D-Link®

DES-6300
Modular L3 Ethernet Switch
MIB Command Line Interface (MCLI)
User's Guide

First Edition (October 2002)

6DES6300C.01

Printed In Taiwan

RECYCLABLE

Wichtige Sicherheitshinweise

1. Bitte lesen Sie sich diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den spätern Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Vervenden Sie keine Flüssig- oder Aerosolreiniger. Am besten dient ein angefeuchtetes Tuch zur Reinigung.
4. Um eine Beschädigung des Gerätes zu vermeiden sollten Sie nur Zubehörteile verwenden, die vom Hersteller zugelassen sind.
5. Das Gerät is vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sichern Stand zu achten. Ein Kippen oder Fallen könnte Verletzungen hervorrufen. Verwenden Sie nur sichere Standorte und beachten Sie die Aufstellhinweise des Herstellers.
7. Die Belüftungsöffnungen dienen zur Luftzirkulation die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Die Netzanschlußsteckdose muß aus Gründen der elektrischen Sicherheit einen Schutzleiterkontakt haben.
10. Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollete auch nichts auf der Leitung abgestellt werden.
11. Alle Hinweise und Warnungen die sich am Geräten befinden sind zu beachten.
12. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
13. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. Elektrischen Schlag auslösen.
14. Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.
15. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
    a – Netzkabel oder Netzstecker sint beschädigt.
    b – Flüssigkeit ist in das Gerät eingedrungen.
    c – Das Gerät war Feuchtigkeit ausgesetzt.
    d – Wenn das Gerät nicht der Bedienungsanleitung ensprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
    e – Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
    f – Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
16. Bei Reparaturen dürfen nur Orginalersatzteile bzw. den Orginalteilen entsprechende Teile verwendet werden. Der Einsatz von ungeeigneten Ersatzteilen kann eine weitere Beschädigung hervorrufen.
17. Wenden Sie sich mit allen Fragen die Service und Repartur betreffen an Ihren Servicepartner. Somit stellen Sie die Betriebssicherheit des Gerätes sicher.
18. Zum Netzanschluß dieses Gerätes ist eine geprüfte Leitung zu verwenden, Für einen Nennstrom bis 6A und einem Gerätegewicht größer 3kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75mm2 einzusetzen.

Trademarks

Copyright Statement

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this user's guide, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Warnung!

Dies ist in Produkt der Klasse A. Im Wohnbereich kann dieses Produkt Funkstoerungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Massnahmen zu ergreifen.

Precaución!

Este es un producto de Clase A. En un entorno doméstico, puede causar interferencias de radio, en cuyo case, puede requerirse al usuario para que adopte las medidas adecuadas.

Attention!

Ceci est un produit de classe A. Dans un environnement domestique, ce produit pourrait causer des interférences radio, auquel cas l`utilisateur devrait prendre les mesures adéquates.

Attenzione!

Il presente prodotto appartiene alla classe A. Se utilizzato in ambiente domestico il prodotto può causare interferenze radio, nel cui caso è possibile che l`utente debba assumere provvedimenti adeguati.

VCCI Warning

注意

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づく第一種情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

BSMI Warning

警告使用者

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下使用者會被要求採取某些適當的對策．

About This Guide

Overview of this User's Guide

- Chapter 1, "*Introduction*." Introduction to the MCLI.
- Chapter 2, "*MCLI Setup*." Starting up the MCLI application.
- Chapter 3, "*Line Mode*." Describes the Line Mode operating instructions.
- Chapter 4, "*Screen Mode*." Describes the Screen Mode operating instructions.
- Chapter 5, "*MCLI File*." Describes the MCLI file and how to use it.
- Appendix A, "*MIB Object Reference*." MIB object reference guide.

Typographical Conventions

Convention	**Description**
Note:	Indicates important information that requires a special mention.
`Typewriter font`	Indicates system messages and prompts appearing on your screen. For example: `You have mail`.
Boldface Typewriter Font	Indicates commands and responses to prompts that must be typed exactly as printed in the manual.
`Typewriter Italic`	Indicates variables or parameters that are replaced with an appropriate word or string. For example: type *filename* means that you should type the actual filename instead of the word shown in typewriter italic.
[ ]	In a command line, square brackets indicate an optional entry. For example: [**copy *filename***] means that optionally you can type copy followed by the name of the file. Do not type the brackets.
Italic font	Indicates a parameter.
Bold font	Indicates a button, a toolbar icon, menu, menu item. For example: Open the **File** menu and choose **Cancel**. Used for emphasis.
Initial capital letter	Indicates a window name. Names of keys on the keyboard have initial capitals. For example: MCLIck Enter.
<Enter>	Any individual key on the keyboard.

Ctrl+F4	Any combination keys pressed simultaneously on the keyboard.

Table of Contents

List of Figures

Chapter 1 Introduction

The Command Line Interface (MCLI*)* is a network management application operated through an ASCII terminal or via Telnet.

In this MCLI, there are two types of commands:

- MCLI commands to control the MCLI operating environment
- Management Information Base (MIB) variable commands to control network operational parameters

The MCLI has a time monitoring application. When the MCLI is dormant for a prescribed period, the MCLI application automatically closes. This prescribed period is set by the system administrator and can be modified at any time.

Management Information Base (MIB)

Network management is based on the concept of a Management Information Base (MIB). The system administrator can use MIB variables to manage, monitor, and control network transmissions. The protocol used to manage MIBs is Simple Network Management Protocol (SNMP). In this MCLI, extra commands are added to the standard SNMP commands to extend control over the MIB variables.

There are two types of MIB variables:

- Table variables
- Scalar variables

If the MIB is a table variable, then the variable parameter names are the names of the table fields. The parameter order within the MIB is always the key parameters followed by the other parameters.

System Command Interfaces

There are two operating modes for entering commands:

- **Line Mode**—Entering MCLI commands

- **Screen Mode**—Entering MIB variable commands to modify MIB variables using parameter menus

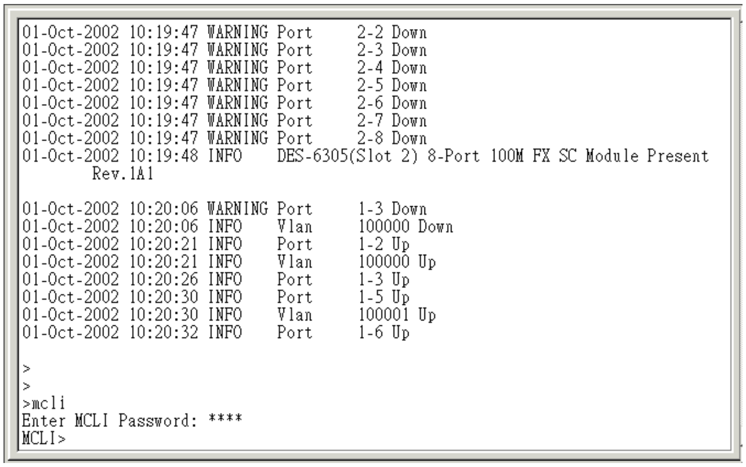
Chapter 2 Starting MCLI

The MCLI is started up from an ASCII terminal or Telnet. Once the MCLI is running, the terminal screen, keyboard and mouse are exclusive to the MCLI application.

To start MCLI:

1. At the “>” prompt type ***MCLI*** and press ***<Enter>***. A password prompt appears.
2. Enter your assigned password. The default password is “**MCLI**”.
   The password characters are displayed as asterisks.

   When the password is accepted, MCLI begins running and the prompt changes from the “>” to “**MCLI>**”. The following figure illustrates the MCLI command, password prompt and MCLI command prompt.



```
01-Oct-2002 10:19:47 WARNING Port     2-2 Down
01-Oct-2002 10:19:47 WARNING Port     2-3 Down
01-Oct-2002 10:19:47 WARNING Port     2-4 Down
01-Oct-2002 10:19:47 WARNING Port     2-5 Down
01-Oct-2002 10:19:47 WARNING Port     2-6 Down
01-Oct-2002 10:19:47 WARNING Port     2-7 Down
01-Oct-2002 10:19:47 WARNING Port     2-8 Down
01-Oct-2002 10:19:48 INFO    DES-6305(Slot 2) 8-Port 100M FX SC Module Present
        Rev.1A1

01-Oct-2002 10:20:06 WARNING Port     1-3 Down
01-Oct-2002 10:20:06 INFO    Vlan     100000 Down
01-Oct-2002 10:20:21 INFO    Port     1-2 Up
01-Oct-2002 10:20:21 INFO    Vlan     100000 Up
01-Oct-2002 10:20:26 INFO    Port     1-3 Up
01-Oct-2002 10:20:30 INFO    Port     1-5 Up
01-Oct-2002 10:20:30 INFO    Vlan     100001 Up
01-Oct-2002 10:20:32 INFO    Port     1-6 Up

>
>
>mcli
Enter MCLI Password: ****
MCLI>
```

Figure 2-1: MCLI Password Prompt and Startup Screen

MCLI starts up in Line Mode.

Chapter 3 Line Mode

The Line Mode is for entering MCLI commands and MIB variable commands.

Note: *Currently the MIB variable commands are not implemented.*

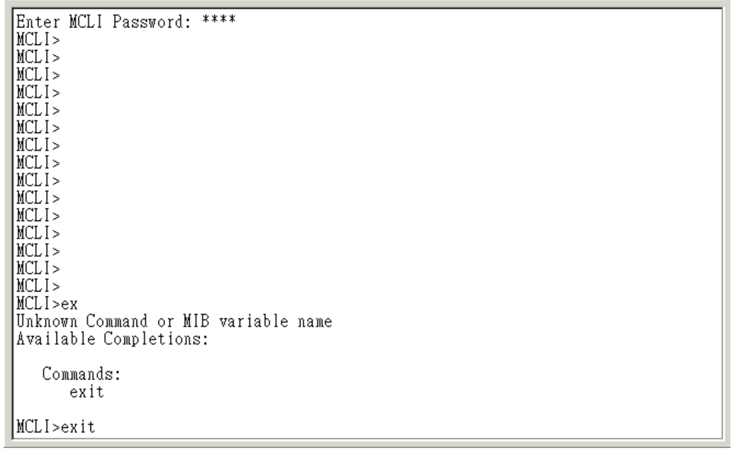
MCLI Commands

The following MCLI commands are available in Line Mode.

- exit or quit
- password
- timer
- ?

Line Mode maintains a command history list of commands entered by the operator during the current session. The keyboard **<Up>** and **<Down>** arrow keys are used to scroll through and view the list.

If a partial command is entered, the system displays the error message and lists the possible MCLI commands with the same character string. The following figure illustrates this function with the incomplete command “***ex***”.



```
Enter MCLI Password: ****
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>ex
Unknown Command or MIB variable name
Available Completions:

   Commands:
      exit

MCLI>exit
```

Figure 3-1: Incomplete MCLI Command

In this example, entering the characters “***ex***” results in a list of all commands with the first two characters corresponding to “***ex***”. In this case, the only command is ***exit***.

The following paragraphs describe and explain each MCLI command.

Command—exit or quit

The commands ***exit*** and ***quit*** have the same application. They both return control back to the ASCII terminal or Telnet.

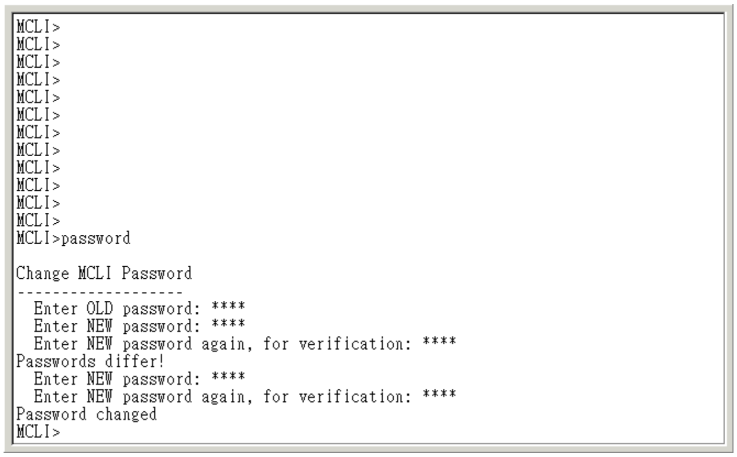
To use the “*exit*” or “*quit*” command:

- At the prompt type ***exit*** or ***quit*** and press ***<Enter>***.

The terminal returns to ASCII control and the prompt changes back to “>”.

Command—password

The command ***password*** is used to modify the MCLI password. Once the ***password*** command is entered, the system prompts you for the new password. The following figure illustrates the password changing process.



```
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>password

Change MCLI Password
-------------------
  Enter OLD password: ****
  Enter NEW password: ****
  Enter NEW password again, for verification: ****
Passwords differ!
  Enter NEW password: ****
  Enter NEW password again, for verification: ****
Password changed
MCLI>
```

Figure 3-2: Password Command Screen

To use the "*password*" command:

3. At the prompt type **password** and press **<Enter>**. The function heading is displayed on the screen with the words "Change MCLI Password", followed by a prompt for the old password.
4. Enter the old password. If the password is incorrect, the prompt keeps reappearing until the correct password is entered. Once the correct old password is entered, a prompt for the new password appears (*see* Figure 3-2).
5. Enter the new password. The password does not have size, font or any other character specifications, but the password is case sensitive.
6. Confirm the new password by re-entering the new password and press ***<Enter>***.

   If the password is not correctly re-entered, the error message "Passwords differ!" appears. This error message continues to appear until the new password is entered correctly. If the password is correctly entered, the command completion message "Password changed" appears. The password is changed and the MCLI prompt reappears.

Command—timer

The MCLI Timer is used to auto-exit MCLI when the program is dormant for a set period of time. The default timer value is 600 seconds and is active in both Line and Screen mode. The MCLI Timer is a MIB variable.

The ***timer*** command modifies the time-out period the MCLI waits before automatically exiting.

Whenever ***<Enter>*** or the up/down arrows are pressed, the MCLI timer is reset. The MCLI Timer is a MIB variable.

To use the timer command:

- At the prompt type ***timer <new value>*** and press ***<Enter>***.

  The parameter ***<new value>*** can be between 5 seconds and 3600 seconds. The default timer value is 600 seconds.

Command—?

The ***?*** command displays all supported commands and MIB variables alphabetically.

To use the* ? *command:

- At the prompt type ***?*** and press ***<Enter>***.

  All the commands begin to scroll down the screen. To stop the scrolling press the ***<Esc>*** button.

Chapter 4 Screen Mode

Screen mode is dedicated to one specific MIB variable at a time. The active MIB variable is called the “working variable.” There are two types of MIB variables:

- Table variables
- Scalar variables

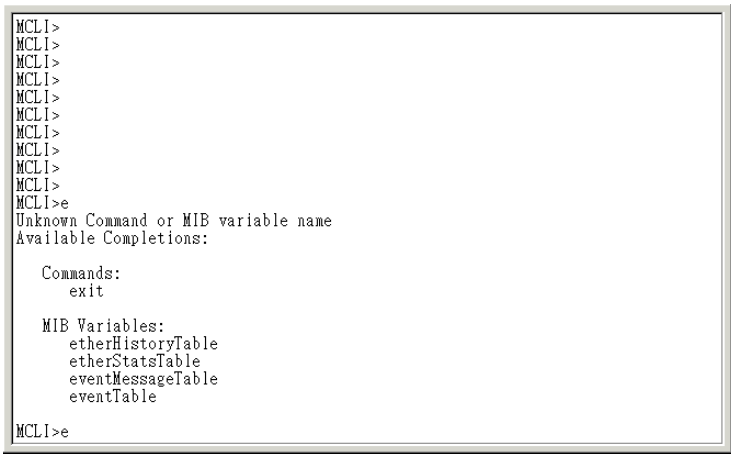
Commands within Screen mode are SNMP based commands. Any SNMP command syntax errors are displayed by an error message.

Note: *To modify a MIB variable that is field in a table, access the table variable. You cannot access the field variable directly via the MCLI.*

To enter the Screen Mode:

- In Line Mode enter the following ***<MIB Variable / OID name>*** and press ***<Enter>***.

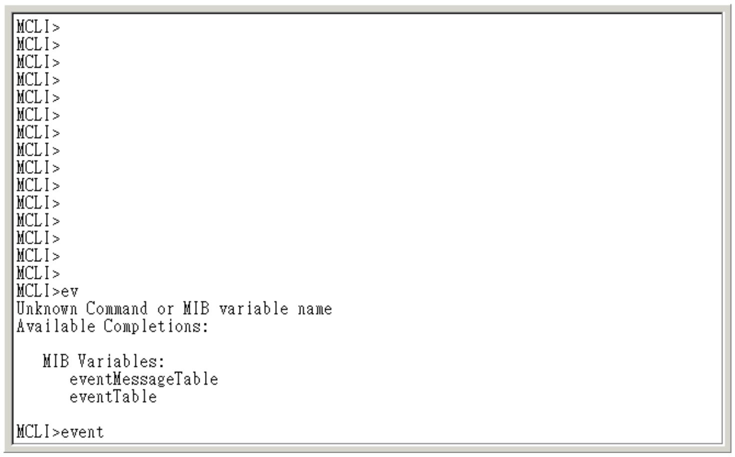
If a command is incorrectly entered, MCLI displays a list of all supported MCLI commands and MIB variables that start with the entered character string. If there is only one matching command or MIB variable, MCLI displays the corrected command or MIB variable at the prompt. The following figure illustrates the entry of the character “***e***” and lists the available MCLI commands and MIB variables.



```
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>e
Unknown Command or MIB variable name
Available Completions:

   Commands:
      exit

   MIB Variables:
      etherHistoryTable
      etherStatsTable
      eventMessageTable
      eventTable

MCLI>e
```

Figure 4-1: Incomplete MCLI Command or MIB Variable

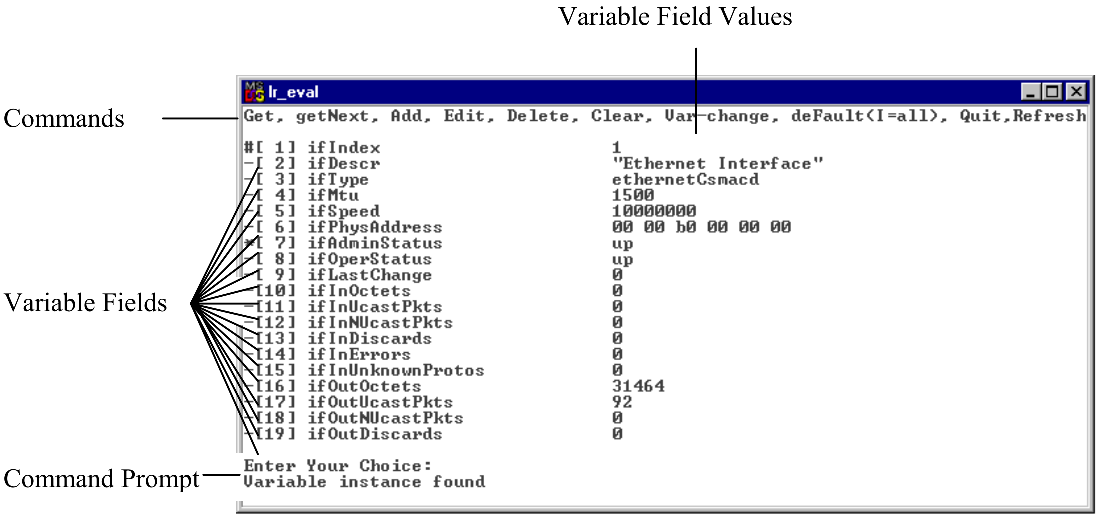
If a variable is incorrectly entered, MCLI displays a list of all supported commands and MIB variables that start with the entered character string. If there is only one MIB variable, MCLI displays the corrected MIB variable at the prompt. The following figure illustrates an example when the characters "***ev***" are entered.



```
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>
MCLI>ev
Unknown Command or MIB variable name
Available Completions:

   MIB Variables:
      eventMessageTable
      eventTable

MCLI>event
```

Figure 4-2: Incorrect MIB Variable Screen

If the variable is correctly entered, the Screen Mode display appears.



```
Get, getNext, Add, Edit, Delete, Clear, Var-change, deFault(I=all), Quit,Refresh

#[ 1] ifIndex                    1
-[ 2] ifDescr                    "Ethernet Interface"
-[ 3] ifType                     ethernetCsmacd
-[ 4] ifMtu                      1500
-[ 5] ifSpeed                    10000000
-[ 6] ifPhysAddress              00 00 b0 00 00 00
*[ 7] ifAdminStatus              up
-[ 8] ifOperStatus               up
-[ 9] ifLastChange               0
-[10] ifInOctets                 0
-[11] ifInUcastPkts              0
-[12] ifInNUcastPkts             0
-[13] ifInDiscards               0
-[14] ifInErrors                 0
-[15] ifInUnknownProtos          0
-[16] ifOutOctets                31464
-[17] ifOutUcastPkts             92
-[18] ifOutNUcastPkts            0
-[19] ifOutDiscards              0

Enter Your Choice:
Variable instance found
```

Figure 4-3: Screen Mode Display

The screen layout is as follows:

Screen top line displays all the available commands. The upper case characters indicate the command keys.

Screen bottom line displays the command prompt. The command prompt varies according to the information required by the MCLI. In some cases a command is required, and in other cases variable values are prompted.

A numbered list of the working variable fields indicating the key fields and regular fields

If the variable is a table variable, the default value are displayed. If the variable is a scalar variable, no values are displayed.

Fields

Up to 19 fields are listed on the screen. If the variable has more than 19 fields, the **<Up>** and **<Down>** keys can be used to scroll though the full list. Scalar variables display a single field. Fields are marked to indicate the type of field (see ***Figure 4-3***):

# — Key fields

* — Mandatory fields

- — Read only fields

All field values can be modified including key fields, standard read/write fields and standard read only fields.

> ***Note:*** *Changing a value on the screen does not change the value in the MIB database. The commands* ***add***, ***edit*** *and* ***delete*** *change values on the MIB database.*

SNMP Commands

Simple Network Management Protocol (SNMP) commands are used to manage network nodes. The following commands are available in Screen Mode:

- Add (a)
- All-default (i)
- Clear (c)
- Default (f)
- Delete (d)
- Edit (e)
- Get (g)
- Get Next (n)
- Quit (q)
- Refresh (r)
- Var-change (v)

To use any command:

1. Complete the field values as required.
2. Enter a command from the list on the top of the screen (by entering the corresponding letter) and pressing **<Enter>.** For example ***a*** for the ***Add*** command.
3. Press **<Enter>**.

Instructions for specific commands are listed below.

Command—Add (a)

The ***Add*** command creates a new table variable.

To use the Add command:

1. Enter **all** key-fields and mandatory fields.
2. Ensure the field values are as required. Values entered into Read-only fields do not affect the Read-only field value. The methods of entering the field values are as follows:
   - Selecting the field and entering the value
   - Accept the default values
   - Use the ***Get*** or ***Get-Next*** command (see below)
   - Use the ***Clear*** command (see below)
   - Use the ***Default*** or ***All-default*** command (see below)
3. Enter the command ***a*** at the command prompt and press ***<Enter>.*** A confirmation prompt appears.
4. Press ***Y***. A new entry is added to the MIB database.

The following errors will cause the command to fail:

- The entry is duplicated
- The working variable is a scalar variable
- All mandatory and key-field values are not set

Command—All-default (i)

The ***All-default*** command displays all fields with their default values on the screen.

To use the All-default command:

- Enter the command ***i*** at the command prompt and press **<*Enter*>**.

After the values are set, the number of affected fields is displayed.

Command—Clear (c)

The ***clear*** command clears all the working variable field values displayed on the screen.

To use the Clear command:

- Enter the command ***c*** at the command prompt and press **<*Enter*>**.

Command—Default (f)

The ***Default*** command changes a field displayed on the screen to its default value.

To use the Default command:

1. Enter the command ***f*** at the command prompt and press **<*Enter*>**.
2. On the prompt select the field to set as the default value.
3. Press **<*Enter*>**.

The field is displayed on the screen with the default value. If the field does not have a default value, an error message is displayed.

Command—Delete (d)

The ***Delete*** command deletes a variable entry. A scalar variable cannot be deleted. ***Delete*** is an SNMP command.

To use the Delete command:

1. Enter **all** key-fields and press **<*Enter*>**.
2. Enter the command ***d*** at the command prompt and press **<*Enter*>.** A confirmation prompt appears.
3. Press ***Y***. The entry is deleted from the MIB database.

Command—Edit (e)

The ***Edit*** command modifies variable fields in the working variable. The ***Edit*** command modifies the MIB database.

To use the Edit command:

1. Enter **all** key-fields and press **<*Enter*>**.
2. Edit the fields using one of the following methods:
   - Accept the default values
   - Selecting the field and entering the value
   - Use the ***Get*** or ***Get-Next*** command (see below)
   - Use the ***Clear*** command (see above)

- Use the ***Default*** or ***All-default*** command (see above)

3. Enter the command ***e*** at the command prompt press <***Enter***>. The entry is edited and the MIB database is modified.

All key fields and mandatory fields must have values entered. Read-only fields are not affected.

The edit command will fail if all mandatory and key field values are not set.

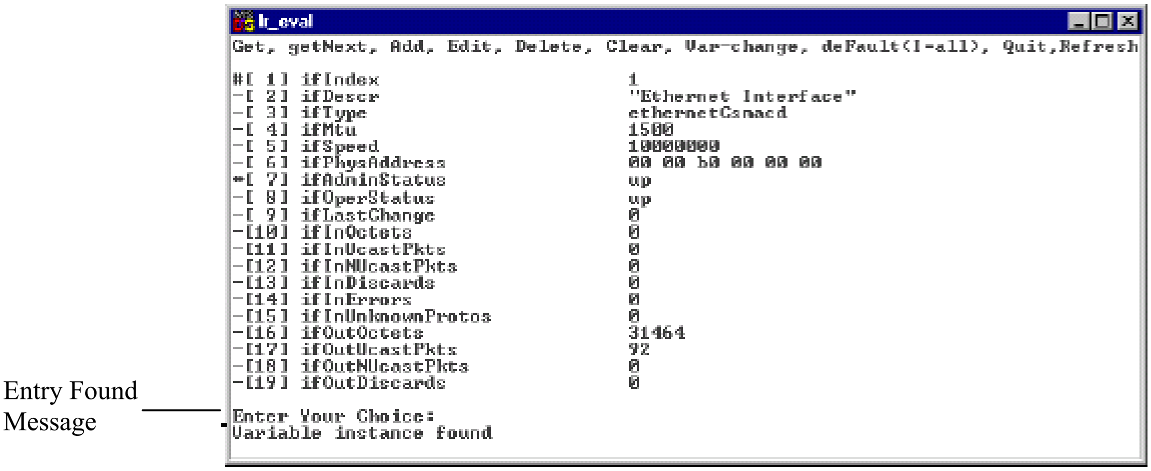
Command—Get (g)

The ***Get*** command retrieves variable entries that match key values. ***Get*** is an SNMP command.

The ***Get*** command uses the key fields as the search parameter.

To use the Get command:

1. Change the displayed key fields to the required entry key value.
2. Enter the command ***g*** at the command prompt press <***Enter***>. If the variable entry key fields match the search parameters, the corresponding entry variable field values are displayed. The following figure illustrates the "entry is found" message.



```
Get, getNext, Add, Edit, Delete, Clear, Var-change, deFault(I-all), Quit,Refresh

#[ 1] ifIndex                          1
-[ 2] ifDescr                          "Ethernet Interface"
-[ 3] ifType                           ethernetCsmacd
-[ 4] ifMtu                            1500
-[ 5] ifSpeed                          10000000
-[ 6] ifPhysAddress                    00 00 b0 00 00 00
*[ 7] ifAdminStatus                    up
-[ 8] ifOperStatus                     up
-[ 9] ifLastChange                     0
-[10] ifInOctets                       0
-[11] ifInUcastPkts                    0
-[12] ifInNUcastPkts                   0
-[13] ifInDiscards                     0
-[14] ifInErrors                       0
-[15] ifInUnknownProtos                0
-[16] ifOutOctets                      31464
-[17] ifOutUcastPkts                   92
-[18] ifOutNUcastPkts                  0
-[19] ifOutDiscards                    0

Enter Your Choice:
Variable instance found
```

Figure 4-4: Variable Entry Found and Displayed

If all the key fields are not given values for the search, the search is cancelled and an error message is displayed.

Note: *Scalar variables do not have key fields.*

Command—getNext (n)

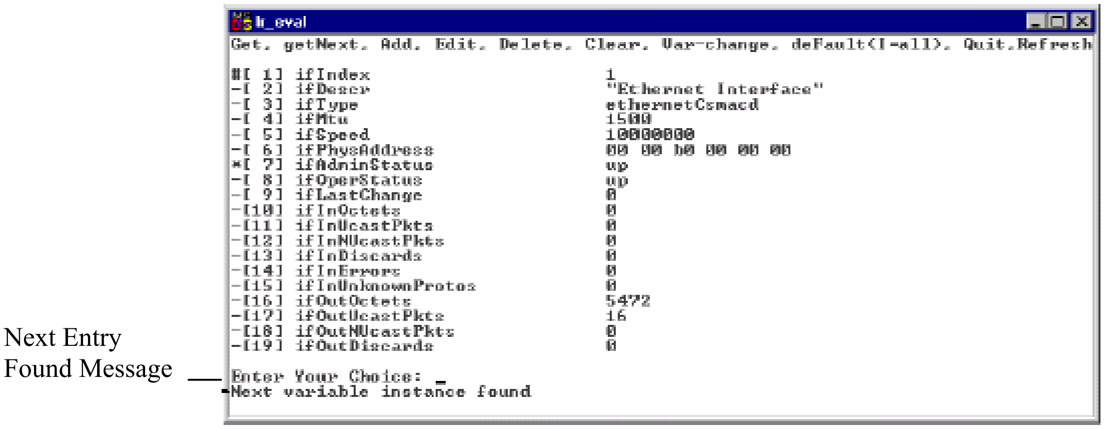
The ***getNext*** command displays the next variable entry on the screen. The order of entries in the table is based on the entry key values. The ***getNext*** command uses the displayed key values as the basis of retrieving the next entry in the table. ***getNext*** is an SNMP command.

To use the getNext command:

1. Change the displayed key fields to the required entry key value.
   getNext field values can be set as follows:
   - All key fields with no values
   - Some key fields with values
   - All key fields with values

Note: *To use a key field value, the lower numbered key fields* ***must*** *first be set.*

Enter the command ***n*** at the command prompt press **<*Enter*>**. If a "next" entry is found, this entry value is displayed on the screen. Pressing ***n*** again displays the next entry in the table. If the displayed entry is the last entry in the table, the message "End of MIB view" is displayed. The following figure illustrates the next entry retrieved with the ***getNext*** command.


lr_eval
Get. getNext. Add. Edit. Delete. Clear. Var-change. deFault(I-all). Quit.Refresh

```
#[ 1] ifIndex                          1
-[ 2] ifDescr                          "Ethernet Interface"
-[ 3] ifType                           ethernetCsmacd
-[ 4] ifMtu                            1500
-[ 5] ifSpeed                          10000000
-[ 6] ifPhysAddress                    00 00 b0 00 00 00
*[ 7] ifAdminStatus                    up
-[ 8] ifOperStatus                     up
-[ 9] ifLastChange                     0
-[10] ifInOctets                       0
-[11] ifInUcastPkts                    0
-[12] ifInNUcastPkts                   0
-[13] ifInDiscards                     0
-[14] ifInErrors                       0
-[15] ifInUnknownProtos                0
-[16] ifOutOctets                      5472
-[17] ifOutUcastPkts                   16
-[18] ifOutNUcastPkts                  0
-[19] ifOutDiscards                    0

Enter Your Choice: _
Next variable instance found
```

Next Entry
Found Message

Figure 4-5: Next Entry Found with getNext Command

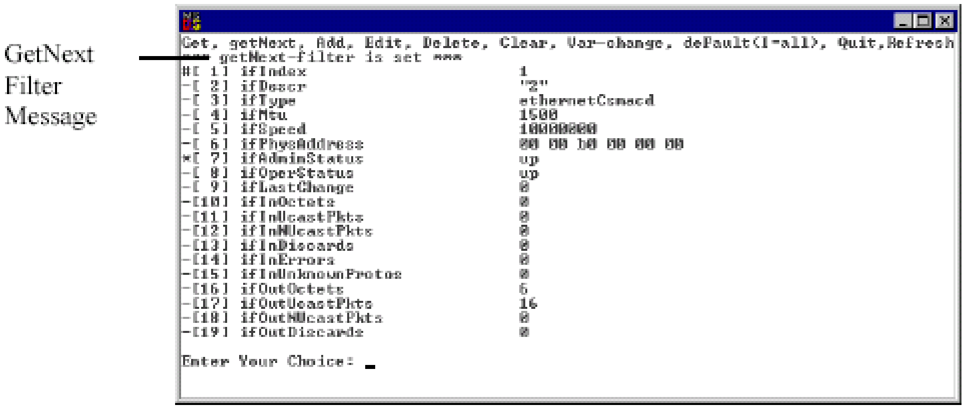
The ***get Next*** command can be used with or without a filter. The filter groups together, for the purposes of the ***getNext*** command, entries that comply with set field values. With a filter, the ***getNext*** command retrieves only entries that comply with the filter parameters.

To use the getNext filter perform the following:

- Enter the field values using the one of the following methods:
  - Select the field and enter the value
  - Accept the default value of a certain field
  - Accept the default value of all fields
  - Accept values displayed on the screen from a previous command, such as Add, Edit, Get and getNext.

The filter is automatically set and a ***getNext*** filter set message is displayed:

The following figure illustrates the message display.



```
Get, getNext, Add, Edit, Delete, Clear, Var-change, deFault(I-all), Quit,Refresh
*** getNext-filter is set ***
#[ 1] ifIndex                      1
-[ 2] ifDescr                      "2"
-[ 3] ifType                       ethernetCsmacd
-[ 4] ifMtu                        1500
-[ 5] ifSpeed                      10000000
-[ 6] ifPhysAddress                00 00 b0 00 00 00
*[ 7] ifAdminStatus                up
-[ 8] ifOperStatus                 up
-[ 9] ifLastChange                 0
-[10] ifInOctets                   0
-[11] ifInUcastPkts                0
-[12] ifInNUcastPkts               0
-[13] ifInDiscards                 0
-[14] ifInErrors                   0
-[15] ifInUnknownProtos            0
-[16] ifOutOctets                  6
-[17] ifOutUcastPkts               16
-[18] ifOutNUcastPkts              0
-[19] ifOutDiscards                0

Enter Your Choice: _
```

Figure 4-6: getNext Filter set Message

> ***Note:*** *The "getNext filter is set" message remains on the screen if the following commands are used, getNext, default and All default. If any other command is used, the filter is automatically removed***:**.

If a ***getNext*** filter is set, pressing ***n*** retrieves the next table entry whose parameter values matches the set filter values. If no value is matched, an "End of MIB view" is displayed, and the screen continues displaying the current entry.

Pressing **n** again uses the initial filter values to retrieve the next entry.

Command—Quit (q)

The ***Quit*** command quits Screen Mode and returns the user back to Line Mode.

To use the Quit command:

- Enter the command ***q*** at the command prompt and press **<*Enter*>**.

Command—Refresh (r)

The ***Refresh*** command refreshes the screen display.

To use the Refresh command:

- Enter the command ***r*** at the command prompt and press **<*Enter*>**.

The working variable screen is re-initialized. The default values are set and the ***getNext*** Filter is reset.

Command—Var-Change (V)

The ***Var-change*** command changes the working variable from within the Screen mode.

To use the Var-Change command:

1. Enter the command ***v*** at the command prompt and press **<*Enter*>**. The MCLI requests the name of the new MIB variable.
2. At the prompt enter the new MIB variable and press **<*Enter*>**.

The working variable is changed

Appendix A—MIB Object Reference

This appendix is a MIB object reference guide for system administrators (when using MCLI to manage a device via Telnet or a local terminal) and quality assurance teams when testing the NMS.

The variable name and its Object ID (OID) are listed in the left-hand column of each table. If the variable is a table field, the table variable is listed first, followed by the field variable name and the field's OID. When using the MCLI, you access fields via the table variable name.

Note: *This appendix is based on Marvell-based (Galileo) devices.*

File Parameters

Use the following variables to modify configuration file parameters.

Object/OID	Description	Field Name in NMS
RsSendConfigFile 1.3.6.1.4.1.171.26.5.3	Name and path of the file in which to save the device's current configuration.	File Name (Send Configuration to Device window)
RsGetConfigFile 1.3.6.1.4.1.171.26.5.4	Name and path of the file from which to update the device configuration.	File Name (Get Configuration From Device window)
rsFileServerAddress 1.3.6.1.4.1.171.26.5.6	The external TFTP server's IP address (when using a TFTP server other than the default TFTP server provided with the device).	External TFTP Server IP Address (Send Configuration to Device and Get Configuration From Device windows)

Object/OID	Description	Field Name in NMS
RsLoadSoftware 1.3.6.1.4.1.171.26.5.5	Name and path of the file from which to update the device software.	File Name (Update Device Software window)

Update Embedded Web Server Files

Object/OID	Description	Field Name in NMS
RsLoadSoftware 1.3.6.1.4.1.171.26.5.5	Name and path of the file from which to update the device software.	File Name (Update Embedded Web Server Files Window)
rsSoftwareDeviceName 1.3.6.1.4.1.171.26.5.7	The Software Device Name specifies a device name, using this Software.	Device Name (Update Embedded Web Server Files Window)
rlEmWebSetEWSfilesStatus 1.3.6.1.4.1.171.66.8	This variable sets the status of the embedded Web Server files to either closed or opened.	EWS Files Status (Update Embedded Web Server Files Window)

Device Parameters

Use the following variables to modify VLAN, port, GVRP, and global device parameters.

Global Parameters

Object/OID	Description	Field Name in NMS
SysDescr 1.3.6.1.2.1.1.1	General description of the devise.	Description (Identification tab)
SysName 1.3.6.1.2.1.1.5	User assigned device name.	Name (Identification tab)
SysLocation 1.3.6.1.2.1.1.6	Geographic location of the devise.	Location (Identification tab)
SysContact 1.3.6.1.2.1.1.4	The person(s) responsible for the device.	Contact Person (Identification tab)
SysUpTime 1.3.6.1.2.1.1.3	Time elapsed since the last reset.	System Up Time (Time tab)
RndManagedTime 1.3.6.1.4.1.171.2.8	Current user-defined device time (entered in the following format: *hours : minutes : seconds*).	System Time (Time tab)
RndManagedDate 1.3.6.1.4.1.171.2.9	Current user-defined device date (entered in the following format: *day : month : year*).	System date (Time tab)

Object/OID	Description	Field Name in NMS
RndBrgVersion 1.3.6.1.4.1.171.2.4	Version of software currently running on the device.	SW Version (Version tab)
genGroupHWVersion 1.3.6.1.4.1.171.2.11.1	Version of hardware currently operated by the device.	HW Version (Version tab)
ReaIpForwardEnable 1.3.6.1.4.1.171.29.7.4	If enabled, IP packets are forwarded via ASIC (hardware). If disabled, packets are forwarded through the CPU.	IP Fast Forward (FFT tab)
sw3IpForwardEnable 1.3.6.1.4.1.171.29.7.27.1.2		
sw3IpxForwardEnable 1.3.6.1.4.1.171.29.7.27.1.6	If enabled, IPX packets are forwarded via ASIC (hardware). If disabled, packets are forwarded through the CPU.	IPX Fast Forward (FFT tab)
reaIpxForwardEnable 1.3.6.1.4.1.171.29.7.5		
RlGalMode 1.3.6.1.4.1.171.56.2	Current GalNet mode, Base (G32iP) or Extended (G33iP).	GalNet Mode (GalNet Mode tab)

VLAN General Parameters

Object/OID	Description	Field Name in NMS
VlanSupportedType 1.3.6.1.4.1.171.48.3	The currently defined VLAN type, Per Port or Per Port/ Per Protocol.	VLAN supported type
vlanSupportedTypeAfterReset 1.3.6.1.4.1.171.48.20	VLAN type after reset, Per Port or Per Port/ Per Protocol.	VLAN supported type After Reset

VLAN Table

Object/OID	Description	Field Name in NMS
VlanTable vlanIfIndex 1.3.6.1.4.1.171.48.17.1.1	Parameter assigned by the NMS to specify logical interfaces with VLANs.	IF Num
VlanTable vlanName 1.3.6.1.4.1.171.48.17.1.6	VLAN name assigned by the user.	Name
VlanTable vlanPriority 1.3.6.1.4.1.171.48.17.1.8	VLAN priority as specified in a special 3-bit field. This field allows the tagged frames to carry the priority information.	Priority
VlanTable ifPhysAddress 1.3.6.1.2.1.2.2.1.6	By default, a VLAN (and each port in the VLAN) is assigned the MAC address of a device.	MAC Address

Object/OID	Description	Field Name in NMS
vlanTable vlanPhysAddressType 1.3.6.1.4.1.171.48.17.1.16	Default (a VLAN is assigned the MAC address of a device) or Reserved (a VLAN is assigned its individual MAC address).	Address Type
vlanTable vlanTag 1.3.6.1.4.1.171.48.17.1.7	VID of a VLAN.	Tag
No MIB associated with this NMS field.	Ports available to add to the VLAN.	Available Ports (Field appears in Insert Window)
No MIB associated with this NMS field.	MCLIck to remove port from VLAN.	Remove Port from VLAN (Field appears in Insert Window)
See “Tagging” below.	See “Tagging” below.	Enable port tagging (Field appears in Insert Window)
vlanPortsTable vlanPortPortIfIndex 1.3.6.1.4.1.171.48.18.1.2	The selected port’s interface number.	VLAN Port Number (Under Selected Ports in Insert Window)
virtualLanPortsTable vLPortIfIndex 1.3.6.1.4.1.171.27.2.1.2		
vlanPortsTable vlanPortType 1.3.6.1.4.1.171.48.18.1.4	Whether the port is static or dynamic.	VLAN Port Type (Under Selected Ports in Insert Window)
virtualLanPortsTable vLPortType 1.3.6.1.4.1.171.27.2.1.3		
vlanPortsTable vlanPortTaggedMode 1.3.6.1.4.1.171.48.18.1.3	Whether port tagging is enabled for this port.	Tagging (Under Selected Ports in Insert Window)
vlanPortsTable vlanPortForbiddenEgressPort 1.3.6.1.4.1.171.48.18.1.6	Use this variable to configure the port to receive packets but not send packets.	Forbidden Egress Port (Under Selected Ports in Insert Window)

User-Defined Ethernet VLANs

Object / Field / OID	Description	Field Name in NMS
vlanEthUserDefProtTable vlanEthUserDefProtName 1.3.6.1.4.1.171.48.14.1.4	The user defined name for the protocol.	Protocol Name

Object / Field / OID	Description	Field Name in NMS
vlanEthUserDefProtTable vlanEthUserDefProtType 1.3.6.1.4.1.171.48.14.1.2	The user-defined VLAN Ethernet type.	Ethernet Type

Port Properties

Object/OID	Description	Field Name in NMS
swIfTable swIfIndex 1.3.6.1.4.1.171.43.1.1.1	Selected port.	Select Port Number (Main tab)
ifTable ifPhysAddress 1.3.6.1.2.1.2.2.1.6	Media Access Control address of the interface. Each router is assigned a unique MAC address by the system.	MAC Address (Main tab)
swIfTable swIfType 1.3.6.1.4.1.171.43.1.1.10	The maximum capacity of the port.	MAX Capacity (Main tab)
rlPhDPortsTable rlPhDConnectorType 1.3.6.1.4.1.171.53.3.1.8	The type of connector used for this port, such as RJ45.	Connector Type (Main tab)
ifTable ifDescr 1.3.6.1.2.1.2.2.1.2	Brief description of interface, such as Ethernet.	Port Descriptor (Main tab)
swIfTable swIfSpeedAdminMode 1.3.6.1.4.1.171.43.1.1.15	From the list, choose the maximum transfer rate for the selected interface (for LAN interfaces only). Auto-negotiation mode should be disabled.	Speed Admin Mode (Main tab)
IfTable ifSpeed 1.3.6.1.2.1.2.2.1.5	The speed (bps) for which the port was configured.	Port Speed (bps) (Main tab)
ifTable ifAdminStatus 1.3.6.1.2.1.2.2.1.7	Controls whether traffic is allowed on this port. By default, traffic is allowed.	Admin Status (Main tab)
IfTable ifOperStatus 1.3.6.1.2.1.2.2.1.8	Whether the interface is operational (UP), non-operational (Down), or engaged in a test procedure so it does not carry traffic (Testing).	Port Status (Main tab)
swIfTable swIfDuplexAdminMode 1.3.6.1.4.1.171.43.1.1.3	Specify the conversation type for the interface.	Duplex Admin. Mode (Main tab)

Object/OID	Description	Field Name in NMS
swIfTable swIfDuplexOperMode 1.3.6.1.4.1.171.43.1.1.4	The mode for which the port was configured.	Duplex Operation Mode (Main tab)
swIfTable swIfPhysAddressType 1.3.6.1.4.1.171.43.1.1.2	Select *Default* to use the default address, or *Reserve* to assign a unique address (up to 264 unique addresses), in incrementing order.	Assign Physical Address (Main tab)
swIfTable swIfSpeedDuplexAutoNegotiation 1.3.6.1.4.1.171.43.1.1.16	Enables or disables autonegotiation.	Autonegotiation Mode (Main tab)
swIfTable swIfBackPressureMode 1.3.6.1.4.1.171.43.1.1.5	When Back Pressure mode is enabled, the device signals the corresponding device to hold traffic when a specific speed is reached. This feature is disabled by default.	Back Pressure Mode (Other tab)
swIfTable swIfFlowControlMode 1.3.6.1.4.1.171.43.1.1.14	Determines the flow control. Auto-negotiation is the default mode. In this mode, the port sends the accompanying device Flow Control packets, when supported by the corresponding device. In ON mode, the flow control mechanism is active regardless of the behavior of the corresponding device. In OFF mode, this feature is disabled completely.	Flow Control Mode (Other tab)
rsIpAddrTable rsIpAdEntAddr 1.3.6.1.4.1.171.26.1.1.1	IP address for the selected port.	IP Address (IP tab)
rsIpAddrTable rsIpAdEntNetMask 1.3.6.1.4.1.171.26.1.1.3	Network Mask for the selected port.	Network Mask (IP tab)
ipxCircTable ipxCircNetNumber 1.3.6.1.4.1.171.12.5.1.1.6	IPX network address for the selected port.	Network Address (IPX tab)
ipxCircTable ipxCircEncaps 1.3.6.1.4.1.171.12.5.1.1.8	IPX Layer II protocol for the selected port.	Layer II Protocol (IPX tab)
rsIpAddrTable rsIpAdEntIfIndex 1.3.6.1.4.1.171.26.1.1.2	The VLAN number.	If Num (VLAN tab)
vlanTable vlanName 1.3.6.1.4.1.171.48.17.1.6	The VLAN name.	Name (VLAN tab)

Object/OID	Description	Field Name in NMS
vlanTable ifPhysAddress 1.3.6.1.2.1.2.2.1.6	The VLAN MAC address.	MAC Address (VLAN tab)

Port Mirroring

Object/OID	Description	Field Name in NMS
rsMonitPort 1.3.6.1.4.1.171.41.2	Use this variable to configure the port as mirrored.	Mirrored Port
rsCopyPort 1.3.6.1.4.1.171.41.1	The number of log entries the device stores before overwriting the first entry. Log entries are stored until the device is reset.	Copy Port

GVRP (GARP VLAN Registration Protocols) General Parameters

Object/OID	Description	Field Name in NMS
dot1qGvrpStatus 1.3.6.1.2.1.17.7.1.1.5	Disables or enables the feature on the device.	GVRP Status (Device Parameters tab)
dot1dBasePortTable dot1dBasePort 1.3.6.1.2.1.17.1.4.1.1	The index number of the active port.	Port (Port Parameters tab)
dot1qPortVlanTable dot1qPortGvrpStatus 1.3.6.1.2.1.17.7.1.4.5.1.4	Enables or disables GVRP per the individual port.	Port GVRP Status (Port Parameters tab)

GVRP Timers Control

Object/OID	Description	Field Name in NMS
dot1dBasePortTable dot1dBasePort 1.3.6.1.2.1.17.1.4.1.1	The index number of the active port.	Port
rlPortGvrpTimersTable rlPortGvrpJoinTime 1.3.6.1.4.1.171.64.1.1.1	Join Time in centiseconds (default 20).	Join Time (milliseconds)
rlPortGvrpTimersTable rlPortGvrpLeaveTime 1.3.6.1.4.1.171.64.1.1.2	Leave Time in centiseconds (default 60).	Leave Time (milliseconds)

Object/OID	Description	Field Name in NMS
rlPortGvrpTimersTable rlPortGvrpLeaveAllTime 1.3.6.1.4.1.171.64.1.1.3	Leave All Time in centiseconds (default 1000).	Leave All Time (milliseconds)

GVRP Information

Object/OID	Description	Field Name in NMS
dot1dBasePortTable dot1dBasePort 1.3.6.1.2.1.17.1.4.1.1	Active port IfIndex number.	Port
dot1qPortVlanTable dot1qPortGvrpStatus 1.3.6.1.2.1.17.7.1.4.5.1.4	The GVRP status of the port.	Port GVRP Status
dot1qPortVlanTable dot1qPortGvrpFailedRegistrations 1.3.6.1.2.1.17.7.1.4.5.1.5	The total number of failed GVRP registrations, for any reason.	Failed Registrations
dot1qPortVlanTable dot1qPortGvrpLastPduOrigin 1.3.6.1.2.1.17.7.1.4.5.1.6	The Source MAC Address of the last GVRP message received on this port.	Last PDU Origin

Trunk Parameters

Object/OID	Description	Field Name in NMS
rlDot3adAggNumOfTrunks 1.3.6.1.4.1.171.65.3	The number of trunks supported by the device.	Aggregate Number Of Trunks (Trunk Parameters Window)
rlDot3adAggMaxPortsInTrunks 1.3.6.1.4.1.171.65.4	The maximum number of ports permitted in a trunk.	Aggregate Max Ports In Trunks (Trunk Parameters Window)
rlDot3adAggMibVersion 1.3.6.1.4.1.171.65.1	MIB's version. The current version is 2.	MIB Version (Trunk Parameters Window)

Trunk Table

Object/OID	Description	Field Name in NMS
dot3adAggEntry 1.2.840.802.10006.300.43.1.1.1.1	A list of the Aggregator parameters. This is indexed by the ifIndex of the Aggregator.	
dot3adAggIndex 1.2.840.802.10006.300.43.1.1.1.1.1	Indicates the Trunk ifIndex.	Index (TRUNK Table Window)
dot3adAggMACAddress 1.2.840.802.10006.300.43.1.1.1.1.2	Indicates the MAC Address of the Trunk.	Trunk MAC Address (TRUNK Table Window)

Object/OID	Description	Field Name in NMS
dot3adAggActorSystemPriority 1.2.840.802.10006.300.43.1.1.1.1.3	A 2-octet read-write value indicating the priority value associated with the Actor's System ID.	
dot3adAggActorSystemID 1.2.840.802.10006.300.43.1.1.1.1.4	A 6-octet read-write MAC address value used as a unique identifier for the System that contains this Aggregator.	
dot3adAggAggregateOrIndividual 1.2.840.802.10006.300.43.1.1.1.1.5	A read-only Boolean value indicating whether the Aggregator represents an Aggregate ('TRUE') or an Individual link ('FALSE').	
dot3adAggActorAdminKey 1.2.840.802.10006.300.43.1.1.1.1.6	The current administrative value of the Key for the Aggregator. The administrative Key value may differ from the operational Key value for the reasons discussed in 43.6.2. This is a 16-bit, read-write value. The meaning of particular Key values is of local significance.	
dot3adAggActorOperKey 1.2.840.802.10006.300.43.1.1.1.1.7	The current operational value of the Key for the Aggregator. The administrative Key value may differ from the operational Key value for the reasons discussed in 43.6.2. This is a 16-bit, read-only value. The meaning of particular Key values is of local significance.	
dot3adAggPartnerSystemID 1.2.840.802.10006.300.43.1.1.1.1.8	A 6-octet read-only MAC address value consisting of the unique identifier for the current protocol Partner of this Aggregator. A value of zero indicates that there is no known Partner. If the aggregation is manually configured, this System ID value will be a value assigned by the local System.	
dot3adAggPartnerSystemPriority 1.2.840.802.10006.300.43.1.1.1.1.9	A 2-octet read-only value that indicates the priority value associated with the Partner's System ID. If the aggregation is manually configured, this System Priority value will be a value assigned by the local System.	
dot3adAggPartnerOperKey 1.2.840.802.10006.300.43.1.1.1.1.10	The current operational value of the Key for the Aggregator's current protocol Partner. This is a 16-bit, read-only value. If the aggregation is manually configured, this Key value will be a value assigned by the local System.	
dot3adAggCollectorMaxDelay 1.2.840.802.10006.300.43.1.1.1.1.11	The value of this 16-bit read-write attribute defines the maximum delay, in tens of microseconds, that may be imposed by the Frame Collector between receiving a frame from an Aggregator Parser, and either delivering the frame to its MAC MCLIent or discarding the frame (see 43.2.3.1.1).	
dot3adAggPortListEntry 1.2.840.802.10006.300.43.1.1.2.1	A list of the ports associated with a given Aggregator. This is indexed by the ifIndex of the Aggregator.	
dot3adAggPortEntry 1.2.840.802.10006.300.43.1.2.1.1	A list of Link Aggregation Control configuration parameters for each Aggregation Port on this device.	

Object/OID	Description	Field Name in NMS
dot3adAggPortIndex 1.2.840.802.10006.300.43.1.2.1.1.1	The ifIndex of the port	
dot3adAggPortActorAdminKey 1.2.840.802.10006.300.43.1.2.1.1.4	The current administrative value of the Key for the Aggregation Port. This is a 16-bit, read-write value. The meaning of particular Key values is of local significance.	
dot3adAggPortAttachedAggID 1.2.840.802.10006.300.43.1.2.1.1.13	The identifier value of the Aggregator that this Aggregation Port is currently attached to. Zero indicates that the Aggregation Port is not currently attached to an Aggregator. This value is read-only.	
dot3adAggPortAggregateOrIndividual 1.2.840.802.10006.300.43.1.2.1.1.24	A read-only Boolean value indicating whether the Aggregation Port is able to Aggregate ('TRUE') or is only able to operate as an Individual link (' FALSE').	
swIfEntry 1.3.6.1.4.1.171.43.1.1	Defines the contents of each line in the swIfTable table.	
swIfIndex 1.3.6.1.4.1.171.43.1.1.1	Index to the swIfTable. The interface defined by a particular value of this index is the same interface as identified by the same value of ifIndex (MIB II).	
swIfPhysAddressType 1.3.6.1.4.1.171.43.1.1.2	This variable indicates whether the physical address assigned to this interface should be the default one or be chosen from the set of reserved physical addresses of the device.	
rlDot3adAggMaxPortsInTrunks 1.3.6.1.4.1.171.65.4	The maximum number of ports in a trunk.	

Trunking Port Table

Object/OID	Description	Field Name in NMS
dot3adAggPortEntry 1.2.840.802.10006.300.43.1.2.1.1	Trunking Port Table Entry.	
dot3adAggPortIndex 1.2.840.802.10006.300.43.1.2.1.1.1	Port interface index.	Index (Trunking Port Table Window)
dot3adAggPortActorSystemID 1.2.840.802.10006.300.43.1.2.1.1.3	Read-only MAC address value that defines the System ID value for the system that contains this Aggregate port.	Actor System ID (Trunking Port Table Window)
dot3adAggPortActorAdminKey 1.2.840.802.10006.300.43.1.2.1.1.4	The Key administrative value for the Aggregation Port.	Actor Admin Key (Trunking Port Table Window)
dot3adAggPortAttachedAggID 1.2.840.802.10006.300.43.1.2.1.1.13	The Aggregator identifier value that this Aggregation Port is attached.	Attached Agg ID (Trunking Port Table Window)
dot3adAggPortAggregateOrIndividual 1.2.840.802.10006.300.43.1.2.1.1.24	Indicates whether the Aggregation Port belongs to any trunk (True) or not (False).	Aggregate Or Individual (Trunking Port Table Window)

TRUNK Balance Table

Object/OID	Description	Field Name in NMS
rlDot3adAggBalanceEntry 1.3.6.1.4.1.171.65.2.1	Trunk Balance Table Entry.	
rlDot3adAggBalanceForwardType 1.3.6.1.4.1.171.65.2.1.1	Balances the trunk in either 1 of 2 modes. The possible values are: Bridging | Routing	Forward Type (Trunk Balance Table)
rlDot3adAggBalanceLayer 1.3.6.1.4.1.171.65.2.1.2	Specifies the Balance Layer that the trunk used for the specified Forward Type.	Layer (Trunk Balance Table)
rlDot3adAggBalanceUsedAddresses 1.3.6.1.4.1.171.65.2.1.3	Specifies the network layer addresses used for balancing unicast frames.	Used Addresses (Trunk Balance Table)
rlDot3adAggBalanceBroadcastType 1.3.6.1.4.1.171.65.2.1.4	Specifies the criterion used for balancing L2 broadcast and unknown frames.	Broadcast Type (Trunk Balance Table)
dot3adAggIndex 1.2.840.802.10006.300.43.1.1.1.1.1	Identifies the trunk number.	Index (Trunk Balance Table)

Bridge Parameters

Use the following variables to modify the system operating parameters, unicast tables, multicast tables, and spanning tree tables.

Operating Parameters

Object/OID	Description	Field Name in NMS
rndBasePhysicalAddress 1.3.6.1.4.1.171.2.12	The device’s MAC address.	Bridge Address
rndBridgeType 1.3.6.1.4.1.171.2.1	Types of bridging the device can perform.	Bridge Type
dot1dTpAgingTime 1.3.6.1.2.1.17.4.2	The number of seconds the learned entries remain in the *Forwarding Table*. The counter is reset each time the entry is used. After this time, entries are deleted from the table. There is a minimum 10 second period.	Forwarding Table Aging Time

Unicast Global Forwarding Table

Object/OID	Description	Field Name in NMS
dot1qFdbTable dot1qFdbId 1.3.6.1.2.1.17.7.1.2.1.1.1	The node’s ID.	VLAN ID

Object/OID	Description	Field Name in NMS
dot1qTpFdbTable dot1qTpFdbAddress 1.3.6.1.2.1.17.7.1.2.2.1.1	The node’s MAC address.	MAC Address
dot1qTpFdbTable dot1qTpFdbPort 1.3.6.1.2.1.17.7.1.2.2.1.2	Port through which the node is learned. That is, the port through which frames are received from this entry.	Port
dot1qTpFdbTable dot1qTpFdbStatus 1.3.6.1.2.1.17.7.1.2.2.1.3	The node’s status: Learned (automatically learned), Self (the entry is a port on the device, Mgmt (the entry is a static node manually entered using the insert button, or Other (the Node status cannot be described by one of the above).	Status

Unicast Global Forwarding Table Size

Object/OID	Description	Field Name in NMS
dot1qFdbTable dot1qFdbId 1.3.6.1.2.1.17.7.1.2.1.1.1	VLAN identifier that uniquely identifies the VLAN.	VLAN ID
dot1qFdbTable dot1qFdbDynamicCount 1.3.6.1.2.1.17.7.1.2.1.1.2	The number of entries per VLAN.	No. of Entries

MAC Multicast Enable

Object/OID	Description	Field Name in NMS
rlMacMulticastEnable 1.3.6.1.4.1.171.55.1	Enable/Disable MAC Multicast bridging in the device.	MAC Multicast Enable

Multicast Forwarding Table

Object/OID	Description	Field Name in NMS
dot1qVlanCurrentTable dot1qVlanIndex 1.3.6.1.2.1.17.7.1.4.2.1.2	VLAN identifier that uniquely identifies the VLAN to which a frame belongs, and for which this entry contains information on Multicast group MAC addresses.	VLAN ID
dot1qTpGroupTable dot1qTpGroupAddress 1.3.6.1.2.1.17.7.1.2.3.1.1	The destination Group MAC address in a frame to which this entry filtering information applies.	MAC Address
dot1qTpGroupTable dot1qTpGroupEgressPorts 1.3.6.1.2.1.17.7.1.2.3.1.2	The complete set of ports in this VLAN, to which frames destined for this group MAC address are being explicitly forwarded. This does not include ports for which this address is only implicitly forwarded. These ports are configured through SNMP.	Egress Ports

Object/OID	Description	Field Name in NMS
dot1qTpGroupTable dot1qTpGroupLearnt 1.3.6.1.2.1.17.7.1.2.3.1.3	The subset of ports, listed in the in Group Egress Ports list that were learnt by the IGMP Snooping dynamic mechanism into this Multicast Filtering database.	Learnt

Multicast Forward All

Object/OID	Description	Field Name in NMS
dot1qForwardAllEntry 1.3.6.1.2.1.17.7.1.2.4.1	Forwarding information for a VLAN, specifying the set of ports to which all multicasts should be forwarded, configured statically by management or dynamically by GMRP.	
dot1qVlanIndex 1.3.6.1.2.1.17.7.1.4.2.1.2	The VLAN-ID or other identifier referring to this VLAN.	VLAN ID
dot1qForwardAllPorts 1.3.6.1.2.1.17.7.1.2.4.1.1	The complete set of ports in this VLAN to which all multicast group-addressed frames are to be forwarded. This includes ports for which this need has been determined dynamically by GMRP, or configured statically by management.	Egress Ports
dot1qForwardAllStaticPorts 1.3.6.1.2.1.17.7.1.2.4.1.2	The set of ports configured by management in this VLAN to which all multicast group-addressed frames are to be forwarded. Ports entered in this list will also appear in the complete set shown by dot1qForwardAllPorts. This value will be restored after the device is reset. This only applies to ports that are members of the VLAN, defined by dot1qVlanCurrentEgressPorts. A port may not be added in this set if it is already a member of the set of ports in dot1qForwardAllForbiddenPorts. The default value is a string of ones of appropriate length, to indicate standard non-EFS behavior, i.e. forward all multicasts to all ports.	Static Ports
dot1qForwardAllForbiddenPorts 1.3.6.1.2.1.17.7.1.2.4.1.3	The set of ports configured by management in this VLAN for which the Service Requirement attribute Forward All Multicast Groups may not be dynamically registered by GMRP. This value will be restored after the device is reset. A port may not be added in this set if it is already a member of the set of ports in dot1qForwardAllStaticPorts. The default value is a string of zeros of appropriate length.	Forbidden Ports

MAC Multicast Forward Unregistered

Object/OID	Description	Field Name in NMS
dot1qForwardUnregisteredEntry 1.3.6.1.2.1.17.7.1.2.5.1	Forwarding information for a VLAN, specifying the set of ports to which all multicasts for which there is no more specific forwarding information shall be forwarded. This is configured statically by management or dynamically by GMRP.	
dot1qVlanIndex 1.3.6.1.2.1.17.7.1.4.2.1.2	The VLAN-ID or other identifier referring to this VLAN.	VLAN ID

Object/OID	Description	Field Name in NMS
dot1qForwardUnregisteredPorts 1.3.6.1.2.1.17.7.1.2.5.1.1	The complete set of ports in this VLAN to which multicast group-addressed frames for which there is no more specific forwarding information will be forwarded. This includes ports for which this need has been determined dynamically by GMRP, or configured statically by management.	Egress Ports
dot1qForwardUnregisteredStatic Ports 1.3.6.1.2.1.17.7.1.2.5.1.2	The set of ports configured by management, in this VLAN, to which multicast group-addressed frames for which there is no more specific forwarding information are to be forwarded. Ports entered in this list will also appear in the complete set shown by dot1qForwardUnregisteredPorts. This value will be restored after the device is reset. The default value is a string of zeros of appropriate length, although this has no effect with the default value of dot1qForwardAllStaticPorts.	Static Ports
dot1qForwardUnregisteredForbid denPorts 1.3.6.1.2.1.17.7.1.2.5.1.3	The set of ports configured by management in this VLAN for which the Service Requirement attribute Forward Unregistered Multicast Groups may not be dynamically registered by GMRP. This value will be restored after the device is reset. The default value is a string of zeros of appropriate length.	Forbidden Ports

Multicast Static Table

Object/OID	Description	Field Name in NMS
dot1qVlanCurrentTable dot1qVlanIndex 1.3.6.1.2.1.17.7.1.4.2.1.2	VLAN identifier that uniquely identifies the VLAN to which a frame belongs and for which this entry contains information on Multicast group MAC addresses.	VLAN ID
dot1qStaticMulticastTable dot1qStaticMulticastAddress 1.3.6.1.2.1.17.7.1.3.2.1.1	The destination MAC address in a frame to which this entry filtering information applies.	Multicast Address
dot1qStaticMulticastTable dot1qStaticMulticastReceiveP ort 1.3.6.1.2.1.17.7.1.3.2.1.2	Based on the source ports for packets received, filtering is applied. All refers to all packets or a specific port is selected.	Receive Ports
dot1qStaticMulticastTable dot1qStaticMulticastStaticEgre ssPorts 1.3.6.1.2.1.17.7.1.3.2.1.3	The set of ports to which frames received from a specific port and destined for a specific Multicast MAC address must always be forwarded, regardless of any dynamic information e.g. from IGMP Snooping. A port may not be added in this set if it is already a member of the set of ports in the Static Multicast Forbidden Egress Ports list.	Static Ports
dot1qStaticMulticastTable dot1qStaticMulticastForbidden EgressPorts 1.3.6.1.2.1.17.7.1.3.2.1.4	The set of ports to which frames received from a specific port and destined for a specific Multicast MAC address must not be forwarded, regardless of any dynamic information e.g. from IGMP Snooping. A port may not be added in this set if it is already a member of the set of ports in the Static Multicast Static Egress Ports list.	Forbidden Ports

Object/OID	Description	Field Name in NMS
dot1qStaticMulticastTable dot1qStaticMulticastStatus 1.3.6.1.2.1.17.7.1.3.2.1.5	Indicates the status of this entry. Options are: **Permanent—**The entry is currently in use and will remain in use after a bridge reset. **Delete On Reset—**The entry is currently in use until the next bridge reset. **Delete On Timeout—**The entry is currently in use until it is aged out.	Status

Spanning Tree Parameters

Object/OID	Description	Field Name in NMS
rldot1dStpEnable 1.3.6.1.4.1.171.57.2.3	Indicates whether STP should run on the device. This is a system-wide proprietary parameter disabled by default.	Global STP Status (General tab)
dot1dStpProtocolSpecification 1.3.6.1.2.1.17.2.1	Indicates the IEEE standard in use.	Protocol Specification (General tab)
rldot1dStpType 1.3.6.1.4.1.171.57.2.2	Indicates the mode of maintaining the STP database, per device or per VLAN.	STP Type (General tab)
rldot1dStpPortMustBelongToVlan 1.3.6.1.4.1.171.57.2.4	This parameter is relevant for per-device mode only. The values are as follows: **True—**Each port that is defined within a VLAN is participating in the STP (default value). **False—**All ports on the device participates in the STP.	Must Belong To VLAN (General tab)
dot1dStpPriority 1.3.6.1.2.1.17.2.2	The Bridge priority within the Spanning Tree. The bridge with the lowest value has the highest priority, and is the root.	Bridge Priority (General tab)
dot1dStpBridgeMaxAge 1.3.6.1.2.1.17.2.12	Identifies the interval a bridge that waits for the receipt of a hello packet before initiating a topology change. It is the time interval that determines when to discard a Configuration Message (CM). This parameter is configured on all the bridges participating in the STP but only the one belonging to the elected Root Bridge is used. **Note:** It is strongly recommended that: Max age is greater or equal to Hello time x 2 + 1.0s.	Bridge Max Age (Seconds) (General tab)
dot1dStpBridgeHelloTime 1.3.6.1.2.1.17.2.13	Identifies the interval of time between each CM sent by the Root Bridge. This interval is configured on all bridges participating in the STP, but is only relevant to the Root Bridge. **Note:** Shortening the recommended 2-second period makes the protocol more robust, but the loss of CMs is high. Lengthening this time lowers the overhead of the algorithm (because the interval between transmission of CMs will be larger).	Bridge Hello Time (Seconds) (General tab)

Object/OID	Description	Field Name in NMS
dot1dStpBridgeForwardDelay 1.3.6.1.2.1.17.2.14	Identifies the time interval a bridge waits (by being in the listening and learning states) before forwarding data packets. This parameter is configured on all the bridges participating in the STP. Only the parameter elected to the Root Bridge is used. **Note:** It is strongly recommended that: 2 x Bridge Forward Delay is greater or equal to Max age	Bridge Forward Delay (Seconds) (General tab)
rldot1dStpMibVersion 1.3.6.1.4.1.171.57.2.1	The installed STP version.	STP MIB Version (Tuning Parameter tab)
dot1dStpPriority 1.3.6.1.2.1.17.2.2	The Bridge Priority value can be used to influence the choice of root and designated bridges; a lower numerical value for bridge priority makes the bridge more likely to become the root. The value of this parameter is not learned from the network and is device specific.	Bridge Priority (Tuning Parameter tab)
dot1dBaseBridgeAddress 1.3.6.1.2.1.17.1.1	The value is part of a Bridge Identifier. This parameter is individual for each device and is not contained in CM. The STP requires that a single unique identifier (Bridge Identifier) be associated with each Bridge transmitting CMs.	Bridge Address (Tuning Parameter tab)
No MIB associated with this NMS field.	The Root Bridge priority within the Spanning Tree. This value is used as part of the Root Identifier parameter in all CMs originated by this node.	Designated Root Priority (Tuning Parameter tab)
No MIB associated with this NMS field.	The Root Bridge MAC address within the Spanning Tree. This value is used as part of the Root Identifier parameter.	Designated Root Address (Tuning Parameter tab)
dot1dStpRootCost 1.3.6.1.2.1.17.2.6	The cost of the path from this Bridge to the Root Bridge. This value is used as part of the Root Identifier parameter.	Root Path Cost (Tuning Parameter tab)
dot1dStpRootPort 1.3.6.1.2.1.17.2.7	The port number which offers the lowest cost path from this bridge to the Root Bridge. It is not significant when the Bridge is the Root, and is set to zero	Root Port (Tuning Parameter tab)
dot1dStpTimeSinceTopologyChange 1.3.6.1.4.1.171.57.2.6.1.3	The time (in seconds) since the last time a topology change was detected by the bridged community.	Topology Change Time (Tuning Parameter tab)
dot1dStpTopChanges 1.3.6.1.4.1.171.57.2.6.1.4	The total number of topology changes detected by this bridge since the manageable bridged community was last reset or initialized.	Topology Changes Count (Tuning Parameter tab)
dot1dStpMaxAge 1.3.6.1.4.1.171.57.2.6.1.8	The maximum age of STP information learned from the network on any port before it is discarded, in seconds. Identifies the timeout value used by all Bridges. This ensures that each Bridge has a consistent value against which to test the age of stored configuration information.	Max Age (Sec) (Tuning Parameter tab)
dot1dStpHelloTime 1.3.6.1.4.1.171.57.2.6.1.9	Defines the time period to elapse between the transmission of CMs through a given port. This value is learned from the network	Hello Time (Sec) (Tuning Parameter tab)

Object/OID	Description	Field Name in NMS
dot1dStpHoldTime 1.3.6.1.4.1.171.57.2.6.1.10	Defines the minimum time period to elapse between the transmission of CMs through a given port. At most, one CM shall be transmitted in any Hold Time period. This value is learned from the network.	Hold Time (Sec) (Tuning Parameter tab)
dot1dStpForwardDelay 1.3.6.1.4.1.171.57.2.6.1.11	Identifies the timeout value to be used by all Bridges as learned from the network. This time value, measured in seconds, controls how fast a port changes its spanning state when moving towards the Forwarding State. The value determines how long the port stays in each of the Listening and Learning states, which precede the Forwarding State. This value is also used, when a topology change has been detected and is underway, to age all dynamic entries in the Forwarding Database. The parameter ensures that each Bridge uses a consistent value for the Forward Delay Timer when changing the State of a Port to the Forwarding State.	Forward Delay (Sec) (Tuning Parameter tab)

Spanning Tree Port Table

Object/OID	Description	Field Name in NMS
rldot1wRStpVlanEdgePortTable rldot1wRStpVlanEdgePortPort 1.3.6.1.4.1.171.57.4.1.1.2	The port number.	Port
rldot1wRStpForceVersionTable rldot1wRStpForceVersionState 1.3.6.1.4.1.171.57.4.2.1.2	The Priority value can be used to influence the choice of port when a bridge has two ports connected in a loop.	Priority
rldot1wRStpVlanEdgePortTable rldot1wRStpEdgePortStatus 1.3.6.1.4.1.171.57.4.1.1.3	The port current state as defined by the STP. This state dictates what action a port takes on reception of a frame. Each STP enabled port can be in one of the following states: blocking, listening, learning, or forwarding.	Port State
dot1dStpPortTable dot1dStpPortEnable 1.3.6.1.2.1.17.2.15.1.4	STP enabled or disabled. If a port has the STP status disabled - it goes to down.	Port Enable
dot1dStpPortTable dot1dStpPortPathCost 1.3.6.1.2.1.17.2.15.1.5	The cost added to the root path cost field contained in a configuration BPDU received by this port. This is to determine the cost of the path to the root through this port.	Path Cost
dot1dStpPortTable dot1dStpPortDesignatedRoot 1.3.6.1.2.1.17.2.15.1.6	Designated Bridge transmits with priority a unique Bridge Identifier as the Root in the CMs and includes the Designated Bridge MAC address.	Designated Root
dot1dStpPortTable dot1dStpPortDesignatedCost 1.3.6.1.2.1.17.2.15.1.7	The Designated Port path cost of network segments connected to this port. This value is compared to the Root Path Cost field in received CMs.	Designated Cost

Object/OID	Description	Field Name in NMS
dot1dStpPortTable dot1dStpPortDesignatedBridge 1.3.6.1.2.1.17.2.15.1.8	The Bridge Identifier that this port considers to be the Designated Bridge for this port segment with priority.	Designated Bridge
dot1dStpPortTable dot1dStpPortDesignatedPort 1.3.6.1.2.1.17.2.15.1.9	The Port Identifier on the Designated Bridge for this port LAN segment.	Port Designated Port
dot1dStpPortTable dot1dStpPortForwardTransitions 1.3.6.1.2.1.17.2.15.1.10	The number of times this port has transitioned from the Learning State to the Forwarding State.	Forward Transitions

Rapid Spanning Tree Ports Table

Object/OID	Description	Field Name in NMS
rldot1wRStpVlanEdgePortTable rldot1wRStpVlanEdgePortVlan 1.3.6.1.4.1.171.57.4.1.1.1	The VLAN number that the port belongs to, which also contains Spanning Tree Protocol management information.	VLAN
rldot1wRStpVlanEdgePortTable rldot1wRStpVlanEdgePortPort 1.3.6.1.4.1.171.57.4.1.1.2	The port containing Spanning Tree Protocol management information.	Port
rldot1wRStpVlanEdgePortTable rldot1wRStpEdgePortStatus 1.3.6.1.4.1.171.57.4.1.1.3	Specifies whether this port is an Edge Port. Potential values are True or False (default).	Status

Rapid Spanning Tree Force Version Table

Object/OID	Description	Field Name in NMS
rldot1wRStpForceVersionTable rldot1wRStpForceVersionVlan 1.3.6.1.4.1.171.57.4.2.1.1	The VLAN number that the port belongs to, which also contains Spanning Tree Protocol management information.	VLAN
rldot1wRStpForceVersionTable rldot1wRStpForceVersionState 1.3.6.1.4.1.171.57.4.2.1.2	Specifies whether this Bridge uses the normal RSTP algorithm, or the STP Compatibility algorithm.	State

MAC Multicast Parameters

Object/OID	Description	Field Name in NMS
rlMacMulticastEnable 1.3.6.1.4.1.171.55.1	Enables MAC Multicast Filtering Services on a device (True/False).	MAC Multicast Filtering Enable
rlIgmpSnoopMibVersion 1.3.6.1.4.1.171.55.2.1	Specifies the current MIB set used for this feature.	IGMP Snooping MIB Version
rlIgmpSnoopEnable 1.3.6.1.4.1.171.55.2.2	Enables Dynamic learning based on IGMP (True/False).	IGMP Snooping Enable
rlIgmpSnoopHostAgingTime 1.3.6.1.4.1.171.55.2.3	The amount of time that passes before aging out an entry in the MAC Multicast Group table.	IGMP Snooping Host Aging Time (Seconds)
rlIgmpSnoopRouterAgingTime 1.3.6.1.4.1.171.55.2.4	The amount of time that passes before aging out an entry in the MAC Multicast Router table.	IGMP Snooping Router Aging Time (Seconds)

MAC Multicast Group Table

Object/OID	Description	Field Name in NMS
rlIgmpSnoopGroupTable rlIgmpSnoopGroupTag 1.3.6.1.4.1.171.55.2.5.1.1	Identifies the VLAN to which a frame belongs and for which this entry contains information on Multicast group MAC addresses.	Tag
rlIgmpSnoopGroupTable rlIgmpSnoopGroupPort 1.3.6.1.4.1.171.55.2.5.1.2	Port number specifying a physical port in the VLAN on which the information concerning multicast groups was learned.	Port
rlIgmpSnoopGroupTable rlIgmpSnoopGroupAddress 1.3.6.1.4.1.171.55.2.5.1.3	The MAC Multicast group address for which this entry contains information.	Address
rlIgmpSnoopGroupTable rlIgmpSnoopGroupExpiryTime 1.3.6.1.4.1.171.55.2.5.1.4	The minimum amount of time remaining before this entry is aged out.	Expiry Time

MAC Multicast Router Table

Object/OID	Description	Field Name in NMS
rlIgmpSnoopRouterTable rlIgmpSnoopRouterTag 1.3.6.1.4.1.171.55.2.6.1.1	Identifies the VLAN to which a frame belongs and for which this entry contains information on Multicast group MAC addresses.	Tag
rlIgmpSnoopRouterTable rlIgmpSnoopRouterPort 1.3.6.1.4.1.171.55.2.6.1.2	Port number specifying a physical port in the VLAN on which the information concerning multicast groups was learned.	Port

Object/OID	Description	Field Name in NMS
rlIgmpSnoopRouterTable rlIgmpSnoopRouterExpiryTime 1.3.6.1.4.1.171.55.2.6.1.3	The minimum amount of time remaining before this entry is aged out.	Expiry Time

Traffic Control Port Priority Table

Object/OID	Description	Field Name in NMS
dot1dBasePortTable dot1dBasePort 1.3.6.1.2.1.17.1.4.1.1	The port number identifying the port within a device.	Port
dot1dPortPriorityTable dot1dPortDefaultUserPriority 1.3.6.1.2.1.17.6.1.2.1.1.1	The default User Priority for this ingress port. The value ranging from 0 to 7 (8 priority levels are supported) is assigned by default to indicate the default user priority. This value is attached to any frame received on this port in the case when no priority was specified. The default value is 0.	Default Priority
rldot1dPortProtPriorityTable rldot1dPortProtDefaultUserPriority 1.3.6.1.4.1.171.57.1.3.1.1		
dot1dPortPriorityTable dot1dPortNumTrafficClasses 1.3.6.1.2.1.17.6.1.2.1.1.2	Number of available priority classes.	Number of Traffic Classes
rldot1dPortProtPriorityTable rldot1dPortProtNumTrafficClasses 1.3.6.1.4.1.171.57.1.3.1.2		

Traffic Control Traffic Class Table

Object/OID	Description	Field Name in NMS
dot1dBasePortTable dot1dBasePort 1.3.6.1.2.1.17.1.4.1.1	The port number identifying the port within a device.	Port
rldot1dPriorityPortGroupTable rldot1dPriorityPortGroupNumber 1.3.6.1.4.1.171.57.1.2.1.1	The group number to which the port belongs. All ports belonging to a group have the same default priority.	Port Group
dot1dPortPriorityTable dot1dPortDefaultUserPriority 1.3.6.1.2.1.17.6.1.2.1.1.1	User priority for the egress port.	P0, P1, P2, P3, P4, P5, P6, P7

Traffic Control Priority Groups Table

Object/OID	Description	Field Name in NMS
dot1dBasePortTable dot1dBasePort 1.3.6.1.2.1.17.1.4.1.1	The port number identifying the port within a device.	Port
rldot1dPriorityPortGroupTable rldot1dPriorityPortGroupNumber 1.3.6.1.4.1.171.57.1.2.1.1	The Priority value assigned on the per-port basis. **Untagged frames—**The value is equal to the Default User Priority value for the ingress port assigned from the table above. **Tagged frames—**The value is equal to the value specified in the 3-bit priority field within the 2-byte VLAN Tag field.	Priority Group

Router Parameters

Use the following variables to modify IP operating and interface parameters, RIP tables, OSPF tables, routing tables, ARP tables, redundancy tables, and DHCP tables; IPX parameters, RIP/SAP tables, and routing tables.

IP Router Operating Parameters

Object/OID	Description	Field Name in NMS
ipRedundAdminStatus 1.3.6.1.4.1.171.26.6.1	If enabled, this device serves as a backup if the current main device fails.	IP Redundancy Admin Status
rsArpInactiveTimeOut 1.3.6.1.4.1.171.26.4.2	Seconds passed between ARP requests about an entry in the ARP table. After this period, the entry is deleted from the table.	Inactive ARP Time Out
rsArpProxy 1.3.6.1.4.1.171.26.4.3	If enabled, the device responds to ARP requests for located nodes. If disabled the device responds with its own MAC address.	ARP Proxy
rsIcmpGenErrMsgEnable 1.3.6.1.4.1.171.26.2.1	If enabled the device generates ICMP error messages.	ICMP Error Messages

IP Router Interface Parameters

Object/OID	Description	Field Name in NMS
rsIpAddrTable rsIpAdEntAddr 1.3.6.1.4.1.171.26.1.1.1	Interface IP address.	IP Address
rsIpAddrTable rsIpAdEntNetMask 1.3.6.1.4.1.171.26.1.1.3	Associated subnet mask.	Network Mask

Object/OID	Description	Field Name in NMS
rsIpAddrTable rsIpAdEntIfIndex 1.3.6.1.4.1.171.26.1.1.2	Interface number. If the interface is a VLAN, the included interfaces are listed in the Interface number box in the IP Router Interface Parameters Insert window.	If Num/Interface Number
rsIpAddrTable rsIpAdEntForwardIpBroadcast 1.3.6.1.4.1.171.26.1.1.4	Indicates if the device forwards incoming broadcasts to this interface.	Fwd Broadcast
rsIpAddrTable rsIpAdEntBcastAddr 1.3.6.1.4.1.171.26.1.1.7	Fills the host ID in the broadcast address with ones or zeros.	Broadcast Type
rsIpAddrTable rsIpAdEntArpServer 1.3.6.1.4.1.171.26.1.1.8	When enabled, the system acts as an ARP requests relay, answering ARP requests to stations on different networks as though the device itself was the host being addressed.	ARP Server

IP RIP Parameters

Object/OID	Description	Field Name in NMS
rsRipEnable 1.3.6.1.4.1.171.26.9	The RIP administrative status in the router. Enabled means the RIP process is active on at least one interface. Disabled means the process is not active on any interfaces.	Administrative Status
ipLeakOspfToRip 1.3.6.1.4.1.171.26.7.3	Controls redistribution of routes from OSPF to RIP. When this parameter is enabled, all routes learned via OSPF are advertised into RIP.	Leak OSPF Routes
ipLeakStaticToRip 1.3.6.1.4.1.171.26.7.1	Controls redistribution of routes from static routes to RIP. When this parameter is enabled, all static routes learned via static are advertised into RIP.	Leak Static Routes

IP RIP Interface Parameters

Object/OID	Description	Field Name in NMS
rip2IfConfTable rip2IfConfAddress 1.3.6.1.2.1.23.3.1.1	Current IP address interfaces.	IP Address
rip2IfConfTable rip2IfConfSend 1.3.6.1.2.1.23.3.1.5	The type of RIP being sent. Options are: **RIP Version 1—**Sending RIP updates compliant with RFC 1058. **RIP Version—**Multicasting RIP2 updates. **Do Not Send—**No RIP updates are sent.	Outgoing RIP
rip2IfConfTable rip2IfConfReceive 1.3.6.1.2.1.23.3.1.6	The type of RIP being received. Options are: **RIP Version 1—**Accepting RIP1. **RIP Version 2—**Accepting RIP2. **Do Not Receive—**No RIP updates are accepted.	Incoming RIP

Object/OID	Description	Field Name in NMS
rip2IfConfTable rip2IfConfStatus 1.3.6.1.2.1.23.3.1.8	The RIP status in the router is either valid or invalid.	Status

IP RIP Filter

Object/OID	Description	Field Name in NMS
rsIpAddrTable rsIpAdEntAddr 1.3.6.1.4.1.171.26.1.1.1	The Interface IP address.	IP Address
rsIpAddrTable rsIpAdEntIfIndex 1.3.6.1.4.1.171.26.1.1.2	The pre-assigned Interface number.	Interface Number

IP OSPF II Parameters

Object/OID	Description	Field Name in NMS
ospfAdminStat 1.3.6.1.2.1.14.1.2	The OSPF administrative status in the router. The field options are the following: **Enabled—**The OSPF process is active on at least one interface. **Disabled—**The process is not active on any interface.	Administrative Status
ospfRouterId 1.3.6.1.2.1.14.1.1	The router ID number. To ensure uniqueness the router ID must be equal to one of the router IP addresses. By default, the router ID takes the IP Interface Address. Reset the device to allow changes in the router ID to take effect.	Router ID
ospfExternLSACount 1.3.6.1.2.1.14.1.6	The number of external Link-State Advertisements in the link-state database.	Number of External LSAs
ospfExternLsaCksumSum 1.3.6.1.2.1.14.1.7	The sum of LS checksums of external LS advertisements contained in the LS database. Use this sum to determine if there has been a change in a router LS database, and to compare the LS database of two routers.	External LS Checksum Sum
ipLeakRipToOspf 1.3.6.1.4.1.171.26.7.4	Controls the route redistribution from RIP into OSPF. When this parameter is enabled, all routes inserted into the IP routing table via SNMP are advertised into OSPF as external routes.	Leak RIP Routes
ipLeakStaticToOspf 1.3.6.1.4.1.171.26.7.2	Controls route redistribution from static routes to RIP. When this parameter is enabled, all static routes learned via static are advertised into RIP.	Leak Static Routes
ipLeakExtDirectToOspf 1.3.6.1.4.1.171.26.7.5	Controls direct route redistribution that are external to OSPF into OSPF. If this parameter is enabled all external routes are advertised into OSPF as external routes.	Leak External Direct Routes

IP OSPF II Interface Parameters

Object/OID	Description	Field Name in NMS
ospfIfTable ospfIfIpAddress 1.3.6.1.2.1.14.7.1.1	The IP address of this OSPF interface.	IP Address
ospfIfTable ospfIfAreaId 1.3.6.1.2.1.14.7.1.3	The IP address of the area.	Area ID
ospfIfTable ospfIfType 1.3.6.1.2.1.14.7.1.4	The interface type, such as Broadcast.	If Type
ospfIfTable ospfIfState 1.3.6.1.2.1.14.7.1.12	The OSPF interface state. Options are: **Down—**The OSPF interface is down. **Loopback—**The OSPF interface is in the Loopback state. **Waiting—**The OSPF interface is currently waiting. **Point to Point—**The OSPF interface is in the point to point state. **Designated Router—**The OSPF interface is the designated router. **Backup Designated Router—**The OSPF interface is the backup designated router. **Other Designated Router—**Other routers are the designated and backup routers.	If State
ospfIfTable ospfIfDesignatedRouter 1.3.6.1.2.1.14.7.1.13	The IP address of the designated router.	Designated Router
ospfIfTable ospfIfBackupDesignatedRouter 1.3.6.1.2.1.14.7.1.14	The IP address of the backup designated router.	Backup Desig. Router

IP OSPF II Area Table

Object/OID	Description	Field Name in NMS
ospfAreaTable ospfAreaId 1.3.6.1.2.1.14.2.1.1	The area IP address.	Area ID

Object/OID	Description	Field Name in NMS
ospfAreaTable ospfImportAsExtern 1.3.6.1.2.1.14.2.1.3	The area support for importing as external link state advertisement. **Area Summary—**Controls the import of summary LSAs into stub areas. This variable has no effect on other areas. **No Area Summary—**The router neither originates nor distributes summary LSAs into the stub area. It relies on its default route.	Import as External
ospfAreaTable ospfAreaSummary 1.3.6.1.2.1.14.2.1.9	Controls the import of summary LSAs into stub areas. This variable has no effect on other areas. **No Area Summary—**The router neither originates nor distributes summary LSAs into the stub area. It relies on its default route. **Send Area Summary—**The router both summarizes and distributes summary LSAs.	Area Summary
ospfStubAreaTable ospfStubStatus 1.3.6.1.2.1.14.3.1.4	The metric for this type of service on the interface.	Metric
ospfStubAreaTable ospfStubMetricType 1.3.6.1.2.1.14.3.1.5	The metric protocol type.	Metric Type

IP OSPF II Link State Database

Object/OID	Description	Field Name in NMS
ospfLsdbTable ospfLsdbAreaId 1.3.6.1.2.1.14.4.1.1	The link IP address.	Area ID
ospfLsdbTable ospfLsdbType 1.3.6.1.2.1.14.4.1.2	Each link state advertisement has a specific format. The link is a Router Link, Network Link, External Link, Summary Link or Stub Link.	Link Type
ospfLsdbTable ospfLsdbLsid 1.3.6.1.2.1.14.4.1.3	Identifies the routing domain piece described by the advertisement. It is either a router ID or an IP address.	Link ID
ospfLsdbTable ospfLsdbRouterId 1.3.6.1.2.1.14.4.1.4	Identifies the originating router in the autonomous system.	Router ID
ospfLsdbTable ospfLsdbSequence 1.3.6.1.2.1.14.4.1.5	The number for the link. This parameter is used to detect old and duplicate links state advertisements. The larger the sequence number the more recent the advertisement.	Sequence Number

Object/OID	Description	Field Name in NMS
ospfLsdbTable ospfLsdbAge 1.3.6.1.2.1.14.4.1.6	The link age state advertisement in seconds.	Age
ospfLsdbTable ospfLsdbChecksum 1.3.6.1.2.1.14.4.1.7	This parameter is a checksum of the advertisement complete contents, excluding the Age value.	Checksum

IP OSPF II External Link State Database

Object/OID	Description	Field Name in NMS
ospfExtLsdbTable ospfExtLsdbType 1.3.6.1.2.1.14.12.1.1	Each link state advertisement has a specific format. The link is a Router Link, Network Link, External Link, Summary Link or Stub Link.	Link Type
ospfExtLsdbTable ospfExtLsdbLsid 1.3.6.1.2.1.14.12.1.2	Identifies the routing domain piece described by the advertisement. It is either a router ID or an IP address.	Link ID
ospfExtLsdbTable ospfExtLsdbRouterId 1.3.6.1.2.1.14.12.1.3	Identifies the originating router in the autonomous system.	Orig. Router ID
ospfExtLsdbTable ospfExtLsdbSequence 1.3.6.1.2.1.14.12.1.4	The number for the link. This parameter is used to detect old and duplicate links state advertisements. The larger the sequence number the more recent the advertisement.	OSPF Sequence Number
ospfExtLsdbTable ospfExtLsdbAge 1.3.6.1.2.1.14.12.1.5	The link state advertisement age, in seconds.	Link State Age
ospfExtLsdbTable ospfExtLsdbChecksum 1.3.6.1.2.1.14.12.1.6	The complete advertisement contents checksum, excluding the Age.	Checksum
ospfExtLsdbTable ospfExtLsdbAdvertisement 1.3.6.1.2.1.14.12.1.7	The link state advertisement, containing the header and contents.	Link State Advertisement

IP OSPF II Neighbors Table

Object/OID	Description	Field Name in NMS
rsIpAddrTable rsIpAdEntAddr 1.3.6.1.4.1.171.26.1.1.1	The neighbor interface IP address.	IP address

Object/OID	Description	Field Name in NMS
rsIpAddrTable rsIpAdEntNetMask 1.3.6.1.4.1.171.26.1.1.3	The neighbor network address interface.	Network Mask

IP Routing Table

Object/OID	Description	Field Name in NMS
ipCidrRouteTable ipCidrRouteDest 1.3.6.1.2.1.4.24.4.1.1	The destination IP address of this router.	Dest IP Address
ipCidrRouteTable ipCidrRouteMask 1.3.6.1.2.1.4.24.4.1.2	The destination for this route.	Network Mask
ipCidrRouteTable ipCidrRouteNextHop 1.3.6.1.2.1.4.24.4.1.4	Address of the next system in this route, central to the interface.	Next Hop
ipCidrRouteTable ipCidrRouteIfIndex 1.3.6.1.2.1.4.24.4.1.5	The central interface Index through which the next hop of this route is reached.	Interface Number
ipCidrRouteTable ipCidrRouteType 1.3.6.1.2.1.4.24.4.1.6	How remote routing is handled. Option are: **Remote —**Forwards packets. **Reject—**Discards packets.	Route Type
ipCidrRouteTable ipCidrRouteMetric1 1.3.6.1.2.1.4.24.4.1.11	Number of hops to the destination network.	Metric
ipCidrRouteTable ipCidrRouteProto 1.3.6.1.2.1.4.24.4.1.7	Through which protocol the route is known.	Protocol

IP ARP Table

Object/OID	Description	Field Name in NMS
ipNetToMediaTable ipNetToMediaIfIndex 1.3.6.1.2.1.4.22.1.1	The interface number on which the station resides.	Interface
ipNetToMediaTable ipNetToMediaNetAddress 1.3.6.1.2.1.4.22.1.3	The station IP address.	IP Address

Object/OID	Description	Field Name in NMS
ipNetToMediaTable ipNetToMediaPhysAddress 1.3.6.1.2.1.4.22.1.2	The station MAC address.	MAC Address
ipNetToMediaTable ipNetToMediaType 1.3.6.1.2.1.4.22.1.4	The entry type. Options are: **Dynamic—**The entry is learned from the ARP protocol. If the entry is not active for a predetermined time, the node is deleted from the table. **Static—**The entry is configured by the network management station and is permanent.	Class
No MIB associated with this NMS field.	In the **Read From** field, select from which interface to start building the table entries displayed.	Read From

IP Redundancy

Object/OID	Description	Field Name in NMS
ipRedundRoutersTable ipRedundRoutersIfAddr 1.3.6.1.4.1.171.26.6.3.1.1	The IP address that the redundancy feature is running on.	Interface IP Address
ipRedundRoutersTable ipRedundRoutersMainRouterAddr 1.3.6.1.4.1.171.26.6.3.1.2	The router IP address that the devices backing up.	Main Router Address
ipRedundRoutersTable ipRedundRoutersOperStatus 1.3.6.1.4.1.171.26.6.3.1.3	The entry status: **Active—**The backup router is active on this interface. **Inactive—**The backup router is not active on this interface.	Operating Status
ipRedundRoutersTable ipRedundRoutersPollInterval 1.3.6.1.4.1.171.26.6.3.1.4	This router-polling interval, in seconds. If the interval is 0 then the router is not polled.	Poll Interval
ipRedundRoutersTable ipRedundRoutersTimeout 1.3.6.1.4.1.171.26.6.3.1.5	The interval in seconds during which the router must signal. If the router does not signal within this interval, it is considered non-operational. If Time Out is equal to 0, the device ignores the table entry.	Time Out

IP DHCP Parameters

Object/OID	Description	Field Name in NMS
rsDhcpServerEnable 1.3.6.1.4.1.171.38.5	Enable (default) or disable the DHCP server. If enabled, the device does not relay DHCP requests, unless the request is from device router. If disabled, the device relays DHCP requests to the DHCP server configured in this window.	Server Enable
rsDhcpNextServerAddress 1.3.6.1.4.1.171.38.7	The DHCP server IP address. The device acts as a DHCP relay if this parameter is not equal to 0.0.0.0.	Next Server Address

Object/OID	Description	Field Name in NMS
rsDhcpRelaySecThreshold 1.3.6.1.4.1.171.38.6	DHCP requests are relayed only if their SEC field is greater or equal to the threshold value, in order to allow local DHCP servers to answer first.	Relay Security Threshold
rsDNSIPAddr 1.3.6.1.4.1.171.38.1	This parameter is the DNS server IP address. It is given here to enable consistent updates for DHCP MCLIent names.	DNS IP address
rsDhcpProbeEnable 1.3.6.1.4.1.171.38.2	Enable (by default) or disable the automatic ICMP echo requests probe of a used address before reallocation. This is used to verify that the address is currently not in use by a MCLIent. If this field is disabled, the Probe retries and Probe Timeout features are also disabled.	Probe Enable
rsDhcpProbeRetries 1.3.6.1.4.1.171.38.4	The number of times the DHCP server sends an ICMP echo request.	Probe Retries
rsDhcpProbeTimeout 1.3.6.1.4.1.171.38.3	The time (in seconds) that the server waits for an acknowledgment from the host that the IP address was accepted.	Probe Timeout (Seconds)
rsDhcpWinsPrime 1.3.6.1.4.1.171.38.11	The primary WINS server IP address.	Primary WINS Server
rsDhcpWinsSecondary 1.3.6.1.4.1.171.38.12	The backup WINS server IP address.	Secondary WINS Server
rsDhcpWinsNodeType 1.3.6.1.4.1.171.38.13	The NetBios type defines how resources are identified and accessed. There are four options: **Broadcast—**Uses broadcast to resolve names. Default when WINS servers are not in place **Point-to-Point—**Uses point-to-point communications with WINS servers to resolve names. **Mixed—**First uses broadcast type, then if routers must be crossed, point-to-point is used. **Hybrid—**First uses point-to-point for name queries. If this fails (i.e., the WINS server fails), broadcast is used to resolve names until the hybrid polling feature learns that the WINS server is functioning again.	Node Type

IP DHCP Address Range

Object/OID	Description	Field Name in NMS
rsDhcpDynamicTable rsDhcpDynamicEntryIPAddrInf 1.3.6.1.4.1.171.38.10.1.1	Displays the interface IP Address	IP Addr If
rsDhcpDynamicTable rsDhcpDynamicEntryIPAddrFrom 1.3.6.1.4.1.171.38.10.1.2	This is a read-only field. It displays the first IP Address allocated in this row.	IP Addr From

Object/OID	Description	Field Name in NMS
rsDhcpDynamicTable rsDhcpDynamicEntryIPAddrTo 1.3.6.1.4.1.171.38.10.1.3	This is a read-only field, displaying the last IP Address allocated in this row.	IP Address To
rsDhcpDynamicTable rsDhcpDynamicEntryDfltRouter 1.3.6.1.4.1.171.38.10.1.4	The IP default gateway Address.	Default Router
rsDhcpDynamicTable rsDhcpDynamicEntryLeaseTime 1.3.6.1.4.1.171.38.10.1.5	This parameter is used to gain the maximum lease-time for a new IP address. Set this field to 0xffffffff for automatic allocation. For dynamic allocation set this field to a value lower than 4,294,967,294 (136 years).	Lease Time
No MIB associated with this NMS field.	If the field **Unlimited** is checked, -1 appears automatically in the **Lease Time** Parameter.	Unlimited (Check box appears in Insert Window)
rsDhcpDynamicTable rsDhcpDynamicEntryProbeEnable 1.3.6.1.4.1.171.38.10.1.6	Enable or disable the automatic ICMP echo request probe of a used address before reallocation. This parameter is used to verify that the address is currently not in use by a MCLIent.	Probe Enable
rsDhcpDynamicTable rsDhcpDynamicEntryTotalNumOfAddr 1.3.6.1.4.1.171.38.10.1.7	This field displays the total number of available IP Addresses to choose from, including those currently in use.	Total Addr No.
rsDhcpDynamicTable rsDhcpDynamicEntryFreeNumOfAddr 1.3.6.1.4.1.171.38.10.1.8	This field displays the number of available IP Addresses for new allocation.	Free Address No.
rsDhcpDynamicTable rsDhcpDynamicEntryUsedByDhcp 1.3.6.1.4.1.171.38.10.1.9	This field displays the number of IP Addresses currently being used by DHCP.	DHCP Addr No.

IP DHCP Allocation Table

Object/OID	Description	Field Name in NMS
rsDhcpIPAddressAllocTable rsDhcpIPAddressAllocEntryIPAddr 1.3.6.1.4.1.171.38.9.1.1	This is a read-only field, displaying the IP Address allocated by the DHCP server.	IP Address
rsDhcpIPAddressAllocTable rsDhcpIPAddressAllocEntryMACAddr 1.3.6.1.4.1.171.38.9.1.2	MAC Addresses are stored in canonical bit order to match incoming DHCP requests. To match all incoming requests from host devices centrally attached to the server, enter an all zero MAC Address.	MAC Address

Object/OID	Description	Field Name in NMS
rsDhcpIPAddressAllocTable rsDhcpIPAddressAllocEntryMechanism 1.3.6.1.4.1.171.38.9.1.5	This is the mechanism used by the server to allocate IP Addresses. The DHCP server supports three mechanisms for IP allocation: **Automatic allocation—**The DHCP server selects a permanent IP Address from a predefined range when a new MCLIent requests configuration. **Dynamic allocation—**The DHCP server allocates an IP Address for a limited period, called a 'lease'. During the lease, the Address is guaranteed this allocation, and the Dynamic allocation mechanism attempts to return to the same network each time the MCLIent requests an address. **Manual allocation—**The network administrator assigns an IP Address to a MCLIent. **Note:** The DHCP Address Allocation Edit option supports the Manual allocation mechanism only. Therefore, if Automatic or Dynamic allocation is defined for a particular DHCP server, its mechanism value is changed to Manual allocation after editing this server and MCLIcking in the Edit dialog box.	Mechanism
rsDhcpIPAddressAllocTable rsDhcpIPAddressAllocEntryHostName 1.3.6.1.4.1.171.38.9.1.4	The host identity requesting the address.	Host Name
rsDhcpIPAddressAllocTable rsDhcpIPAddressAllocEntryApplication 1.3.6.1.4.1.171.38.9.1.6	This is a read-only field. It displays the application that allocated the IP Address. The application is either DHCP or RIP.	Application
rsDhcpIPAddressAllocTable rsDhcpIPAddressAllocEntryAgeTime 1.3.6.1.4.1.171.38.9.1.7	This is a read-only field, displaying the IP Address age time.	Age Time
rsDhcpIPAddressAllocTable rsDhcpIPAddressAllocEntryDfltRouter 1.3.6.1.4.1.171.38.9.1.8	The default gateway IP Address.	Default Router
rsDhcpIPAddressAllocTable rsDhcpIPAddressAllocEntryConfigServIPAddr 1.3.6.1.4.1.171.38.9.1.9	The server address containing the TFTP configuration file to which the device relays the configuration file download request.	Config Server IP Address
rsDhcpIPAddressAllocTable rsDhcpIPAddressAllocEntryConfigFileName 1.3.6.1.4.1.171.38.9.1.10	The path and the configuration file name on the server.	Config File Name

UDP Relay

Object/OID	Description	Field Name in NMS
rsUdpRelayEntry 1.3.6.1.4.1.171.42.1.1		
rsUdpRelayDstPort 1.3.6.1.4.1.171.42.1.1.1	The destination UDP port ID number of UDP frames to be relayed.	UDP Destination Port
rsUdpRelaySrcIpInf 1.3.6.1.4.1.171.42.1.1.2	The input IP interface that relays UDP frames. If this field is 255.255.255.255, UDP frames from all interfaces are relayed.	Source IP Address
rsUdpRelayDstIpAddr 1.3.6.1.4.1.171.42.1.1.3	The IP interface that receives UDP frame relays. If this field is 0.0.0.0, UDP frames are discarded. If this field is 255.255.255.255, UDP frames are flooded to all IP interfaces.	Destination IP Address
rsUdpRelayStatus 1.3.6.1.4.1.171.42.1.1.4	The status of a table entry. It is used to delete an entry from this table.	Status

TCP General Parameters

Object/OID	Description	Field Name in NMS
tcpRtoAlgorithm 1.3.6.1.2.1.6.1	The Algorithm used to determine the timeout value used for re-transmitting unacknowledged octets.	Algorithm Type
tcpRtoMin 1.3.6.1.2.1.6.2	The minimum value permitted by a TCP implementation for the re-transmission timeout, measured in milliseconds.	Min. Timeout (ms)
tcpRtoMax 1.3.6.1.2.1.6.3	The maximum value permitted by a TCP implementation for the re-transmission timeout, measured in milliseconds.	Max. Timeout (ms)
tcpMaxConn 1.3.6.1.2.1.6.4	The limit on the total number of TCP connections the entity can support. In entities where the maximum number of connections is dynamic, this object contains the value -1.	Max. Connections

TCP Connection Table

Object/OID	Description	Field Name in NMS
tcpConnTable tcpConnLocalAddress 1.3.6.1.2.1.6.13.1.2	The local IP address for this TCP connection. In the case of a connection in the Listen State, the value 0.0.0.0 is used. In this case, the device accepts connections for any IP interface associated with the node.	Local Address
tcpConnTable tcpConnLocalPort 1.3.6.1.2.1.6.13.1.3	The local port number for this TCP connection.	Local Port

Object/OID	Description	Field Name in NMS
tcpConnTable tcpConnRemAddress 1.3.6.1.2.1.6.13.1.4	The remote IP address for this TCP connection.	Remote Address
tcpConnTable tcpConnRemPort 1.3.6.1.2.1.6.13.1.5	The remote port number for this TCP connection.	Remote Port
tcpConnTable tcpConnState 1.3.6.1.2.1.6.13.1.1	The status of this TCP connection. The only value set by a management station is "DeleteTCB" (TCP Control Block). This is achieved by deleting the Specific entry, using the management system.	Connection State

IPM: IGMP Parameters

Object/OID	Description	Field Name in NMS
rlIgmpMibVersion 1.3.6.1.4.1.171.46.2.1	MIB's version. The current version is 2.	IGMP MIB Version

IPM: IGMP Interface Table

Object/OID	Description	Field Name in NMS
IpAddrEntry 1.3.6.1.2.1.4.20.1	The addressing information for one of this entity's IP addresses.	
IpAdEntAddr 1.3.6.1.2.1.4.20.1.1	The IP address to which this entry's addressing information pertains.	
IpAdEntIfIndex 1.3.6.1.2.1.4.20.1.2	The index value, which uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of RFC 1573's ifIndex.	
IgmpInterfaceEntry 1.3.6.1.2.1.85.1.1.1	An entry (conceptual row) representing an interface on which IGMP is enabled.	
IgmpInterfaceIfIndex 1.3.6.1.2.1.85.1.1.1.1	The ifIndex value of the interface for which IGMP is enabled.	IFIndex (IGMP Interface Table Window)
IgmpInterfaceQueryInterval 1.3.6.1.2.1.85.1.1.1.2	The frequency at which IGMP Host-Query packets are transmitted on this interface.	Query Interval (IGMP Interface Table Window)
IgmpInterfaceStatus 1.3.6.1.2.1.85.1.1.1.3	The activation of a row enables IGMP on the interface. The destruction of a row disables IGMP on the interface.	Status (IGMP Interface Table Window)

Object/OID	Description	Field Name in NMS
igmpInterfaceVersion 1.3.6.1.2.1.85.1.1.1.4	The version of IGMP, which is running on this interface. This object can be used to configure a router capable of running either value. For IGMP to function correctly, all routers on a LAN must be configured to run the same version of IGMP on that LAN.	Version (IGMP Interface Table Window)
igmpInterfaceQuerier 1.3.6.1.2.1.85.1.1.1.5	The address of the IGMP Querier on the IP subnet to which this interface is attached.	Querier (IGMP Interface Table Window)
igmpInterfaceQueryMaxResponseTime 1.3.6.1.2.1.85.1.1.1.6	The maximum query response time advertised in IGMPv2 queries on this interface.	Query Max Response Time (IGMP Interface Table Window)
igmpInterfaceQuerierUpTime 1.3.6.1.2.1.85.1.1.1.7	The time since igmpInterfaceQuerier was last changed.	Querier Up Time (IGMP Interface Table Window)
igmpInterfaceQuerierExpiryTime 1.3.6.1.2.1.85.1.1.1.8	The amount of time remaining before the Other Querier Present Timer expires. If the local system is the querier, the value of this object is zero.	Querier Expiry Time (IGMP Interface Table Window)
igmpInterfaceWrongVersionQueries 1.3.6.1.2.1.85.1.1.1.10	The number of queries received whose IGMP version does not match igmpInterfaceVersion, over the lifetime of the row entry. IGMP requires that all routers on a LAN be configured to run the same version of IGMP. Thus, if any queries are received with the wrong version, this indicates a configuration error.	Wrong Version Queries (IGMP Interface Table Window)
igmpInterfaceJoins 1.3.6.1.2.1.85.1.1.1.11	The number of times a group membership has been added on this interface; that is, the number of times an entry for this interface has been added to the Cache Table. This object gives an indication of the amount of IGMP activity over the lifetime of the row entry.	Joins (IGMP Interface Table Window)
igmpInterfaceProxyIfIndex 1.3.6.1.2.1.85.1.1.1.12	Some devices implement a form of IGMP proxying whereby memberships learned on the interface represented by this row, cause IGMP Host Membership Reports to be sent on the interface whose ifIndex value is given by this object. Such a device would implement the igmpV2RouterMIBGroup only on its router interfaces (those interfaces with non-zero igmpInterfaceProxyIfIndex). Typically, the value of this object is 0, indicating that no proxying is being done.	Proxy IfIndex (IGMP Interface Table Window)
igmpInterfaceGroups 1.3.6.1.2.1.85.1.1.1.13	The current number of entries for this interface in the Cache Table.	Groups (IGMP Interface Table Window)
igmpInterfaceRobustness 1.3.6.1.2.1.85.1.1.1.14	The Robustness Variable allows tuning for the expected packet loss on a subnet. If a subnet is expected to be lossy, the Robustness Variable may be increased. IGMP is robust to (Robustness Variable-1) packet losses.	Robustness (IGMP Interface Table Window)

Object/OID	Description	Field Name in NMS
igmpInterfaceLastMembQueryIntvl 1.3.6.1.2.1.85.1.1.1.15	The Last Member Query Interval is the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query messages. This value may be tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. The value of this object is irrelevant if igmpInterfaceVersion is 1.	Last Member Query Intvl (IGMP Interface Table Window)

IPM: IGMP Cache Table

Object/OID	Description	Field Name in NMS
igmpCacheEntry 1.3.6.1.2.1.85.1.2.1	An entry (conceptual row) in the igmpCacheTable.	
igmpCacheTable igmpCacheAddress 1.3.6.1.2.1.85.1.2.1.1	The IP multicast group address for which this entry contains information.	Cache Address (IGMP Cache Table)
igmpCacheTable igmpCacheIfIndex 1.3.6.1.2.1.85.1.2.1.2	The interface for which this entry contains information for an IP multicast group address.	IfIndex (IGMP Cache Table)
igmpCacheTable igmpCacheSelf 1.3.6.1.2.1.85.1.2.1.3	An indication of whether the local system is a member of this group address on this interface.	Cache Self (IGMP Cache Table)
igmpCacheTable igmpCacheLastReporter 1.3.6.1.2.1.85.1.2.1.4	The IP address of the source of the last membership report received for this IP Multicast group address on this interface. If no membership report has been received, this object has the value 0.0.0.0.	Last Reporter (IGMP Cache Table)
igmpCacheTable igmpCacheUpTime 1.3.6.1.2.1.85.1.2.1.5	The time elapsed since this entry was created.	Up Time (IGMP Cache Table)
igmpCacheTable igmpCacheExpiryTime 1.3.6.1.2.1.85.1.2.1.6	The minimum amount of time remaining before this entry will be aged out. A value of 0 indicates that the entry is only present because igmpCacheSelf is true and that if the router left the group, this entry would be aged out immediately. Note that some implementations may process membership reports from the local system in the same way as reports from other hosts, so a value of 0 is not required.	Expiry Time (IGMP Cache Table)
igmpCacheTable igmpCacheStatus 1.3.6.1.2.1.85.1.2.1.7	The status of this entry.	Status (IGMP Cache Table)

Object/OID	Description	Field Name in NMS
igmpCacheTable igmpCacheVersion1HostTimer 1.3.6.1.2.1.85.1.2.1.8	The time remaining until the local router will assume that there are no longer any IGMP version 1 members on the IP subnet attached to this interface. Upon hearing any IGMPv1 Membership Report, this value is reset to the group membership timer. While this time remaining is non-zero, the local router ignores any IGMPv2 Leave messages for this group that it receives on this interface.	Version1 Host Number (IGMP Cache Table)

IPM: PIM Parameters

Object/OID	Description	Field Name in NMS
rlPimMibVersion 1.3.6.1.4.1.171.46.3.2	MIB's version. The current version is 2.	PIM MIB Version

IPM: PIM Interface Table

Object/OID	Description	Field Name in NMS
ipAddrEntry 1.3.6.1.2.1.4.20.1	The addressing information for one of this entity's IP addresses.	
ipAdEntAddr 1.3.6.1.2.1.4.20.1.1	The IP address to which this entry's addressing information pertains.	
ipAdEntIfIndex 1.3.6.1.2.1.4.20.1.2	The index value, which uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of RFC 1573's ifIndex.	
pimInterfaceEntry 1.3.6.1.3.61.1.1.2.1	An entry (conceptual row) in the pimInterfaceTable.	
pimInterfaceTable pimInterfaceIfIndex 1.3.6.1.3.61.1.1.2.1.1	The ifIndex value of this PIM interface.	IfIndex (PIM Interface Table Window)
pimInterfaceTable pimInterfaceAddress 1.3.6.1.3.61.1.1.2.1.2	The IP address of the PIM interface.	Interface Address (PIM Interface Table Window)
pimInterfaceTable pimInterfaceNetMask 1.3.6.1.3.61.1.1.2.1.3	The network mask for the IP address of the PIM interface.	Interface Mask (PIM Interface Table Window)
pimInterfaceTable pimInterfaceMode 1.3.6.1.3.61.1.1.2.1.4	The configured mode of this PIM interface.	Mode (PIM Interface Table Window)

Object/OID	Description	Field Name in NMS
pimInterfaceTable pimInterfaceDR 1.3.6.1.3.61.1.1.2.1.5	The Designated Router on this PIM interface. For point-to-point interfaces, this object has the value 0.0.0.0.	Designated Router (PIM Interface Table Window)
pimInterfaceTable pimInterfaceHelloInterval 1.3.6.1.3.61.1.1.2.1.6	The frequency at which PIM Hello messages are transmitted on this interface.	Hello Interval (PIM Interface Table Window)
pimInterfaceTable pimInterfaceStatus 1.3.6.1.3.61.1.1.2.1.7	The status of this entry. Creating the entry enables PIM on the interface; destroying the entry disables PIM on the interface.	(PIM Interface Table Window)
pimInterfaceTable pimInterfaceJoinPruneInterval 1.3.6.1.3.61.1.1.2.1.8	The frequency at which PIM Join/Prune messages are transmitted on this PIM interface. The default value of this object is the pimJoinPruneInterval.	JoinPrune Interval (PIM Interface Table Window)

IPM: PIM Neighbor Table

Object/OID	Description	Field Name in NMS
pimNeighborTable pimNeighborEntry 1.3.6.1.3.61.1.1.3.1	An entry (conceptual row) in the pimNeighborTable.	
pimNeighborTable pimNeighborAddress 1.3.6.1.3.61.1.1.3.1.1	The IP address of the PIM neighbor for which this entry contains information.	Neighbor Address (PIM Neighbor Table Window)
pimNeighborTable pimNeighborIfIndex 1.3.6.1.3.61.1.1.3.1.2	The value of ifIndex for the interface used to reach this PIM neighbor.	IfIndex (PIM Neighbor Table Window)
pimNeighborTable pimNeighborUpTime 1.3.6.1.3.61.1.1.3.1.3	Indicates the time lapse since the PIM neighbor became the neighbor to the local router.	Up Time (PIM Neighbor Table Window)
pimNeighborTable pimNeighborExpiryTime 1.3.6.1.3.61.1.1.3.1.4	Indicates time in ticks before the PIM neighbor is aged out.	Expiry Time (PIM Neighbor Table Window)
pimNeighborTable pimNeighborMode 1.3.6.1.3.61.1.1.3.1.5	The active PIM mode of this neighbor. This object is deprecated for PIMv2 routers since all neighbors on the interface must be either dense or sparse as determined by the protocol running on the interface.	Mode (PIM Neighbor Table Window)

IPM: PIM Route Table

Object/OID	Description	Field Name in NMS

Object/OID	Description	Field Name in NMS
pimIpMRouteEntry 1.3.6.1.3.61.1.1.4.1	An entry (conceptual row) in the imIpMRouteTable. There is one entry per entry in the ipMRouteTable whose incoming interface is running PIM.	
imIpMRouteTable pimIpMRouteUpstreamAssertTimer 1.3.6.1.3.61.1.1.4.1.1	The time remaining before the router changes its upstream neighbor back to its RPF neighbor. This timer is called the Assert timer in the PIM Sparse and Dense mode specification. A value of 0 indicates that no Assert has changed the upstream neighbor away from the RPF neighbor.	Upstream Assert Timer (PIM Route Table Window)
imIpMRouteTable pimIpMRouteAssertMetric 1.3.6.1.3.61.1.1.4.1.2	The metric advertised by the assert winner on the upstream interface, or 0 if no such assert is in received.	AssertMetric (PIM Route Table Window)
imIpMRouteTable pimIpMRouteAssertMetricPref 1.3.6.1.3.61.1.1.4.1.3	The preference advertised by the assert winner on the upstream interface, or 0 if no such assert is in effect.	Assert MetricPref (PIM Route Table Window)
imIpMRouteTable pimIpMRouteAssertRPTBit 1.3.6.1.3.61.1.1.4.1.4	The value of the RPT-bit advertised by the assert winner on the upstream interface, or false if no such assert is in effect.	Assert RPT Bit (PIM Route Table Window)
imIpMRouteTable pimIpMRouteFlags 1.3.6.1.3.61.1.1.4.1.5	This object describes PIM-specific flags related to a multicast state entry. See the PIM Sparse Mode specification for the meaning of the RPT and SPT bits.	Flags (PIM Route Table Window)
imIpMRouteTable ipMRouteGroup 1.3.6.1.2.1.83.1.1.2.1.1	Specifies the multicast group IP address. The range is 244.0.0.0-239.255.255.255.	Group (PIM Route Table Window)
imIpMRouteTable ipMRouteSource 1.3.6.1.2.1.83.1.1.2.1.2	Specifies the source IP address from where the multicast packets are being sent.	Source (PIM Route Table Window)
imIpMRouteTable ipMRouteSourceMask 1.3.6.1.2.1.83.1.1.2.1.3	Mask all or part of the source IP address.	Source Mask (PIM Route Table Window)

IPM: PIM Route Next Hop

Object/OID	Description	Field Name in NMS
ipMRouteNextHopTable ipMRouteNextHopGroup 1.3.6.1.2.1.83.1.1.3.1.1	The IP multicast group for which this entry specifies a next-hop on an outgoing interface.	Group (PIM Route Next Hop Window)
ipMRouteNextHopTable ipMRouteNextHopSource 1.3.6.1.2.1.83.1.1.3.1.2	The network address which when combined with the corresponding value of ipMRouteNextHopSourceMask identifies the sources for which this entry specifies a next-hop on an outgoing interface.	Source (PIM Route Next Hop Window)

Object/OID	Description	Field Name in NMS
ipMRouteNextHopTable ipMRouteNextHopSourceMask 1.3.6.1.2.1.83.1.1.3.1.3	The network mask which when combined with the corresponding value of ipMRouteNextHopSource identifies the sources for which this entry specifies a next-hop on an outgoing interface.	Source Mask (PIM Route Next Hop Window)
ipMRouteNextHopTable ipMRouteNextHopIfIndex 1.3.6.1.2.1.83.1.1.3.1.4	The ifIndex value of the interface for the outgoing interface for this next-hop.	IfIndex (PIM Route Next Hop Window)
ipMRouteNextHopAddress 1.3.6.1.2.1.83.1.1.3.1.5	The address of the next-hop specific to this entry. For most interfaces, this is identical to ipMRouteNextHopGroup. NBMA interfaces, however, may have multiple next-hop addresses out a single outgoing interface.	Next Hop Address (PIM Route Next Hop Window)
ipMRouteNextHopTable pimIpMRouteNextHopEntry 1.3.6.1.3.61.1.1.7.1	An entry (conceptual row) in the pimIpMRouteNextHopTable. There is one entry per entry in the ipMRouteNextHopTable whose interface is running PIM and whose ipMRouteNextHopState is pruned(1).	
pimIpMRouteNextHopTable pimIpMRouteNextHopPruneReason 1.3.6.1.3.61.1.1.7.1.2	This object indicates why the downstream interface was pruned, whether in response to a PIM prune message or due to PIM Assert processing.	Prune Reason (PIM Route Next Hop Window)

IPM Routing: Route Table

Object/OID	Description	Field Name in NMS
pimIpMRouteTable pimIpMRouteEntry 1.3.6.1.3.61.1.1.4.1	An entry (conceptual row) in the pimIpMRouteTable. There is one entry per entry in the ipMRouteTable whose incoming interface is running PIM.	
pimIpMRouteTable pimIpMRouteUpstreamAssertTimer 1.3.6.1.3.61.1.1.4.1	The time remaining before the router changes its upstream neighbor back to its RPF neighbor. This timer is called the Assert timer in the PIM Sparse and Dense mode specification. A value of 0 indicates that no Assert has changed the upstream neighbor away from the RPF neighbor.	
pimIpMRouteTable pimIpMRouteAssertMetric 1.3.6.1.3.61.1.1.4.1	The metric advertised by the assert winner on the upstream interface, or 0 if no such assert is in received.	
pimIpMRouteTable pimIpMRouteAssertMetricPref 1.3.6.1.3.61.1.1.4.1	The preference advertised by the assert winner on the upstream interface, or 0 if no such assert is in effect.	
pimIpMRouteTable pimIpMRouteAssertRPTBit 1.3.6.1.3.61.1.1.4.1	The value of the RPT-bit advertised by the assert winner on the upstream interface, or false if no such assert is in effect.	

Object/OID	Description	Field Name in NMS
pimIpMRouteTable pimIpMRouteFlags 1.3.6.1.3.61.1.1.4.1	This object describes PIM-specific flags related to a multicast state entry. See the PIM Sparse Mode specification for the meaning of the RPT and SPT bits.	
ipMRouteGroup 1.3.6.1.2.1.83.1.1.2.1.1	The IP multicast group address for which this entry contains multicast routing information.	Group (IPM Route Table Window)
IpMRouteSource 1.3.6.1.2.1.83.1.1.2.1.2	The network address which when combined with the corresponding value of ipMRouteSourceMask identifies the sources for which this entry contains multicast routing information.	Source (IPM Route Table Window)
IpMRouteSourceMask 1.3.6.1.2.1.83.1.1.2.1.3	The network mask which when combined with the corresponding value of ipMRouteSource identifies the sources for which this entry contains multicast routing information.	Source Mask (IPM Route Table Window)

IPM Routing: Next Hop Table

Object/OID	Description	Field Name in NMS
ipMRouteNextHopEntry 1.3.6.1.2.1.83.1.1.3.1	An entry (conceptual row) in the list of next-hops on outgoing interfaces to which IP multicast datagrams from particular sources to an IP multicast group address are routed. Discontinuities in counters in this entry can be detected by observing the value of ipMRouteUpTime.	
ipMRouteNextHopGroup 1.3.6.1.2.1.83.1.1.3.1.1	The IP multicast group for which this entry specifies a next-hop on an outgoing interface.	Group (IPM Route Next Hop Window)
ipMRouteNextHopSource 1.3.6.1.2.1.83.1.1.3.1.2	The network address which when combined with the corresponding value of ipMRouteNextHopSourceMask identifies the sources for which this entry specifies a next-hop on an outgoing interface.	Source (IPM Route Next Hop Window)
ipMRouteNextHopSourceMask 1.3.6.1.2.1.83.1.1.3.1.3	The network mask which when combined with the corresponding value of ipMRouteNextHopSource identifies the sources for which this entry specifies a next-hop on an outgoing interface.	Source Mask (IPM Route Next Hop Window)
ipMRouteNextHopIfIndex 1.3.6.1.2.1.83.1.1.3.1.4	The ifIndex value of the interface for the outgoing interface for this next-hop.	IfIndex (IPM Route Next Hop Window)
ipMRouteNextHopAddress 1.3.6.1.2.1.83.1.1.3.1.5	The address of the next-hop specific to this entry. For most interfaces, this is identical to ipMRouteNextHopGroup. NBMA interfaces, however, may have multiple next-hop addresses out a single outgoing interface.	Next Hop Address (IPM Route Next Hop Window)

Object/OID	Description	Field Name in NMS
ipMRouteNextHopState 1.3.6.1.2.1.83.1.1.3.1.6	An indication of whether the outgoing interface and next-hop represented by this entry is currently being used to forward IP datagrams. The value 'forwarding' indicates it is currently being used; the value 'pruned' indicates it is not.	State (IPM Route Next Hop Window)
ipMRouteNextHopUpTime 1.3.6.1.2.1.83.1.1.3.1.7	The time, since the multicast routing information represented by this entry was learned by the router.	Up Time (IPM Route Next Hop Window)
ipMRouteNextHopExpiryTime 1.3.6.1.2.1.83.1.1.3.1.8	The minimum amount of time remaining before this entry will be aged out. If ipMRouteNextHopState is pruned(1), the remaining time until the prune expires and the state reverts to forwarding(2). Otherwise, the remaining time until this entry is removed from the table. The time remaining may be copied from ipMRouteExpiryTime if the protocol in use for this entry does not specify next-hop timers. The value 0 indicates that the entry is not subject to aging.	Expiry Time (IPM Route Next Hop Window)
ipMRouteNextHopProtocol 1.3.6.1.2.1.83.1.1.3.1.10	The routing mechanism via which this next-hop was learned.	Protocol (IPM Route Next Hop Window)
pimIpMRouteNextHopPruneReason 1.3.6.1.3.61.1.1.7.1.2	This object indicates why the downstream interface was pruned, whether in response to a PIM prune message or due to PIM Assert processing.	

IPX Interface Parameters

Object/OID	Description	Field Name in NMS
IpxCircTable ipxCircIndex 1.3.6.1.4.1.171.12.5.1.1.2	IPX circuit number.	Circuit Number
ipxCircTable ipxCircIfIndex 1.3.6.1.4.1.171.12.5.1.1.5	The IF Index used by this circuit.	Interface Number
No MIB associated with this NMS field.	Interface’s Ports.	Interface’s Ports (Field appears in Insert Window)
ifTable ifPhysAddress 1.3.6.1.2.1.2.2.1.6	MAC Address.	MAC Address (Field appears in Insert Window)
ipxCircTable ipxCircNetNumber 1.3.6.1.4.1.171.12.5.1.1.6	Network Address.	Network Address

Object/OID	Description	Field Name in NMS
ipxCircTable ipxCircTimeToNet 1.3.6.1.4.1.171.12.5.1.1.7	Time to net value associated with this interface, in 1/18ths of a second.	Time to Network
ipxCircTable ipxCircEncaps 1.3.6.1.4.1.171.12.5.1.1.8	Encapsulation method associated with this interface. If the Interface Number refers to a VLAN, this must be the same encapsulation as used by the VLAN.	Layer II Protocol
ipxCircTable ipxCircNetbiosDeliver 1.3.6.1.4.1.171.12.5.1.1.9	NetBios type 20 broadcast frames are forwarded to this interface.	NetBios
ipxCircTable ipxCircExistState 1.3.6.1.4.1.171.12.5.1.1.3	Indicates whether this circuit entry is valid, or Sleeping (currently inactive).	Admin. Status

IPX RIP/SAP Filter Table General Parameters

Object/OID	Description	Field Name in NMS
ipxCircTable ipxCircIndex 1.3.6.1.4.1.171.12.5.1.1.2	Circuit Number.	Circuit Number
ipxCircTable ipxCircNetNumber 1.3.6.1.4.1.171.12.5.1.1.6	Network Number.	Network Number

RIP Global Filter Table

Object/OID	Description	Field Name in NMS
rndIPXRipFilterGlbTable rndIPXRipFilterGlbFLtype 1.3.6.1.4.1.171.12.2.10.1.1	Defines whether the current filter entry works on traffic coming into or out of the device.	Type
rndIPXRipFilterGlbTable rndIPXRipFilterGlbFLnetworkPatern 1.3.6.1.4.1.171.12.2.10.1.4	Type in the network pattern the filter entry is to affect. The network pattern works in conjunction with the network mask to define the filter entry.	Network Address

Object/OID	Description	Field Name in NMS
rndIPXRipFilterGlbTable rndIPXRipFilterGlbFLnetwork Mask 1.3.6.1.4.1.171.12.2.10.1.5	Type in the letters F, 8, C, E, and 0 as many times as desired to indicate which network pattern part is important. The mask must be continuous from left to right. 00000000 means all addresses, ffffffff means one address (no address range). A combination of fs and 0s indicates a specific range. This combination must have f on the left side, 0 on the right side, and a single F, 8, C, or E, or 0 between them. For example, if the network pattern is set to 12345678, the network mask can be set to ffff0000. This indicates that only the first four network pattern numbers are checked, and the remaining numbers are irrelevant. In this example, only RIP messages with the numbers 1234 as their first four digits are affected.	Network Mask
rndIPXRipFilterGlbTable rndIPXRipFilterGlbFLaction 1.3.6.1.4.1.171.12.2.10.1.6	Defines whether the indicated packets are forwarded (permit) or blocked (denied) when the current filter entry conditions are met. The parameter is used to fine-tune other filter entries. For example, set a filter entry to block all RIP messages with a network pattern starting with 123, and set another filter entry to permit all RIP messages with a network pattern starting with 1234. As a result, all RIP messages with a network pattern starting with 123 that do not have 4 as the fourth digit are blocked. The default is forward, but the default can be set by creating a general filter entry with the network mask 00000000, and setting it to permit or deny.	Action

RIP Circuit Filter Table

Object/OID	Description	Field Name in NMS
rndIPXRipFilterCircuitTable rndIPXRipFilterCircFLType 1.3.6.1.4.1.171.12.2.11.1.2	Defines whether the current filter entry works on traffic coming into or out of the device.	Type
rndIPXRipFilterCircuitTable rndIPXRipFilterCircFLnetwork Patern 1.3.6.1.4.1.171.12.2.11.1.5	The network pattern to affect the filter entry. The network pattern works in conjunction with the network mask to define the filter entry.	Network Address

Object/OID	Description	Field Name in NMS
rndIPXRipFilterCircuitTable rndIPXRipFilterCircFLnetwork Mask 1.3.6.1.4.1.171.12.2.11.1.6	Type in the letters F, 8, C, E, and 0 as many times as desired to indicate which part of the network pattern is important. The mask must be continuous from left to right. 00000000 means all addresses, ffffffff means one address (no address range). A combination of f 0 indicates a specific range. This combination must have f on the left side, 0 on the right side, and a single F, 8, C, or E, or 0 between them. For example, if the network pattern is set to 12345678, set the network mask to ffff0000 to indicate that only the first four numbers of the network pattern are checked, and the remaining numbers are irrelevant. In this example, only RIP messages with the numbers 1234 as their first four digits are affected.	Network Mask
rndIPXRipFilterCircuitTable rndIPXRipFilterCircFLaction 1.3.6.1.4.1.171.12.2.11.1.7	Defines whether the indicated packets are forwarded (permit) or blocked (denied) when the current filter entry conditions are met. This parameter can be used to fine-tune other filter entries. For example, a filter entry can be set to block all RIP messages with a network pattern starting with 123, and set another filter entry to permit all RIP messages with a network pattern starting with 1234. As a result, all RIP messages with a network pattern starting with 123 that do not have 4 as the fourth digit are blocked.	Action

SAP Global Filter Table

Object/OID	Description	Field Name in NMS
rndIPXSapFilterGlbTable rndIPXSapFilterGlbFLtype 1.3.6.1.4.1.171.12.3.10.1.1	Defines whether the current filter entry works on traffic coming into or out of the device.	Type
rndIPXSapFilterGlbTable rndIPXSapFilterGlbFLnetwork Patern 1.3.6.1.4.1.171.12.3.10.1.4	Type in the network pattern to affect the filter entry. The network pattern works in conjunction with the network mask to define the filter entry.	Network Address
rndIPXSapFilterGlbTable rndIPXSapFilterGlbFLnetwork Mask 1.3.6.1.4.1.171.12.3.10.1.5	Type in the letters F, 8, C, E, and 0 as many times as desired to indicate which part of the network pattern is important. The mask must be continuous from left to right. 00000000 means all addresses, ffffffff means one address (no address range). A combination of f 0 indicates a specific range. This combination must have f on the left side, 0 on the right side, and a single F, 8, C, or E, or 0 between them. *For example*, if the network pattern is set to 12345678, the network mask can be set to ffff0000 to indicate that only the first four numbers of the network pattern are only checked, and the remaining numbers are irrelevant. In this example, only SAP messages with the numbers 1234 as their first four digits are affected.	Network Mask

Object/OID	Description	Field Name in NMS
rndIPXSapFilterGlbTable rndIPXSapFilterGlbFLserviceType 1.3.6.1.4.1.171.12.3.10.1.6	Type in the type of server (in hex) the filter entry affects, such as file server or print server. Value 0xFFFF applies for all types of service and is the default.	Service Type
rndIPXSapFilterGlbTable rndIPXSapFilterGlbFLserviceName 1.3.6.1.4.1.171.12.3.10.1.7	Type in the server name the filter entry affects. An asterisk (*) at the end of the name as a wild card, designates any number of characters. For example, * indicates any server name, and sh* indicates any server name starting with sh. The name may be up to 47 characters.	Service Name
rndIPXSapFilterGlbTable rndIPXSapFilterGlbFLaction 1.3.6.1.4.1.171.12.3.10.1.8	Defines whether the indicated packets are to be forwarded (permit) or blocked (denied) when the current filter entry conditions are met. This parameter is used to fine-tune other filter entries. For example, a filter entry can be set to block all SAP messages with a network pattern starting with 123, and set another filter entry to permit all SAP messages with a network pattern starting with 1234. All SAP messages with a network pattern starting with 123 that do not have 4 as the fourth digit are blocked. The default is forward, but the default can be set by creating a general filter entry with the network mask 00000000, and setting it to permit or deny.	Action

SAP Circuit Filter Table

Object/OID	Description	Field Name in NMS
rndIPXSapFilterCircuitTable rndIPXSapFilterCircFLtype 1.3.6.1.4.1.171.12.3.11.1.2	Defines whether the current filter entry works on traffic coming into or out of the device.	Type
rndIPXSapFilterCircuitTable rndIPXSapFilterCircFLnetworkPatern 1.3.6.1.4.1.171.12.3.11.1.5	The network pattern the filter entry affects. The network pattern works in conjunction with the network mask to define the filter entry.	Network Address
rndIPXSapFilterCircuitTable rndIPXSapFilterCircFLnetworkMask 1.3.6.1.4.1.171.12.3.11.1.6	Type in the letters F, 8, C, E, and 0 as many times as desired to indicate which part of the network pattern is important. The mask must be continuous from left to right. 00000000 means all addresses, ffffffff means one address (no address range). A combination of f 0 indicates a specific range. This combination must have f on the left side, 0 on the right side, and a single F, 8, C, or E, or 0 between them. For example, if the network pattern is set to 12345678, set the network mask to ffff0000 to indicate that only the first four numbers of the network pattern are checked, and the remaining numbers are irrelevant. In this example, only RIP messages with the numbers 1234 as their first four digits are affected.	Network Mask

Object/OID	Description	Field Name in NMS
rndIPXSapFilterCircuitTable rndIPXSapFilterCircFLserviceType 1.3.6.1.4.1.171.12.3.11.1.7	Type in the type of server (in hex) the filter entry affects, such as file server or print server. Value 0xFFFF applies for all types of service and is the default.	Service Type
rndIPXSapFilterCircuitTable rndIPXSapFilterCircFLserviceName 1.3.6.1.4.1.171.12.3.11.1.8	Type in the server name the filter entry affects. An asterisk (*) at the end of the name as a wild-card, designating any number of characters. For example, * indicates any server name, and sh* indicates any server name starting with sh. The name may be up to 47 characters.	Service Name
rndIPXSapFilterCircuitTable rndIPXSapFilterCircFLaction 1.3.6.1.4.1.171.12.3.11.1.9	Defines whether the indicated packets are to be forwarded (permit) or blocked (denied) when the current filter entry conditions are met. This parameter can be used to fine-tune other filter entries. For example, a filter entry can be set to block all SAP messages with a network pattern starting with 123, and set another filter entry to permit all SAP messages with a network pattern starting with 1234. As a result, all SAP messages with a network pattern starting with 123 that do not have 4 as the fourth digit are blocked. The default is forward, but the default can be set by creating a general filter entry with the network mask 00000000, and setting it to permit or deny.	Action

IPX Routing Table

Object/OID	Description	Field Name in NMS
ipxDestTable ipxDestNetNum 1.3.6.1.4.1.171.12.6.1.1.2	Destination IPX network numbers in ascending order.	Destination Network/Network Addresss
ipxDestTable ipxDestNextHopCircIndex 1.3.6.1.4.1.171.12.6.1.1.3	The circuit number used to reach the next hop.	Circuit/ Circuit Number
ipxDestTable ipxDestProtocol 1.3.6.1.4.1.171.12.6.1.1.4	The routing protocol from which knowledge of this destination was obtained: **Static—**User-defined entry (SNMP). **Local—**The entry derived from an IPX interface definition. **RIP—**The entry learned from the RIP protocol.	Dest Protocol
ipxDestTable ipxDestTicks 1.3.6.1.4.1.171.12.6.1.1.5	Time estimate required for the propagation of a packet sent along the route described by this table entry to the destination network. This estimate is given in ticks (there are 18.21 ticks in a second), and does not include delays introduced by buffers used for temporary storage of packets in routers.	Ticks to Net

Object/OID	Description	Field Name in NMS
ipxDestTable ipxDestHopCount 1.3.6.1.4.1.171.12.6.1.1.6	Describes this table entry number of hops on the route to the destination network. Entries with more than 15 hops are removed from the table.	Hops to Net
ipxDestTable ipxDestNextHopNICAddress 1.3.6.1.4.1.171.12.6.1.1.7	IPX node address (12 hexadecimal digits) of the next IPX router in the route to the destination network, described by this table entry. If the destination network is one of the network segments directly connected to this IPX router, this field is all zeroes.	Forwarding Router Address
ipxDestTable ipxDestNextHopNetNum 1.3.6.1.4.1.171.12.6.1.1.8	Next hop IPX network number.	Next Hop Net Num
ipxDestTable ipxDestExistState 1.3.6.1.4.1.171.12.6.1.1.9	Defines whether the RIP interface is active. OFF is inactive but not deleted.	Status

IPX SAP Table

Object/OID	Description	Field Name in NMS
ipxServTable ipxServName 1.3.6.1.4.1.171.12.7.1.1.3	Server type and server name to identify a server. The name can include up to 47 characters.	Server Name
ipxServTable ipxServNetNum 1.3.6.1.4.1.171.12.7.1.1.5	Network portion (eight hexadecimal digits) from the IPX server address.	Network
ipxServTable ipxServNode 1.3.6.1.4.1.171.12.7.1.1.6	Node portion 12 hexadecimal digits) from the IPX server address.	Server Address
ipxServTable ipxServSocket 1.3.6.1.4.1.171.12.7.1.1.7	Socket portion up to four hexadecimal digits) from the IPX server address.	Socket
ipxServTable ipxServType 1.3.6.1.4.1.171.12.7.1.1.2	Type of service (assigned by Novell) provided by the server.	Server Type
ipxServTable ipxServHopCount 1.3.6.1.4.1.171.12.7.1.1.8	Number of hops on the route to the server, as determined by the IPX SAP routing algorithm.	Hops to Server
ipxServTable ipxServProtocol 1.3.6.1.4.1.171.12.7.1.1.4	The information source protocol. **Static—**User-defined entry (SNMP) **SAP—**SAP protocol.	Protocol Type

Object/OID	Description	Field Name in NMS
ipxServTable ipxServExistState 1.3.6.1.4.1.171.12.7.1.1.9	Defines whether the SAP interface is active. OFF is inactive but not deleted.	Status

Security Parameters

Use the following variables to modify the community tables.

Security Community Table

Object/OID	Description	Field Name in NMS
rndCommunityTable rndCommunityMngStationAddr 1.3.6.1.4.1.171.2.7.2.1.1	Management station IP address.	Management Address
rndCommunityTable rndCommunityString 1.3.6.1.4.1.171.2.7.2.1.2	Management station community name. This parameter operates as a password for gaining various access rights: for each device various communities with different names and access rights can be created.	Community String
rndCommunityTable rndCommunityAccess 1.3.6.1.4.1.171.2.7.2.1.3	Defines whether the management station access is Read Only or Read Write. Choose Super Community to set the name used to access this Community Table.	Community Access
rndCommunityTable rndCommunityTrapsEnable 1.3.6.1.4.1.171.2.7.2.1.4	Whether the management station receives traps from the device (Enable) or not (Disable).	Send Traps

WEB User Authorization Table

Object/OID	Description	Field Name in NMS
rlEmWebSecurityTable rlEmWebSecurityEntry 1.3.6.1.4.1.171.66.3.1	The row definition for this table.	
rlEmWebSecurityTable rlEmWebSecurityUserName 1.3.6.1.4.1.171.66.3.1.1	The user name.	Security User Name (WEB User Authorization Table)
rlEmWebSecurityTable rlEmWebSecurityPassword 1.3.6.1.4.1.171.66.3.1.2	The user password.	Security Password (WEB User Authorization Table)
rlEmWebSecurityTable rlEmWebSecurityAccess 1.3.6.1.4.1.171.66.3.1.3	Access rights for the user.	Security Access (WEB User Authorization Table)

Object/OID	Description	Field Name in NMS
rlEmWebSecurityTable rlEmWebSecurityStatus 1.3.6.1.4.1.171.66.3.1.7	The status of the security table entry. It's used to delete an entry.	Security Status (WEB User Authorization Table)

QoS Parameters

Use the following variables to modify the QoS (Quality of Service) global parameters, QoS profile, IP classification fields and IP rules.

QoS Global Parameters

Object/OID	Description	Field Name in NMS
rlPolicySimpleGalMibVersion 1.3.6.1.4.1.171.56.9.1	The version of the QoS program.	Policy Version
rlPolicySimpleGalMibPolicyEnable 1.3.6.1.4.1.171.56.9.4	If enabled, this policy is enabled on the device.	Policy Enable

QoS Profile Table

Object/OID	Description	Field Name in NMS
rlPolicySimpleGalMibProfileTable rlPolicySimpleGalMibDescription 1.3.6.1.4.1.171.56.9.5.1.2	The user-defined description of the profile.	Description
rlPolicySimpleGalMibProfileTable rlPolicySimpleGalMibProfileType 1.3.6.1.4.1.171.56.9.5.1.3	The type of forwarding service to be applied to packets. The possible values are: **BandwidthGuarantee—**Defines the bandwidth size for packets being forwarded. Packets must meet the bandwidth requirements to be forwarded. Packets exceeding the defined bandwidth size are dropped. **minbandwidthGuarantee—**Defines the minimum bandwidth size for packets being forwarded. Packets beyond the defined bandwidth size receive a best-effort forwarding priority. **minDelay—**Forwards packets with a priority of real time forwarding. Packets exceeding the assigned amount of bandwidth are dropped. **minDelayPerSession—**Defines the amount of bandwidth per session for a real time forwarding priority. Sessions exceeding the defined amount of sessions are dropped.	Profile Type

Object/OID	Description	Field Name in NMS
rlPolicySimpleGalMibProfileTable rlPolicySimpleGalMibRate 1.3.6.1.4.1.171.56.9.5.1.4	The rate in kilobits/seconds assigned to a profile for forwarding a packet. The values are 0-12 Gbps depending on the output port.	Rate (kbps)
rlPolicySimpleGalMibProfileTable rlPolicySimpleGalMibMaxSession 1.3.6.1.4.1.171.56.9.5.1.6	Max Session is only relevant to the **minDelayPerSession** profile type. Indicates the maximum number of sessions that can occur for a profile instance.	Max Session
rlPolicySimpleGalMibProfileTable rlPolicySimpleGalMibNewVpt 1.3.6.1.4.1.171.56.9.5.1.7	Maps the VLAN Priority Tag (Vpt) to a priority tag value. The Vpt tag value is used to override the packets value. The possible values are 0-7. Zero is the default. The higher the Vpt tag value the lower the forwarding priority.	New VPT
rlPolicySimpleGalMibProfileTable rlPolicySimpleGalMibChangeTosOrDscp 1.3.6.1.4.1.171.56.9.5.1.8	Type of Service. Enables you to override the ToS value. The possible values are 0–3.	New TOS (Field appears on the Advanced tab of the Insert Window)
rlPolicySimpleGalMibProfileTable rlPolicySimpleGalMibBurstSize 1.3.6.1.4.1.171.56.9.5.1.5	The amount of bytes that can be forwarded back-to-back faster than normal speed. If the value is 0, the device uses a predefined value. The default size is 0. If the burst size value is 0, the value for **minDelayPerSession** and **minDelay** is 1,536 bytes. **MinbandwidthGuarantee** and **BandwidthGuarantee** are forwarded with a value of 3x 1,536 bytes.	Burst Size (bytes) (Field appears on the Advanced tab of the Insert Window)

QoS IP Classification Fields

Object/OID	Description	Field Name in NMS
rlPolicySimpleGalMibProfileTable rlPolicySimpleGalMibNewTosOrDscp 1.3.6.1.4.1.171.56.9.5.1.9	Type of Service. Enables classification by the ToS tagging for forwarding packets.	TOS
rlPolicySimpleGalMibIpFcogTable rlPolicySimpleGalMibIpFcogProtocol 1.3.6.1.4.1.171.56.9.6.1.3	Enables classification of packets by their type of protocol.	Protocol
rlPolicySimpleGalMibIpFcogTable rlPolicySimpleGalMibIpFcogSrcIpMask 1.3.6.1.4.1.171.56.9.6.1.4	Used to mask all or part of the source IP address. If selected, QoS looks for and classifies packets arriving from the indicated source IP address, within the limits of the source IP mask. The values are 0-32.	Source IP Bit Mask (0-32)

Object/OID	Description	Field Name in NMS
rlPolicySimpleGalMibIpFcogTable rlPolicySimpleGalMibIpFcogDstIpMask 1.3.6.1.4.1.171.56.9.6.1.5	Used to mask all or part of the destination IP address. If selected, QoS looks for and classifies packets being sent to the indicated destination IP address, within the limits of the destination IP mask.	Destination IP Bit Mask (0-32)
rlPolicySimpleGalMibIpFcogTable rlPolicySimpleGalMibIpFcogSrcPort 1.3.6.1.4.1.171.56.9.6.1.6	Enables the classification of packets by their type of source port protocol.	Source Port Protocol
rlPolicySimpleGalMibIpFcogTable rlPolicySimpleGalMibIpFcogDstPort 1.3.6.1.4.1.171.56.9.6.1.7	Enables the classification of packets by their type of destination port protocol.	Destination Port Protocol
rlPolicySimpleGalMibIpFcogTable rlPolicySimpleGalMibIpFcogInIfIndex 1.3.6.1.4.1.171.56.9.6.1.8	Enables the classification of arriving packets by the physical input port.	Input Ports

QoS IP Rules Table

Note: *The first rule matching a packet is applied, therefore, the order of the rules in the Rule Table is important.*

Object/OID	Description	Field Name in NMS
rlPolicySimpleGalMibIpRulesTable rlPolicySimpleGalMibIpRulesDescription 1.3.6.1.4.1.171.56.9.7.1.3	The user-defined description of the rule.	Description
rlPolicySimpleGalMibIpRulesTable rlPolicySimpleGalMibIpRulesTosOrDscp 1.3.6.1.4.1.171.56.9.7.1.4	Type of Service. Indicates the predefined ToS used to classify packets. If selected, the rule applies to packets matching the ToS type. The possible values are 0-3. The default is disabled.	ToS
rlPolicySimpleGalMibIpRulesTable rlPolicySimpleGalMibIpRulesProtocol 1.3.6.1.4.1.171.56.9.7.1.5	The protocol type. Indicates the type of predefined protocols used to classify packets. If selected, the rule applies to packets of this indicated protocol. The possible values are TCP and UDP.	Protocol

Object/OID	Description	Field Name in NMS
rlPolicySimpleGalMibIpRulesTable rlPolicySimpleGalMibIpRulesSrcIp 1.3.6.1.4.1.171.56.9.7.1.6	The source IP address of packets being matched to the rule. If selected, QoS looks for and applies the rule to packets arriving from the indicated source IP address.	Source IP
rlPolicySimpleGalMibIpRulesTable rlPolicySimpleGalMibIpRulesSrcIpMask 1.3.6.1.4.1.171.56.9.7.1.7	Used to mask all or part of the source IP address. If selected, QoS looks for and matches the rule to packets being sent from the indicated source IP address, within the limits of the Source IP Mask. The Source IP Mask must not exceed the limits set in the IP Classification fields.	Source IP Mask
rlPolicySimpleGalMibIpRulesTable rlPolicySimpleGalMibIpRulesDstIp 1.3.6.1.4.1.171.56.9.7.1.8	The destination address of packets being matched to the rule. If selected, QoS looks for and applies the rule to packets being sent to the indicated IP address.	Destination IP
rlPolicySimpleGalMibIpRulesTable rlPolicySimpleGalMibIpRulesDstIpMask 1.3.6.1.4.1.171.56.9.7.1.9	Used to mask all or part of the destination IP address. If selected, QoS looks for and matches the rule to packets being sent to the indicated destination IP address, within the limits of the destination IP mask. The Destination IP Mask must not exceed the limits set in the IP Classification fields.	Destination IP Mask
rlPolicySimpleGalMibIpRulesTable rlPolicySimpleGalMibIpRulesSrcPort 1.3.6.1.4.1.171.56.9.7.1.10	Indicates if and which source port should be used when matching the rule to packets.	Source Port
rlPolicySimpleGalMibIpRulesTable rlPolicySimpleGalMibIpRulesDstPort 1.3.6.1.4.1.171.56.9.7.1.11	Indicates if and which destination port should be used when matching the rule to packets.	Destination Port

Object/OID	Description	Field Name in NMS
rlPolicySimpleGalMibIpRulesTable rlPolicySimpleGalMibIpRulesCondition 1.3.6.1.4.1.171.56.9.7.1.13	Specifies whether packets' value should be different from the rules' value. The possible values are: **Bigger—**Looks for more than the exact data. Indicates that the parameter values of a packet should be larger than the parameter values of the rule. **Smaller—**Looks for less than the exact data. Indicates that the parameter values of a packet should be smaller than the parameter values of the rule. **Equal—**Looks for the exact data. Indicates that all of the parameter values of a packet should match all of the parameter values of the rule. **Not Equal—**Looks for non-matching data. Indicates that none of the parameter values of a packet should match the parameter values of the rule. All values must be different.	Condition
rlPolicySimpleGalMibIpRulesTable rlPolicySimpleGalMibIpRulesInIfIndexList 1.3.6.1.4.1.171.56.9.7.1.12	Indicates to which ports this rule applies. Packets arriving from the defined port are forwarded according to the rule definition.	Input Ports
rlPolicySimpleGalMibIpRulesTable rlPolicySimpleGalMibIpRulesAction 1.3.6.1.4.1.171.56.9.7.1.14	The action to be taken on packets when matched to the rule. The possible values are: **Block—**Drops packets. **Block and Trap—**Drops packets and notifies the CPU that packets were dropped. **Permit—**Forwards packets. If the action is permit, then the output ports to which this rule applies can be selected. This is the default value.	Action
rlPolicySimpleGalMibIpRulesTable rlPolicySimpleGalMibIpRulesProfilePointer 1.3.6.1.4.1.171.56.9.7.1.15	Indicates which profile is attached to the rule. This field is only active if the forwarding condition of the packet is **permit**. The default value is 0. Zero is illegal if the action is **permit**.	Profile Pointer
rlPolicySimpleGalMibIpRulesTable rlPolicySimpleGalMibIpRulesOutIfIndexList 1.3.6.1.4.1.171.56.9.7.1.16	Indicates to which ports this rule applies. This field is only active if the forwarding condition of the packet is **permit**. The default value is all ports.	Output Ports

Object/OID	Description	Field Name in NMS
rlPolicySimpleGalMibIpRulesTable rlPolicySimpleGalMibIpRulesErrorDescrip 1.3.6.1.4.1.171.56.9.7.1.18	Indicates if the rule is valid. The error description can be one of the following: **The bandwidth specified exceeds the available specified bandwidth on the output ports—** Indicates that the amount of the bandwidth specified exceeds the available amount of bandwidth as defined for the profile matching the rule. **The QoS lock failed—**Indicates that auto-negotiation is enabled, or that the port is not in full duplex mode. To edit the port configuration see Port Properties.	Error Description
rlPolicySimpleGalMibIpRulesTable rlPolicySimpleGalMibIpRulesStatus 1.3.6.1.4.1.171.56.9.7.1.19	Indicates if the rule is currently active and can be applied to a packet. The status can be one of the following: **Active—**The rule is legal and currently active. **Not in Service—**The rule is currently not active. **Not Ready—**Indicates that some of the output ports do not meet the bandwidth allocation prerequisites or QoS locking prerequisites. Auto-negotiation should be disabled and that the output port in full duplex mode.	Status

Statistics Parameters

Use the following variables to modify the element, port, IP/IPX interface, alarm, trap table, and log table statistics parameters.

Element Statistics

Object/OID	Description	Field Name in NMS
ipInAddrErrors 1.3.6.1.2.1.4.5	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For entities which are not IP routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.	Datagrams discarded - IP address not valid
ipInDiscards 1.3.6.1.2.1.4.8	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.	Input IP fine datagrams discarded
ipInDelivers 1.3.6.1.2.1.4.9	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).	IP datagrams successfully delivered

Object/OID	Description	Field Name in NMS
ipOutRequests 1.3.6.1.2.1.4.10	The total number of IP datagrams which local IP user protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.	Total IP datagrams requests for transmission
ipOutDiscards 1.3.6.1.2.1.4.11	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.	Output IP fine datagrams discarded
snmpInPkts 1.3.6.1.2.1.11.1	The total number of messages delivered to the SNMP entity from the transport service.	**Total SNMP messages received**
snmpOutPkts 1.3.6.1.2.1.11.2	The total number of SNMP Messages, which were passed from the SNMP protocol entity to the transport service.	Total SNMP output messages passed
snmpInTotalReqVars 1.3.6.1.2.1.11.13	The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.	SNMP "get" requests retrieved successfully
snmpInTotalSetVars 1.3.6.1.2.1.11.14	The total number of MIB objects, which have been altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.	SNMP "set" requests retrieved successfully
snmpInGetRequests 1.3.6.1.2.1.11.15	The total number of SNMP Get-Request PDUs, which have been accepted and processed by the SNMP protocol entity.	SNMP "Get-Request" PDUs processed
snmpInGetNexts 1.3.6.1.2.1.11.16	The total number of SNMP Get-Next PDUs, which have been accepted and processed by the SNMP protocol entity.	SNMP 'Get-Next' PDUs processed
snmpInSetRequests 1.3.6.1.2.1.11.17	The total number of SNMP Set-Request PDUs, which have been accepted and processed by the SNMP protocol entity.	SNMP 'Set-Request' PDUs processed
snmpOutTooBigs 1.3.6.1.2.1.11.20	The total number of SNMP PDUs, which were generated by the SNMP protocol entity and for which the value of the error-status field is ‘tooBig’.	SNMP output PDUs - tooBig
snmpOutNoSuchNames 1.3.6.1.2.1.11.21	The total number of SNMP PDUs, which were generated by the SNMP protocol entity and for which the value of the error-status is ‘noSuchName’.	SNMP output PDUs - noSuchName
snmpOutBadValues 1.3.6.1.2.1.11.22	The total number of SNMP PDUs, which were generated by the SNMP protocol entity and for which the value of the error-status field is ‘badValue’.	SNMP output PDUs - badValues
snmpOutGenErrs 1.3.6.1.2.1.11.24	The total number of SNMP PDUs, which were generated by the SNMP protocol entity and for which the value of the error-status field is ‘genErr’.	SNMP output PDUs - 'genErr'

Object/OID	Description	Field Name in NMS
snmpOutGetResponses 1.3.6.1.2.1.11.28	The total number of SNMP Get-Response PDUs, which have been generated by the SNMP protocol entity.	SNMP generated 'Get-Response' PDUs
snmpOutTraps 1.3.6.1.2.1.11.29	The total number of SNMP Trap PDUs, which have been generated by the SNMP protocol entity.	SNMP generated 'Trap' PDUs
ipForwDatagrams 1.3.6.1.2.1.4.6	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP routers, this counter will include only those packets, which were Source-Routed via this entity, and the Source-Route option processing was successful.	Input IP datagrams forwarded
ipInUnknownProtos 1.3.6.1.2.1.4.7	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.	Input IP datagrams discarded - protocol problems
ipOutNoRoutes 1.3.6.1.2.1.4.12	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams, which meet this 'no-route' criterion. This includes any datagrams, which a host cannot route because all of its default routers are down.	Output IP datagrams discarded - no route found
ipRoutingDiscards 1.3.6.1.2.1.4.23	The number of routing entries, which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.	Valid routing entries discarded
rip2GlobalRouteChanges 1.3.6.1.2.1.23.1.1	The number of route changes made to the IP Route Database by RIP. This does not include the refresh of a route's age.	RIP - changes made to IP Route Database
rip2GlobalQueries 1.3.6.1.2.1.23.1.2	The number of responses sent to RIP queries from other systems.	RIP - global responses sent to RIP queries
ospfOriginateNewLsas 1.3.6.1.2.1.14.1.9	The number of new link-state advertisements that have been originated. This number is incremented each time the router originates a new LSA.	OSPF - new LSAs originated
ospfRxNewLsas 1.3.6.1.2.1.14.1.10	The number of link-state advertisements received determined to be new instantiations. This number does not include newer instantiations of self-originated link-state advertisements.	OSPF - LSAs received - new instantiations
ipxBasicSysInReceives 1.3.6.1.4.1.171.12.4.1.1.3	The total number of IPX packets received, including those received in error.	Total IPX packets received
ipxBasicSysInHdrErrors 1.3.6.1.4.1.171.12.4.1.1.4	The number of IPX packets discarded due to errors in their headers, including any IPX packet with a size less than the minimum of 30 bytes.	Packets discarded - IPX header error

Object/OID	Description	Field Name in NMS
ipxBasicSysInUnknownSockets 1.3.6.1.4.1.171.12.4.1.1.5	The number of IPX packets discarded because the destination socket was not open.	IPX packets discarded - destination socket not open
ipxBasicSysInDiscards 1.3.6.1.4.1.171.12.4.1.1.6	The number of IPX packets received but discarded due to reasons other than those accounted for by ipxBasicSysInHdrErrors, ipxBasicSysInUnknownSockets, ipxAdvSysInDiscards, and ipxAdvSysInCompressDiscards.	IPX packets discarded - other reasons
ipxBasicSysInDelivers 1.3.6.1.4.1.171.12.4.1.1.7	The total number of IPX packets delivered locally, including packets from local applications.	IPX packets delivered locally
ipxBasicSysNoRoutes 1.3.6.1.4.1.171.12.4.1.1.8	The number of times no route to a destination was found.	IPX - no route found
ipxBasicSysOutRequests 1.3.6.1.4.1.171.12.4.1.1.9	The number of IPX packets supplied locally for transmission, not including any packets counted in ipxAdvForwPackets.	IPX packets supplied locally for transmission
ipxBasicSysOutMalformedRequests 1.3.6.1.4.1.171.12.4.1.1.10	The number of IPX packets supplied locally that contained errors in their structure.	IPX packets supplied locally that contained errors
ipxBasicSysOutDiscards 1.3.6.1.4.1.171.12.4.1.1.11	The number of outgoing IPX packets discarded due to reasons other than those accounted for in ipxBasicSysOutMalformedRequests, ipxAdvSysOutFiltered, and ipxAdvSysOutCompressDiscards.	Outgoing IPX packets discarded - other reasons
ipxBasicSysOutPackets 1.3.6.1.4.1.171.12.4.1.1.12	The total number of IPX packets transmitted.	Total IPX packets transmitted
icmpInMsgs 1.3.6.1.2.1.5.1	The total number of ICMP messages, which the entity has received. Note that this counter includes all those counted by icmpInErrors.	ICMP messages which the entity received
icmpOutMsgs 1.3.6.1.2.1.5.14	The total number of ICMP messages which this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.	ICMP messages which this entity attempted to send
icmpOutErrors 1.3.6.1.2.1.5.15	The number of ICMP messages, which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of errors, which contribute to this counter's value.	ICMP messages not sent - problems within ICMP
icmpOutEchos 1.3.6.1.2.1.5.21	The number of ICMP Echo (request) messages sent.	ICMP Echo (request) messages sent
icmpOutEchoReps 1.3.6.1.2.1.5.22	The number of ICMP Echo Reply messages sent.	ICMP Echo Reply messages sent
udpInDatagrams 1.3.6.1.2.1.7.1	The total number of UDP datagrams delivered to UDP users.	UDP datagrams delivered to UDP users

Object/OID	Description	Field Name in NMS
udpNoPorts 1.3.6.1.2.1.7.2	The total number of received UDP datagrams for which there was no application at the destination port.	UDP datagrams - no application at destination port
udpInErrors 1.3.6.1.2.1.7.3	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.	UDP datagrams not delivered - other reasons
udpOutDatagrams 1.3.6.1.2.1.7.4	The total number of UDP datagrams sent from this entity.	UDP datagrams sent from this entity

IP Interface Statistics

Object/OID	Description	Field Name in NMS
rsIpAddrTable rsIpAdEntIfIndex 1.3.6.1.4.1.171.26.1.1.2	Interface Number.	Interface Number
rsIpAddrTable rsIpAdEntAddr 1.3.6.1.4.1.171.26.1.1.1	IP address.	IP address

IPX Interface Statistics

Object/OID	Description	Field Name in NMS
ipxCircTable ipxCircIndex 1.3.6.1.4.1.171.12.5.1.1.2	Circuit Number.	Circuit Number
ipxCircTable ipxCircNetNumber 1.3.6.1.4.1.171.12.5.1.1.6	Network Address.	Network Address

History Control Table

Object/OID	Description	Field Name in NMS
historyControlEntry 1.3.6.1.2.1.16.2.1.1	A list of parameters that set up a periodic sampling of statistics. As an example, an instance of the historyControlInterval object might be named historyControlInterval.2	
historyControlTable historyControlIndex 1.3.6.1.2.1.16.2.1.1.1	An index that uniquely identifies an entry in the historyControl table. Each such entry defines a set of samples at a particular interval for an interface on the device.	Index (History Control Table Window)

Object/OID	Description	Field Name in NMS
historyControlTable historyControlDataSource 1.3.6.1.2.1.16.2.1.1.2	This object identifies the source of the data for which historical data was collected and placed in a media-specific table on behalf of this historyControlEntry. This source can be any interface on this device. In order to identify a particular interface, this object shall identify the instance of the ifIndex object, defined in RFC 1213 and RFC 1573 [4,6], for the desired interface. For example, if an entry were to receive data from interface #1, this object would be set to ifIndex.1. The statistics in this group reflect all packets on the local network segment attached to the identified interface. This object may not be modified if the associated historyControlStatus object is equal to valid (1).	Port Number (History Control Table Window)
historyControlTable historyControlBucketsRequested 1.3.6.1.2.1.16.2.1.1.3	The requested number of discrete time intervals over which data is to be saved in the part of the media-specific table associated with this historyControlEntry. When this object is created or modified, the probe should set historyControlBucketsGranted as closely to this object as is possible for the particular probe implementation and available resources.	Buckets Requested (History Control Table Window)

Object/OID	Description	Field Name in NMS
historyControlTable historyControlBucketsGranted 1.3.6.1.2.1.16.2.1.1.4	The number of discrete sampling intervals over which data shall be saved in the part of the media-specific table associated with this historyControlEntry. When the associated HistoryControlBucketsRequested object is created or modified, the probe should set this object as closely to the requested value as is possible for the particular probe implementation and available resources. The probe must not lower this value except as a result of a modification to the associated historyControlBucketsRequested object. There will be times when the actual number of buckets associated with this entry is less than the value of this object. In this case, at the end of each sampling interval, a new bucket will be added to the media-specific table. When the number of buckets reaches the value of this object and a new bucket is to be added to the media-specific table, the oldest bucket associated with this historyControlEntry shall be deleted by the agent so that the new bucket can be added. When the value of this object changes to a value less than the current value, entries are deleted from the media-specific table associated with this historyControlEntry. Enough of the oldest of these entries shall be deleted by the agent so that their number remains less than or equal to the new value of this object. When the value of this object changes to a value greater than the current value, the number of associated media- specific entries may be allowed to grow.	Buckets Granted (History Control Table Window)
historyControlTable historyControlInterval 1.3.6.1.2.1.16.2.1.1.5	The interval in seconds over which the data is sampled for each bucket in the part of the media-specific table associated with this historyControlEntry. This interval can be set to any number of seconds between 1 and 3600 (1 hour). Because the counters in a bucket may overflow at their maximum value with no indication, a prudent manager will take into account the possibility of overflow in any of the associated counters. It is important to consider the minimum time in which any counter could overflow on a particular media type and set the historyControlInterval object to a value less than this interval. This is typically most important for the 'octets' counter in any media-specific table. For example, on an Ethernet network, the etherHistoryOctets counter could overflow in about one hour at the Ethernet's maximum utilization. This object may not be modified if the associated historyControlStatus object is equal to valid(1).	Interval (History Control Table Window)

Object/OID	Description	Field Name in NMS
historyControlTable historyControlOwner 1.3.6.1.2.1.16.2.1.1.6	The entity that configured this entry and is therefore using the resources assigned to it.	(History Control Table Window)
historyControlTable historyControlStatus 1.3.6.1.2.1.16.2.1.1.7	The status of this historyControl entry. Each instance of the media-specific table associated with this historyControlEntry will be deleted by the agent if this historyControlEntry is not equal to valid(1).	Status (History Control Table Window)

Either History Table

Object/OID	Description	Field Name in NMS
etherHistoryEntry 1.3.6.1.2.1.16.2.2.1	An historical sample of Ethernet statistics on a particular Ethernet interface. This sample is associated with the historyControlEntry, which set up the parameters for a regular collection of these samples. As an example, an instance of the etherHistoryPkts object might be named etherHistoryPkts.2.171	
etherHistoryIndex 1.3.6.1.2.1.16.2.2.1.1	The history of which this entry is a part. The history identified by a particular value of this index is the same history as identified by the same value of historyControlIndex.	Index (Either History Table Window)
etherHistorySampleIndex 1.3.6.1.2.1.16.2.2.1.2	An index that uniquely identifies the particular sample this entry represents among all samples associated with the same historyControlEntry. This index starts at 1 and increases by one as each new sample is taken.	Sample Index (Either History Table Window)
etherHistoryIntervalStart 1.3.6.1.2.1.16.2.2.1.3	The value of sysUpTime at the start of the interval over which this sample was measured. If the probe keeps track of the time of day, it should start the first sample of the history at a time such that when the next hour of the day begins, a sample is started at that instant. Note that following this rule may require the probe to delay collecting the first sample of the history, as each sample must be of the same interval. Also note that the sample, which is currently being collected, is not accessible in this table until the end of its interval.	Interval Start (Either History Table Window)
etherHistoryDropEvents 1.3.6.1.2.1.16.2.2.1.4	The total number of events in which packets were dropped by the probe due to lack of resources during this sampling interval. Note that this number is not necessarily the number of packets dropped, it is just the number of times this condition has been detected.	Drop Events (Either History Table Window)
etherHistoryOctets 1.3.6.1.2.1.16.2.2.1.5	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).	Octets (Either History Table Window)
etherHistoryPkts 1.3.6.1.2.1.16.2.2.1.6	The number of packets (including bad packets) received during this sampling interval.	Pkts (Either History Table Window)

Object/OID	Description	Field Name in NMS
etherHistoryBroadcastPkts 1.3.6.1.2.1.16.2.2.1.7	The number of good packets received during this sampling interval that were directed to the broadcast address.	Broadcast Pkts (Either History Table Window)
etherHistoryMulticastPkts 1.3.6.1.2.1.16.2.2.1.8	The number of good packets received during this sampling interval that were directed to a multicast address. Note that this number does not include packets addressed to the broadcast address.	Multicast Pkts (Either History Table Window)
etherHistoryCRCAlignErrors 1.3.6.1.2.1.16.2.2.1.9	The number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).	CRC Align Errors (Either History Table Window)
etherHistoryUndersizePkts 1.3.6.1.2.1.16.2.2.1.10	The number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.	Undersize Pkts (Either History Table Window)
etherHistoryOversizePkts 1.3.6.1.2.1.16.2.2.1.11	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.	Oversize Pkts (Either History Table Window)
etherHistoryFragments 1.3.6.1.2.1.16.2.2.1.12	The total number of packets received during this sampling interval that were less than 64 octets in length (excluding framing bits but including FCS octets) had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).	Fragments (Either History Table Window)
etherHistoryJabbers 1.3.6.1.2.1.16.2.2.1.13	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).	Jabbers (Either History Table Window)
etherHistoryCollisions 1.3.6.1.2.1.16.2.2.1.14	The best estimate of the total number of collisions on this Ethernet segment during this sampling interval.	Collisions (Either History Table Window)
etherHistoryUtilization 1.3.6.1.2.1.16.2.2.1.15	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.	Utilization (Either History Table Window)

Alarm Table Statistics

Object/OID	Description	Field Name in NMS
alarmTable alarmInterval 1.3.6.1.2.1.16.3.1.1.2	The value used is Time (in seconds). The default is the value specified in the graph Sample Time parameter. Modifications are done by changing the Sample Time parameters. Sample Time settings are as follows: **Delta—**Counter is reset **Absolute—**ROS monitors the counter for the defined interval	Alarm Interval (Seconds)
alarmTable alarmVariable 1.3.6.1.2.1.16.3.1.1.3	The selected MIB variable.	Alarm Variable
alarmTable alarmIndex 1.3.6.1.2.1.16.3.1.1.1	The port to which the alarm is configured.	Alarm Port
alarmTable alarmSampleType 1.3.6.1.2.1.16.3.1.1.4	There are two Sample Time settings: **Delta—**The counter is reset at the times defined by the interval (default value). **Absolute—**The counter is not reset until the counter is overflowed. If the counter overflows, the threshold is set according to the aggregated counter results.	Sample Time
alarmTable alarmValue 1.3.6.1.2.1.16.3.1.1.5	The value that a predefined parameter reached, after crossing the defined threshold for that parameter.	Value
alarmTable alarmStartupAlarm 1.3.6.1.2.1.16.3.1.1.6	The trigger that activates the alarm generation. The trigger can be a Rising alarm, Falling alarm, or a combination of both Rising and Falling. Rising is defined by crossing the threshold from low value threshold to a higher value threshold.	Startup Alarm
alarmTable alarmFallingThreshold 1.3.6.1.2.1.16.3.1.1.8	The falling counter value that triggers the Falling Threshold alarm.	Falling Threshold
alarmTable alarmRisingThreshold 1.3.6.1.2.1.16.3.1.1.7	The rising counter value that triggers the Rising Threshold alarm.	Rising Threshold
alarmTable alarmRisingEventIndex 1.3.6.1.2.1.16.3.1.1.9	The mechanism in which the alarms will be reported. Either LOGed or TRAPed or combination of both. When LOG is selected, there is no saving mechanism either in the device or in the management system. However, if the device is not being reset, it will remain in the device LOG table. If TRAP is selected, a TRAP via SNMP is generated and reported via the TRAPs general mechanism. The TRAP can be saved using the same mechanism.	Rising Action

Object/OID	Description	Field Name in NMS
alarmTable alarmFallingEventIndex 1.3.6.1.2.1.16.3.1.1.10	The mechanism in which the alarms will be reported. Either LOGed or TRAPed or combination of both. When LOG is selected, there is no saving mechanism either in the device or in the management system. However, if the device is not being reset, it will remain in the device LOG table. If TRAP is selected, a TRAP via SNMP is generated and reported via the TRAPs general mechanism. The TRAP can be saved using the same mechanism.	Falling Action

General Statistics Table

Object/OID	Description	Field Name in NMS
etherStatsTable etherStatsIndex 1.3.6.1.2.1.16.1.1.1.1	Index number.	Index
etherStatsTable etherStatsDataSource 1.3.6.1.2.1.16.1.1.1.2	Port number.	Port
etherStatsTable etherStatsDropEvents 1.3.6.1.2.1.16.1.1.1.3	The total number of events in which packets were dropped by the probe due to lack of resources. Note that this number is not necessarily the number of packets dropped; it is just the number of times this condition has been detected.	Drop Events
etherStatsTable etherStatsOctets 1.3.6.1.2.1.16.1.1.1.4	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. The differences in the sampled values are Pkts and Octets, respectively, and the number of seconds in the interval is Interval. These values are used to calculate the Utilization as follows: $\text{Utilization} = \frac{\text{Pkts} * (9.6 + 6.4) + (\text{Octets} * .8)}{\text{Interval} * 10{,}000}$ The result of this equation is the value “Utilization”. The value is the ethernet segment percent utilization on a scale of 0 to 100 percent.	Octet Received
etherStatsTable etherStatsPkts 1.3.6.1.2.1.16.1.1.1.5	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.	Packet Received
etherStatsTable etherStatsBroadcastPkts 1.3.6.1.2.1.16.1.1.1.6	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.	Broadcast Packet Received

Object/OID	Description	Field Name in NMS
etherStatsTable etherStatsMulticastPkts 1.3.6.1.2.1.16.1.1.1.7	The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.	Multicast Packet Received
etherStatsTable etherStatsCRCAlignErrors 1.3.6.1.2.1.16.1.1.1.8	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).	CRC & Align Errors
etherStatsTable etherStatsUndersizePkts 1.3.6.1.2.1.16.1.1.1.9	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.	Undersize Packets
etherStatsTable etherStatsOversizePkts 1.3.6.1.2.1.16.1.1.1.10	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.	Oversize Packets
etherStatsTable etherStatsFragments 1.3.6.1.2.1.16.1.1.1.11	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that it is entirely normal for etherStatsFragments to increment. This is because it counts both runts (which are normal occurrences due to collisions) and noise hits.	Fragments
etherStatsTable etherStatsJabbers 1.3.6.1.2.1.16.1.1.1.12	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). **Note:** This definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.	Jabbers
etherStatsTable etherStatsCollisions 1.3.6.1.2.1.16.1.1.1.13	The best total collisions estimate on this Ethernet segment. The value returned will depend on the RMON probe location. (10BASE-T) of IEEE standard 802.3 defines a collision as the simultaneous presence of signals on the DO and RD circuits (transmitting and receiving at the same time). A 10BASE-T station can only detect collisions when it is transmitting. Thus probes placed on a station and a repeater, should report the same number of collisions. **Note:** An RMON probe inside a repeater should ideally report collisions between the repeater and one or more other hosts (transmit collisions as defined by IEEE 802.3k) plus receiver collisions observed on any coax segments to which the repeater is connected.	Collisions

Object/OID	Description	Field Name in NMS
etherStatsTable etherStatsPkts64Octets 1.3.6.1.2.1.16.1.1.1.14	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).	64 Bits
etherStatsTable etherStatsPkts65to127Octets 1.3.6.1.2.1.16.1.1.1.15	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).	65 – 127 Bits
etherStatsTable etherStatsPkts128to255Octets 1.3.6.1.2.1.16.1.1.1.16	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).	128 – 255 Bits
etherStatsTable etherStatsPkts256to511Octets 1.3.6.1.2.1.16.1.1.1.17	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).	256 – 511 Bits
etherStatsTable etherStatsPkts512to1023Octets 1.3.6.1.2.1.16.1.1.1.18	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).	512 – 1023 Bits
etherStatsTable etherStatsPkts1024to1518Octets 1.3.6.1.2.1.16.1.1.1.19	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).	1024 – 1518 Bits

Trap Statistics Table

Object/OID	Description	Field Name in NMS
No MIB associated with these NMS fields.	A consecutive number given to each event to make information retrieval more efficient.	Trap Number
	The level of the event, which can be one of the following: **Informational** **Warning** **Error** **Fatal**	Severity
	Date when the trap occurred.	Date
	Time when the trap occurred.	Time
	The IP address of the device sending the trap.	Source
	A description of the event. For example, *Link Up.*	Information
	MCLIck this checkbox to hear the beep every time a new trap arrives.	Beep when a trap arrives

Traps Configuration

Object/OID	Description	Field Name in NMS
No MIB associated with these NMS fields.	Defines the number of times that the device will try to reach the server.	SNMP/TFTP Retries
	Defines the number of seconds the device will waits for a response from the server before the request is timed out.	SNMP/TFTP Timeout

Statistics Log Table

Object/OID	Description	Field Name in NMS
logTable logEventIndex 1.3.6.1.2.1.16.9.2.1.1	Type of event. Options are: • **NONE** • **LOG** • **TRAP** • **LOG-AND-TRAP**	Event Index
logTable logIndex 1.3.6.1.2.1.16.9.2.1.2	Log event number.	Log Index
logTable logTime 1.3.6.1.2.1.16.9.2.1.3	The time the event occurred.	Log Time
logTable logDescription 1.3.6.1.2.1.16.9.2.1.4	A description of the event.	Description

Services Parameters

Use the following variables to modify device tuning, polling configuration, community change, and ping parameters.

General Device Tuning

Object/OID	Description	Field Name in NMS
rsMaxBrgFrwEntries 1.3.6.1.4.1.171.29.8.1.1	Maximum number of entries (MAC addresses) possible for this table.	Bridge Forwarding Table Current Value (General tab)
rsMaxBrgFrwEntriesAfterReset 1.3.6.1.4.1.171.29.8.1.2	Value for after reset.	Bridge Forwarding Table After Reset (General tab)
rsMaxRmonLogEntries 1.3.6.1.4.1.171.29.8.13.1	The number of log entries the device keeps in the table before overwriting the first entry. It is kept until the device is reset.	RMON Log Table Current Value (General tab)
rsMaxRmonLogEntriesAfterReset 1.3.6.1.4.1.171.29.8.13.2	After reset value.	RMON Log Table After Reset (General tab)
rsMaxGvrpVlans 1.3.6.1.4.1.171.29.8.17.1	The maximum number of VLANs that in GVRP.	Max GVRP VLANs Current Value (General tab)
rsMaxGvrpVlansAfterReset 1.3.6.1.4.1.171.29.8.17.2	After reset value.	Max GVRP VLANs After Reset (General tab)
rsMaxPolicySimpleMibMaxRulesEntries 1.3.6.1.4.1.171.29.8.16.3	The maximum number of rules that can be defined.	Max Policy Simple MIB Max Rules Entries Current Value (General tab)
rsMaxPolicySimpleMibMaxRulesEntriesAfterReset 1.3.6.1.4.1.171.29.8.16.4	After reset value.	Max Policy Simple MIB Max Rules Entries After Reset (General tab)
rsMaxPolicySimpleMibMaxProfilesEntries 1.3.6.1.4.1.171.29.8.16.5	The maximum number of profiles.	Max Policy Simple MIB Max Profiles Entries Current Value (General tab)
rsMaxPolicySimpleMibMaxProfilesEntriesAfterReset 1.3.6.1.4.1.171.29.8.16.6	After reset value.	Max Policy Simple MIB Max Profiles Entries After Reset (General tab)
rsDbgLevel 1.3.6.1.4.1.171.29.3	Determines the level of errors sent to the terminal (0–255). 0 sends the least amount of errors and 255 sends the most.	Error Report Level Current Value (General tab)

Event Log

Object/OID	Description	Field Name in NMS
eventMessageTable eventMessageEntry 1.3.6.1.4.1.171.29.6.1	The row definition for this table.	
eventMessageTable eventNum 1.3.6.1.4.1.171.29.6.1.1	The event number. The index of this table.	Event Number (Event Log Window)
eventMessageTable eventDesc 1.3.6.1.4.1.171.29.6.1.1	The event description. This text will include time and severity.	Event Description (Event Log Window)
rsConfirmMessagTab 1.3.6.1.4.1.171.29.5	This variable enables the operator to confirm all the messages in the event Message Table.	

IP Device Tuning

Object/OID	Description	Field Name in NMS
rsMaxIpFrwEntries 1.3.6.1.4.1.171.29.8.2.1	Maximum number of routing table entries allowed for this table.	IP RIP Table Current Value (IP tab)
rsMaxIpFrwEntriesAfterReset 1.3.6.1.4.1.171.29.8.2.2	After reset value.	IP RIP After Reset (IP tab)
rsMaxArpEntries 1.3.6.1.4.1.171.29.8.3.1	Maximum number of entries allowed for this table.	ARP Forwarding Table Current Value (IP tab)
rsMaxArpEntriesAfterReset 1.3.6.1.4.1.171.29.8.3.2	After reset value.	ARP Forwarding Table After Reset (IP tab)
rsMaxIpSFftEntries 1.3.6.1.4.1.171.29.8.9.1	Maximum number of IP Fast Forwarding Table entries allowed.	Max IP FFT Entries Current Value (IP tab)
rsMaxIpSFftEntriesAfterReset 1.3.6.1.4.1.171.29.8.9.2	After reset value.	Max IP FFT Entries After Reset (IP tab)
rsMaxIpSFftSysEntries 1.3.6.1.4.1.171.29.8.9.5	Maximum number of entries in the IP FFT table.	Max IP System FFT Entries Current Value (IP tab)
rsMaxIpSFftSysEntriesAfterReset 1.3.6.1.4.1.171.29.8.9.6	After reset value.	Max IP System FFT Entries After Reset (IP tab)

Object/OID	Description	Field Name in NMS
rsMaxDhcpConns 1.3.6.1.4.1.171.29.8.11.1	The amount of NVRAM contained in the device determines its maximum capacity for Power IP and Virtual IP connections.	Max DHCP Connections Current Value (IP tab)
rsMaxDhcpConnsAfterReset 1.3.6.1.4.1.171.29.8.11.2	After reset value.	Max DHCP Connections After Reset (IP tab)
rsIpFftNetworkUpperLimit 1.3.6.1.4.1.171.29.10.1	Maximum percentage of entries that the device can hold in FFT without overflowing.	IP FFT Upper Limit (percent) Current Value (IP tab)
rsIpFftNetworkLowerLimit 1.3.6.1.4.1.171.29.10.2	Minimum percentage of entries in which the device would stop the overflowing process.	IP FFT Lower Limit (percent) Current Value (IP tab)

IPX Device Tuning

Object/OID	Description	Field Name in NMS
rsMaxIpxFrwEntries 1.3.6.1.4.1.171.29.8.4.1	Maximum number of routing table entries allowed for this table.	IPX RIP Table Current Value (IPX tab)
rsMaxIpxFrwEntriesAfterReset 1.3.6.1.4.1.171.29.8.4.2	After reset value.	IPX RIP Table After Reset (IPX tab)
rsMaxIpxSapEntries 1.3.6.1.4.1.171.29.8.5.1	Maximum number of server entries allowed.	IPX SAP Table Current Value (IPX tab)
rsMaxIpxSapEntriesAfterReset 1.3.6.1.4.1.171.29.8.5.2	After reset value.	IPX SAP Table After Reset (IPX tab)
rsMaxIpxSFftEntries 1.3.6.1.4.1.171.29.8.10.1	Maximum number of IPX Fast Forwarding Table entries allowed.	Max IPX FFT Entries Current Value (IPX tab)
rsMaxIpxSFftEntriesAfterReset 1.3.6.1.4.1.171.29.8.10.2	After reset value.	Max IPX FFT Entries After Reset (IPX tab)
rsMaxIpxSFftSysEntries 1.3.6.1.4.1.171.29.8.10.5	Maximum number of entries in the IPX FFT table.	Max IPX System FFT Entries Current Value (IPX tab)
rsMaxIpxSFftSysEntriesAfterReset 1.3.6.1.4.1.171.29.8.10.6	After reset value.	Max IPX System FFT Entries After Reset (IPX tab)
rlIpxFftRedBoundary 1.3.6.1.4.1.171.47.2.9	Maximum percentage of entries the device can hold in FFT whiteout flowing.	IPX FFT Upper Limit (percent) Current Value (IPX tab)

Object/OID	Description	Field Name in NMS
rlIpxFftYellowBoundary 1.3.6.1.4.1.171.47.2.10	Minimum percentage in which the device would stop the overflowing process.	IPX FFT Lower Limit (percent) Current Value (IPX tab)

Polling Configuration

Object/OID	Description	Field Name in NMS
No MIB associated with this NMS field.	Polling Configuration in milliseconds.	Polling Configuration in milliseconds

Community Change

Object/OID	Description	Field Name in NMS
No MIB associated with this NMS field.	The system administrator manages access rights (read and write, read only, etc.) by making communities in the device, in the Community Table. When the community name is changed, the access rights are changed. **Note:** Type in the new community name exactly as it appears in the system administrator Community Table or the station with Super access. Any incorrect community name is accepted by the Community Change window, but access to read or write data is unavailable.	Community

Ping

Object/OID	Description	Field Name in NMS
rsPingTable rsPingAddress 1.3.6.1.4.1.171.35.4.1.1.1	The device address pinged.	IP Address
rsPingTable rsPingSentPackets 1.3.6.1.4.1.171.35.4.1.1.7	The number of packets sent to the device.	Sent Packets
rsPingTable rsPingReceivedPackets 1.3.6.1.4.1.171.35.4.1.1.8	The number of packets received from the device.	Received Packets
rsPingTable rsPingAvgReturnTime 1.3.6.1.4.1.171.35.4.1.1.10	The average amount of time it took for data to return from the device.	Avg Return Time

Object/OID	Description	Field Name in NMS
rsPingTable rsPingCompletionStatus 1.3.6.1.4.1.171.35.4.1.1.12	The ping operation status, such as OK for a successful ping, or Timeout for a ping operation that resulted in a timeout.	Completion Status
rsPingTable rsPingTimeStamp 1.3.6.1.4.1.171.35.4.1.1.13	Indicates the time and date the ping operation was requested or changed.	Time Stamp
rsPingTable rsPingPacketCount 1.3.6.1.4.1.171.35.4.1.1.2	The number of packets to be delivered in the ping operation.	Packet Count (Field appears in Insert Window)
rsPingTable rsPingPacketSize 1.3.6.1.4.1.171.35.4.1.1.3	The size of each packet to be delivered to the device.	Packet Size (Field appears in Insert Window)
rsPingTable rsPingPacketTimeout 1.3.6.1.4.1.171.35.4.1.1.4	The amount of time the system will wait until it stops sending the packet.	Packet Timeout (Field appears in Insert Window)
rsPingTable rsPingDelay 1.3.6.1.4.1.171.35.4.1.1.5	The amount of time the system will wait between the last packet it sent, and the next packet to be sent in the sequence.	Delay (Field appears in Insert Window)
rsPingTable rsPingTrapOnCompletion 1.3.6.1.4.1.171.35.4.1.1.6	Whether or not to send traps to the management station after ping is completed.	Trap On Completion (Field appears in Insert Window)

Appendix B—Tree Structure

This appendix displays the default MENU file tree structure. In the left-hand column are the main menus listed under the Root. Menus and submenus are in black. MIB variables are in blue. MIB variables in this appendix are referred to by their user-friendly names defined in the MENU file.

Note: *This appendix is based on Marvell-based (Galileo) devices.*

Menu	Submenu (Level Two) or MIB Variable	Submenu (Level Three) or MIB Variable	Submenu (Level Four) or MIB Variable	Submenu (Level Five) or MIB Variable	MIB Variable
File	Configuration_File	Send_Configuration_To_Device	Send_File_Name		
		Get_Configuration_From_Device	Get_File_Name		
		TFTP_Server_IP_Address			
	Update_Device_Software	Update_Device_Software_File_Name Update_Device_Software_Type			
	Enable_EWS_Files				
Device	Erase_NVRAM_After_Reset	Device Selected_Application			
	Global_Parameters	Identification	device_Description device_Name device_Location device_Contact_Person		
		Time	System_Up_Time System_Time System_Date		
		Version	SW_Version HW_Version		
		BootP	Relay_Server_Address Threshold		
		Galnet_Mode			

Menu	Submenu (Level Two) or MIB Variable	Submenu (Level Three) or MIB Variable	Submenu (Level Four) or MIB Variable	Submenu (Level Five) or MIB Variable	MIB Variable
Device (cont.)	VLAN	VLAN_Parameters	VLAN_Supported_Type		
			Vlan_Supported_Type_After_Reset		
			IP_VLAN_Auto_Config		
			Auto_Config_Aging_Time		
			VLAN_Ethernet_Type		
			VLAN_Ethernet_Type_Mask		
			VLAN_polling_timeout		
		VLAN_Table			
		VLAN_Port_Table			
		Ethernet_User_Defined_Protocols_Table			
	Port	Port_Properties	Connector_Type		
			sw_If_Table		
			If_Table		
		Port_Mirroring	Mirrored_Port		
			Copy_Port		
	GVRP	GVRP_Parameters	Device_Parameters	GVRP_Status	
			GVRP_Port_Parameters		
		GVRP_Timers_Control			
	Trunk	Trunk_Parameters	Aggregate_Num_Of_Trunks		
			Aggregate_Max_Ports_In_Trunks		
			Mib_Version		
		Trunk_Table			
		Trunking_Port_Table			

Menu	Submenu (Level Two) or MIB Variable	Submenu (Level Three) or MIB Variable	Submenu (Level Four) or MIB Variable	Submenu (Level Five) or MIB Variable	MIB Variable
Bridge	Operating_Parameters	Bridge_Address			
		Bridge_Type			
		Bridge_Forwarding_Table_Aging_Time			
	Unicast	Unicast_Global_Forwarding_Table			
		Unicast_Global_Forwarding_Table_Size			
	Multicast	Multicast_Forwarding_Table			
		Multicast_Forward_All			
		Multicast_Forward_Unregistered			
		Multicast_Static_Table			
	Spanning_Tree	Parameters	General_Parameters	General_Parameter	Global_STP_Status
					STP_Protocol_Specification
					STP_STP_Type
					STP_Must_Belong_To_Vlan
					STP_Number_Format
				Bridge_Setup	STP_Bridge_Priority
					STP_Bridge_Max_Age(Sec)
					STP_Bridge_Hello_Time(Sec)
					STP_Bridge_Forward_Delay (Sec)
			Tuning_Parameter	Tuning_Parameter_Root	STP_Mib_Version
					STP_Bridge_Priority
					STP_Base_Bridge_Address
					STP_Root_Path_Cost
					STP_Root_Port
					STP_Topology_Change_Time
					STP_Topology_Changes_Count

Menu	Submenu (Level Two) or MIB Variable	Submenu (Level Three) or MIB Variable	Submenu (Level Four) or MIB Variable	Submenu (Level Five) or MIB Variable	MIB Variable

Bridge (cont.)				STP_Setup	STP_Max_Age(Sec)
					STP_Hello_Time(Sec)
					STP_Hold_Time(Sec)
					STP_Forward_Delay_(Sec)

		Spanning_Tree_Port_Table			
	Rapid_Spanning_Tree	RSTP_Ports_Table RSTP_Force_Version_Table			
	MAC_Multicast	MAC_Multicast_Parameters	Mac_Multicast_Enable Igmp_Snoop_Mib_Version Igmp_Snoop_Enable Igmp_Snoop_Host_Aging_Time Igmp_Snoop_Router_Aging_Time		
		MAC_Multicast_Group_Table MAC_Multicast_Router_Table			
	Traffic_Control	Traffic_Control_Port_Priority_Table Traffic_Class_Table Traffic_Control_Priority_Groups_Table			

Menu	Submenu (Level Two) or MIB Variable	Submenu (Level Three) or MIB Variable	Submenu (Level Four) or MIB Variable	Submenu (Level Five) or MIB Variable	MIB Variable
Router	IP	IP_Operating_Parameters	IP_Redundancy_Admin_Status IP_Inactive_ARP_Time_Out IP_ARP_Proxy ICMP_Error_Messages		
		IP_RIP	IP_RIP_Parameters	IP_RIP_Administrative_Status IP_Leak_OSPF_Routes_RIP IP_Leak_Static_Routes_RIP	
			IP_RIP_Interface_Parameters IP_Interface_RIP_Filter_Table IP_RIP_Global_Filter_Table		
		IP_OSPF_II	IP_OSPF_II_Parameters	IP_OSPF_Administrative_Status IP_OSPF_Router_ID IP_OSPF_Number_of_External_LSAs IP_OSPF_External_LS_Checksum_Sum IP_Leak_RIP_Routes_OSPF IP_Leak_Static_Routes_OSPF IP_Leak_External_Direct_Routes_OSPF	
			Neighbors	IP_OSPF_II_Interface_Parameters IP_OSPF_II_Neighbors_Table	

Menu	Submenu (Level Two) or MIB Variable	Submenu (Level Three) or MIB Variable	Submenu (Level Four) or MIB Variable	Submenu (Level Five) or MIB Variable	MIB Variable
Router (cont.)			IP_OSPF_II_Interface_Parameters IP_OSPF_II_Metric_Table IP_OSPF_II_Area_Table IP_OSPF_II_Stub_Area_Table IP_OSPF_II_Link_State_Database IP_OSPF_II_External_Link_State_Database		
		IP_DHCP	IP_DHCP_Parameters	Probe	IP_DHCP_Probe_Enable IP_DHCP_Probe_Retries IP_DHCP_Probe_Timeout(Seconds)
				WINS	IP_DHCP_Primary_WINS_Server IP_DHCP_Secondary_WINS_Server IP_DHCP_Node_Type
				IP_DHCP_Server_Enable IP_DHCP_Next_Server_Address IP_DHCP_Relay_Security_Threshold IP_DHCP_DNS_IP_Address	
			IP_DHCP_Address_Range IP_DHCP_Allocation_Table		

		TCP_General_Parameters	IP_TCP_Algorithm_Type
			IP_TCP_Min.Timeout(ms)
			IP_TCP_Max.Timeout(ms)
			IP_TCP_Max.Connections		

Menu	Submenu (Level Two) or MIB Variable	Submenu (Level Three) or MIB Variable	Submenu (Level Four) or MIB Variable	Submenu (Level Five) or MIB Variable	MIB Variable
Router (cont.)		IP_Interface_Parameters IP_Routing_Table ARP_Table IP_Redundancy TCP_Connection_Table IP_UDP_Relay_Table			
	IPM	IPM_Operating_Parameters	IPM_route_enable		
		IGMP	IGMP_Parameters	IGMP_Mib_Version	
			IGMP_Interface_Table IGMP_Cache_Table		
		IGMP_Proxy	IGMP_Proxy_Parameters	IGMP_Proxy_Enable	
		PIM	PIM_Parameters	Pim_Mib_Version Pim_Enable	
			PIM_Interface_Table PIM_Neighbor_Table PIM_Route_Table PIM_Route_Next_Hop		
		IPM_Routing	IPM_Routing_Route_Table IPM_Routing_Route_Next_Hop_Table		
	IPX	IPX_Interface_Parameters IPX_Routing_Table IPX_SAP_Table			

Security	Community_Table WEB_User_Authorization_Table

Menu	Submenu (Level Two) or MIB Variable	Submenu (Level Three) or MIB Variable	Submenu (Level Four) or MIB Variable	Submenu (Level Five) or MIB Variable	MIB Variable
QoS	Qos_Global_Parameters	Qos_Policy_Version Qos_Policy_Enable			
	Qos_IP	Qos_Classification_Fields_Table Qos_IP_Rules_Table			
	Qos_Profile_Table				
Statistics	Alarm_Table Statistics_Table Log_Table				
Services	Device_Tuning	Device_Tuning_General	MaxEntriesIn_Bridge_Forwarding_Table MaxEntriesIn_Bridge_Forwarding_Table_After_Reset MaxEntriesIn_Rmon_Log_Table MaxEntriesIn_Rmon_Log_Table_After_Reset MaxEntriesIn_Max_GVRP_Vlans MaxEntriesIn_Max_GVRP_Vlans_After_Reset MaxEntriesIn_Max_Policy_SM_Max_Rules_Entries MaxEntriesIn_Max_Policy_SM_Max_Rules_Entries_After_Reset MaxEntriesIn_Max_Policy_SM_Max_Profiles_Entries MaxEntriesIn_Max_Policy_SM_Max_Profiles_Entries_After_Reset MaxEntriesIn_Error_Report_Level		

Menu	Submenu (Level Two) or MIB Variable	Submenu (Level Three) or MIB Variable	Submenu (Level Four) or MIB Variable	Submenu (Level Five) or MIB Variable	MIB Variable
Services (cont.)		Device_Tuning_IP	MaxEntriesIn_IP_RIP_Table		
			MaxEntriesIn_IP_RIP_Table_After_Reset		
			MaxEntriesIn_ARP_Forwarding_Table		
			MaxEntriesIn_ARP_Forwarding_Table_After_Reset		
			MaxEntriesIn_Max_IP_FFT_Entries		
			MaxEntriesIn_Max_IP_FFT_Entries_After_Reset		
			MaxEntriesIn_Max_IP_System_FFT_Entries		
			MaxEntriesIn_Max_IP_System_FFT_Entries_After_Reset		
			MaxEntriesIn_Max_DHCP_Connections		
			MaxEntriesIn_Max_DHCP_Connections_After_Reset		
			MaxEntriesIn_IP_FFT_Upper_Limit(percents)		
			MaxEntriesIn_IP_FFT_Lower_Limit(percents)		
		Device_Tuning_IPX	MaxEntriesIn_IPX_RIP_Table		
			MaxEntriesIn_IPX_RIP_Table_After_Reset		
			MaxEntriesIn_IPX_SAP_Table		
			MaxEntriesIn_IPX_SAP_Table_After_Reset		
			MaxEntriesIn_Max_IPX_FFT_Entries		
			MaxEntriesIn_Max_IPX_FFT_Entries_After_Reset		
			MaxEntriesIn_Max_IPX_System_FFT_Entries		
			MaxEntriesIn_Max_IPX_System_FFT_Entries_After_Reset		
			MaxEntriesIn_IPX_FFT_Upper_Limit(percents)		
			MaxEntriesIn_IPX_FFT_Lower_Limit(percents)		
	Event_Log				
	Ping				