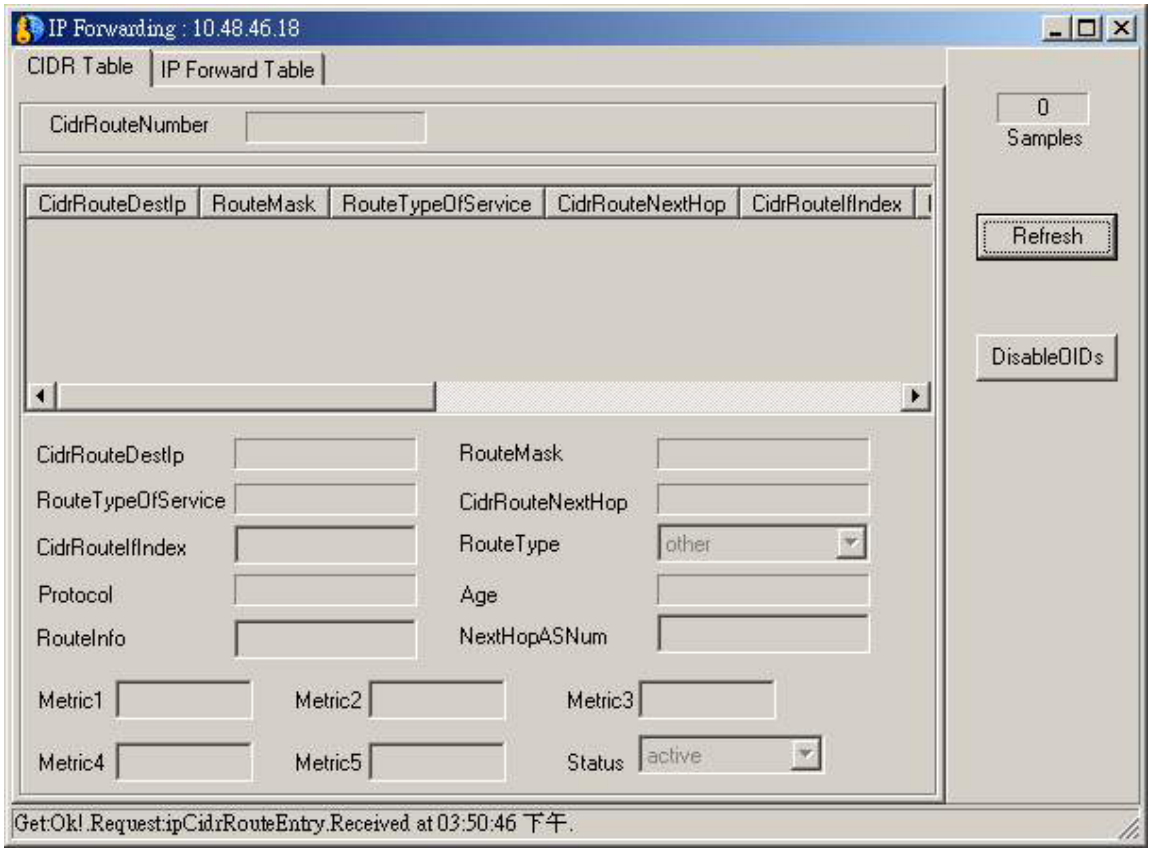


Figure134. IP Forwarding

Path: MIBs → Layer 3 utilities → IP Forwarding		
CIDR Table	**Table Information**	CidrRouteNumber, CidrRouteDestIp, RouteMask, RouteTypeOfService, CidrRouteNextHop, CidrRouteIndex, RouteType, Protocol, Age, RouteInfo, NextHopASNum, Metric 1, Metric 2, Metric 3, Metric 4, Metric 5, Status
	Configure	CidrRouteNumber, CidrRouteDestIp, RouteMask, RouteTypeOfService, CidrRouteNextHop, CidrRouteIndex, RouteType, Protocol, Age, RouteInfo, NextHopASNum, Metric 1, Metric 2, Metric 3, Metric 4, Metric 5, Status
IP Forward Table	**Table information**	IpForwardEntriesNumber, ipForwardMask, ipForwardIndex, ipForwardNextHopAS, ipForwardType, IpForwardInfo
	Configure	IpForwardEntriesNumber, ipForwardMask, ipForwardIndex, ipForwardNextHopAS, ipForwardType, IpForwardInfo

Table 27. IP Forwarding

RIP 2

RIP2 (RFC 1724) MIB
The RIP-2 MIB contains global counters, useful for detecting the deleterious effects of RIP incompatibilities; two "interfaces" tables, which contains interface-specific statistics and configuration information; and an optional "peer" table, containing information that may be helpful in debugging neighbor relationships. Like the protocol itself, this MIB takes great care to preserve compatibility with RIP-1 systems and controls for monitoring and controlling system interactions.
Global Counters
These counters are intended to facilitate debugging quickly changing routes or failing neighbors
Implementation of this Group is Optional
This group provides information about active peer relationships intended to assist in debugging. An active peer is a router from which a valid RIP updated has been heard in the last 180 seconds.

Table 28. RIP 2 Form

Path: MIBs → Layer 3 utilities → RIP 2		
Subnet Information	**Read-only Information**	GlobalRouteChanges, GlobalQueriesResponse SubnetIPAddress, NumOfTriggeredRIPStates, Status
	Set	Subnet IP Address, Status
Subnet Configuration	**Read-only Information**	IP Address

	Set	AuthenticationType, AuthenticationKey, InterfaceSends, AcceptedRIPVersion, DefaultMetric, Status, InterfaceSourceAddress
Routing Peer Information	**Table Information**	SrcIpAddress, PeerDomainReceivedPackets, sysUpTimeOfLastUpdate, VersionNumber, RcvBadPackets, RcvBadRoutes

Table 29. RIP 2

OSPF

OSPF (RFC 1850)

OSPF is a powerful routing protocol, equipped with features to handle virtually any configuration requirement that might reasonably be found within an Autonomous System. With this power comes a fair degree of complexity, which the sheer number of objects in the MIB will attest to. Care has therefore been taken, in constructing this MIB, to define default values for virtually every object, to minimize the amount of parameterization required in the typical case. That default configuration is as follows: Given the following assumptions:

- -IP has already been configured
- -The if Table has already been configured
- -if Speed is estimated by the interface drivers
- -The OSPF Process automatically discovers all IP
- -Interfaces and creates corresponding OSPF Interfaces
- -The TOS 0 metrics are autonomously derived from if Speed
- -The OSPF Process automatically creates the Areas required for the Interfaces

The simplest configuration of an OSPF process requires that:

- The OSPF Process is enabled.
- Area Data Structure and Area Stub Metric Table
- The Area Data Structure describes the OSPF Areas that the router participates in. The Area Stub Metric Table describes the metrics advertised into a stub area by the default router(s).

Link State Database and External Link State Database

The Link State Database is provided primarily to provide detailed information for network debugging.

Address Table and Host Tables

The Address Range Table and Host Table are provided to view configured Network Summary and Host Route information.

Interface and Interface Metric Tables

The Interface Table and the Interface Metric Table together describe the various IP interfaces to OSPF. The metrics are placed in separate tables in order to simplify dealing with multiple types of service, and to provide flexibility in the event that the IP TOS definition is changed in the future. A Default Value specification is supplied for the TOS 0 (default) metric.

Virtual Interface Table

Likewise, the Virtual Interface Table describes virtual links to the OSPF Process.

Neighbor and Virtual Neighbor Tables
The Neighbor Table and the Virtual Neighbor Table describe the neighbors to the OSPF Process.
OSPF Traps
OSPF is an event driven routing protocol, where an event can be a change in an OSPF interface's link-level status, the expiration of an OSPF timer or the reception of an OSPF protocol packet. Many of the actions that OSPF takes as a result of these events will result in a change of the routing topology. As routing topologies become large and complex it is often difficult to locate the source of a topology change or unpredicted routing path by polling a large number or routers. Another approach is to notify a network manager of potentially critical OSPF events with SNMP traps.

Table 30.

.

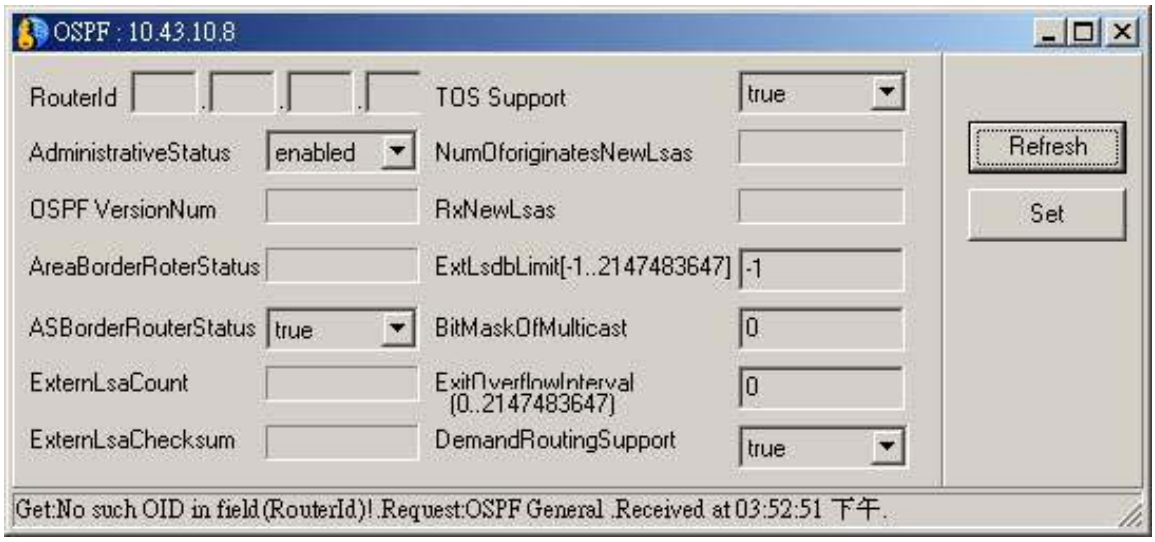


Figure 135. OSPF General Information

Path: MIBs → Layer 3 utilities → OSPF → OSPF General	
Read-only	NumOforiginatesLsas, OSPF VersionNum, RxNewLsas, AreaBorderRouterStatus, ExternLsaCount, ExternLsaChecksum
Set	RouterId, Support Service Type, ASBorderRouterStatus, ExtLsdbLimit, ASBorderRouterStatus, BitMaskOfMulticast, ExitOverflowInterval, DemandRoutingSupport

Table 31. OSPF General Information

Path: MIBs → Layer 3 utilities → OSPF → OSPF Area Information		
Area Table	**Read-only Information**	GlobalRouteChanges, GlobalQueriesResponse SubnetIPAddress, NumOfTriggeredRIPStates, Status
	Set	AreaId, Type Area Summary, Area Status, ImportASExternLsa
Stub Area Table	**Read-only Information**	Stub Area, Type Of Service
	Set	Metric, Metric Type, Status
Area Aggregate Table	**Read-only Information**	AggreagateAreaID, AggregateNet, AggregateMask
	Set	AggregateEffect, LsdbType, AggregateStatus
Area Range Table	**Set**	AreaRangeAreaId, AreaRangeNet, AreaRangeMask, AreaRangeEffect, AreaRangeStatus

Table 32. OSPF Area Information

Path: MIBs → Layer 3 utilities → OSPF → OSPF Lsdb Form		
Link State Database	**Table Information**	LsdbAreaId, Type, LinkStatID, RouterID, SequenceNum, Age, Checksum, Advertisement
Ext Link State Database	**Table Information**	LsdbType, LinkStateID, RouterID, SequenceNum, Age, Checksum, Advertisement

Table 33. OSPF Lsdb Form

OSPF Host Table

Path: MIBs → Layer 3 utilities → OSPF → OSPF Host Table Form	
Table Information	HostIpAddress, TypeOfService, Metric, Status, HostAreaID
Set	HostIpAddress, TypeOfService, Metric, Status

Table 34. OSPF Host Table Form

Path: MIBs → Layer 3 utilities → OSPF → OSPF Interface		
Interface Table	**Table Read-only Information**	IfIpAddress, AddressLessInterface
	Set	Type, Priority, Status, AreaIdOfInterfaceConnected, TransitDelay, AuthenticationKey, RetransInterval, IfMulticastForwarding, HelpInterval, Administrative Status, RouterDeadInterval, IfDemand, PollInterval, Authentication Type
Interface Metric Table	**Table/Read-only Information**	IpAddress, AddressLessInterface, TypeOfService
	Set	MetricValue, Status
Virtual Interface Table	**Table Read-only Information**	AreaId, NeighborID
	Set	TransitDelay, Hellointerval, RetransInterval, RtrDeadInterval,

Table 35. OSPF Interface

OSPF Neighbor Form

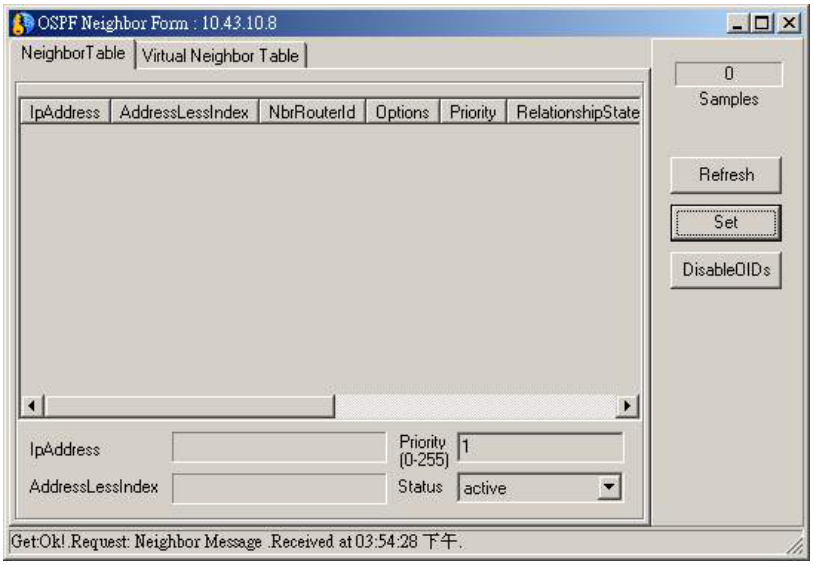


Figure 136. OSPF Neighbor Form

Path: MIBs → Layer 3 utilities → OSPF → OSPF Neighbor		
Neighbor Table	**Table/Read-only Information**	IpAddress, AddressLessIndex
	Set	Priority, Status

Virtual Neighbor Table	**Table Information**	TransitAreaID, NbrRouterId, VirtualNbrIpAddr, Options, State, Events, RetransmissionQueueLen, HelloSuppressed

Table 36. OSPF Neighbor

Path: MIBs → Layer 3 utilities → OSPF → OSPF Trap Form	
Table Information	OspfSetTrap, ConfigErrorType, PacketType, PacketSrc
OSPF Trap Events	

Table 37. OSPF Trap Form

IP Mroute

IP MRoute (RFC 2932) MIB
This MIB module contains one scalar and five tables. The tables are: 6. The IP Multicast Route Table containing multicast routing information for IP data grams sent by particular sources to the IP multicast groups known to a router. 7. The IP Multicast Routing Next Hop Table containing information on the next-hops for the routing IP multicast data grams. Each entry is one of a list of next-hops on outgoing interfaces for particular sources sending to a particular multicast group address. 8. The IP Multicast Routing Interface Table containing multicast routing information specific to interfaces. 9. The IP Multicast Scope Boundary Table containing the boundaries configured for multicast scopes. 10. The IP Multicast Scope Name Table containing human-readable names of multicast scope.

Table 38.

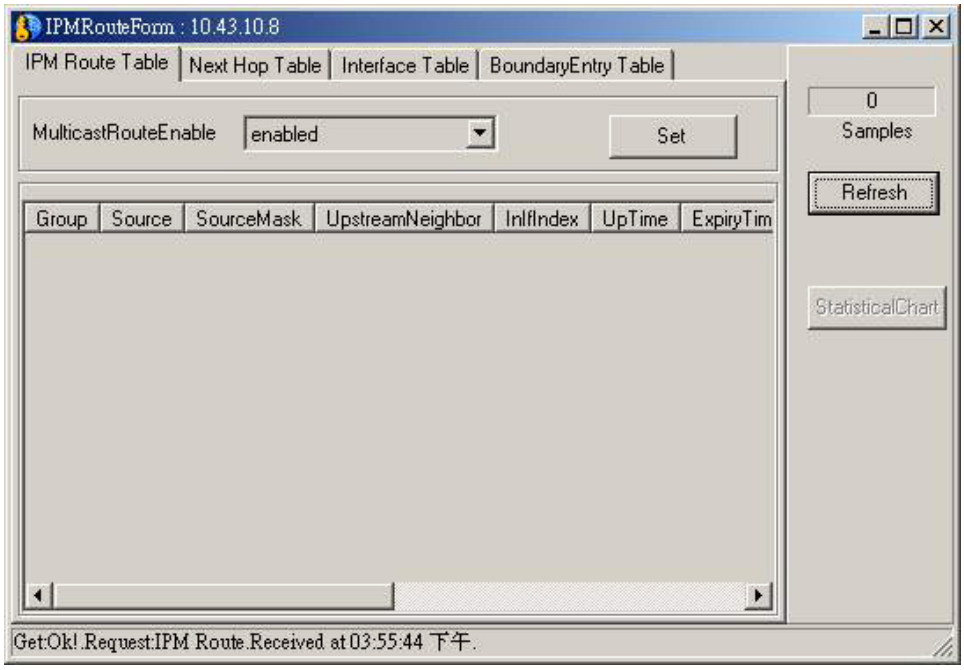


Figure 137. IPMroute Form

Path: MIBs → Layer 3 utilities → IP Mroute		
IPMRoute Table	**Table Information**	Group, Source, Source Mask, Upstream Neighbor, ReceivedIpDatagramsSource, UpTime, ExpiryTime, RoutePkts, DiferentSourcePackets, NumOfOctetsInIPDatagrams, RouterProtocol
	Set	MulticastRouteEnable

Next Hop Table	**Table Information**	NextHopGroup, NextHopSource, NextHopSoureMask, NextHopIndex, NextHopAddress, State, UpTime, ExpiryTime, ClosestMemeberHops, Protocol, ForwardPkts
Interface Table	**Table Read-only Information**	Index
	Set	TTL Threshold, Interface Protocol
BoundaryEntry Table	**Table Read-only Information**	IfIndex, Address, AddressMask, Status
	Set	Status

Table 39. IP Mroute

DVMRP

DVMRP
DVMRP is an "interior gateway protocol"; suitable for use within an autonomous system, but not between different autonomous systems. DVMRP is not currently developed for use in routing non-multicast data grams, so a router that routes both multicast and unicast data grams must run two separate routing processes. DVMRP is designed to be easily extensible and could be extended to route unicast data grams. DVMRP was developed to experiment with the algorithms in RIP was used as the starting point for the development because an implementation was available and distance vector algorithms are simple, as compared to link-state algorithms. In addition, to allow experiments to traverse networks that do not support multicasting, a mechanism called "tunneling" was developed. The multicast-forwarding algorithm requires the building of trees based on routing information. This tree building needs more state information than RIP is designed to provide, so DVMRP is much more complicated in some places than RIP. A link-state algorithm, which already maintains much of the state needed, might prove a better basis for Internet multicasting routing and forwarding. DVMRP differs from RIP in one very important way. RIP thinks in terms of routing and forwarding data grams to a particular destination. The purpose of DVMRP is to keep track of the return paths to the source of multicast data grams. To make explanation of DVMRP more consistent with RIP, the word "destination" is used instead of the more proper "source", but the reader must remember that data grams are not forwarded to these destinations, but originate from them.

Table 40.

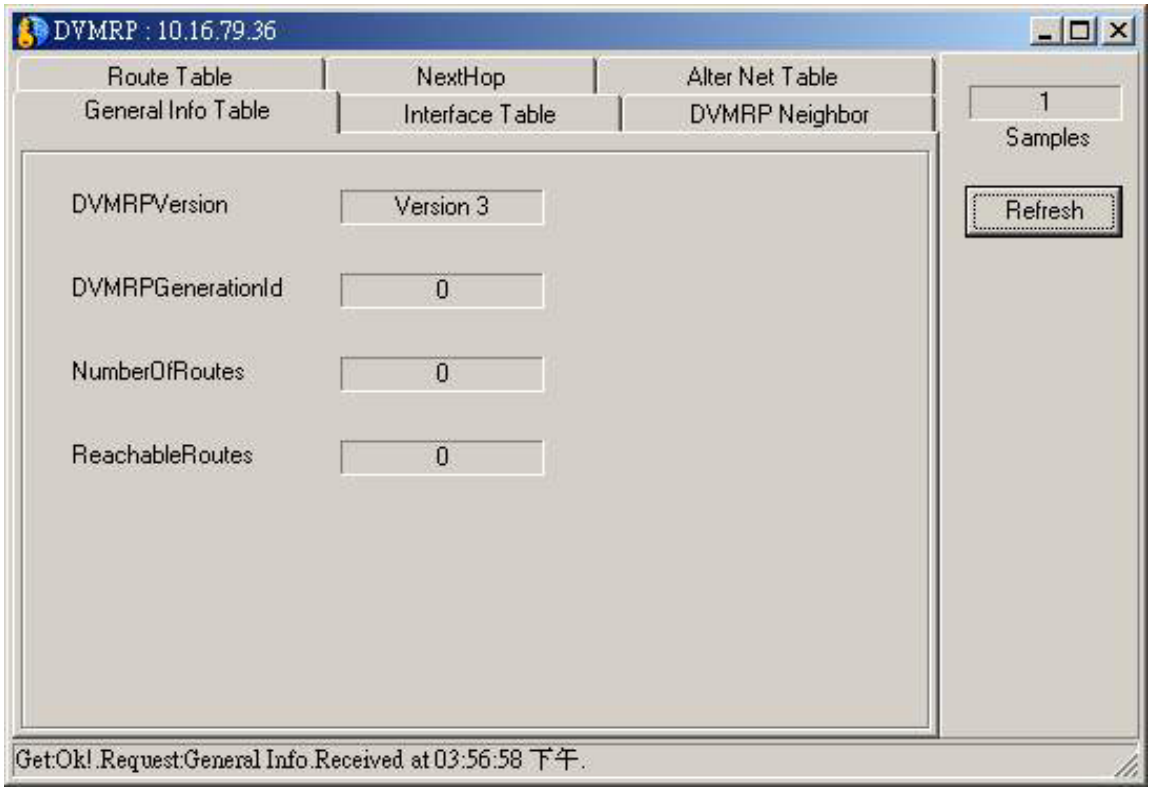


Figure 138. DVMRP

Path: MIBs → Layer 3 utilities → DVMRP		
General Info Table	**Read-only Information**	DVMRPVersion, DVMRPGenerationId, NumberOfRoutes, ReachableRoutes

Table 41. DVMRP

PIM

PIM MIB
This MIB module contains one scalar and eight tables. The tables contained in this MIB are: 1. The PIM Interface Table contains one row for each of the router's PIM interfaces. 2. The PIM Neighbor Table contains one row for each of the router's PIM neighbors. 3. The PIM IP Multicast Route Table contains one row for each multicast routing entry whose incoming interface is running PIM. 4. The PIM Next Hop Table which contains one row for each outgoing interface list entry in the multicast routing table whose interface is running PIM, and whose state is pruned. 5. The (deprecated) PIM RP Table contains the PIM (version 1) information for IP multicast groups which is common to all RPs of a group. 6. The PIM RP-Set Table contains the PIM (version 2) information for sets of candidate Rendezvous Points (RPs) for IP multicast group addresses with particular address prefixes. 7. The PIM Candidate-RP Table contains the IP multicast groups for which the local router is to advertise itself as a Candidate-RP. If this table is empty, then the local router advertises itself as a Candidate-RP for all groups. 8. The PIM Component Table contains one row for each of the PIM domains to which the router is connected.

Table 42.

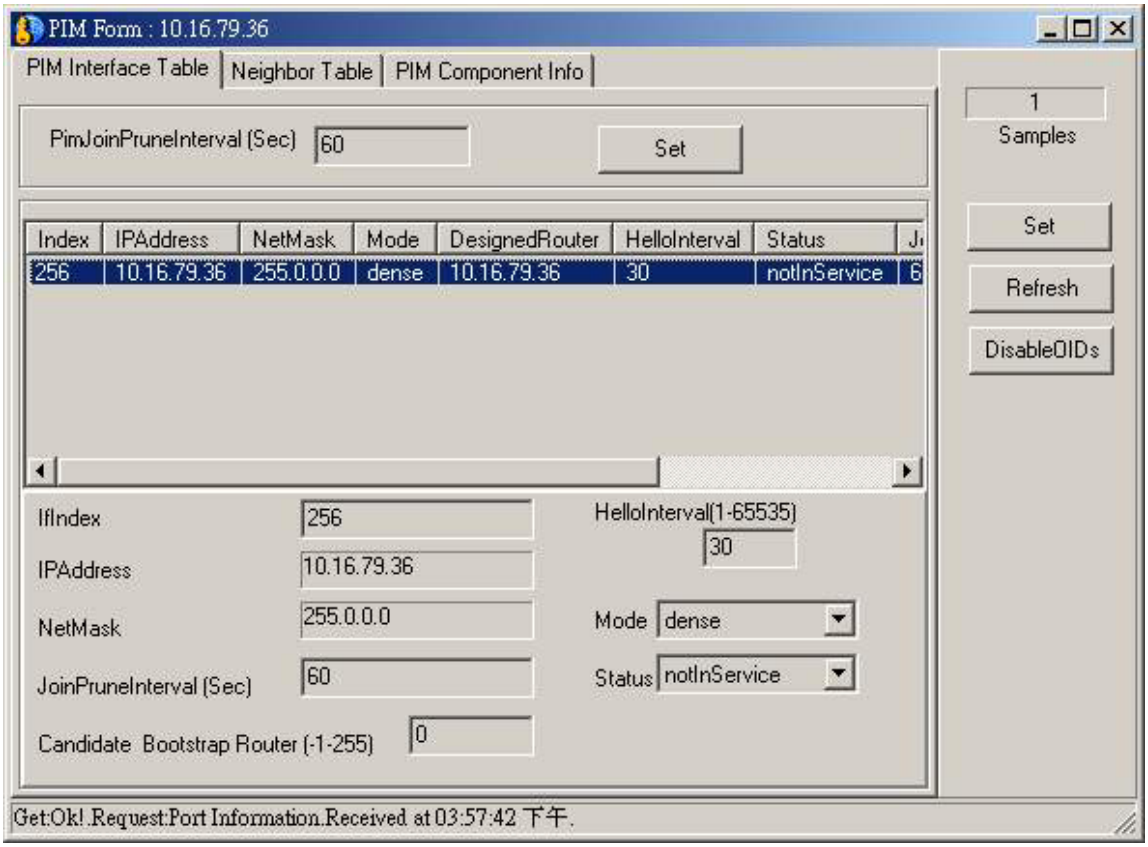


Figure 139. PIM

Path: MIBs → Layer 3 utilities → PIM → PIM Info		
RP Table	**Table Information**	RPGroupAddress, RPAddress, RPState, RPStateTimer, RPLastChange
	Set	RPRowStatus
RpSetTable	**Table Information**	RPSetGorupAddress, RPSetGrouMask, RPSetAddress, RPSetHoldTime, RPSetExpiryTime
CandidateRPEntryTable	**Table Information**	CandidateRPGroupAddress, CandidateRPGroupMask
	Set	RowStatus

Table 43. PIM Information

Path: MIBs → Layer 3 utilities → PIM → Rendezvous Points Info		
PIM Interface Table	**Table/Read-only Information**	IPAddress, NetMask
	Set	PimJoinPruneInterval, IfIndex, JoinPruneInterval, Candidate Bootstrap Router, HelloInterval, Mode, Status
Neighbor Table	**Table Information**	NeighborAddress, IfIndex, UpTime, ExpiryTime, Mode
PIM Component Info	**Table/Read-only Information**	ComponentIndex
	Set	Status, CRPHoldTime

Table 44. Rendezvous Points Information

SNMPv3 Configuration

Use the SNMPv3 menu to configure SNMPv3 security settings and new user setup. Choose SNMPv1, SNMPv2 or SNMPv3 as appropriate in the SNMP Version entry field.

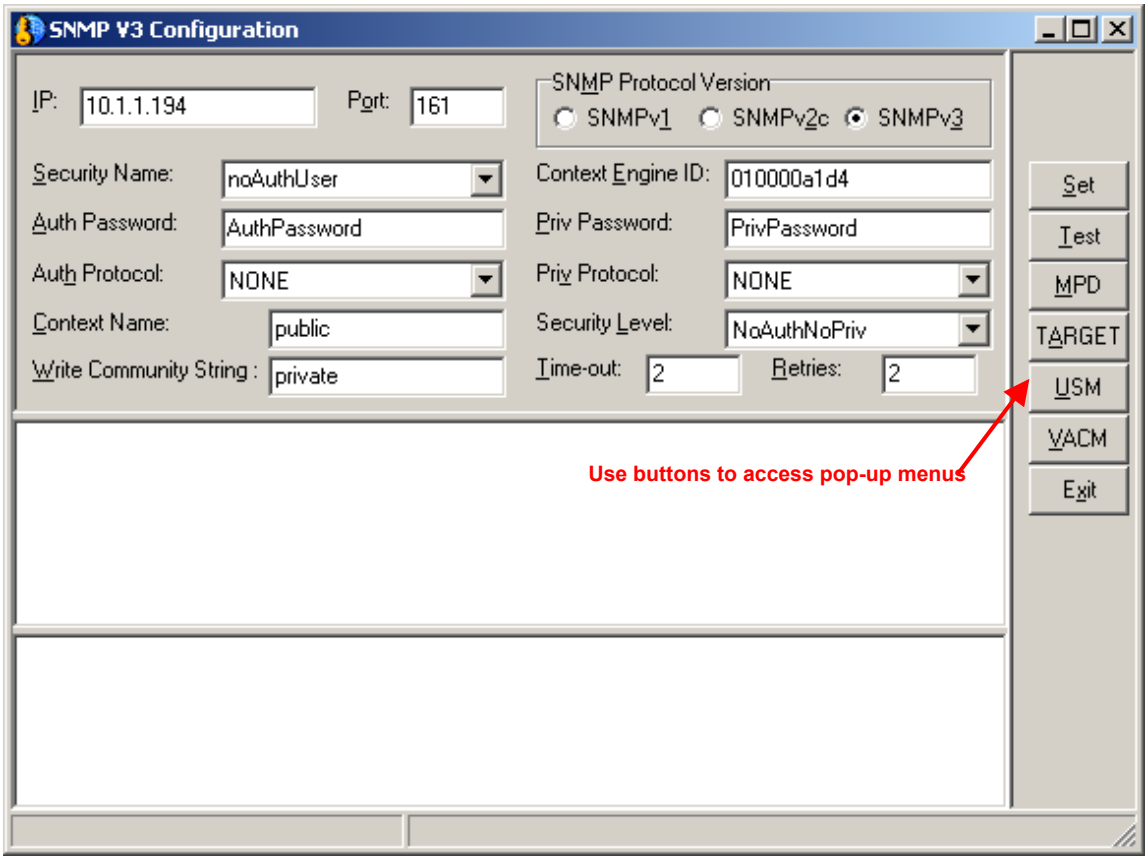


Figure 140. SNMPv3 – SNMP Protocol Preferences

Path: MIBs → SNMPv3	
Table/Read-only Information	System Description, System Object ID, Sytem Uptime, System Contact, System Name, System Location
User Defined Parameters	IP Address, Port Number, Security Name, Context Engine ID, Auth Password, Priv Password, Auth Protocol, Priv Protocol, Contact Name, Security Level, Write Community String, Time-out, Retries

Table 45. SNMPv3 – SNMP Protocol Preferences

SNMP Protocol Settings Pop-up Menus

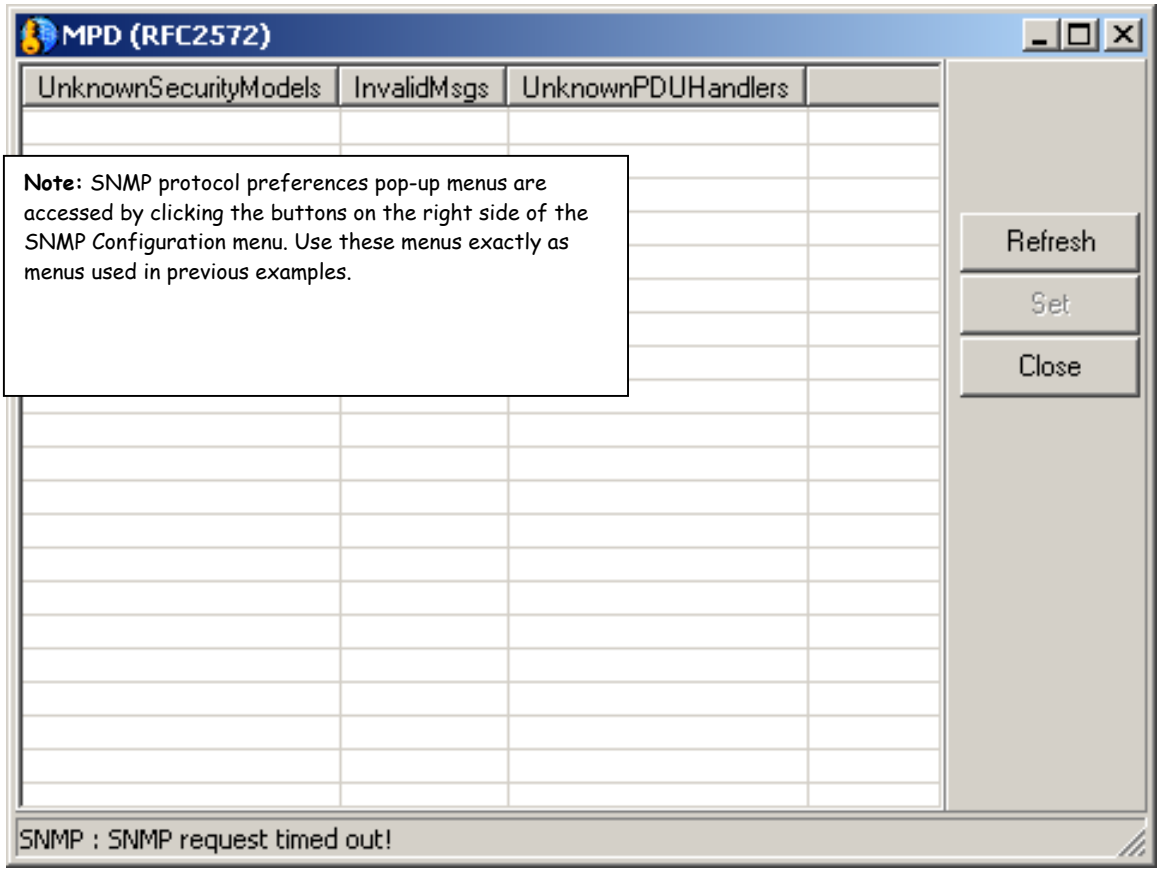


Figure 141. MPD (RFC 2572)

Path: MIBs → SNMPv3 (click MPD button)	
MPD (RFC 2572) Table	SecurityModels, InvalidMsgs, UnknownPDUHandlers

Table 46. MPD (RFC 2572) SNMP Parameter Pop-up Menu

Path: MIBs → SNMPv3 (click Target button)	
AddEntry_Table	AddrName, AddrTDomain, AddrTAddress, AddrTimeout, AddrRetryCount, AddrTagList, AddrParams, AddrStorageType, AddrRowStatus
ParamsEntry_Table	ParamsName, ParamsMPModel, ParamsSecurityModel, ParamsSecurityName, ParamsSecurityLevel, ParamsStorageType, ParamsRowStatus

Table 47. Target (RFC 2573) SNMP Parameter Pop-up Menu

Path: MIBs → SNMPv3 (click USM button)	
Stats_Table	UnsupportedSecLevels, NotInTimeWindows, UnknownUserNames, UnknownEngineIDs, WrongDigests, DecryptionErrors
UserEntry_Table	EngineID, Name, SecurityName, CloneForm, AuthProtocol, AuthKeyChange, OwnAuthKeyChange, PrivChange, PrivKeyChange, OwnPrivKeyChange, Public, StorageType, Status

Table 48. USM (RFC 2574) SNMP Parameter Pop-up Menu

Path: MIBs → SNMPv3 (click VACM button)	
ContextEntry_Table	vacmContextEntryName
SecurityToGroupEntry_Table	SecurityName, SecurityModel, GroupName, SecurityToGroupStorageType, SecurityToGroupStatus
Entry_Table	ContextPrefix, SecurityLevel, SecurityModel, ContextName, ReadViewName, WriteViewName, NotifyViewName, StroageType, Status

Table 49. VACM (RFC 2575) SNMP Parameter Pop-up Menu

5

INTERNET TOOLS

This chapter explains items in the "Tools" drop-down menu in the order of the descending menu items.

DIAP

D-View includes standard network management utilities such as TFTP and Ping Test user convenience. D-View 5. 1 also includes D-Link's proprietary administration utility DIAP. DIAP allows the user to have limited administrative access to D-Link broadband devices such as ADSL and ISDN routers, ADSL modems and Wireless routers. This tool can be used to assign IP settings to such devices. DIAP will automatically discover all DIAP enabled devices and display IP settings and MAC information in a separate window.

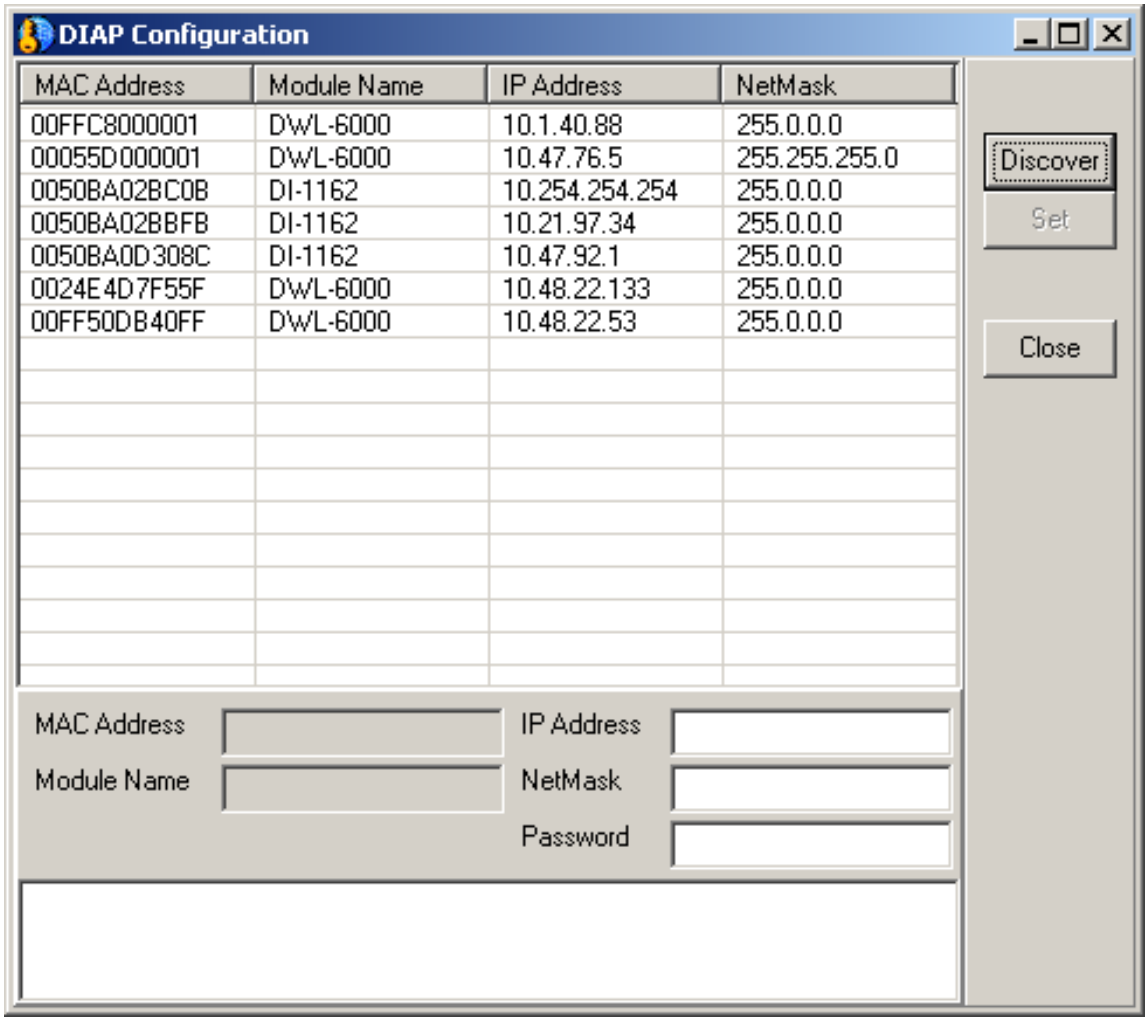


Figure 142. DIAP

TFTP

The Trivial File Transfer Protocol server can be activated under the Tools heading of the Main Menu. The TFTP server is active upon launch and can transfer files located on the host system to any SNMP device. File transfer information is displayed in the TFTP Server window. This information includes the IP address of the file recipient, the type and name of the file transferred and the status of the transfer. Error messages appear in the bottom field display.

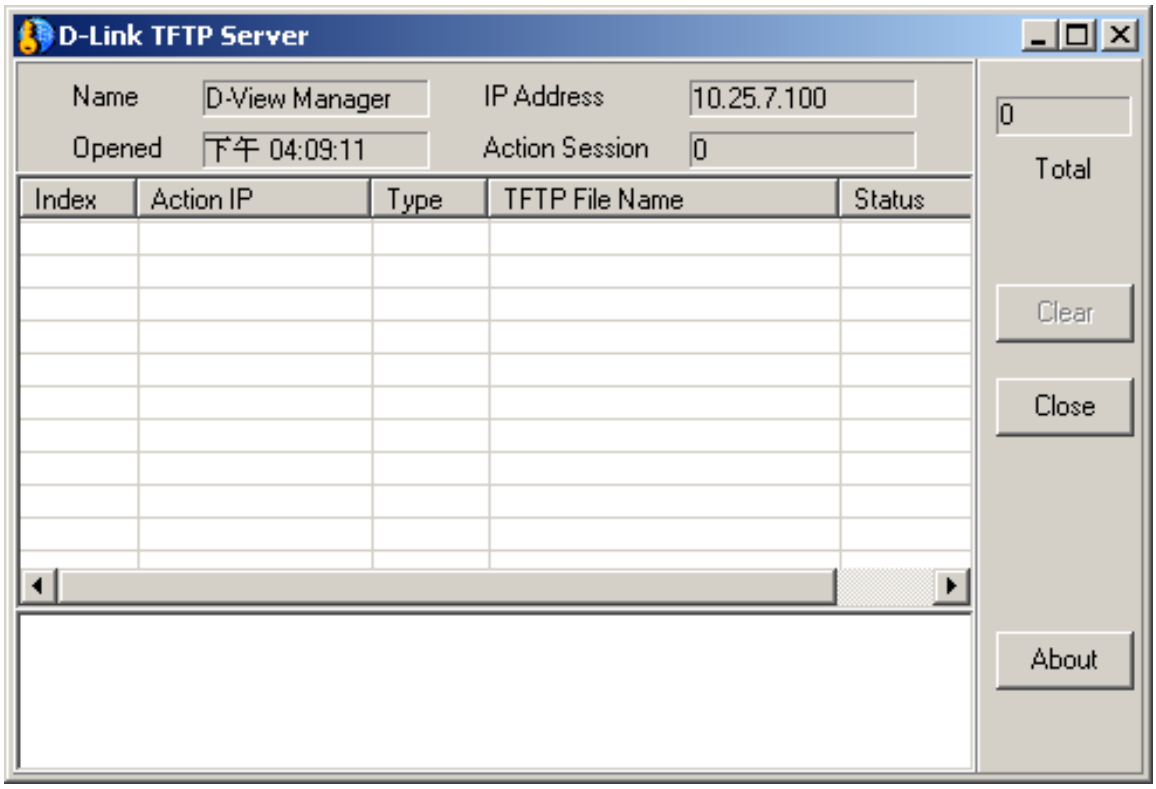


Figure 143. TFTP Server

BOOTP Server

Use the BOOTP server window to set up BOOTP service for BOOTP enabled devices. This utility is similar to the TFTP server except it does not require that the host system or D-View be running at the time of the transfer. D-View can assign other servers on the network to act as BOOTP servers or it may use the host system as the server.

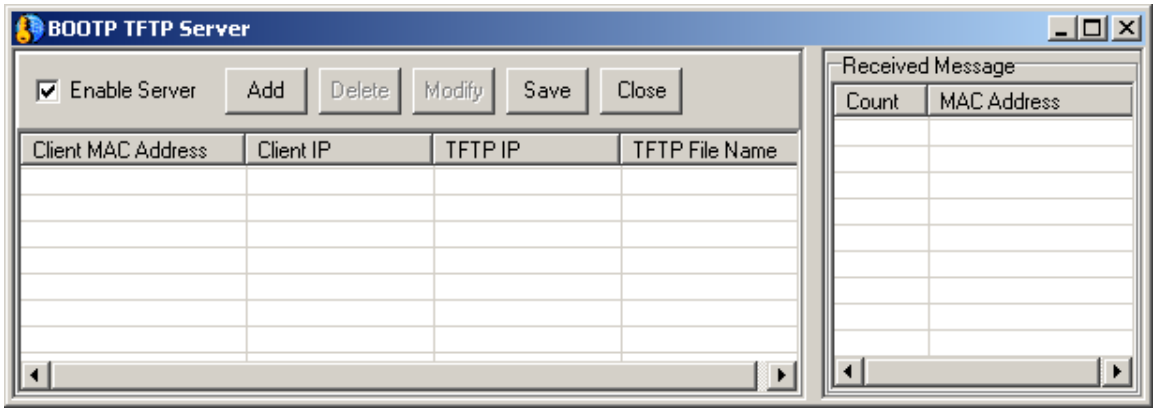


Figure 144. BOOTP Server

PING Test

The PING Test utility uses this standard test for connectivity. This tests connectivity from the D-View host to the tested device. Type the IP address of the device you want to Ping, You may also define the Data Length, Interval, Time Out and Iteration.

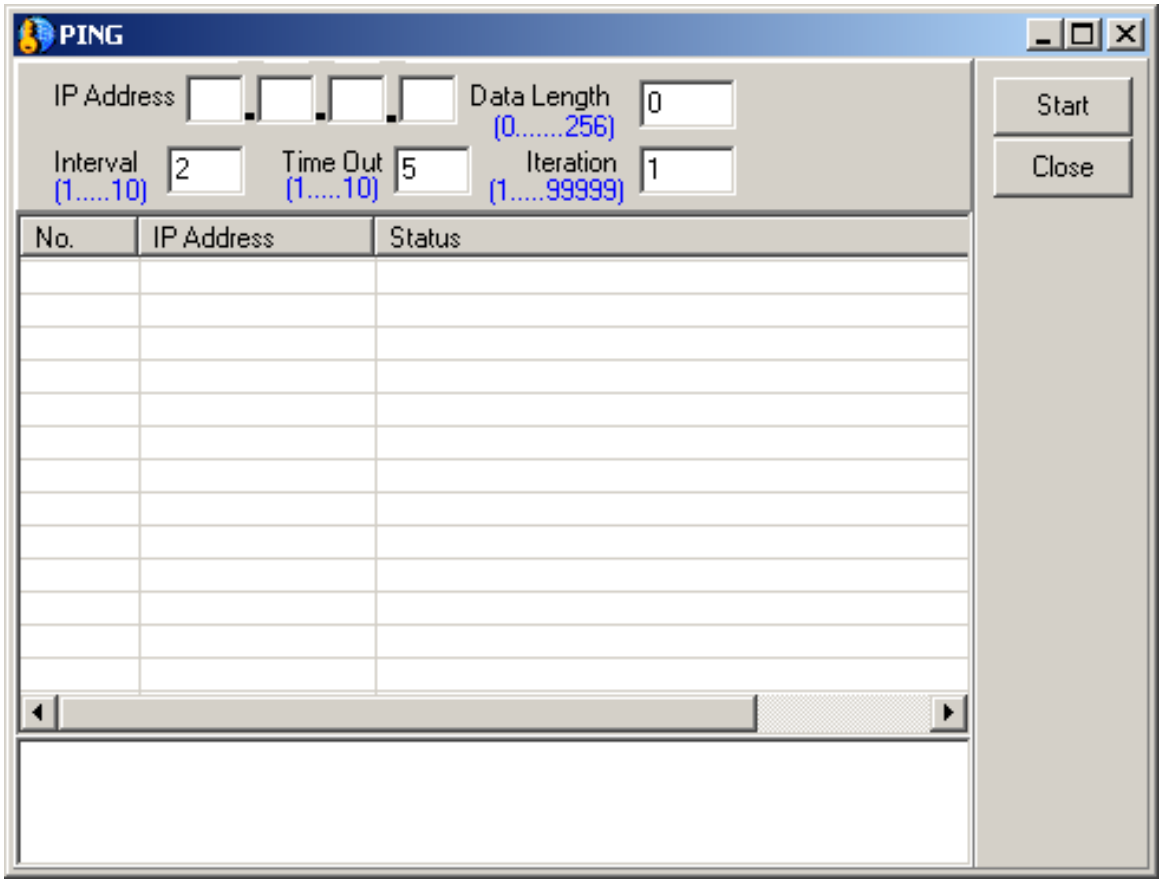


Figure 145. PING Test

6

ADVANCED MANAGEMENT

This chapter explains how to use **trap management** functions found under the System drop-down menu. It is organized in the order of the descending menu items. It explains how to access the Trap Editor, how to edit a TRF file, how to control and view the trap log, and how to change SMTP trap settings.

This chapter then explains how to add plug-in utilities.

The end of this chapter describes how to use the Account administration utilities to monitor and analyze client devices and maintain client records. It is organized in the order of the descending menu items under the Account drop-down menu.

Trap Management

Trap Editor

Use the Trap Editor to modify MIB object names for modules and devices on the network. Select the device/module from the list in the top panel. MIB objects are indexed according to class. Click on the index number to view that object class group. To change the alias name of a single object, double click it or highlight it and click on the Modify icon just above the object list. Use the Change Alias Name pop up window to modify the object alias name.

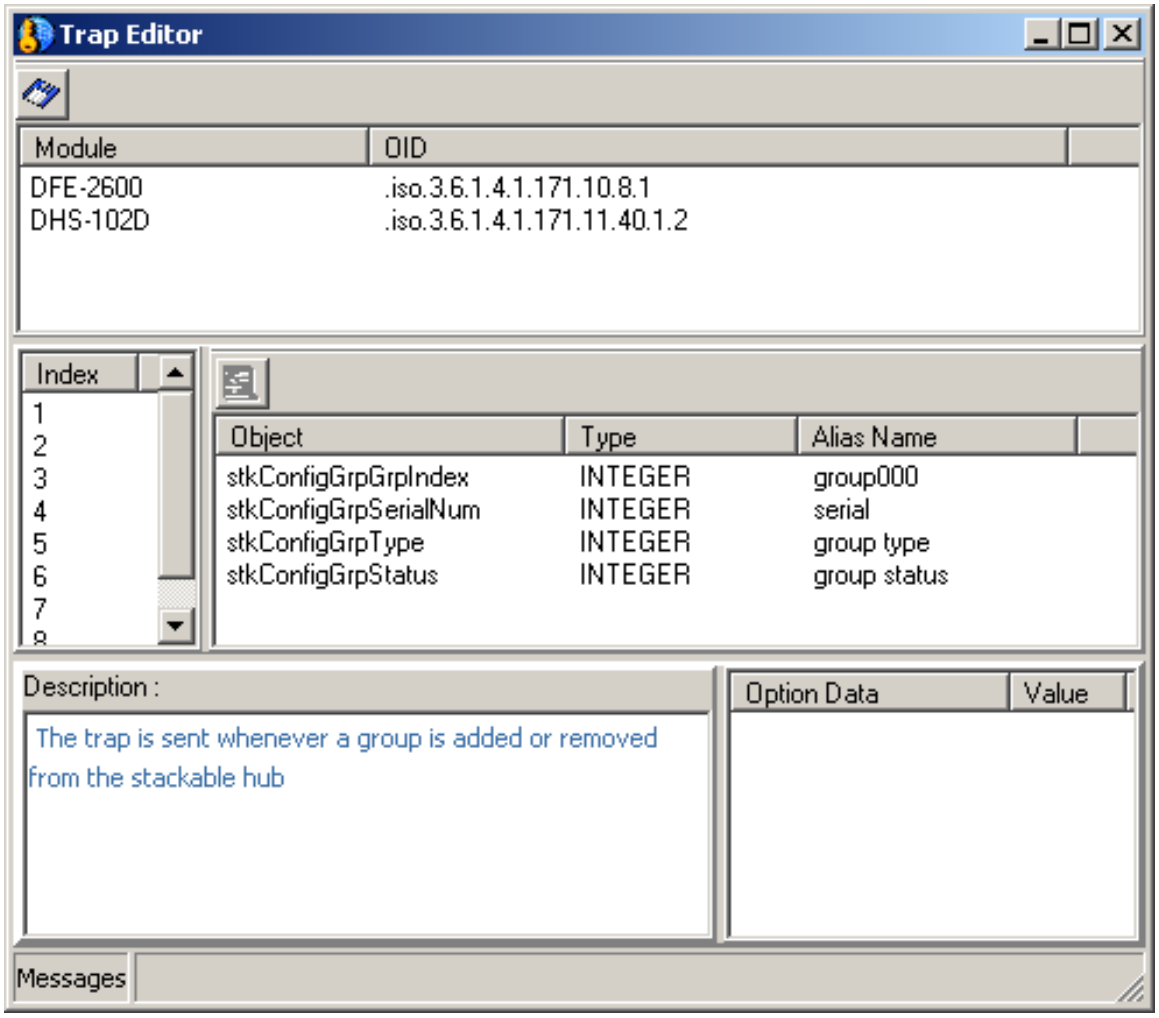

Trap Editor
Module
OID
DFE-2600
.iso.3.6.1.4.1.171.10.8.1
DHS-102D
.iso.3.6.1.4.1.171.11.40.1.2
Index
1
2
3
4
5
6
7
Object
Type
Alias Name
stkConfigGrpGrpIndex
INTEGER
group000
stkConfigGrpSerialNum
INTEGER
serial
stkConfigGrpType
INTEGER
group type
stkConfigGrpStatus
INTEGER
group status
Description :
The trap is sent whenever a group is added or removed from the stackable hub
Option Data
Value
Messages

Figure 146.

Clear Trap Alerts

To clear the trap alerts from the scrolling message panel (Trap tab) at the bottom of the main menu, under System go to Trap Management and left click on Clear.

Sort Trap Alerts

To change the order of presentation of the trap alerts, under System go to Trap Management then to Sort By and left click on your choice of Time (default), Received From or Trap Message (type).

Trap Type Properties

Trap alerts can be color coded by type to make them easier to distinguish in the list. Open the Trap Type Properties pop-up window to edit the font and background color of the most urgent trap types.

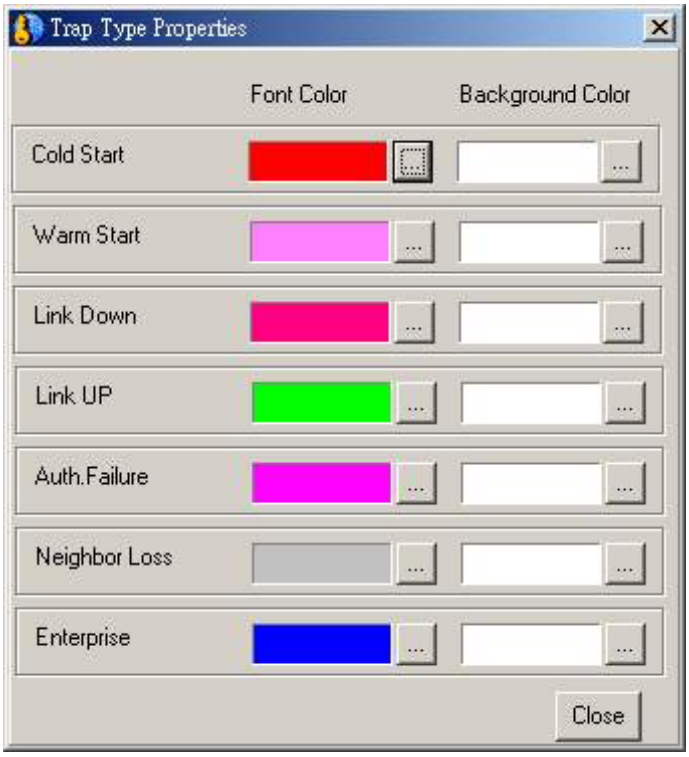


Figure 147.

Trap View Filter Settings

Use the Trap View Filter Setting pop up window to limit both the device from which trap alerts are listed and the type of traps listed. Type the IP address of any device you want to designate for trap viewing and click the Add button. Highlight a device in the list and click Remove to remove that device from the trap list.

The OIDs tab allows you to limit traps to specific OIDs. Specify OIDs to view by typing in the OID and clicking Add. To remove an OID from the list, highlight it and click Remove.

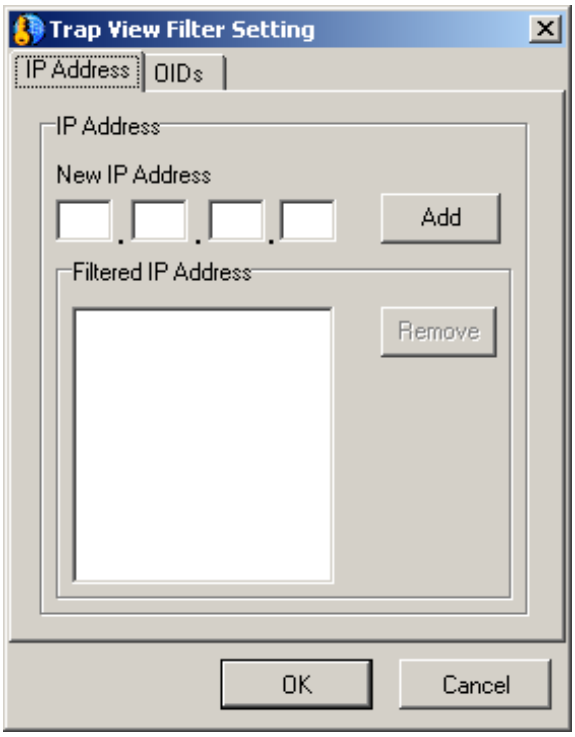


Figure 148.

How to Edit a TRF File

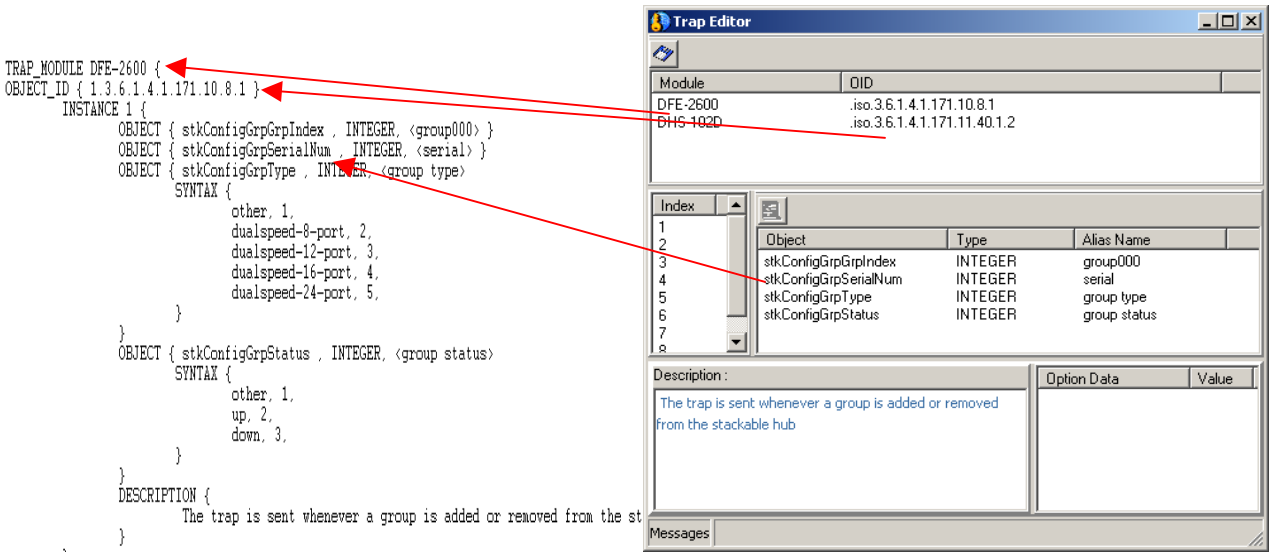


Figure 149.

Note: ***Before editing a TRF file, you need to compile the primary module's MIB files and view their trap entires, type, and value to know how to edit the module's TRF file.***

<Install Directory>\5.1\Conf\Trap\ gives the path for a TRF file. TRF files that are .txt files are composed with the following syntax and parameters:

1. TRAP_MODULE <Module Name>

At the beginning of the TRF file, define which device is associated with the file. The <Module Name> parameter is the device name.

2. OBJECT_ID {<Module's OID>}

Define this device's OID number. <Module's OID> parameter is this device's OID number.

3. INSTANCE <Index>

Define the trap group index number of this device. <Index> is the trap group number of this device.

4. OBJECT {<trap's original name>,<trap type>,<trap's alias name>,……}

Define trap entry's name, trap data type and its alias name. <Trap's original name> is the trap entry name, <trap type> is this trap's data type, and <trap's alias name> is this trap's entry alias name.

5. SYNTAX {<option name>,<option value>……..}

Define trap entry's option value, if the trap has option value. <Option name> is this trap entry's option name; <option value> is the associated value.

6. DESCRIPTION {<description>}

<description> gives a definition of the MIB group.

Trap Log

To turn the trap log on or off, or to view the log, go to System → Trap Management → Log select: Log On, Log Off or View Log.

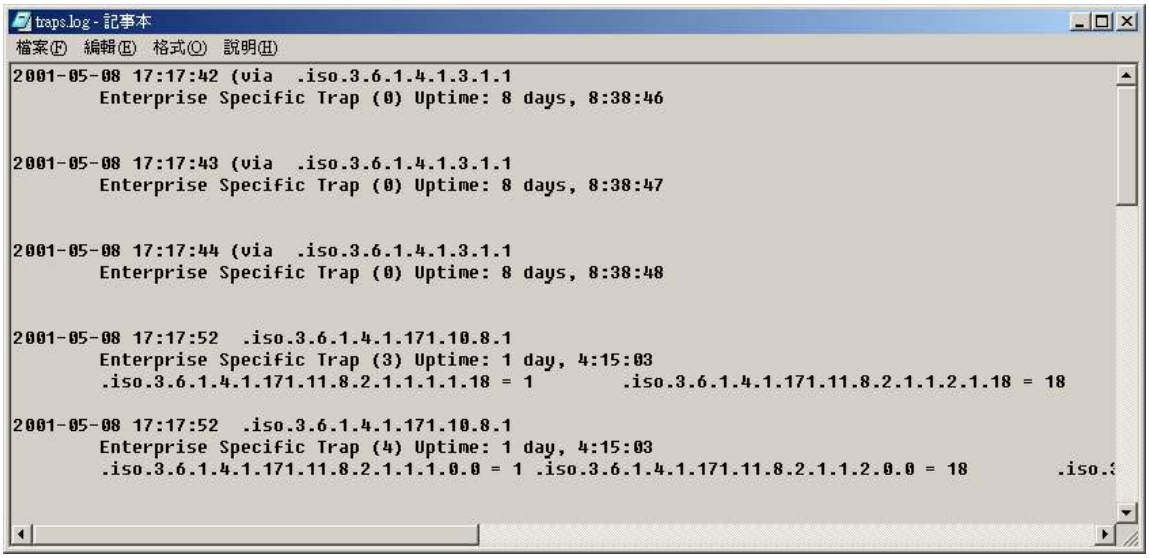


Figure150. Trap Log File

SMTP Setting Form

Use the SMTP Setting form to enable email alerts to be sent to the network administrator. Type the SMTP server and domain name, and Port number used, choose Simple Login and provide the account and password information if you prefer to use authentication, otherwise select None. Mail Sender Name is the name that appears as the sender in the email summary. Supply a sender and

receiver address, and you can option to send a CC to one other email account. Use the Mail Test button to test if all information has been correctly entered and the system is functioning.

Use the Trap Mail Setting Form to specify the type of alert sent and how frequently mail alerts should be sent.

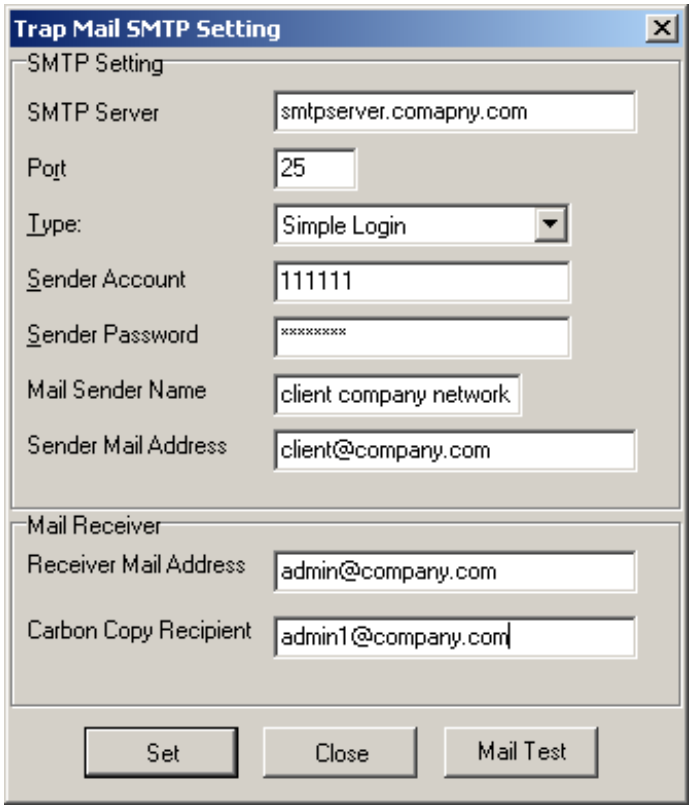


Figure 151. Trap Mail SMTP Settings Form

Trap Mail Settings Forms

Use the IP Address tab specify the device and alarm. The Alarm Level pull-down menu has standard alarms to choose from. Type the message that accompanies the mail alert in Alarm Message.

The OID tab is used for proprietary or other objects used to trigger the email alert. Add and remove items for email alerts the same as with other menus.

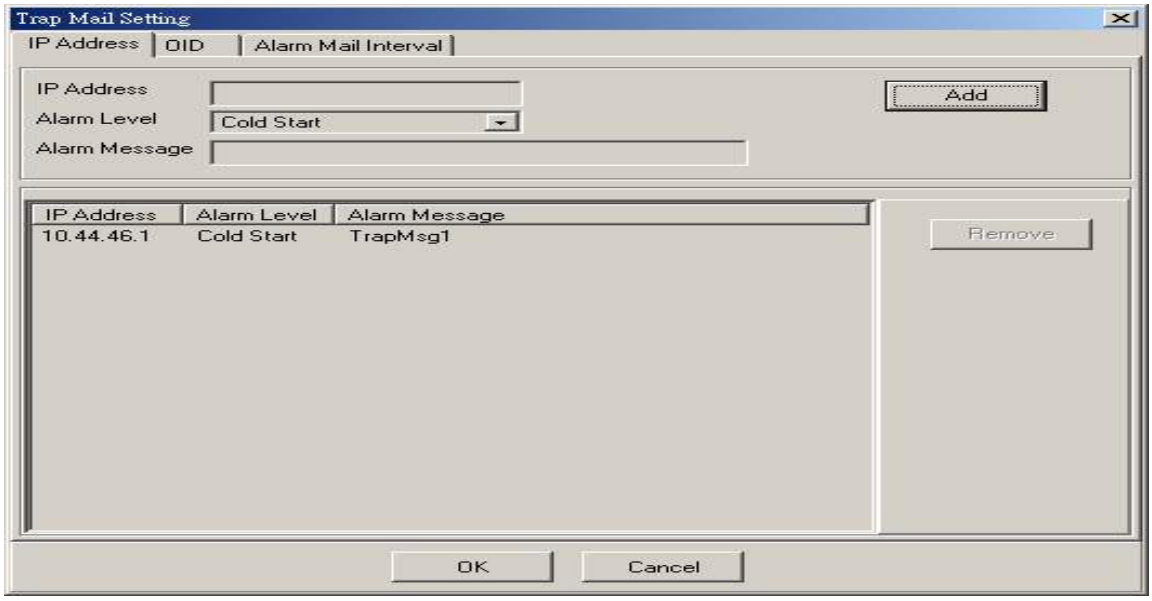


Figure 152. Trap Mail Setting Forms

Alarm Mail Interval

Use the Alarm Mail Interval menu tab to specify the frequency with which email alarms are sent. Alarm mail intervals may be specified using the Alarm Interval to specify the number of minutes between emails, or use the Alarm Time to specify times when emails are sent daily. Alarm mail intervals can be set up using both definitions if desired. Alarm Time asks you to specify the hour (HH) and minute (MM) using 24-hour military time.

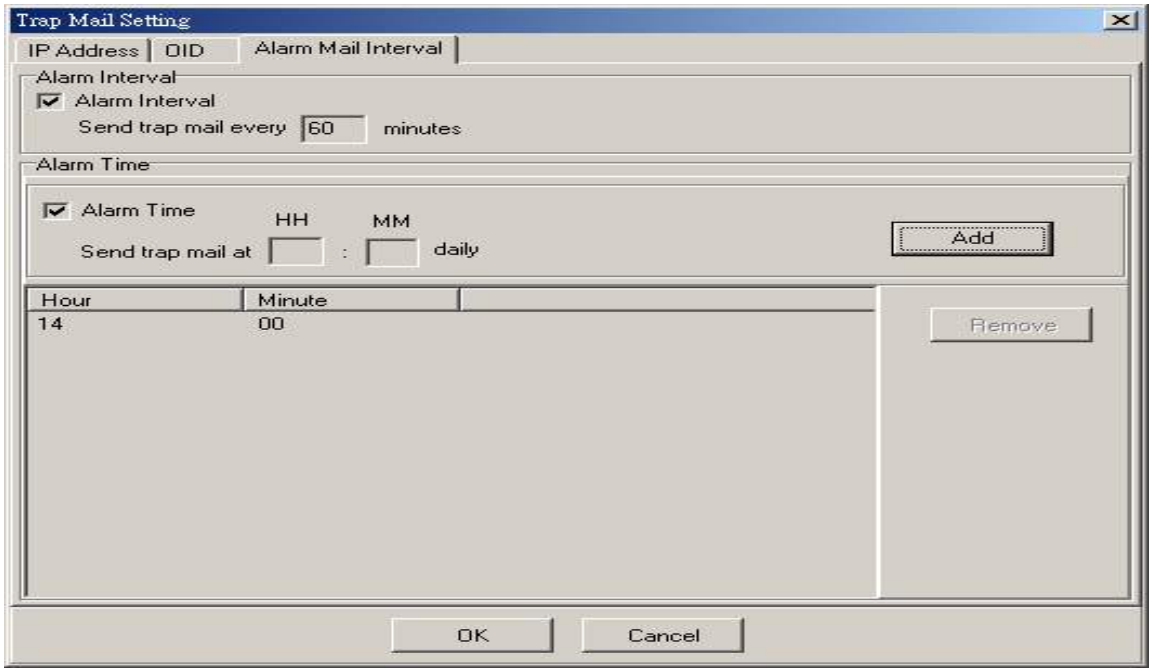


Figure 153. Alarm Mail Interval

Example: Receiving alarm/trap messages by e-mail

Step 1: Set the SMTP settings

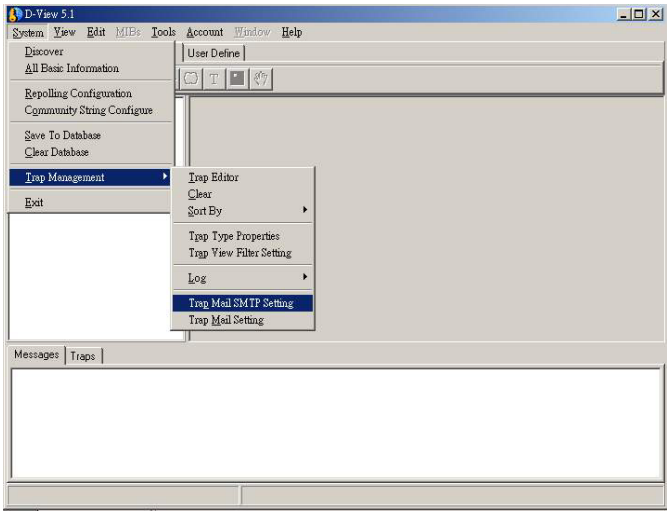


Figure 154.

Step 2: After setting the settings you can use "Mail Test" to test whether the settings are correct.

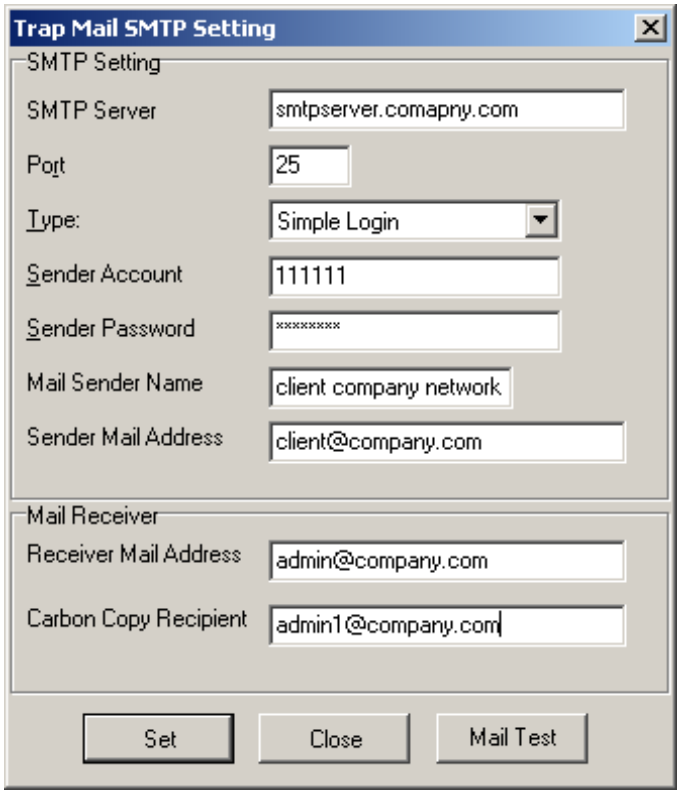

Trap Mail SMTP Setting
SMTP Setting
SMTP Server
smtpserver.comapny.com
Port
25
Type:
Simple Login
Sender Account
111111
Sender Password
****
Mail Sender Name
client company network
Sender Mail Address
client@company.com
Mail Receiver
Receiver Mail Address
admin@company.com
Carbon Copy Recipient
admin1@company.com
Set
Close
Mail Test

Figure 155.

Step 3

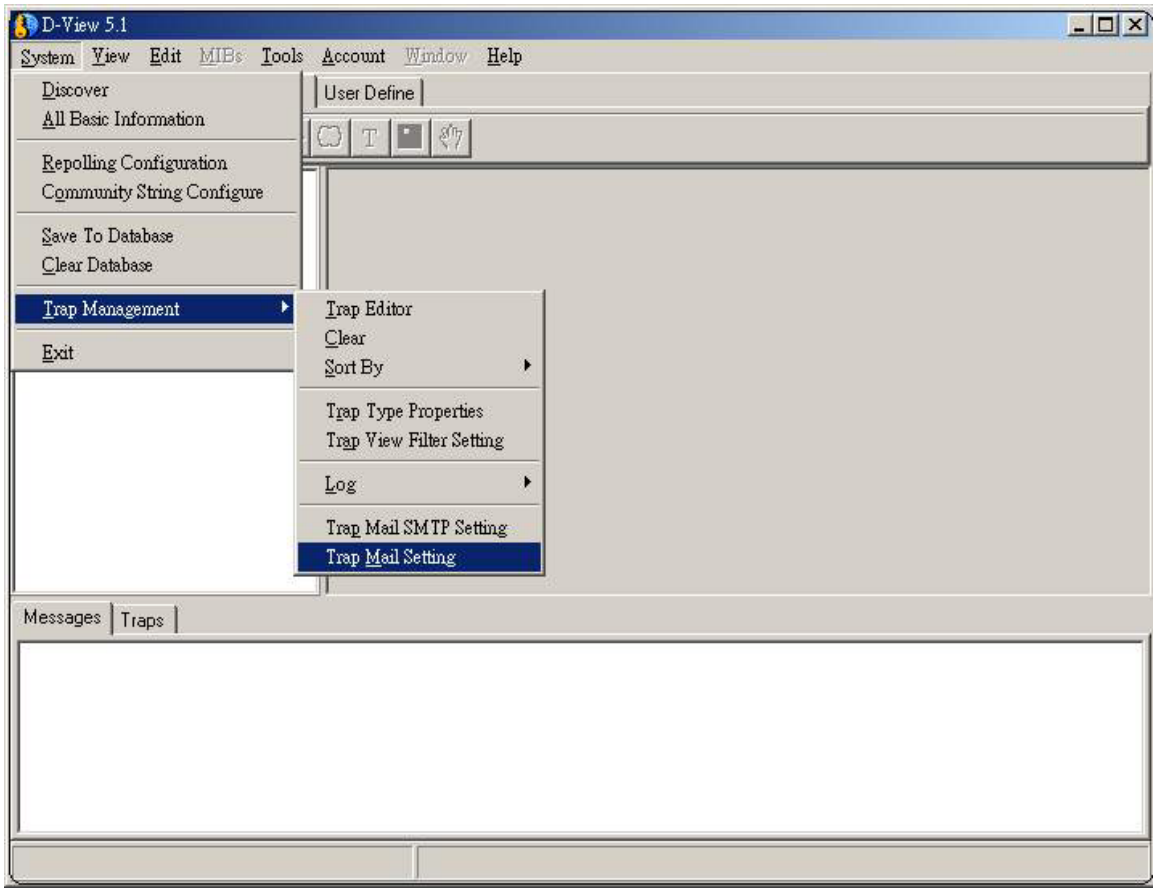


Figure 156.

Step 4: Set alarm time, alarm interval and conditions for sending trap mail.

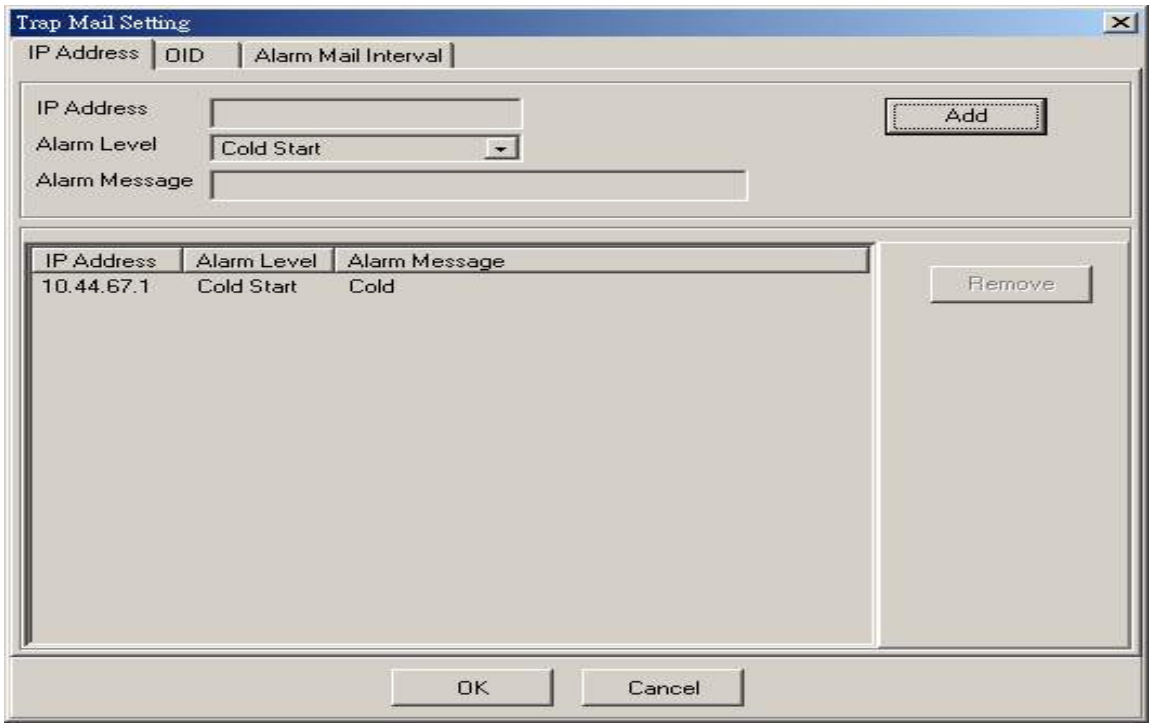


Figure 157.

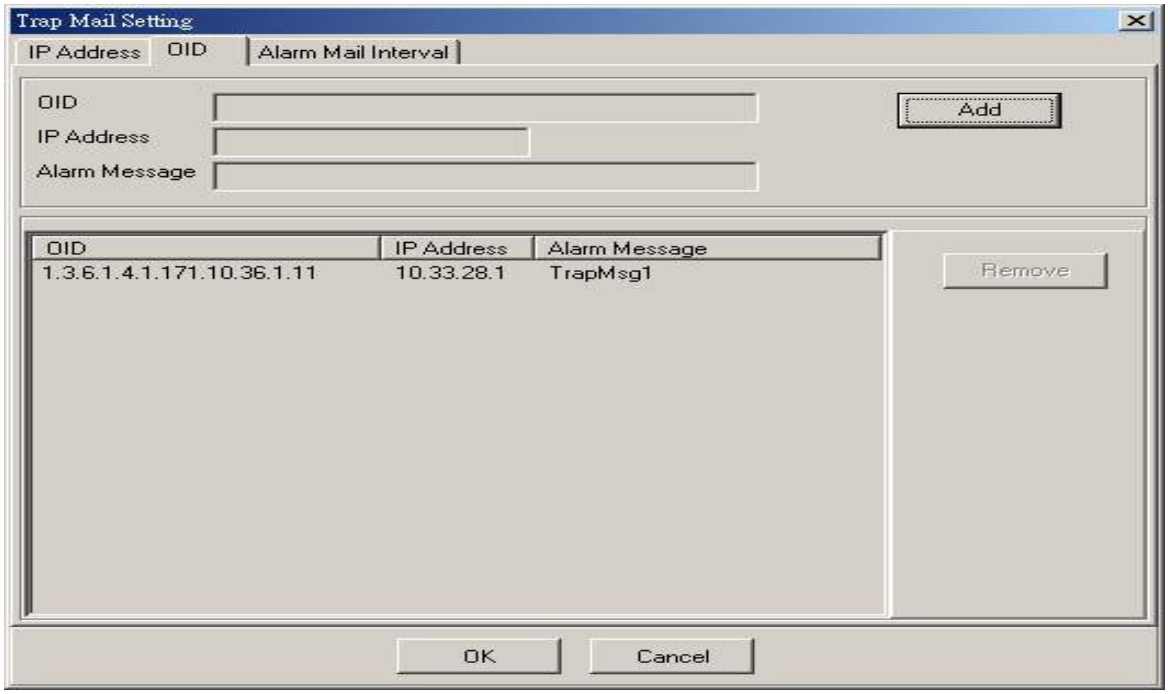

Trap Mail Setting
IP Address
OID
Alarm Mail Interval
OID
IP Address
Alarm Message
Add
OID
IP Address
Alarm Message
1.3.6.1.4.1.171.10.36.1.11
10.33.28.1
TrapMsg1
Remove
OK
Cancel

Figure 158.

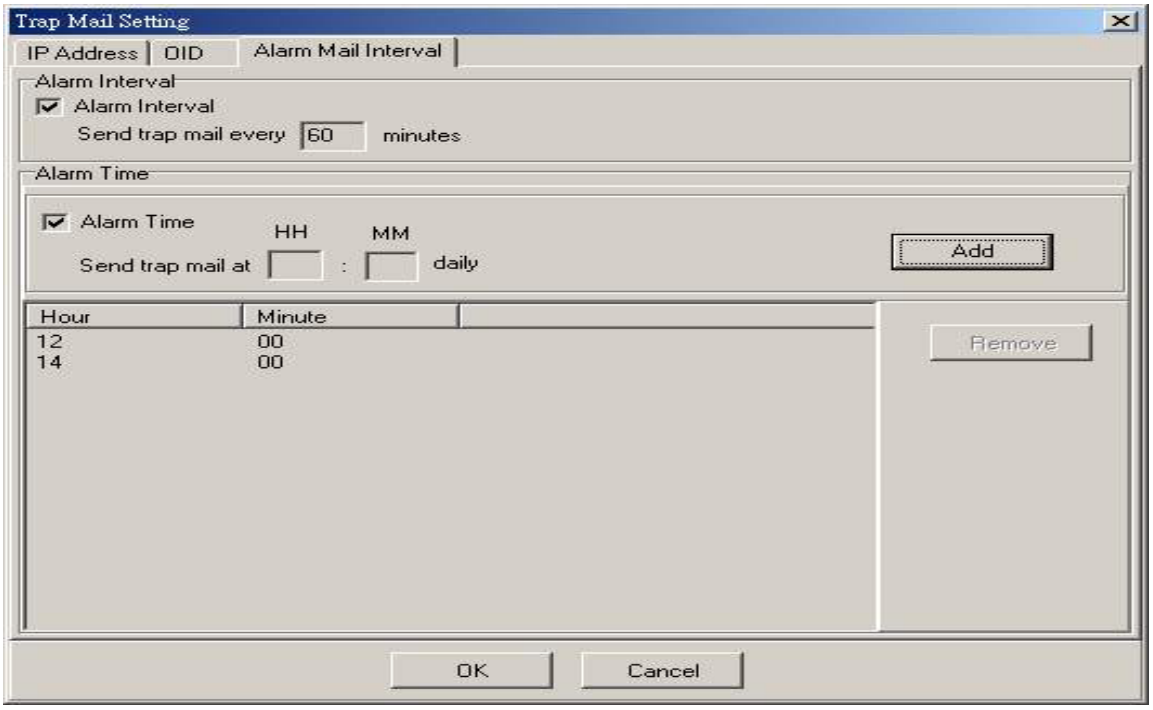

Trap Mail Setting
IP Address
OID
Alarm Mail Interval
Alarm Interval
Alarm Interval
Send trap mail every 60 minutes
Alarm Time
Alarm Time
HH
MM
Send trap mail at : daily
Add
Hour
Minute
12 00
14 00
Remove
OK
Cancel

Figure 159.

Adding Plug-In Utilities

You can develop execution files to plug into the D-View platform

How to install self-developed device SNMP module:

SNMP Module execution files must have four parameters:

/NdeviceModuleName /IIPAddress /RreadCommunityString /WwriteCommunity String

"/N," "/I,""/R,""/W" respectively stand for Module Name, IP Address, Write Community String, Read Community String.

Re-install Windows Registry and set up as follows:

Execute Regedit.

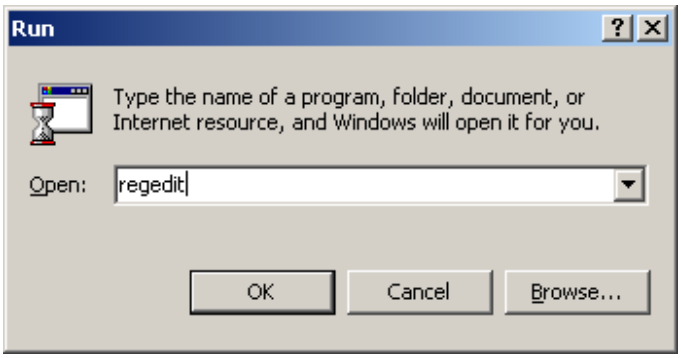


Figure 160.

Under **HKEY_LOCAL_MACHINE→SOFTWARE→D-Link→Modules** there are four data folders. Enter data into these four data folders as below:

1. **ExePath:** Record SNMP Device Module execution file with Device OID as Key. Select and then right-click with mouse on newly added words value. At the value name input Device OID. Input execution file name. Add /N before the execution file name.

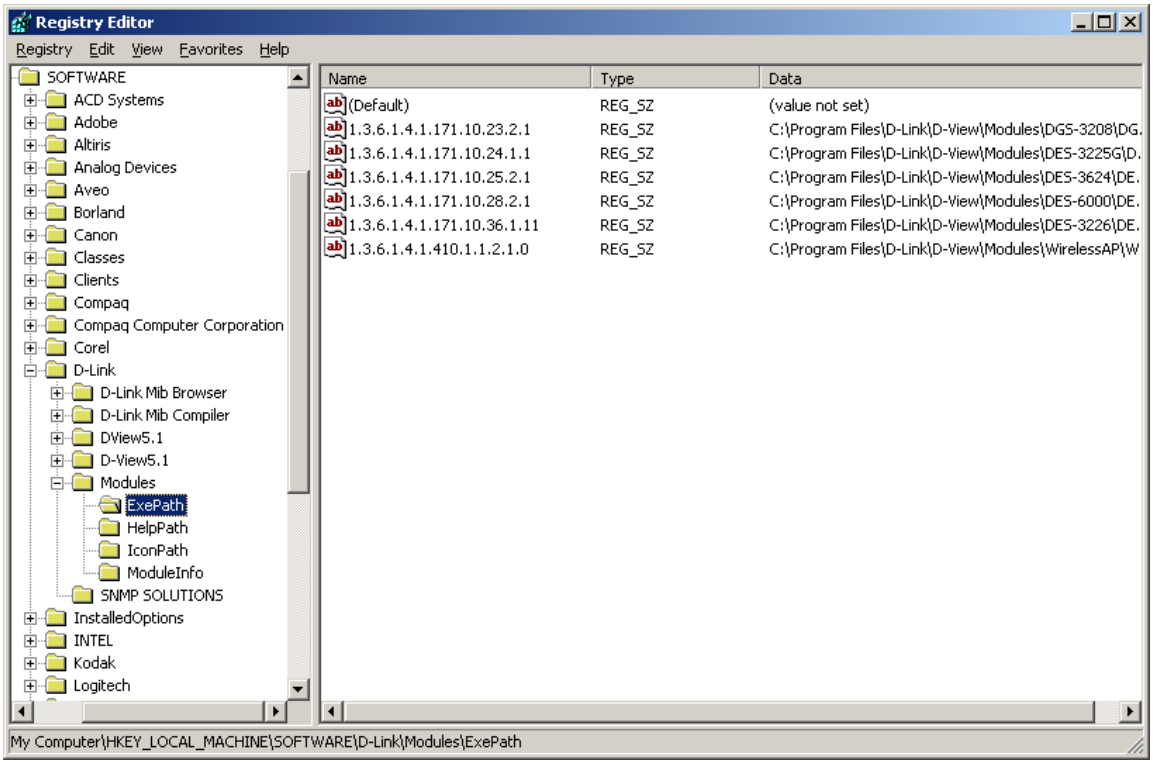


Figure 161.

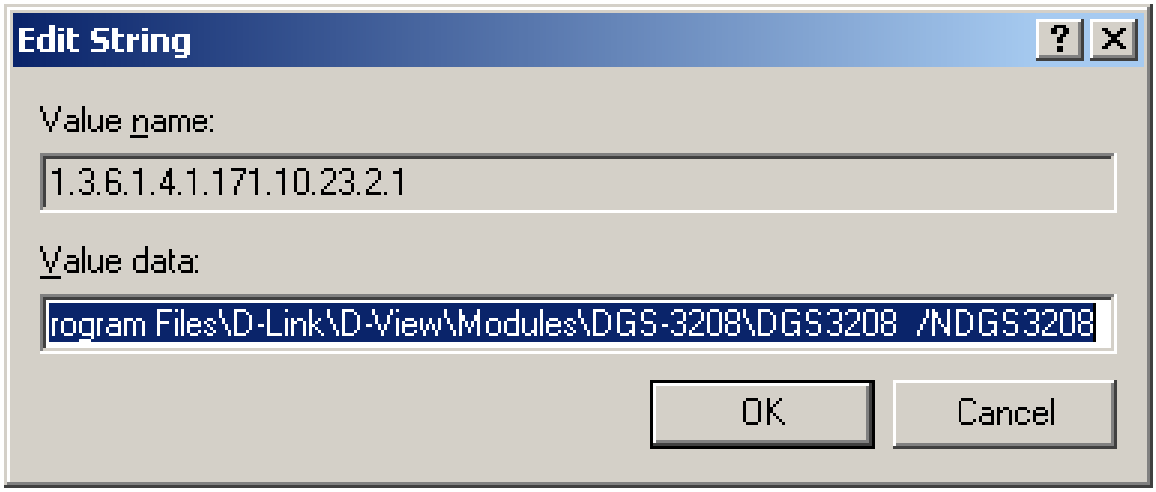

Edit String
Value name:
1.3.6.1.4.1.171.10.23.2.1
Value data:
rogram Files\D-Link\D-View\Modules\DGS-3208\DGS3208 /NDGS3208
OK
Cancel

Figure 162.

2. **HelpPath:** Record Help file location using Device OID as Key. Select and right click to added words value. At name value input Device OID. Under data value input Help file location and full path name.

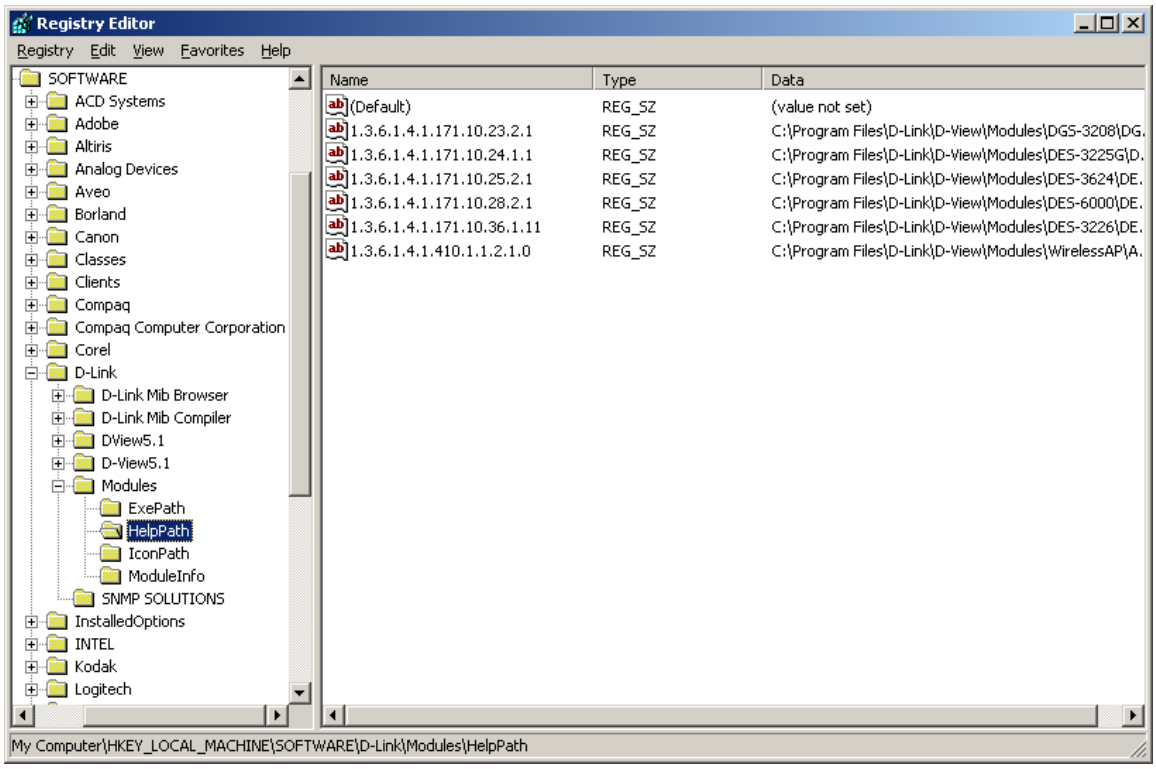


Figure 163.

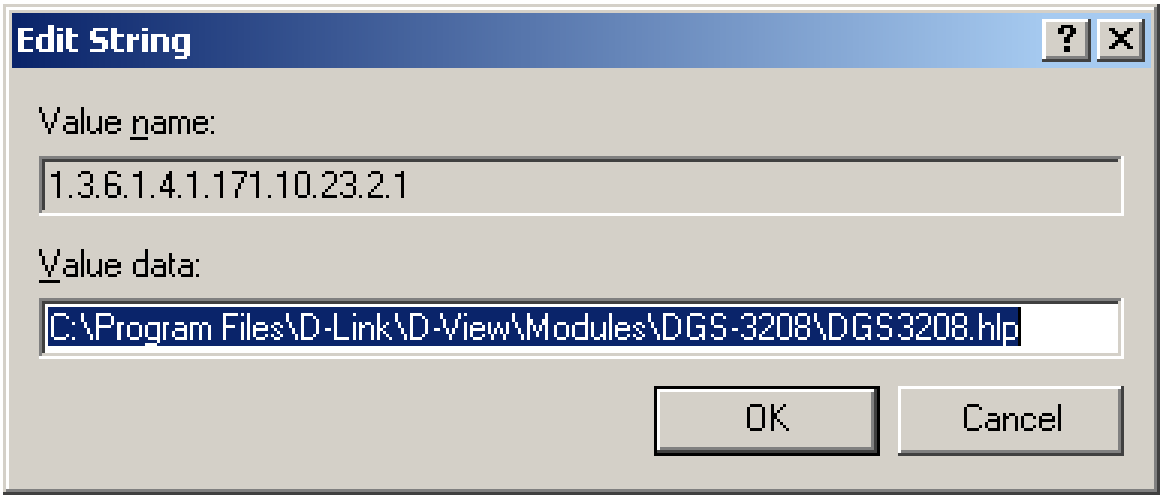


Figure 164.

3. **Icon Path**: Record the position of icons used using the Device OID as Key. Select and right click on mouse on newly added words value. Under name value input Device OID. Under data value input Icon file location and full path name.

Note: ***Please make sure you have both the .ico file and the .bmp file of the same picture. For example, you must have dgs3208.ico and dgs3208.bmp.***

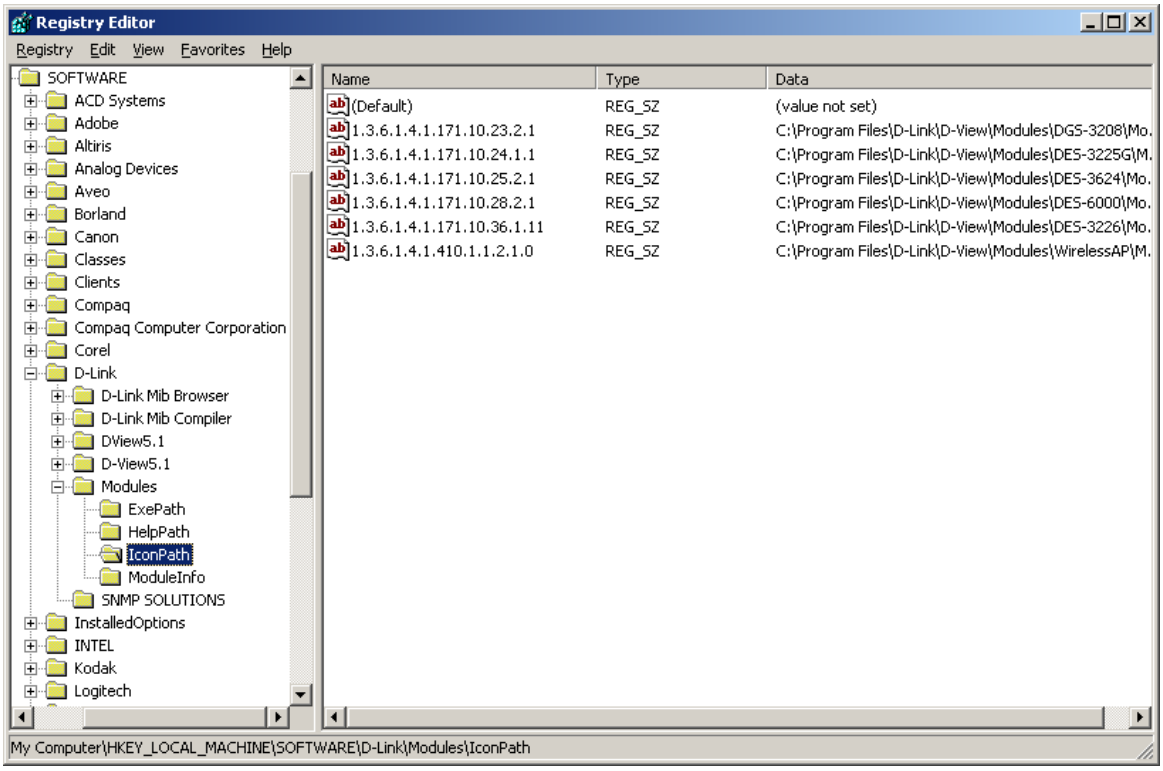

Registry Editor
Registry Edit View Favorites Help
SOFTWARE
ACD Systems
Adobe
Altiris
Analog Devices
Aveo
Borland
Canon
Classes
Clients
Compaq
Compaq Computer Corporation
Corel
D-Link
D-Link Mib Browser
D-Link Mib Compiler
DView5.1
D-View5.1
Modules
ExePath
HelpPath
IconPath
ModuleInfo
SNMP SOLUTIONS
InstalledOptions
INTEL
Kodak
Logitech
Name
Type
Data
(Default)
REG_SZ
(value not set)
1.3.6.1.4.1.171.10.23.2.1
REG_SZ
C:\Program Files\D-Link\D-View\Modules\DGS-3208\Mo.
1.3.6.1.4.1.171.10.24.1.1
REG_SZ
C:\Program Files\D-Link\D-View\Modules\DES-3225G\M.
1.3.6.1.4.1.171.10.25.2.1
REG_SZ
C:\Program Files\D-Link\D-View\Modules\DES-3624\Mo.
1.3.6.1.4.1.171.10.28.2.1
REG_SZ
C:\Program Files\D-Link\D-View\Modules\DES-6000\Mo.
1.3.6.1.4.1.171.10.36.1.11
REG_SZ
C:\Program Files\D-Link\D-View\Modules\DES-3226\Mo.
1.3.6.1.4.1.410.1.1.2.1.0
REG_SZ
C:\Program Files\D-Link\D-View\Modules\WirelessAP\M.
My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\D-Link\Modules\IconPath

Figure 165.

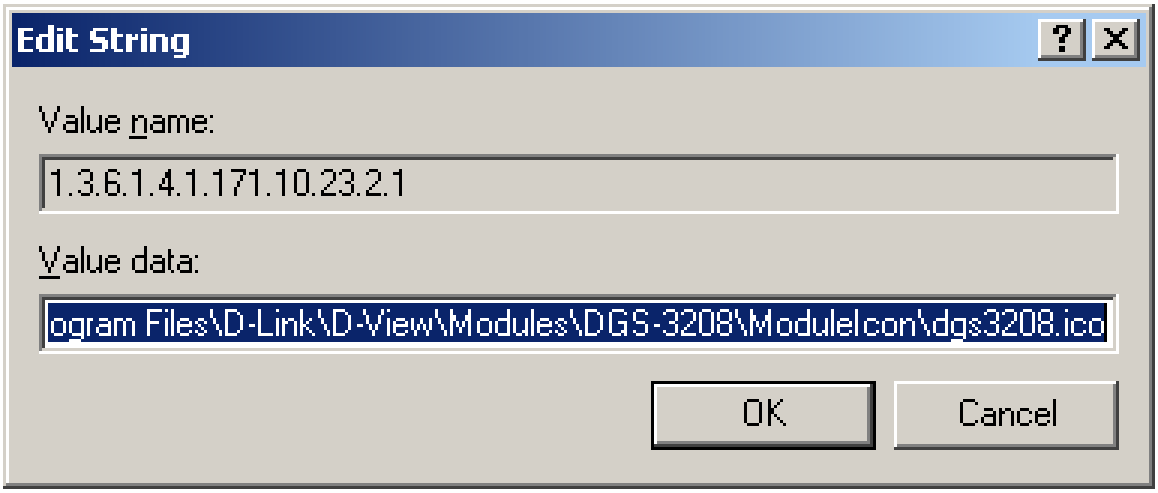


Figure 166.

4. **Module Info**: Record utility related information with OID of Device as Key. Select and right-click on mouse for newly added words value. Under name value input Device OID. Under data value there are four values separated by commas: Device Role, Module Name, Home page, Company Name.

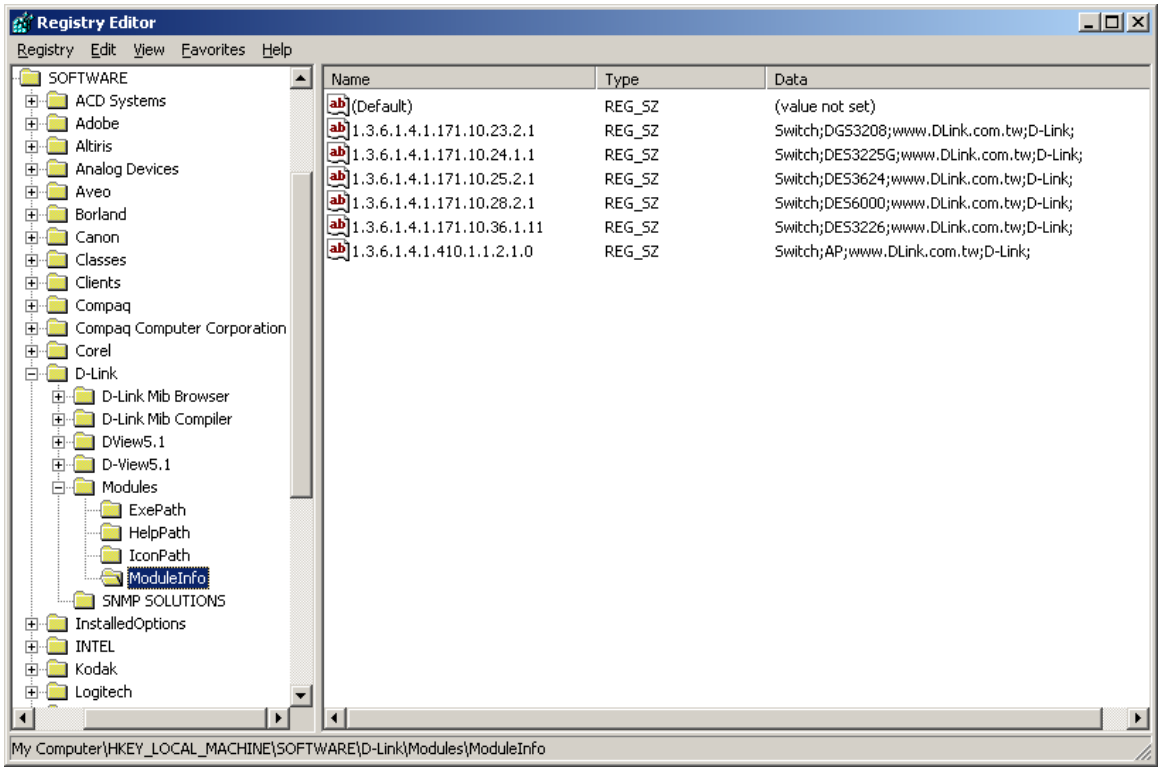

Registry Editor
Registry Edit View Favorites Help
SOFTWARE
ACD Systems
Adobe
Altiris
Analog Devices
Aveo
Borland
Canon
Classes
Clients
Compaq
Compaq Computer Corporation
Corel
D-Link
D-Link Mib Browser
D-Link Mib Compiler
DView5.1
D-View5.1
Modules
ExePath
HelpPath
IconPath
ModuleInfo
SNMP SOLUTIONS
InstalledOptions
INTEL
Kodak
Logitech
Name
Type
Data
(Default)
REG_SZ
(value not set)
1.3.6.1.4.1.171.10.23.2.1
REG_SZ
Switch;DGS3208;www.DLink.com.tw;D-Link;
1.3.6.1.4.1.171.10.24.1.1
REG_SZ
Switch;DES3225G;www.DLink.com.tw;D-Link;
1.3.6.1.4.1.171.10.25.2.1
REG_SZ
Switch;DES3624;www.DLink.com.tw;D-Link;
1.3.6.1.4.1.171.10.28.2.1
REG_SZ
Switch;DES6000;www.DLink.com.tw;D-Link;
1.3.6.1.4.1.171.10.36.1.11
REG_SZ
Switch;DES3226;www.DLink.com.tw;D-Link;
1.3.6.1.4.1.410.1.1.2.1.0
REG_SZ
Switch;AP;www.DLink.com.tw;D-Link;
My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\D-Link\Modules\ModuleInfo

Figure 167.

Figure 168.

Install common tools and plug-in to menu item.

Step 1: Type /DLINK_INSTALL_PATH?Conf/Resources/NewMenu.ini. For example, install DIAP2 pathway under Tools Menu.

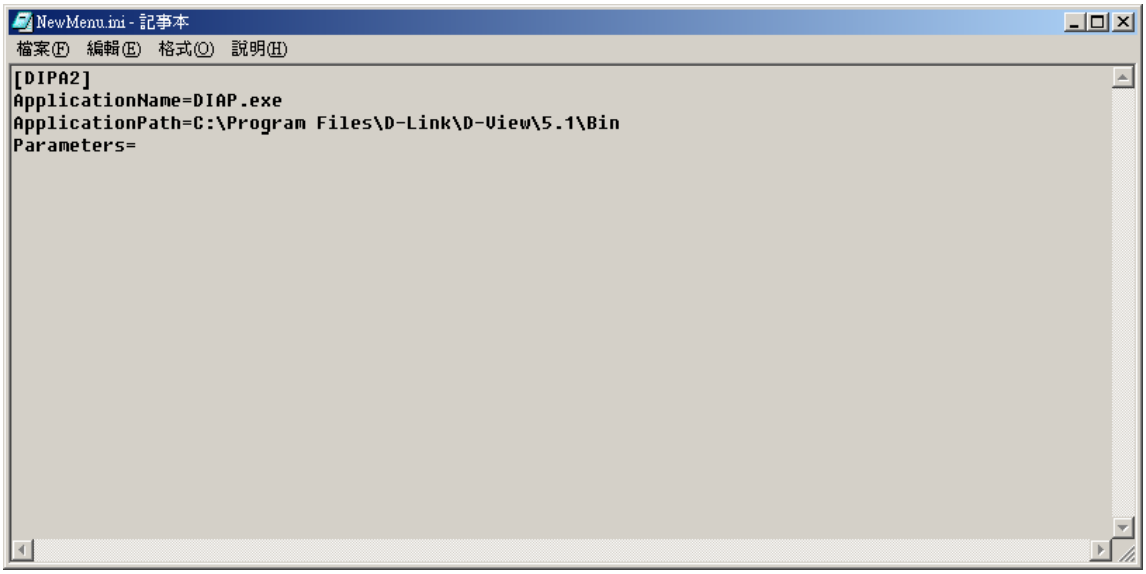


Figure 169.

Application Name: execution file name

Application Path: execution file pathway

Parameters: Execution file parameters

Step2: execution outcome

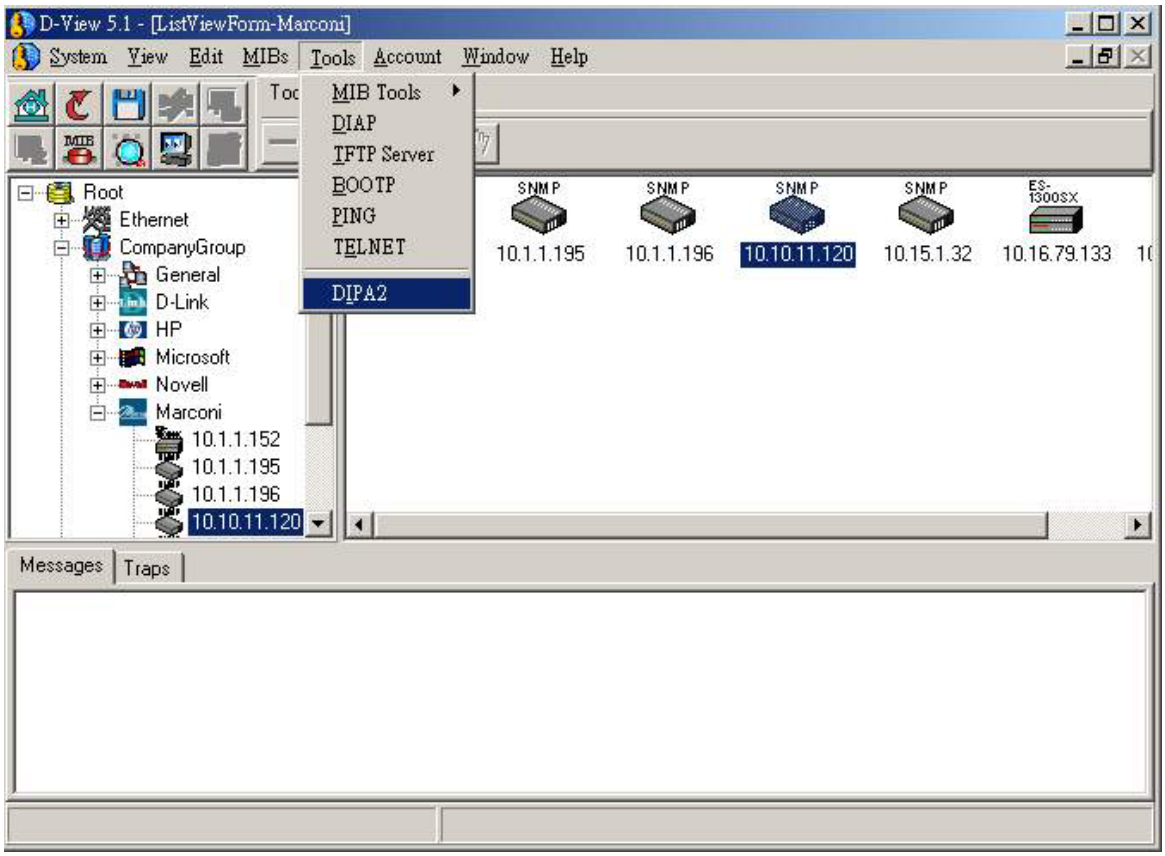


Figure 170.

Account

Account is a simple account management system to keep track of the bills. It has the following new features:

- Each client is assigned an account with personal authorization IP Address. Each IP Address will link to one Device Port. The system can verify and track devices in this manner.
- Setting statement schedule allows flexibility. Different groups of clients can generate statements at difference schedules.
- Detects abnormal usage for clients
- Assigns custom taxes to service charges (weekly, monthly, every three months, biannually, annually)
- Credit adjust function allows you to insert credit records manually and give credit for wrong or misdialed work.
- Late fee assessment function allows you to assign late payment charges with fixed charge or a percentage of late pay amount.
- Real-time reporting, including current client summary, credit limit status report, payment report, and the like.

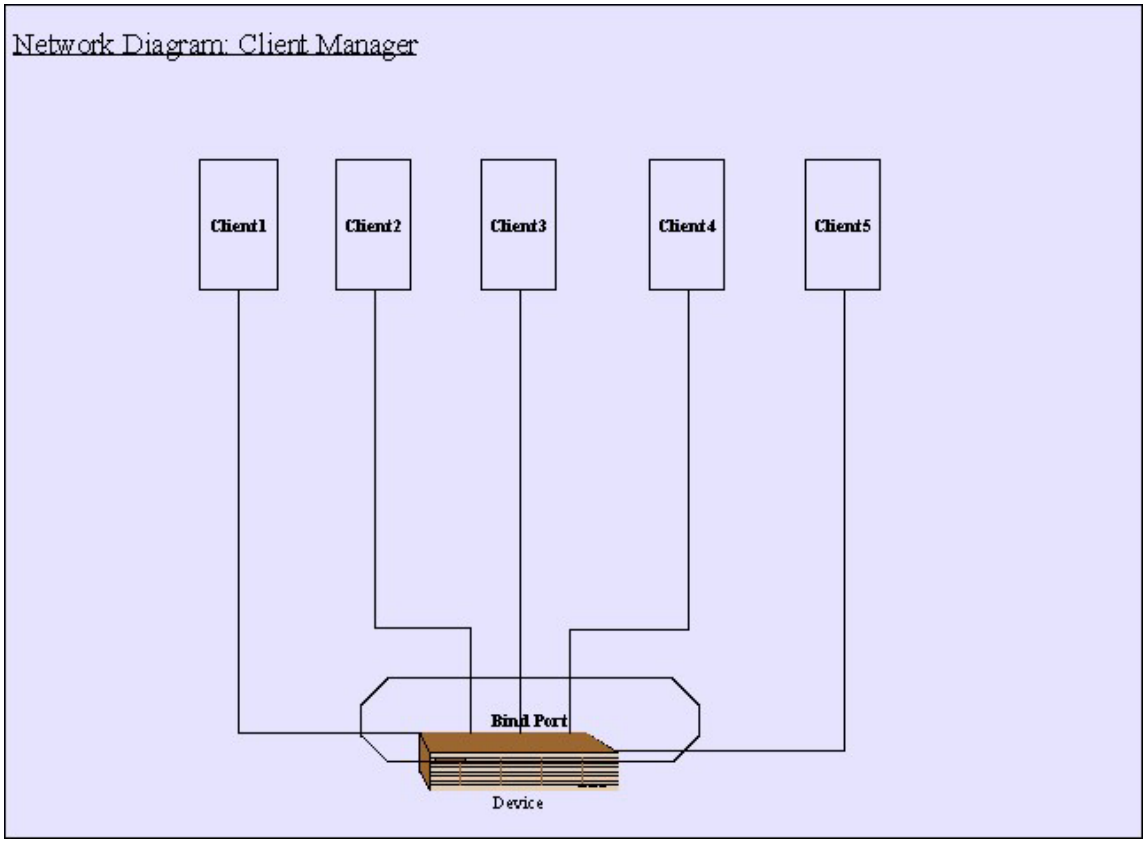


Figure 171.

The Account system can bundle customer equipment just like the telephone system. As with telephone numbers, you can manage customers by means of equipment management.

The menus available are the following:

- **Client Update**
- **Client Record Query**
- **Client Online Query**
- **Client Abnormal Situation**
- **Device Utilization**
- **Pay Rate Configuration**

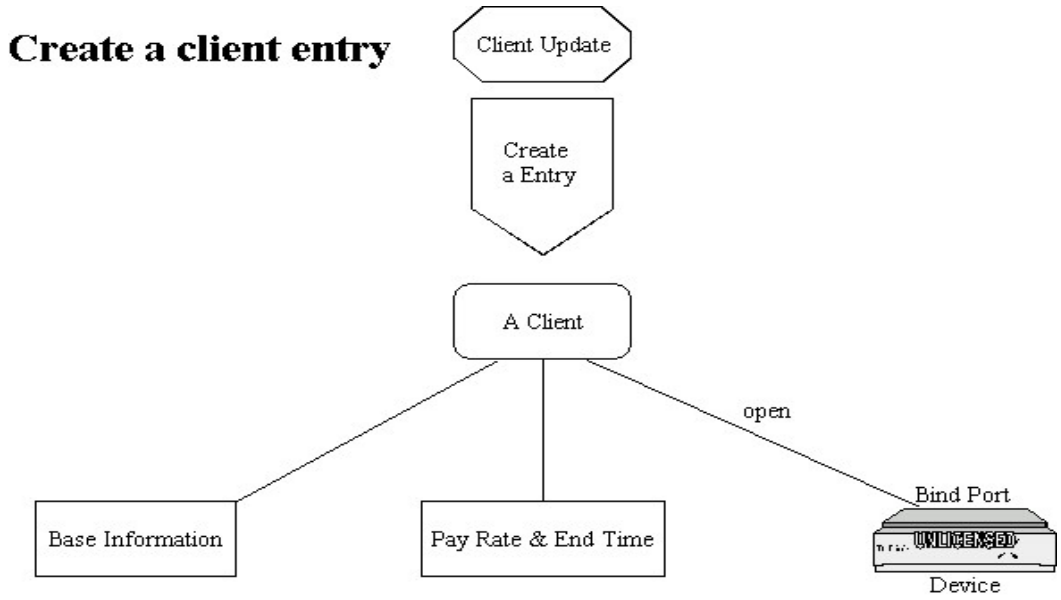


Figure 172. Creating a Client Entry

In the previous figure we establish a new customer entry by setting up the basic information. We charge users a service charge, place time limits on usage, and create an IP Address that corresponds to a specific port in a device. Thus customer data is established.

Client Update

Use the client update menu to view basic client information including Name, Phone, IP Address, Switch IP Address, Switch Port used, Status, Pay and E-Mail address. To add a new client, click the Add button to bring up the Client Manager menu (see below). Update or change existing client information by highlighting the client on the table and clicking the Modify button. Use the Query button to locate client records form the database.

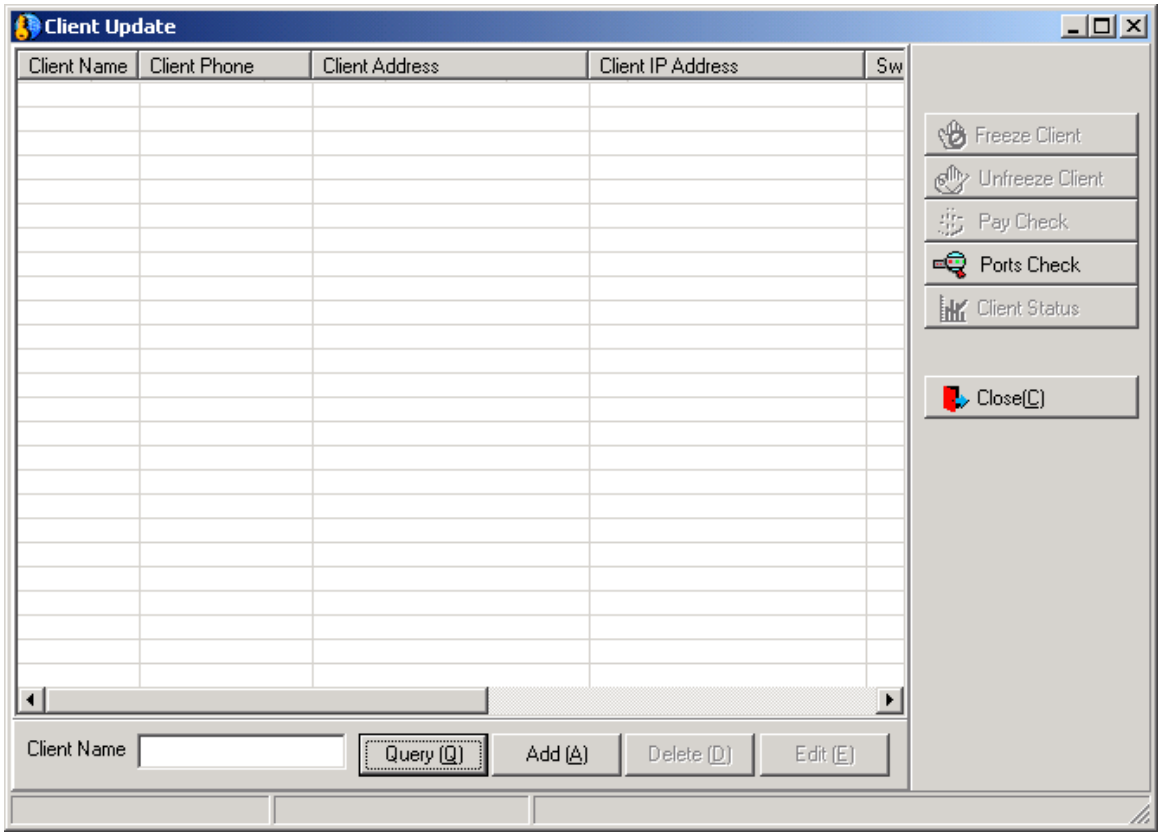


Figure 173. Client Update

Use the Freeze Client and Unfreeze Client buttons to disable (Freeze) or enable (Unfreeze) a frozen port linked to the selected client. The Pay Check button is used to view the client's payment status. The Port Check button is used to detect the port number and status of the client and update the device records from the database. The Client Status button is used to check a client's expiration status or to change client payment terms and expiration deadline.

Client Manager

The Client Manager "Add" is identical to the "Modify" menu.

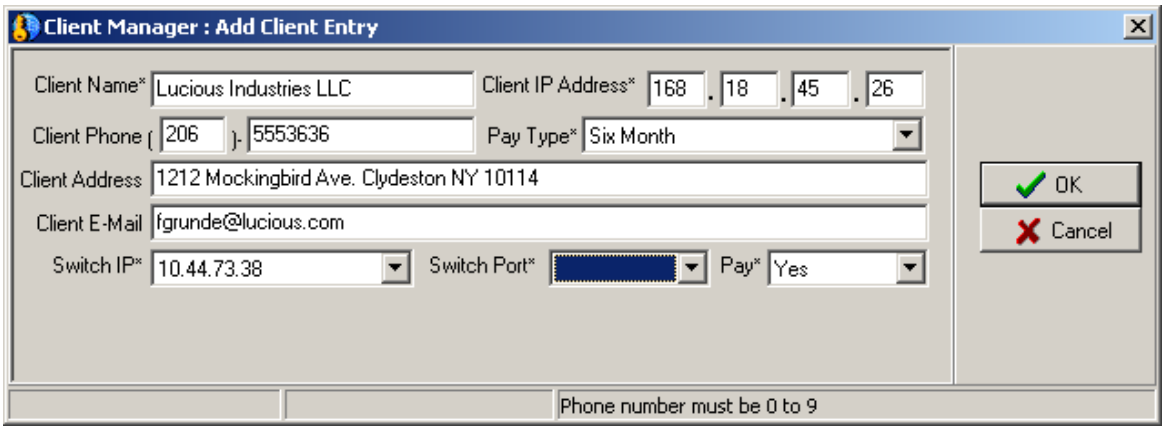


Figure 174.

How to Manage a Client

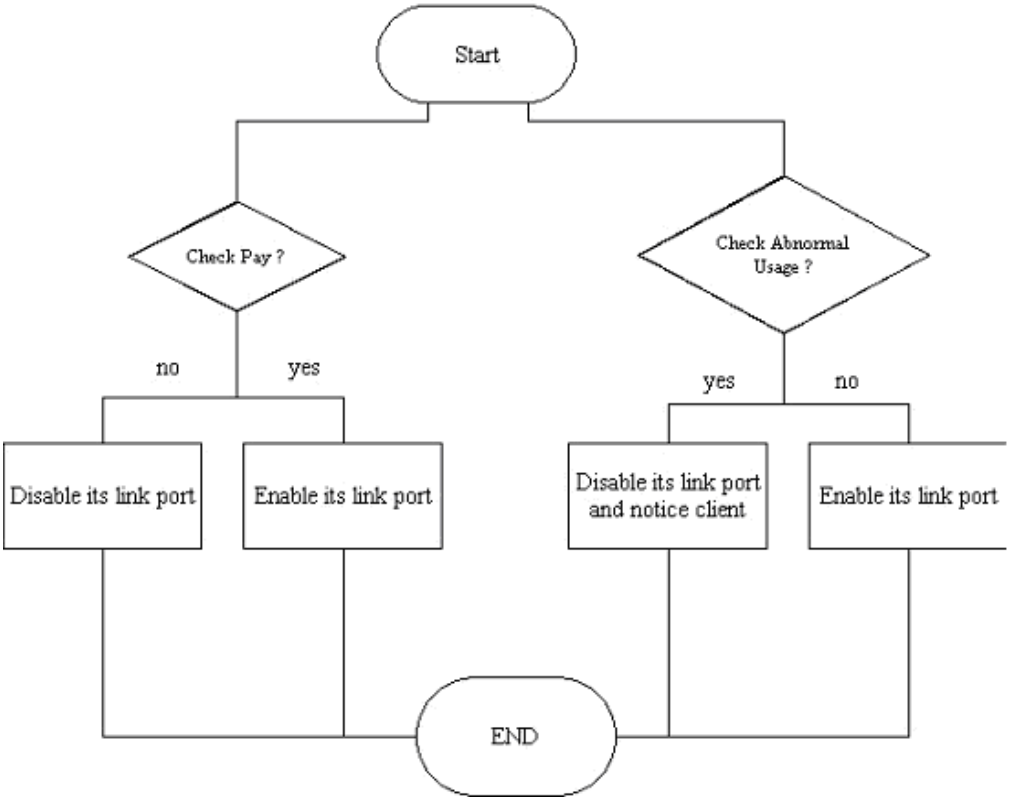


Figure 175.

When we begin to manage a client we need to determine first whether the client has paid for services or whether it is past due. If payment is past due we close the connection (disable its link port) and prevent the client from being connected to the network. We also need to decide whether

the client is experiencing abnormal usage. Depending on the situation, we may disable the client's link port and notify the client so as to not jeopardize other clients.

Client Record Query

Locate and view client records using various search conditions including device IP address, link port, client name and client pay status. Define the parameters and click the Query button to view the record search results in the record table.

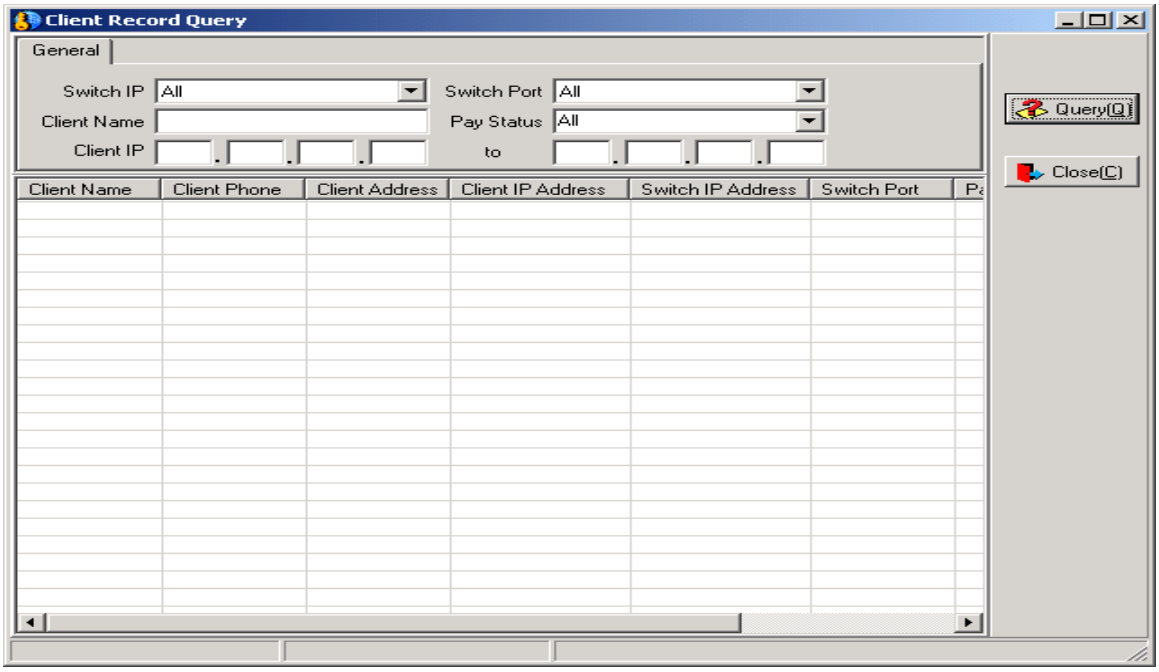


Figure 176. Client Online Record Query

Client Online Query

View client users currently connected to a selected device.

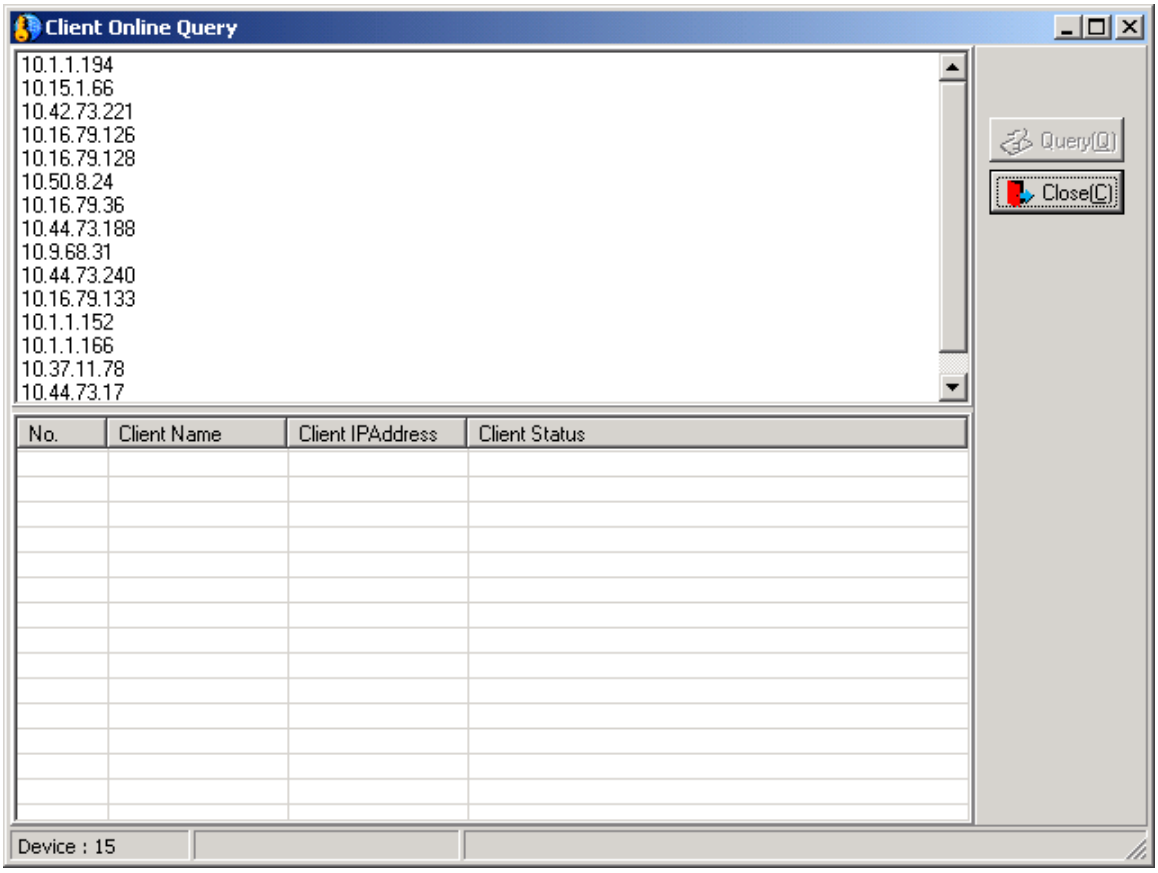


Figure 177. Client Online Query Information

Client Abnormal Situation

Use this to check client usage and logs of abnormal situations for a chosen device.

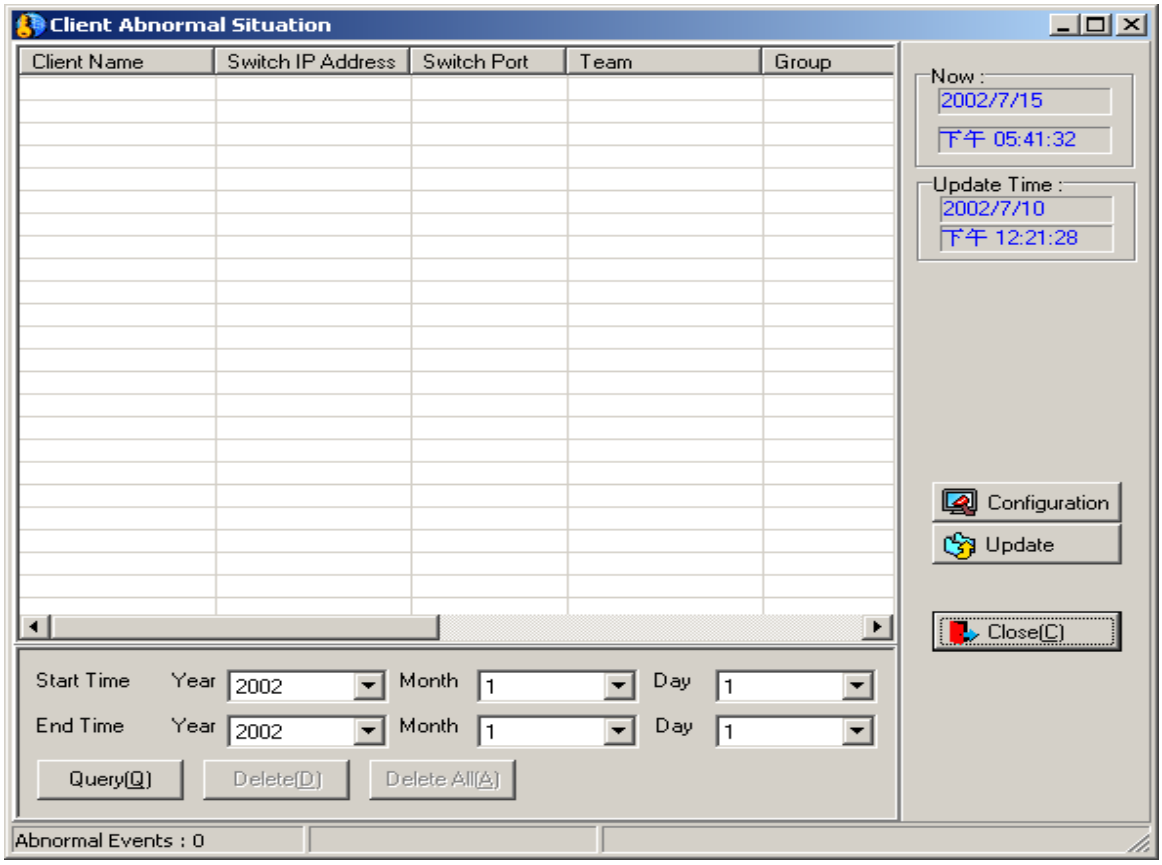


Figure 178. Client Abnormal Situation

Device Utilization

Analyze network usage and query total number of ports and ports open for a device.

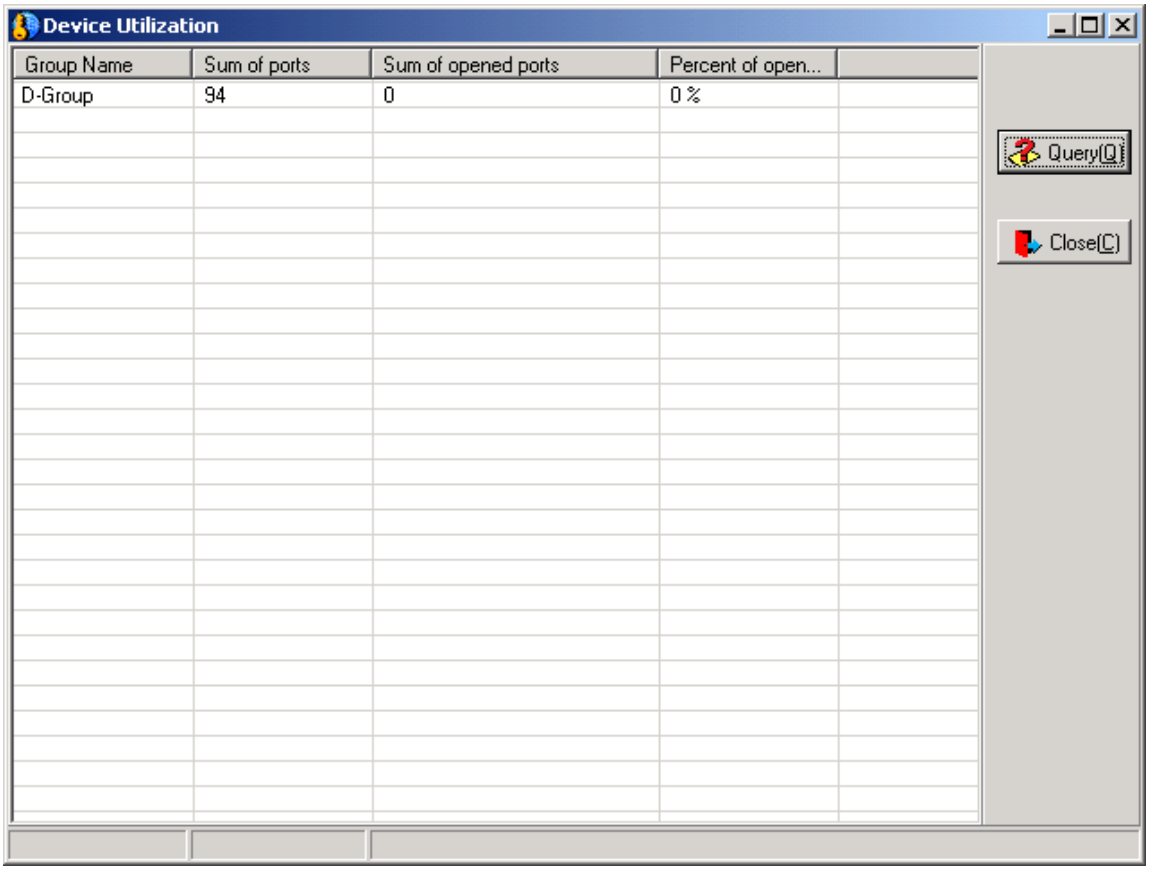


Figure 179. Device Utilization

Device Group Manager

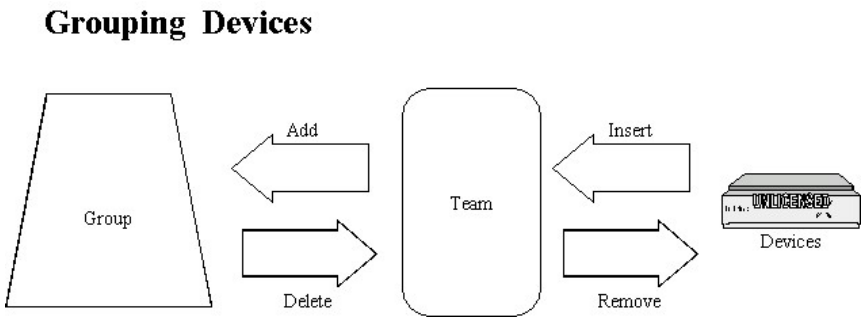


Figure 180.

Use the Group Manager to group devices according to purpose, location, team etc. Select devices from the tree and drag them to another group. Add or Delete groups and teams with the buttons on the bottom of the menu.

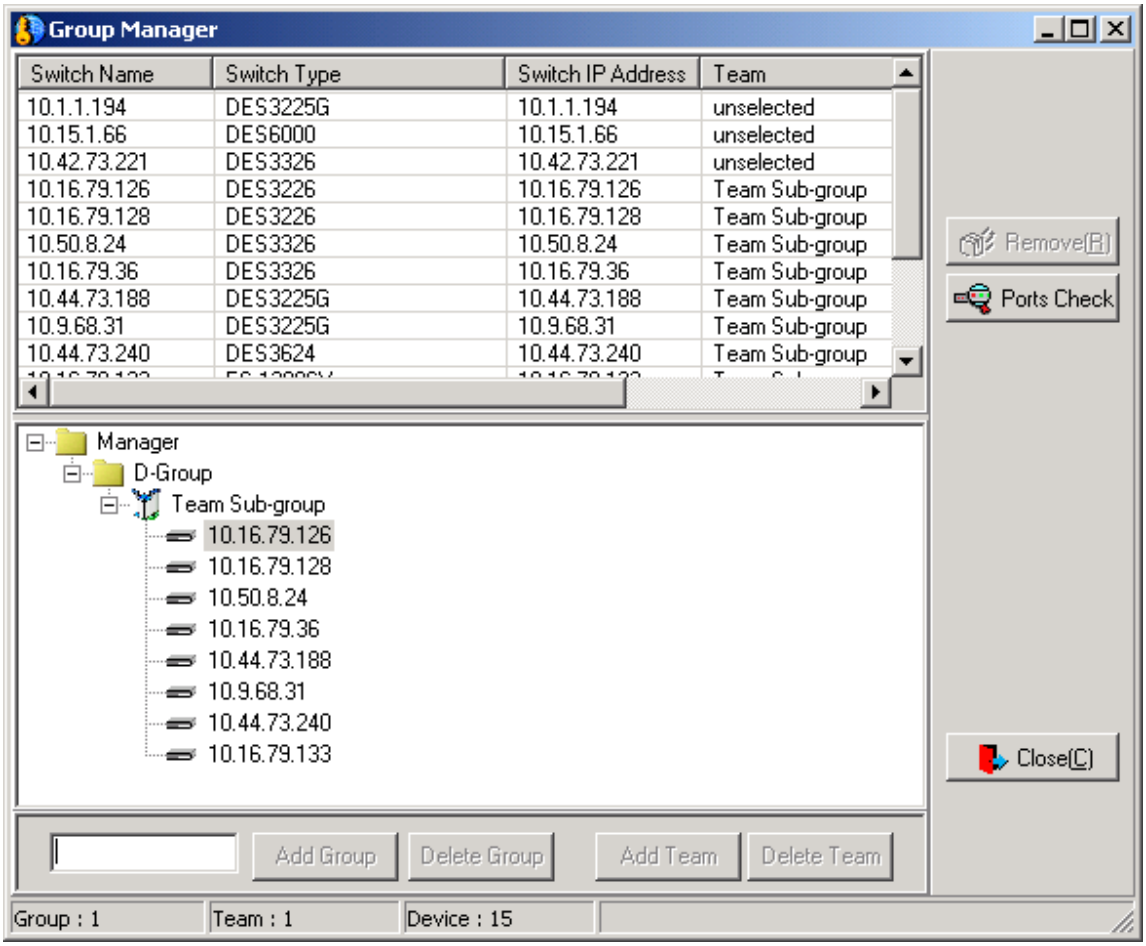


Figure 181. Device Group Manager

Pay Rate Configuration

To Add, Modify or Delete pay rate categories, type or select information in the spaces provided at the bottom of the menu.

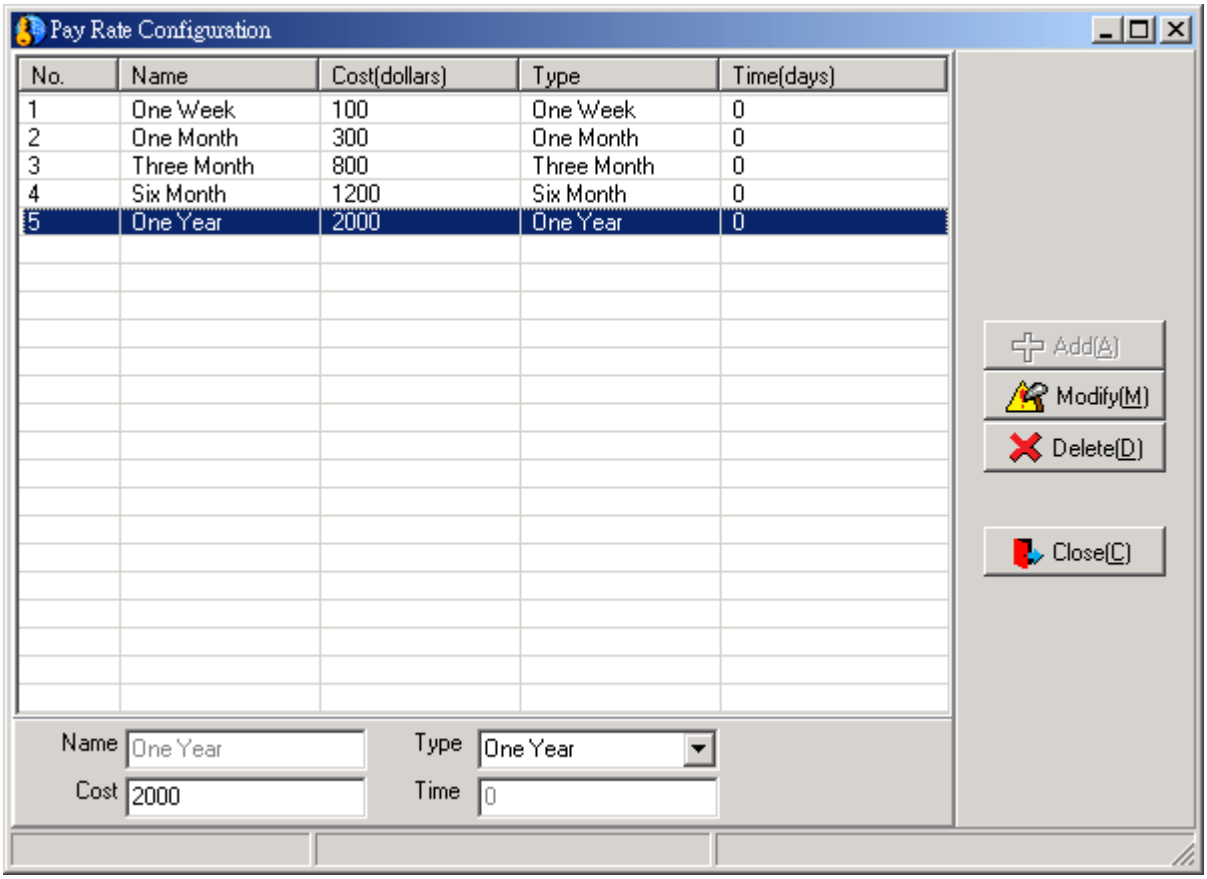


Figure 182. Pay Rate Configuration

A

TROUBLESHOOTING

- **Problem:** Can't open D-View with database error.
- **Solution:** Please install Access 2000.

- **Problem:** Can't find any SNMP devices in D-View.
- **Solution:** Please check the SNMP read community string.

Figure 183.

- **Problem:** Can't use MIB Utilities to manage the device in D-View
- **Solution:** Please check the write community string and read community string in the device and check if this device supports MIBs.

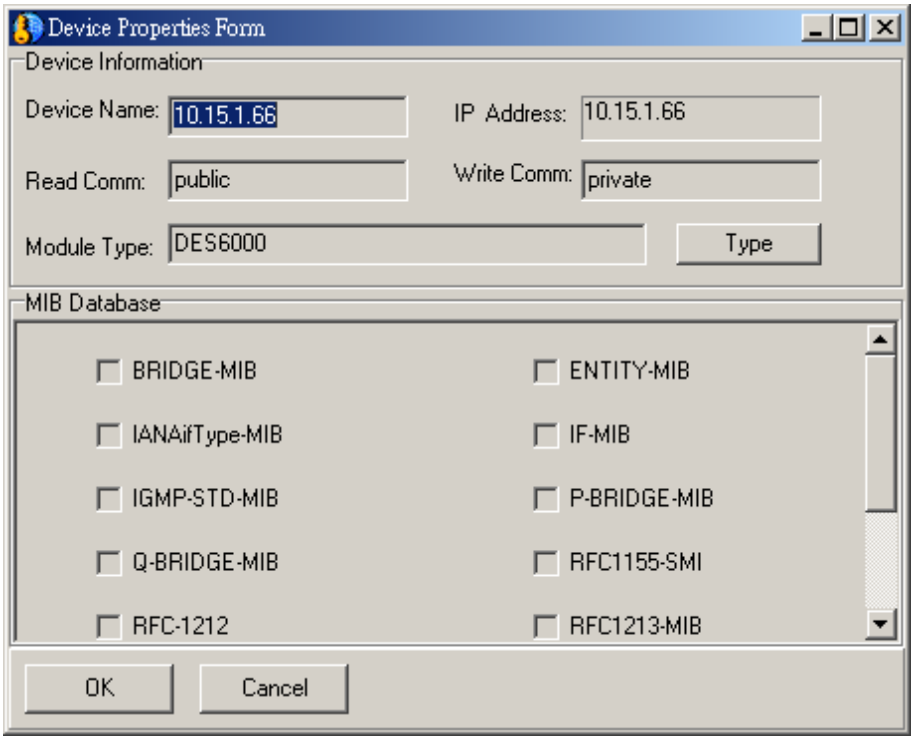


Figure 184.

- **Problem:** Can't send trap mail.
- **Solution:** Check the Trap Mail SMTP Settings (SMTP Server, Port, Type, etc.) and Trap Mail Interval Settings (IP Address, Alarm Level, Alarm Message)

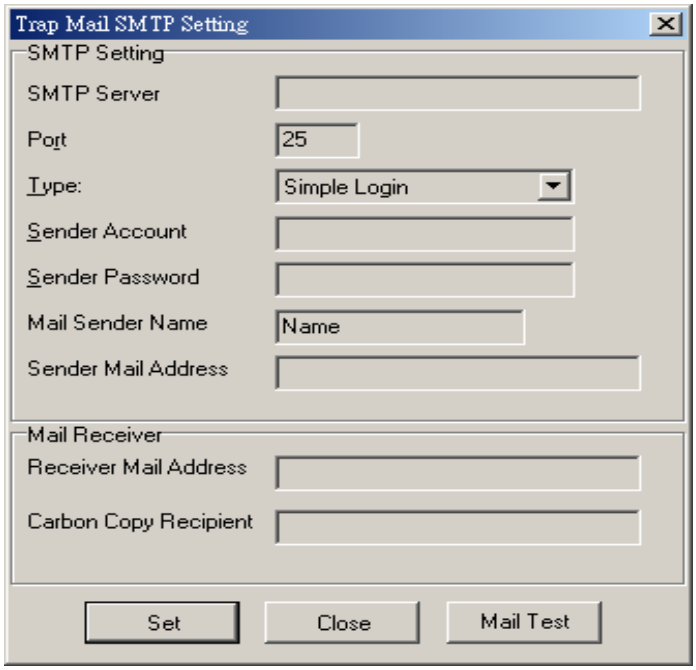

Trap Mail SMTP Setting
SMTP Setting
SMTP Server
Port
25
Type:
Simple Login
Sender Account
Sender Password
Mail Sender Name
Name
Sender Mail Address
Mail Receiver
Receiver Mail Address
Carbon Copy Recipient
Set
Close
Mail Test

Figure 185.

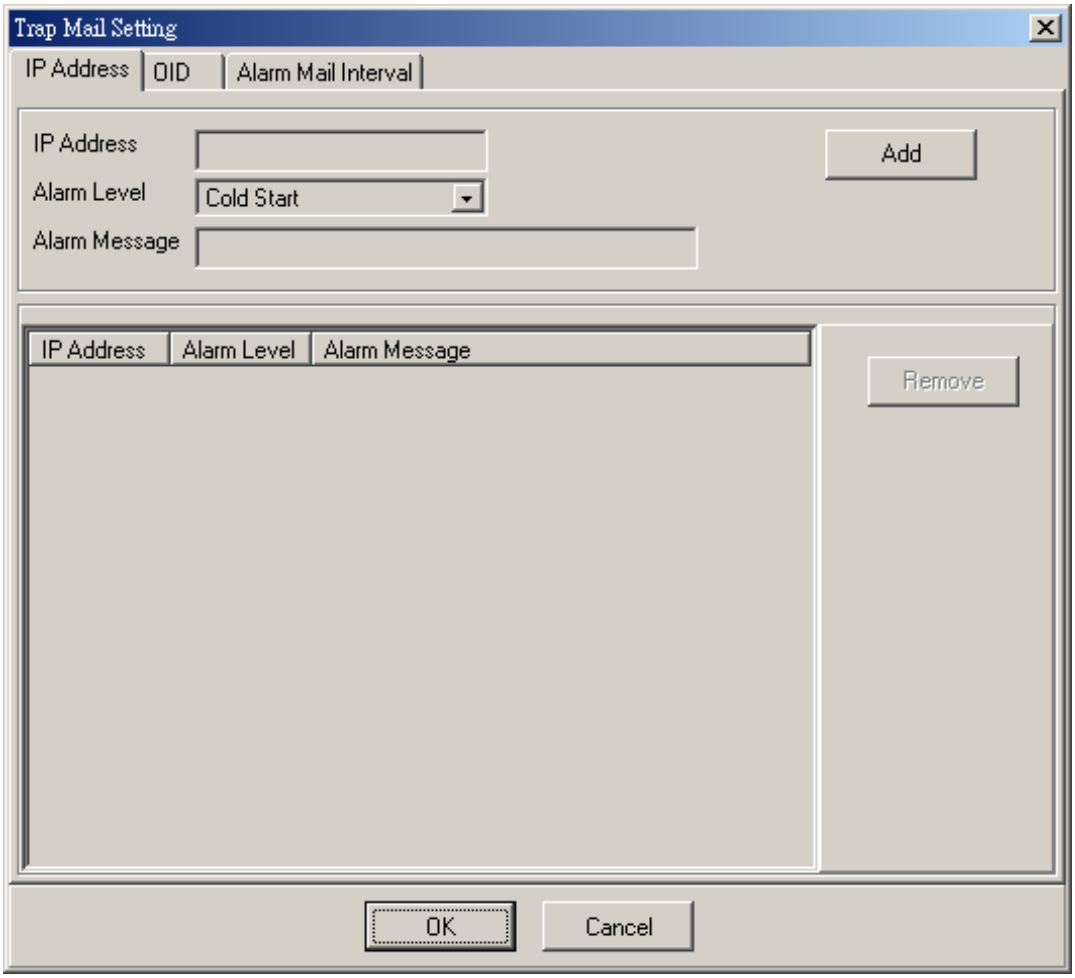

Trap Mail Setting
IP Address
OID
Alarm Mail Interval
IP Address
Alarm Level
Cold Start
Alarm Message
Add
IP Address
Alarm Level
Alarm Message
Remove
OK
Cancel

Figure 186.

- **Problem:** Auto-discover can't find the device you want.
- **Solution:** Use the Discover function (under System) to find the device you want.

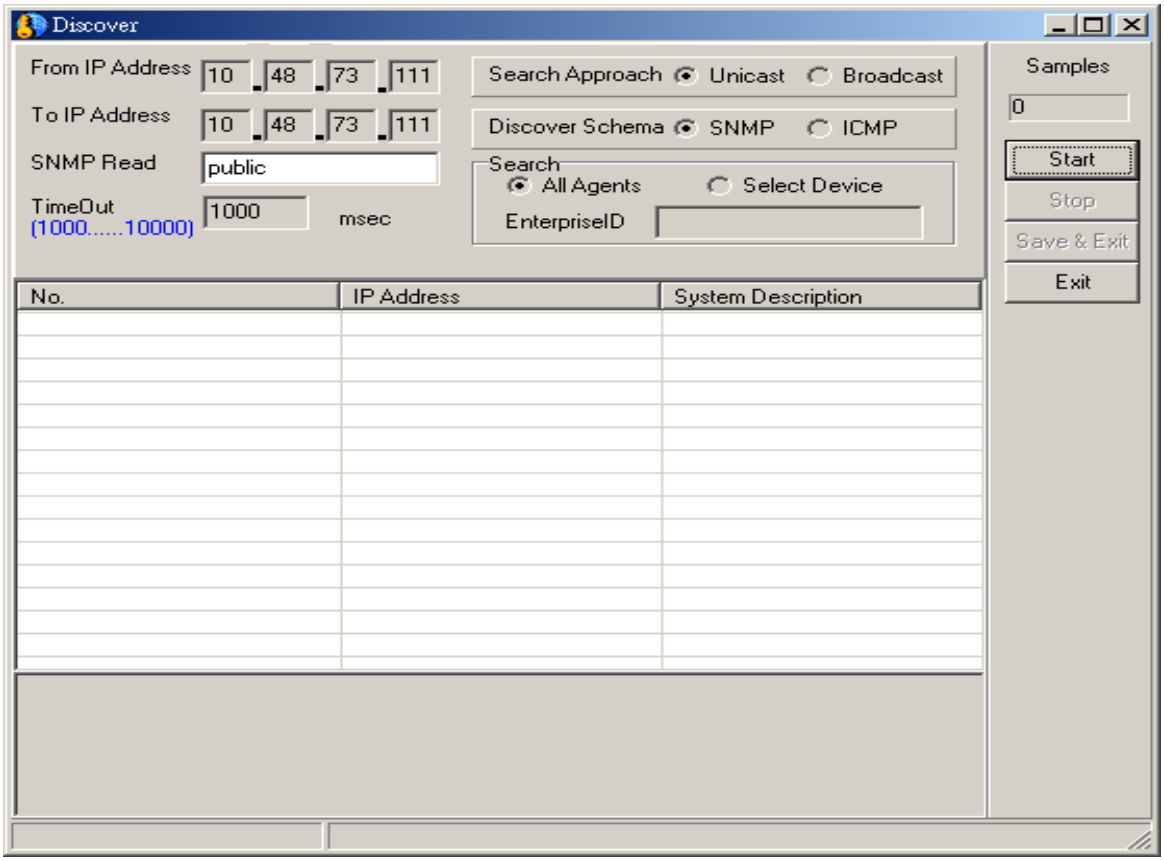


Figure 187.

- **Problem:** Can't inset a device into the D-View 5.1 platform manually.
- **Solution:** To insert a device into D-View 5.1 manually, right-click on tree view or list view in the D-View Platform with the mouse to bring up the pop-up menu. Select "Add Device" then shows the "new device form." Input parameters and click the ok button.

- **Problem:** Can't import the new device module into D-View 5.1.
- **Solution:** You can install the device module from the D-View 5.1 CD-Rom. If you want to upgrade the device module, you can download the latest Module Setup file from the D-Link web site http://www.dlink.com.

- **Problem:** Can't find wireless AP module in D-View 5.1
- **Solution:** You can't find wireless AP because the wireless AP does not support standard MIB (RFC1213), thus D-View 5.1 can't find it. You can only insert it manually.

B

MENU/COMMAND QUICK REFERENCE

System	View	Edit	MIBs	Tools	Account	Window
Discover Basic Information Repolling Configuration Community String Configuration Save to Database Trap Management *Trap Editor* *Trap Mail SMTP Settings*	Topology View Tree View List View MessagesTraps View Background Color	Device *Properties* *Copy* *Delete* Domain *New SubDomain* *New Device* *Copy* *Paste* *Delete* New Topology Find Object	SNMP Device Configuration MIB II (read-only menus) *Information,* *IF Table,* *IF Counters,* *IP Counters,* *IP Routing,* *IP Address Table, ICMP Counters, UDP Counters, SNMP Counters* Bridge 802.1d *Information,* *Port Table* Spanning Tree *Information,* *Port Table* Transparent Bridge *Forwarding Table, Static Table,* *Port Counters* RMON *Statistics, History, Alarm/Event* 802.1P *Basic Configuration, Priority Information, Port Capability, GMRP, GARP* 802.1Q *(802.1Q Bridge →) Basic Configuration,* *Ports Information, General Information, Learning Constraint Information* *802.1Q VLAN,* *Forwarding/Filtering,* *Unicast//Multicast, Static Filtering* Traffic statistics *Port VLAN Statistics Information, High Capacity Port, VLAN Statistics Information* Layer 3 Utilities *IP Forwarding, RIP 2, OSPF → (OSPF pop-up menus)* *IP mroute, DVMRP* SNMP V3	MIB tools MIB Browser, MIB Compiler DIAP TFTP Server BootP Ping Telnet	Client Update Client Record Query Client Online Query Client Unusual Situations Device Utilization Device Group *(Tools →) Rate Configuration,* *Detect Device Ports*	Cascade Tile Minimize

INDEX

D-Link Offices

Australia — **D-Link Australasia**
Unit 16, 390 Eastern Valley Way, Roseville, NSW 2069 Australia
TEL: 61-2-9417-7100 FAX: 61-2-9417-1077 TOLL FREE (Australia): 1800-177100
TOLL FREE (New Zealand): 0800-900900
URL: www.dlink.com.au E-MAIL: support@dlink.com.au & info@dlink.com.au

Level 1, 434 St. Kilda Road, Melbourne, Victoria 3004 Australia
TEL: 61-3-9281-3232 FAX: 61-3-9281-3229 MOBILE: 0412-660-064

Canada — **D-Link Canada**
2180 Winston Park Drive, Oakville, Ontario, L6H 5W1 Canada
TEL: 1-905-829-5033 FAX: 1-905-829-5095 BBS: 1-965-279-8732
TOLL FREE: 1-800-354-6522 URL: www.dlink.ca
FTP: ftp.dlinknet.com E-MAIL: techsup@dlink.ca

Chile — **D-Link South America**
Isidora Goyeechea 2934 of 702, Las Condes, Santiago, Chile, S. A.
TEL: 56-2-232-3185 FAX: 56-2-232-0923 URL: www.dlink.cl
E-MAIL: ccasassu@dlink.cl & tsilva@dlink.cl

China — **D-Link China**
2F, Sigma Building, 49 Zhichun Road, Haidan District, 100080 Beijing, China
TEL: 86-10-88097777 FAX: 86-10-88096789 URL: www.dlink.com.cn
E-MAIL: liweii@digitalchina.com.cn

Denmark — **D-Link Denmark**
Naverland 2, DK-2600 Glostrup, Copenhagen, Denmark
TEL: 45-43-969040 FAX:45-43-424347 URL: www.dlink.dk E-MAIL: info@dlink.dk

Egypt — **D-Link Middle East**
7 Assem Ebn Sabet Street, Heliopolis, Cairo, Egypt
TEL: 20-2-635-6176 FAX: 20-2-635-6192 URL: www.dlink-me.com
E-MAIL: support@dlink-me.com & fateen@dlink-me.com

Finland — **D-Link Finland**
Thlli-ja Pakkahuone Katajanokanlaituri 5, FIN– 00160 Helsinki
TEL: 358-9-622-91660 FAX: 358-9-622-91661 URL: www.dlink-fi.com

France — **D-Link France**
Le Florilege #2, Allee de la Fresnerie, 78330 Fontenay le Fleury, France
TEL: 33-1-3023-8688 FAX: 33-1-3023-8689 URL: www.dlink-france.fr
E-MAIL: info@dlink-france.fr

Germany — **D-Link Central Europe/D-Link Deutschland GmbH**
Schwalbacher Strasse 74, D-65760 Eschborn, Germany
TEL: 49-6196-77990 FAX: 49-6196-7799300 URL: www.dlink.de
BBS: 49-(0) 6192-971199 (analog) BBS: 49-(0) 6192-971198 (ISDN)

INFO: 00800-7250-0000 (toll free) HELP: 00800-7250-4000 (toll free)
REPAIR: 00800-7250-8000 E-MAIL: info@dlink.de

India **D-Link India**
Plot No.5, Kurla-Bandra Complex Rd., Off Cst Rd., Santacruz (E), Bombay, 400 098 India
TEL: 91-22-652-6696 FAX: 91-22-652-8914 URL: www.dlink-india.com
E-MAIL: service@dlink.india.com

Italy **D-Link Mediterraneo Srl/D-Link Italia**
Via Nino Bonnet n. 6/b, 20154, Milano, Italy
TEL: 39-02-2900-0676 FAX: 39-02-2900-1723 URL: www.dlink.it E-MAIL: info@dlink.it

Japan **D-Link Japan**
10F, 8-8-15 Nishi-Gotanda, Shinagawa-ku, Tokyo 141, Japan
TEL: 81-3-5434-9678 FAX: 81-3-5434-9868 URL: www.d-link.co.jp
E-MAIL: kida@d-link.co.jp

Netherlands **D-Link Benelux**
Fellenoord 1305611 ZB, Eindhoven, the Netherlands
TEL: 31-40-2668713 FAX: 31-40-2668666 URL: www.d-link-benelux.nl

Norway **D-Link Norway**
Waldemar Thranesgt. 77, 0175 Oslo, Norway
TEL: 47-22-991890 FAX: 47-22-207039

Russia **D-Link Russia**
Michurinski Prospekt 49, 117607 Moscow, Russia
TEL: 7-095-737-3389 & 7-095-737-3492 FAX: 7-095-737-3390 URL: www.dlink.ru
E-MAIL: vl@dlink.ru

Singapore **D-Link International**
1 International Business Park, #03-12 The Synergy, Singapore 609917
TEL: 65-774-6233 FAX: 65-774-6322 E-MAIL: info@dlink.com.sg
URL: www.dlink-intl.com

South Africa **D-Link South Africa**
102 – 106 Witchhazel Avenue, Einstein Park 2, Block B, Highveld Technopark,
Centurion, South Africa
TEL: 27 (0) 12-665-2165 FAX: 27 (0) 12-665-2186 URL: www.d-link.co.za
E-MAIL: attie@d-link.co.za

Spain **D-Link Iberia**
C/Sabino De Arana, 56 Bajos, 08028 Barcelona, Spain
TEL: 34 93 4090770 FAX: 34 93 4910795 URL: www.dlinkiberia.es
E-MAIL: info@dlinkiberia.es

Sweden **D-Link Sweden**
P. O. Box 15036, S-167 15 Bromma, Sweden
TEL: 46-(0) 8-564-61900 FAX: 46-(0) 8-564-61901 E-MAIL: info@dlink.se
URL: www.dlink.se

Taiwan **D-Link Taiwan**
2F, No. 119 Pao-Chung Rd, Hsin-Tien, Taipei, Taiwan
TEL: 886-2-2910-2626 FAX: 886-2-2910-1515 URL: www.dlinktw.com.tw
E-MAIL: dssqa@tsc.dlinktw.com.tw

Turkey **D-Link Middle East**
Deniz Bilgisayar, Buyukdere Cad. Naci Kasim Sk., No. 5 Mecidiyekoy, Istanbul, Turkey
TEL: 90-212-213-3400 FAX: 90-212-213-3420 E-MAIL: smorovati@dlink-me.com

U.A.E. **D-Link Middle East**
CHS Aptec (Dubai), P.O. Box 33550 Dubai U.A.E.
TEL: 971-4-366-885 FAX: 971-4-355-941 E-MAIL: Wxavier@dlink-me.com

U.K. **D-Link Europe**
4th Floor, Merit House, Edgware Road, Colindale, London NW9 5AB United Kingdom
TEL: 44 (0) 20-8731-5555 FAX: 44 (0) 20-8731-5511 BBS: 44 (0) 181-235-5511
URL: www.dlink.co.uk E-MAIL: info@dlink.co.uk

U.S.A. **D-Link U.S.A.**
53 Discovery Drive, Irvine, CA 92618, USA
TEL: 1-949-788-0805 FAX: 1-949-753-7033 BBS: 1-949-455-1779 & 1-949-455-9616
INFO: 1-800-326-1688 URL: www.dlink.com
E-MAIL: tech@dlink.com & support@dlink.com

Registration Card

Print, type or use block letters.

Your name: Mr./Ms_____
Organization: _____ Dept. _____
Your title at organization: _____
Telephone: _____ Fax:_____
Organization's full address: _____
_____
Country: _____
Date of purchase (Month/Day/Year): _____

Product Model	Product Serial No.	* Product installed in type of computer (e.g., Compaq 486)	* Product installed in computer serial No.

(* Applies to adapters only)

Product was purchased from:
Reseller's name: _____
Telephone: _____ Fax:_____
Reseller's full address: _____
_____
_____

Answers to the following questions help us to support your product:

1. Where and how will the product primarily be used?
☐Home ☐Office ☐Travel ☐Company Business ☐Home Business ☐Personal Use

2. How many employees work at installation site?
☐1 employee ☐2-9 ☐10-49 ☐50-99 ☐100-499 ☐500-999 ☐1000 or more

3. What network protocol(s) does your organization use ?
☐XNS/IPX ☐TCP/IP ☐DECnet ☐Others_____

4. What network operating system(s) does your organization use ?
☐D-Link LANsmart ☐Novell NetWare ☐NetWare Lite ☐SCO Unix/Xenix ☐PC NFS ☐3Com 3+Open
☐Banyan Vines ☐DECnet Pathwork ☐Windows NT ☐Windows NTAS ☐Windows '95
☐Others_____

5. What network management program does your organization use ?
☐D-View ☐HP OpenView/Windows ☐HP OpenView/Unix ☐SunNet Manager ☐Novell NMS
☐NetView 6000 ☐Others_____

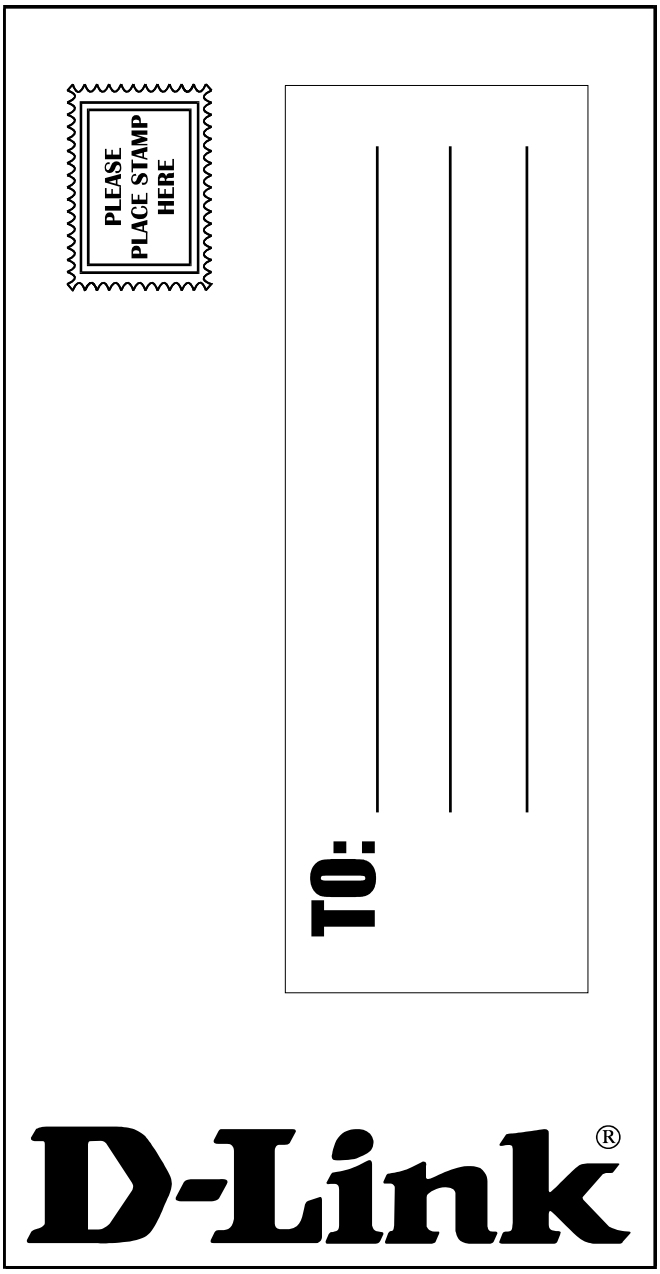
6. What network medium/media does your organization use ?
☐Fiber-optics ☐Thick coax Ethernet ☐Thin coax Ethernet ☐10BASE-T UTP/STP
☐100BASE-TX ☐100BASE-T4 ☐100VGAnyLAN ☐Others_____

7. What applications are used on your network?
☐Desktop publishing ☐Spreadsheet ☐Word processing ☐CAD/CAM
☐Database management ☐Accounting ☐Others_____

8. What category best describes your company?
☐Aerospace ☐Engineering ☐Education ☐Finance ☐Hospital ☐Legal ☐Insurance/Real Estate ☐Manufacturing
☐Retail/Chainstore/Wholesale ☐Government ☐Transportation/Utilities/Communication ☐VAR
☐System house/company ☐Other_____

9. Would you recommend your D-Link product to a friend?
☐Yes ☐No ☐Don't know yet

10.Your comments on this product?
_____


PLEASE
PLACE STAMP
HERE
TO:
D-Link®