BLACK BOX®
NETWORK SERVICES

MNS-BB

CUSTOMER
SUPPORT
INFORMATION

Order **toll-free** in the U.S. 24 hours, 7 A.M. Monday to midnight Friday: **877-877-BBOX**
FREE technical support, 24 hours a day, 7 days a week: Call **724-746-5500** or fax **724-746-0746**
Mail order: **Black Box Corporation**, 1000 Park Drive, Lawrence, PA 15055-1018
Web site: **www.blackbox.com** • E-mail: **info@blackbox.com**

LE2425 Switch

BLACK BOX
NETWORK SERVICES

Software User Guide

(MNS-BB)

Preface

Use of This Guide

This guide describes how to use the command line interface (CLI), for LE2425 Switch.

If you need information on a specific command in the CLI, type the command name after you type the word “help” (help <*comman*d>) or just type <command> [Enter].

If you need further information on Black Box switch technology, refer to the Black Box website at:

http://www.blackbox.com

FEDERAL COMMUNICATIONS COMMISSION
AND
CANADIAN DEPARTMENT OF COMMUNICATIONS
RADIO FREQUENCY INTERFERENCE STATEMENTS

This equipment generates, uses, and can radiate radio frequency energy and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par le ministère des Communications du Canada.

Normas Oficiales Mexicanas (NOM)
Electrical Safety Statement

INSTRUCCIONES DE SEGURIDAD

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.
2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.
3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.
4. Todas las instrucciones de operación y uso deben ser seguidas.
5. El aparato eléctrico no deberá ser usado cerca del agua—por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc.
6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.
7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.
8. Servicio—El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.
9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.
10. El equipo eléctrico deber ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.
11. El aparato eléctrico deberá ser connectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.
12. Precaución debe ser tomada de tal manera que la tierra fisica y la polarización del equipo no sea eliminada.
13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.
14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.
15. En caso de existir, una antena externa deberá ser localizada lejos de las lineas de energia.
16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.
17. Cuidado debe ser tomado de tal manera que objectos liquidos no sean derramados sobre la cubierta u orificios de ventilación.

18.Servicio por personal calificado deberá ser provisto cuando:

A: El cable de poder o el contacto ha sido dañado; u

B: Objectos han caído o líquido ha sido derramado dentro del aparato; o

C: El aparato ha sido expuesto a la lluvia; o

D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o

E: El aparato ha sido tirado o su cubierta ha sido dañada.

Table of Contents .... Page

1.0 Getting Started

1.1 Getting Started with Switch Configuration

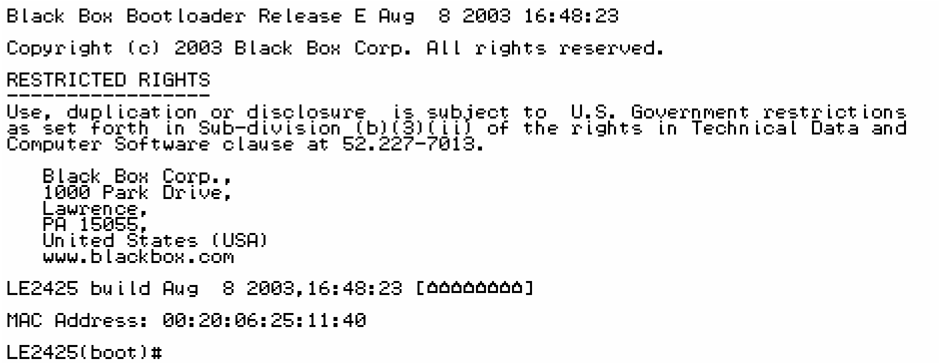
This section is a guide for using the console Switch Setup commands to quickly assign an IP (Internet Protocol) address and subnet mask to the switch. You can also set a Manager password and configure other basic features from Switch Setup commands.

(For Hardware Installation and configuration, please see the user guide for hardware).

1.2 Software Upgrade

If your LE2425 already has the software then you will get the Login prompt when you boot up the switch, otherwise you will get the Boot prompt and you will have to upgrade the software (For details refer Appendix D)

Below is a screen example of the boot prompt.



```
Black Box Bootloader Release E Aug  8 2003 16:48:23

Copyright (c) 2003 Black Box Corp. All rights reserved.

RESTRICTED RIGHTS
-----------------
Use, duplication or disclosure  is subject to  U.S. Government restrictions
as set forth in Sub-division (b)(3)(ii) of the rights in Technical Data and
Computer Software clause at 52.227-7013.

   Black Box Corp.,
   1000 Park Drive,
   Lawrence,
   PA 15055,
   United States (USA)
   www.blackbox.com

LE2425 build Aug  8 2003,16:48:23 [⌂⌂⌂⌂⌂⌂⌂⌂]

MAC Address: 00:20:06:25:11:40

LE2425(boot)#
```

1.3 Recommended Minimal Configuration

In the factory default configuration, the switch has no IP (Internet Protocol) address and subnet mask. In this state, it can be managed only through a direct console connection. To manage the switch through in-band (networked) access, you should configure the switch with an IP address and subnet mask compatible with your network. Also, you should change the Manager password to control access privileges from the console. The default password is “manager” for the Manager user and “operator” for the Operator user respectively. Many other features such as optimizing the switch’s performance, enhancing your control of the network traffic, and improving network security can be configured through the switch’s console interface. Once an IP address has been configured on the switch, these features can be accessed more conveniently through an SNMP network management station running anetwork management program. For a listing of switch features available with and without an IP address, refer to Chapter: “How IP Configuration”.

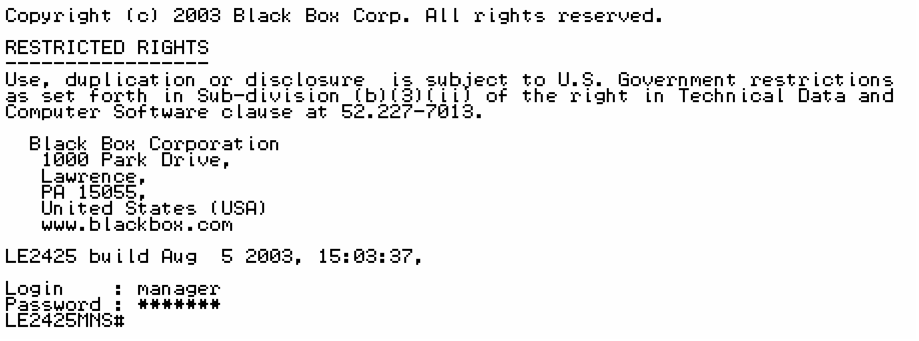
1.4 Using the Console Setup Screen

The quickest and easiest way to minimally configure the switch for management and password protection in your network is to use the following sequence. Use a direct console connection to the switch, start a console session, and access the Switch Setup screen.

1. Using the method described in the preceding section, connect a terminal device to the switch and it will display the switch console command (CLI) prompt (the default display).

The CLI prompt appears displaying the switch model number:
LE2425MNS#

Below is an example of the above prompt.



```
Copyright (c) 2003 Black Box Corp. All rights reserved.

RESTRICTED RIGHTS
-----------------
Use, duplication or disclosure  is subject to U.S. Government restrictions
as set forth in Sub-division (b)(3)(ii) of the right in Technical Data and
Computer Software clause at 52.227-7013.

  Black Box Corporation
   1000 Park Drive,
   Lawrence,
   PA 15055,
   United States (USA)
   www.blackbox.com

LE2425 build Aug  5 2003, 15:03:37,

Login    : manager
Password : *******
LE2425MNS#
```

Below is the sequence of activities that must be completed for the network to find your switch.
1. Boot up the switch.
2. Set the **Manager Password** (optional).
3. Configure the **IP Address** and enter the IP address that is compatible with your network.
4. Configure the **Subnet Mask** and enter the subnet mask used for your network.
5. Configure the **Default Gateway** of your Network.

Syntax: ipconfig ip=<ipaddress> mask=<subnet mask> dgw=<default-gateway>
Example: **ipconfig ip=192.168.1.150 mask=255.255.255.0 dgw=192.168.1.10**

6. Save
7. Restart the unit.

The switch is now configured with a Manager password, IP address, and subnet mask, and can be accessed through the Console or an SNMP-based network management tools. Here is some information about the basic fields.

Parameter	**Default**	
System Name	LE2425	Optional;
System Contact	support@blackbox.com	Optional;
Manager Password	manager	Recommended;
Logon Default	CLI	The default setting .
Time Zone	0 (none)	Optional;
Community Name (Get)	public	Default setting recommended;
Community Name (Set)	private	Default setting recommended;
Default Gateway	blank	Optional;
IP Address	blank	Recommended;

Note: The IP address and subnet mask assigned for the switch must be compatible with the IP addresses used in your network. For more information on IP addressing, see the *Chapter 3.*

1.5 To Recover from a Lost Manager Password:

If you cannot start a console session at the manager level because of a lost Manager password, please contact support@blackbox.com.

2.0 Console Management Interface

This chapter describes the following:

- Management interfaces for the LE2425 Switches.
- Advantages of using CLI interface.

2.1 Understanding Management Interfaces

The console interface is accessed through the DB-9 RS232 connector. Attach a VT100 compatible terminal or a PC running a terminal emulation program to the serial port.

Management interfaces enable you to reconfigure the switch and to monitor switch status and performance. The LE2425 switches offer the CLI interface:

- CLI – A command line interface offering the full set of switch commands through the VT-100 or equivalent console built into the switch.

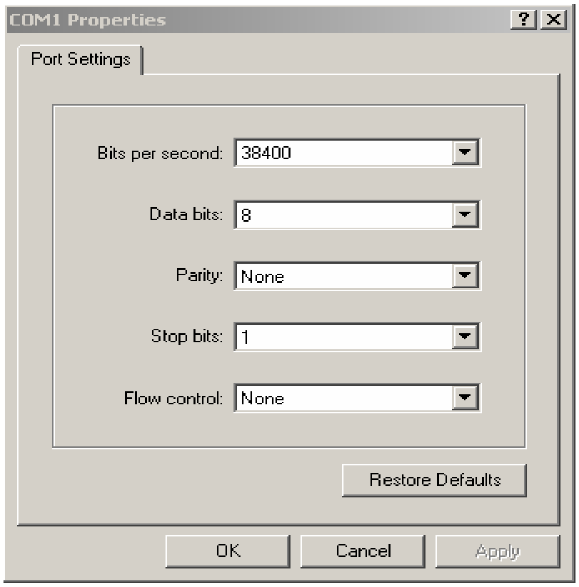
This manual describes how to use the CLI and how to use these interfaces to configure and monitor the switch.

The MNS software supports a command-line interface (CLI) through the serial port.
***Note**: CLI is also accessible through Telnet.*
The command-line interface enables local or remote unit installation and maintenance. A set of system commands allow effective monitoring, configuration and debugging of the device.

2.2 Console Port Connection

Attach a VT100 compatible terminal or a PC running a terminal emulation program to the serial port on the switch. Use the null-modem cable.

When attaching to a PC, set terminal emulation type to VT100, specify the port used by your PC (i.e, COM 1~4), and then set communications to 8 data bits, 1 stop bit, no parity, and 38400 bps (for initial configuration). Also be sure to set flow control to 'none'.



COM1 Properties

Port Settings

Bits per second: 38400

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

2.3 Advantages of Using the CLI

LE2425MNS>	Operator Level
LE2425MNS#	Manager Level
LE2425MNS##	Configuration Level

- Provides access to the complete set of switch configuration, performance, and diagnostic features.
- Enables quick management level access of the detailed system configuration to system operators and administrators experienced in command prompt interfaces.
- Provides help at each level for determining available options and variables.

2.4 CLI Usage

- To perform specific procedures such as configuring IP addressing or VLAN.
- To monitor and analyze switch operations.
- For more information on individual CLI commands, refer to the Index or to the “Command Line Interface Reference Guide” available on Black Box’s web site.

3.0 Using the Command Line Interface (CLI)

The **CLI (Command Line Interface)** is a text-based command interface for configuring and monitoring the switch. The CLI gives you access to the switch's full set of commands while providing password protection.

The switch executes a multi-tasking operating system on its control processor that manages all system activities. This system allows the administrator to query and configure the switch from either an attached terminal or any of its attached network interfaces.

3.1 Accessing the CLI

This section provides information on how to access the console commands and set or enable the advanced configuration features in the switch.

The CLI is accessed through the switch console. You can access the console out-of-band by directly connecting a terminal device to the switch, or in-band by using Telnet either from a terminal device or through the network interface.

3.2 Using the CLI

The CLI offers the following privilege levels to prevent unauthorized access to the switch:

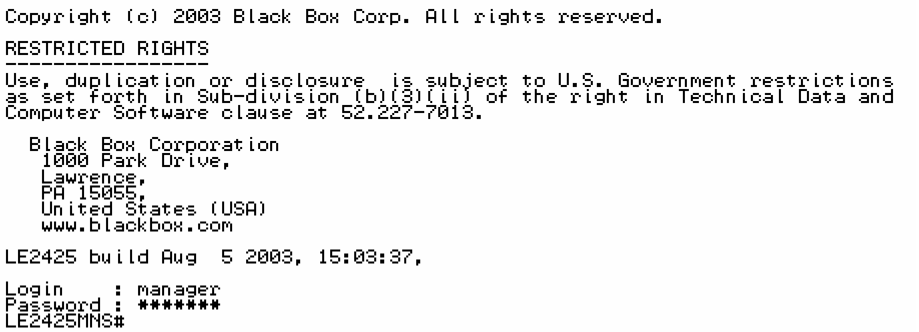
Operator
Manager

When you use the CLI mode to make a configuration change, the switch writes the changes to the Running Configuration file in volatile memory. This allows you to test your configuration changes before making them permanent. To make changes permanent, you must use the **save** command to save them to the Startup Configuration file in non-volatile memory. If you reboot the switch without first using **save**, all changes made since the last reboot or **save**   (whichever is later) will be lost.

3.3 Privilege Levels at Logon

Privilege levels control the type of access to the CLI. To implement this control, you must set the Manager password (By default, the manager password is "manager". If passwords are set when you use the CLI to log on to the switch, you will be prompted to enter a user then enter a password.

For example:
Example of CLI Login Screen



```
Copyright (c) 2003 Black Box Corp. All rights reserved.

RESTRICTED RIGHTS
-----------------
Use, duplication or disclosure  is subject to U.S. Government restrictions
as set forth in Sub-division (b)(3)(ii) of the right in Technical Data and
Computer Software clause at 52.227-7013.

  Black Box Corporation
   1000 Park Drive,
   Lawrence,
   PA 15055,
   United States (USA)
   www.blackbox.com

LE2425 build Aug  5 2003, 15:03:37,

Login    : manager
Password : *******
LE2425MNS#
```

In the above case, you will enter the CLI at the level corresponding to the user and password combination you provide (operator or manager). Suppose you log onto the CLI at the Manager level, the following prompt will appear:
LE2425MNS#_

We strongly recommend that you change both the Manager and the operator password. Note that changing only an Operator password *does not* prevent access to the Manager level by intruders who have the Manager password.

3.3.1 Operator Privileges

At the Operator level you can examine the current configuration and move between interfaces without being able to change the configuration. A ">" character delimits the Operator-level prompt.

For example:

```
LE2425MNS>_   (Example of the Operator prompt.)
```

3.3.2 Manager Privileges

Manager privileges give you three additional levels of access: Manager, Global Configuration, and Context Configuration. A “#” character delimits any Manager prompt. For example:

```
LE2425MNS#_   (Example of the Manager prompt.)
```

Manager level: Provides all Operator level privileges plus the ability to perform system-level actions. The prompt for the Manager level contains only the system name and the “#” delimiter, as shown above. To select this level, enter the **enable <manager>** command at the Operator level prompt and enter the Manager password, when prompted. For example:

```
LE2425MNS> enable <Manager>  (Enter enable at the Operator prompt.)
LE2425MNS# _ (The Manager prompt.)
```

Global Configuration level: Provides all Operator and Manager level privileges, and enables you to make configuration changes to any of the switch’s software features. The prompt for the Global Configuration level includes the system IP, System Date, time etc.

Context Configuration level: Provides all Operator and Manager privileges, and enables you to make configuration changes in a specific context, such as one or more ports or a VLAN. The prompt for the Context Configuration level includes the system name and the selected context.

For example:

```
LE2425MNS# configure vlan type=port
LE2425MNS(port-vlan)##_          (The Configuration Prompt)
```

3.4 User Management

Using this module you can add, modify and delete user names and passwords. You can add 5 users maximum. Two privilege levels are available; **Manager** and **Operator**. Level 1 is meant for OPERATOR and Level 2 for MANAGER. For example, if you want to set up user name for basic monitoring capabilities then use lower number (Level 1).

Note: You can add more then one manager but total limit of users is five (including OPERATORS and MANAGERS).

3.4.1 CLI Commands

To Add User

Syntax: **add user=<name> level=<number>**

```
LE2425MNS(user)##add user=Raj level=2

Enter User Password     :******
Confirm New Password :******
```

In this example, User ‘Raj’ will be added with Manager privilege.

To Delete User

Syntax: **delete user=<name>**

```
LE2425MNS(user)##delete user=Raj

Confirm User Deletion(Y/N): Y
User successfully deleted
```

To modify Password
Syntax: **passwd user=<name>**

```
LE2425MNS(user)## passwd user=Raj

Enter New Password      :******
Confirm New Password :******
Password has been modified successfully
```

To modify the Privilege Level
Syntax: **chlevel user=<name> level=<number>**

```
LE2425MNS(user)## chlevel user=Raj level=1
Access Permission Modified
```

In this example, User 'Raj' has been modified with Operator privilege.

3.5 Listing Commands and Command Options

At any privilege level you can:

- List all of the commands available at that level
- List the options for a specific command

Listing Commands Available at Any Privilege Level

At a given privilege level you can execute the commands that level offers plus all of the commands available at preceding levels. For example, at the Operator level you can list and execute only the Operator level commands. However, at the Manager level you can list and execute the commands available at both the Operator and Manager levels.
Privilege Level Example of Prompt and Permitted Operations

3.5.1 Operator Privilege

-View status and configuration information.
-Perform connectivity tests.
-Move from the Operator level to the Manager level using the '**enable**' command.
-Exit from the CLI interface and terminate the console
session using the '**logout**' command.

For a list of available commands, enter 'help' at the prompt.
For example, to view status and configuration information of the Operator Level use the **show** command:
LE2425MNS> **show** <*command*>

3.5.2 Manager Privilege

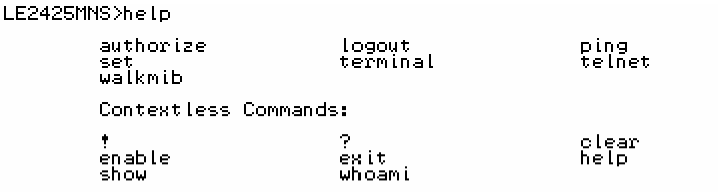
At the Manager Level (LE2425MNS#) prompt you can perform system-level actions such as system control, configuration, monitoring, and diagnostic commands, plus any of the Operator-level commands. For a list of available commands, enter 'help' at the prompt.

At the Configuration (LE2425MNS##) prompt you can execute configuration commands, plus all Operator and Manager commands. For a list of available commands, enter 'help' at the Context Configuration prompt.

3.5.3 Type "help" To List Available Commands.

Typing the '**help**' command lists the commands you can execute at the current privilege level. For example, typing '**help**' at the Operator level produces this listing:

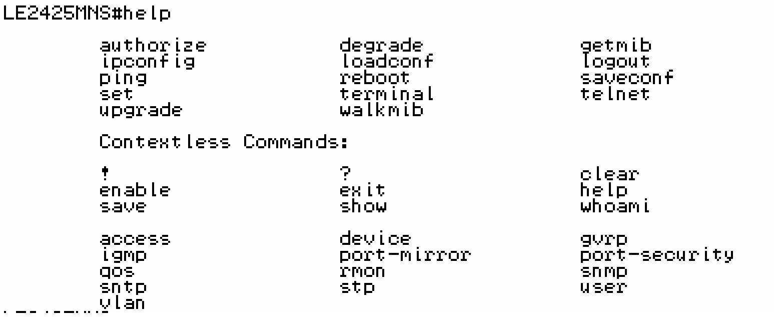
```
LE2425MNS> help
```



```
LE2425MNS>help

        authorize           logout              ping
        set                 terminal            telnet
        walkmib

        Contextless Commands:

        !                   ?                   clear
        enable              exit                help
        show                whoami
```

Typing ‘**help**’ at the Manager level produces this listing

LE2425MNS# help



```
LE2425MNS#help

        authorize           degrade             getmib
        ipconfig            loadconf            logout
        ping                reboot              saveconf
        set                 terminal            telnet
        upgrade             walkmib

        Contextless Commands:

        !                   ?                   clear
        enable              exit                help
        save                show                whoami

        access              device              gvrp
        igmp                port-mirror         port-security
        qos                 rmon                snmp
        sntp                stp                 user
        vlan
```

3.5.4 Displaying CLI "Help"

CLI Help provides four types of context-sensitive information:

- Command list with a brief summary of each command’s purpose.
- Detailed information on how to use individual commands.
- Command line verbosity with possible options.
- Command usage of specific commands.

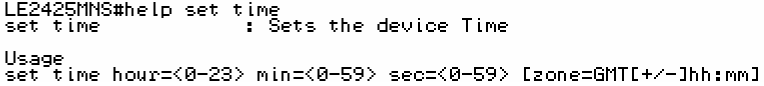
3.5.5 Displaying Help for an Individual Command.

You can display Help for any command that is available at the current context level by typing help then entering enough of the command string to identify the command.

Syntax: **help** <*command string*>

For example, to list the Help for the **set time** command at the Configuration privilege level type:

LE2425MNS# **help set time**

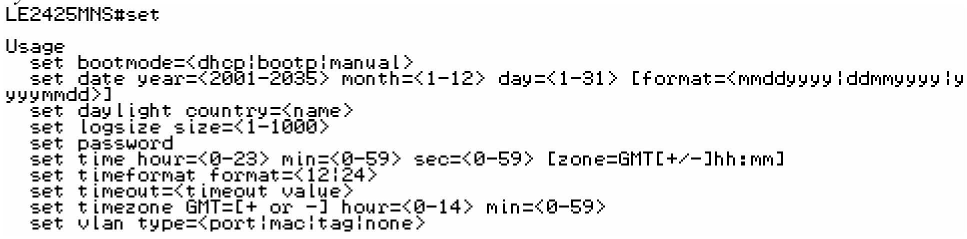


```
LE2425MNS#help set time
set time             : Sets the device Time

Usage
set time hour=<0-23> min=<0-59> sec=<0-59> [zone=GMT[+/-]hh:mm]
```

3.5.6 Displaying Help for a particular command.

You can display the command usage of a specific command by typing the command and pressing enter.

Syntax: **<Command Name> <Enter>**



```
LE2425MNS#set

Usage
   set bootmode=<dhcp|bootp|manual>
   set date year=<2001-2035> month=<1-12> day=<1-31> [format=<mmddyyyy|ddmmyyyy|y
yyymmdd>]
   set daylight country=<name>
   set logsize size=<1-1000>
   set password
   set time hour=<0-23> min=<0-59> sec=<0-59> [zone=GMT[+/-]hh:mm]
   set timeformat format=<12|24>
   set timeout=<timeout value>
   set timezone GMT=[+ or -] hour=<0-14> min=<0-59>
   set vlan type=<port|mac|tag|none>
```

3.5.7 Displaying Help with all possibilities.

You can display Help for all possible commands and options that are available by pressing the <TAB> key.

Syntax: <TAB>

Or <Command string> <TAB>

Or <First character of the command> <TAB>

For example, <TAB> will list the available commands in the particular privilege level:

```
LE2425MNS> <TAB>
 clear
 enable
 exit
 help
 logout
 ping
 set
 show
 telnet
 terminal
 walkmib
 whoami

LE2425MNS> s <TAB>
 set
 show

 LE2425MNS# set <TAB>
  bootmode
 date
 daylight
 logsize
 password
 time
 timeformat
 timeout
 timezone
 vlan
```

4.0 Configuring IP Addressing, Interface Access, and System Information

4.1 IP Configuration

4.1.1 IP Address and Subnet Mask Overview.

Configuring the switch with an IP address expands your ability to manage the switch and use its features. To configure IP addressing, use the web interface (R2 only) or the CLI to manually configure the initial IP values.

4.1.2 IP Address and Subnet Mask.

By default, the switch is set to manual IP addressing. To arrange the manual IP addressing, use the CLI to configure the initial IP values. If you want to configure the IP automatically then enable the DHCP/Bootp server that has been set correctly with information to support the switch, and it will auto configure the IP. (Refer to “DHCP/Bootp Operation” for information on setting up automatic configuration from a server.). For information on how IP addressing affects switch performance, refer to “How IP Addressing Affects Switch Operation”.

4.1.3 Default Gateway Operation.

The default gateway is required for tasks such as reaching off-subnet destinations or forwarding traffic across multiple VLANs. The gateway value is the IP address of the next-hop gateway node for the switch which is used if the requested destination address is not on a local subnet/VLAN. If the switch does not have a manually-configured default gateway and DHCP/Bootp is configured, then the default gateway value provided by the DHCP or Bootp server will be used. If the switch has a manually configured default gateway, then the switch uses this gateway.

4.1.4 Configuring IP Address, Gateway, DHCP

Do one of the following:

- To manually enter an IP address and subnet mask, set the IP Config parameter to Manual and then manually enter the IP address and subnet mask values you want for the switch.
- To use DHCP or Bootp, use the “set bootmode” command to ensure that the bootmode parameter is set to DHCP or Bootp(this enables the DHCP/Bootp), then refer to “DHCP/Bootp Operation”.

Syntax: **set bootmode=<dhcp|bootp|manual>**

```
LE2425MNS# set bootmode=dhcp
```

And **restart** the switch. It will fetch an IP address from the DHCP Server.

4.2 DHCP/Bootp Operation

4.2.1 Overview

DHCP/Bootp is used to provide configuration data from a DHCP or Bootp server to the switch. This data can be the IP address, subnet mask, default gateway, and TFTP server address. If a TFTP server address is provided, this allows the switch to TFTP a previously saved configuration file from the TFTP server to the switch. With either DHCP or Bootp, the servers must be configured prior to the switch being connected to the network.

4.2.2 The DHCP/Bootp Process.

Whenever the IP Config parameter in the switch is configured to **DHCP/Bootp** , or when the switch is rebooted with this configuration then follow the steps below:

4.2.3 Configuring IP Addressing,

1.DHCP/Bootp requests are automatically broadcast on the local network.
(The switch sends one type of request to which either a DHCP or Bootp server can respond.)

2. When a DHCP or Bootp server receives the request, it replies with a previously configured IP address and subnet mask for the switch. The switch also receives an IP Gateway address if the server has been configured to provide one. In the case of Bootp, the server must first be configured with an entry that has the MAC address of the switch. To determine the switch’s MAC address, use CLI command:

```
LE2425MNS#show mac
MAC Address  : 00:20:06:25:00:11
```

Note If you manually configure a gateway on the switch, it will ignore any gateway address received via DHCP or Bootp.
If the switch is initially configured for DHCP/Bootp operation, or if it is rebooted with this configuration, it immediately begins sending request packets on the network. If the switch does not receive a reply to its DHCP/Bootp requests, it continues to periodically send request packets, but with decreasing frequency. Thus, if a DHCP or Bootp server is not available or accessible to the switch when DHCP/Bootp is first configured, the switch may not immediately receive the desired configuration. After verifying that the server has become accessible to the switch, reboot the switch to re-start the process immediately.

4.2.4 DHCP Operation.

A significant difference between a DHCP configuration and a Bootp configuration is that an IP address assignment from a DHCP server is automatic. Depending on how the DHCP server is configured, the switch may receive an IP address that is temporarily leased from the DHCP. Periodically the switch may be required to renew its lease of the IP configuration. Thus, the IP addressing provided by the server may be different each time the switch reboots or renews its configuration from the server. However, you can fix the address assignment for the switch by doing either of the following:
_ Configure the server to issue an “infinite” lease.
_ Using the switch’s MAC address as an identifier, configure the server with a “Reservation” so that it will always assign the same IP address to the switch.
For more information on either of these procedures, refer to the documentation provided with the DHCP server.
For DHCP operation:

- The entire scope of DHCP configuration has been updated on the appropriate DHCP server.
- The necessary network connections are in place
- A DHCP server is accessible from the switch

After you reconfigure or reboot the switch while in a network providing DHCP/Bootp service with DHCP/Bootp enabled, the switch does the following:
_ Receives an IP address, subnet mask, and (if configured in the server) a gateway IP address.
_ Uses TFTP to download the file from the designated source, then reboots itself. (This assumes that the switch or VLAN has connectivity to the TFTP file server specified in the reply, that the configuration file is correctly named, and that the configuration file exists in the TFTP directory.) This is done if the DHCP/Bootp reply to the switch provides information for downloading a configuration file.

4.2.5 Bootp Operation.

When a Bootp server receives a request, it searches its Bootp database for a record entry that matches the MAC address in the Bootp request from the switch. If a match is found, the configuration data in the associated database record is returned to the switch. For many Unix systems, the Bootp database is contained in the **/etc/bootptab** file. In contrast to DHCP operation, Bootp configurations are always the same for a specific receiving device. That is, the Bootp server replies to a request with a configuration previously stored in the server and designated for the requesting device. **Bootp Database Record Entries.** A minimal entry in the Bootp table file **/etc/bootptab** to update an IP address and subnet mask to the switch would be similar to this entry:

```
LE2425switch:\
ht=ether:\
ha=002006250065:\
ip=192.168.1.88:\
sm=255.255.255.0:\
gw=192.168.1.1:\
hn:\
vm=rfc1048
```

where:
LE2425switch is a user-defined symbolic name to help you find the correct section of the bootptab file. If you have multiple switches that will be using Bootp to get their IP configuration, you should use a unique symbolic

name for each switch. ht is the “hardware type”. For the Magnum Managed Switches, set this to **ether** (for Ethernet). *This tag must precede the* ha *tag*. ha is the “hardware address”. Use the switch’s 12-digit MAC address. ip is the IP address to be assigned to the switch. sm is the subnet mask of the subnet in which the switch is installed.

Note: The above Bootp table entry is a sample that will work for the Magnum Switches when the appropriate addresses and file names are used.

Network Preparations for Configuring DHCP/Bootp

In its default configuration, the switch is configured for DHCP/Bootp operation. However, the DHCP/Bootp feature will not acquire IP addressing for the switch unless the following tasks have already been completed:

For Bootp operation:

- A Bootp database record has already been entered into an appropriate Bootp server.
- The necessary network connections are in place
- The Bootp server is accessible from the switch

4.2.6 Globally Assigned IP Network Addresses

If you intend to connect your network to other networks that use globally administered IP addresses, Black Box strongly recommends that you use IP addresses that have a network address assigned to you. There is a formal process for assigning unique IP addresses to networks worldwide. For more information please contact your internet service provider (ISP).

4.3 A Quick Start

If you just want to give the switch an IP address so that it can communicate on your network, or if you are not using VLANs, Black Box recommends that you use the CLI commands to quickly configure IP addressing. To do so, do one of the following:

Enter the following command at the CLI Manager level prompt.

```
LE2425MNS# ipconfig ip = <ipaddress> mask = <subnet-mask>
dgw= <default-gateway>
```

Syntax: **show ipconfig**

```
LE2425MNS> show ipconfig
IP Address       : 192.168.1.25
Subnet Mask      : 255.255.255.0
Default Gateway : 192.168.1.10
```

Note: In the factory-default configuration there is no IP addressing assigned to the switch.

4.4 Interface Access: Console/Serial Link, Telnet Features

In most cases, the default configuration is acceptable for standard operation.

Note Basic switch security is through passwords. You can gain additional security using IP authorized managers. However if unauthorized access is gained to the switch through in-band (Telnet), then you can disallow in-band access (as described in this section) and install the switch in a locked environment.

Feature	**Default**
Inactivity Time	10 Minutes
Terminal Type	VT-100
Baud Rate	38400
Flow Control	None

4.4.1 TELNET

The Telnet protocol is often thought of simply as a provider for remote logins to computer via the Internet. This was its original purpose although it can be used for many other purposes.

It is best understood in the context of a user with a local computer accessing the local telnet program (known as the client program) to run a login session on a remote computer where his communication needs are handled by a telnet server program running on the remote computer. It should be emphasized that the telnet server can pass on the data it has received from the client to many other types of processes including a remote login server.

A user can telnet a remote host (Computer or switch) from the LE2425.

syntax: **telnet** <ipaddress> [**port**=<port number>]

E.g. **telnet 192.168.1.1** [port is optional]. The *default port* is 23.

We also have the **Telnet Client** on the LE2425. Users can telnet the LE2425 from the host (Computer or switch) remotely. In other words users can manage the switch remotely.

Note: (i) we have to have an IP configuration on the switch before starting the telnet session.
(ii) Once the Telnet session starts, the serial connection will close automatically.
(iii) In the default configuration, inbound and outbound Telnet access is enabled.

To disable or enable Telnet access:
Syntax: **telnet <enable/disable>**

LE2425MNS (access) ## **telnet disable**
Disabling Access to Telnet

LE2425MNS (access) ## **telnet enable**
Enabling Access to Telnet

4.5 System Information

Configuring system information is optional, but recommended.

System Name: Using a unique name helps you to identify individual devices in stacking environments and when using SNMPc, HP Open View or any other NMS software for Hubs & Switches. For more details see chapter *SNMP.*

4.5.1 System Contact and Location:

This information is helpful for identifying the person administratively responsible for the switch and for identifying the locations of individual switches.

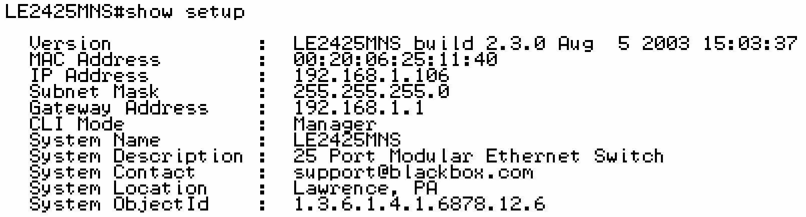
4.5.2 Time Zone:

The number of minutes your time zone location is to the West (+) or East (-) of Coordinated Universal Time (formerly GMT). The default **0** means no time zone is configured.

4.6 CLI: Listing the Current System Information.

4.6.1 List the current system information settings.

type: **show setup**
This example shows the switch's default console configuration.



```
LE2425MNS#show setup

  Version            :  LE2425MNS build 2.3.0 Aug  5 2003 15:03:37
  MAC Address        :  00:20:06:25:11:40
  IP Address         :  192.168.1.106
  Subnet Mask        :  255.255.255.0
  Gateway Address    :  192.168.1.1
  CLI Mode           :  Manager
  System Name        :  LE2425MNS
  System Description :  25 Port Modular Ethernet Switch
  System Contact     :  support@blackbox.com
  System Location    :  Lawrence, PA
  System ObjectId    :  1.3.6.1.4.1.6878.12.6
```

4.6.2 Configure the Time Zone and Daylight Time Rule.

These commands:

- Set the time zone you want to use
- Define the daylight time rule for keeping the correct time when daylight-saving-time shifts occur.

Syntax: **set timezone GMT**=[+ or -] **hour**=<0-14> **min**=<0-59>
set timeformat format=<12|24>
set daylight country=<name>

4.6.3 Configure the Date.

The switch uses the date command to configure the date. Note that the CLI uses either a 12 or 24-hour clock scheme; that is, hour *(hh)* values from 1 p.m. to midnight are input either as 1 or 13. You can set the format with the help of the **set time** command.
Syntax: **set date year**=<2000-2036> **month**=<1-12> **day**=<1-31>

For example, to set the switch to 3:45 p.m. on October 1, 2001 in California USA input "GMT – 08:00" :
LE2425MNS# **set timezone GMT**=[+ or -] **hour**=<0-14> **min**=<0-59>
LE2425MNS# **set date year**=<2001-2035> **month**=<1-12> **day**=<1-31**>**
Note: Executing **reboot** resets the time and date to their default startup values.

4.7 SNTP

Simple Network Time Protocol

The SNTP protocol is used to allow network access to accurate clocks and other sources of time base information that is an adaptation of the Network Time Protocol (NTP) used to synchronize device clocks in the Internet.

The SNTP client of the LE2425 has the ability to set the SNTP server IP address. The SNTP client synchronizes the time and date with the SNTP server.

4.7.1 CLI Commands

LE2425MNS# sntp
LE2425MNS(sntp)##
Syntax: **setsntp server** = <ipaddress> **timeout** = <1-10> **retry** = <1-3>
E.g., LE2425MNS(sntp)## **setsntp server = 204.65.129.201 timeout = 3 retry = 3**

Once the IP address of SNTP assigned then enable the SNTP service.
LE2425MNS(sntp)## **sntp** <enable|disable>

4.8 CLI: Configuration commands

The LE2425 has the following CLI commands available for configuration management.

- Saveconf
- Loadconf
- Kill config (**Hidden Command**)

Note: These commands are available in '*Manager*' privilege only.

4.8.1 To save the configuration

You can save the configuration as a binary file on the local console or FTP or TFTP Server using the '**saveconf**' command

Syntax: **saveconf mode=<serial|tftp|ftp> [<ipaddress>] [file=<name>]**
LE2425MNS# **saveconf mode**=serial **file**=leconfig
Note: File name is a user define name.

4.8.2 To load or restore the configuration

You can load the configuration from the location you have saved the configuration e.g., the local console, FTP or TFTP Server using '**loadconf**' command.

Syntax: **loadconf mode=<serial|tftp|ftp> [<ipaddress>] [file=<Name>]**
LE2425MNS# **loadconf mode**=serial **file**=leconfig

4.8.3 To erase the current configuration

Syntax: **kill config**

Note: This is a hidden command. It erases the current configuration and loads the factory default configuration. It is highly recommended to use this command only if you really need to erase the current configuration.

```
LE2425MNS# kill config
```

> **Warning**: Before erasing the current configuration using the **'kill config'** command it is suggested that you save the current configuration using the '**saveconf**' command. The '**kill config'** command will erase the current configuration and load the default configuration values. The '**kill config'** command will not erase or change any saved configuration settings in memory.

The **'Kill config'** command asks for confirmation. If you are sure press 'Y', otherwise press 'N'.
Do you want to erase the configuration? ['Y' or 'N']
If you press 'Y', it displays a confirmation message
Successfully erased configuration...Please reboot.

Note: Please restart the switch to get a default configuration. **kill config'** will not erase the current configuration until or unless you restart the switch.

4.8.4 Summary (Steps)

1. Save the current configuration on local console or FTP or TFTP Server.
Command: **saveconf**
2. Erase current configuration.
Command: **kill config**
3. Hard boot the switch to get the factory default configuration.

5.0 Security Features

5.1 Manager and Operator passwords:

You can gain access and privileges for the command line through either the console port or through the network by using Telnet . The features described in this chapter enhance security controls against unauthorized access through the network.

5.2 Console access interface and the CLI.

There are two levels of console access: *Manager* and *Operator*. For security, you can set a password on each of these levels.

5.2.1 Manager

This level allows access to all console interface areas.

Please change the default Manager Password to limit access of unauthorized people to the configuration area of the console interface.

5.2.2 Operator

This level allows access to the Status, Event Log, and CLI levels but does not allow Configuration capabilities.

On the Operator level, the Configuration Context, Download Application, and Reboot Switch option are not accessible.

5.3 To use password security:

1.Set a Manager password (and an Operator password, if applicable for your system).

2. Exit from the current console session. A Manager password will now be needed for full access to the console. Assuming that both a Manager password and an Operator password have been set, the level of access to the console interface will be determined by which password is entered in response to the prompt. The manager and operator passwords control access to the CLI.

Note: Passwords are case-sensitive.

5.4 CLI: Setting Manager and Operator Passwords

5.4.1 Configuring Manager and Operator Passwords

This procedure prompts you to enter a password twice to help verify that you have correctly entered the desired characters.

Syntax: ***set*** **password**

```
LE2425MNS# set  password
Enter old  password:********
Enter new password:*********
Confirm password :*********
Password changed successfully
```

Note: Password must be 4-10 characters

(For more details, Please refer *Chapter 3*).

5.5 Access Levels

For each authorized user, the Manager & Operator have specific access levels (For Details, Please see *Chapter 2*).

5.6 Configuring and Monitoring Port Security

The port security feature can be used to block input to an Ethernet, Fast Ethernet, or Gigabit Ethernet port when the MAC (Media Control Address) of the station attempting to access the port is different from any of the MAC addresses specified for that port. In the event of security violation, the port can be configured to go into the disable mode or drop mode. The drop mode allows the user to configure the port to remain enabled during a security violation and drop only packets that are coming in from insecure hosts.

5.6.1 Basic Operation

Default Port Security Operation: The default port security setting for each port is off. That is, any device can access a port without causing a security reaction.

Intruder Protection: A port that detects an " intruder" blocks the intruding device or drops the packets from transmitting to the network through that port.

General Operation for Port Security: On a per-port basis, you can set up security measures to block unauthorized devices and send notice of security violations. Once you have configured port security, you can then monitor the network for security violations through the Event Log.

For any port, you can configure the following:

Authorized (MAC) Addresses: Specify devices (MAC addresses) that are allowed to send inbound traffic through the port.

This feature:

- Closes the port to inbound traffic from any unauthorized devices that are connected to the port.
- Provides the option for sending information to the log of a detected attempted security violation to a network management station and disables the port.

Note: There is a limitation of 25 MAC addresses per port for Port Security. The more MAC addresses programmed, the larger the burden on the CPU.

5.6.2 Blocking Unauthorized Traffic

Unless you configure the switch to disable a port or drop the packets when a security violation is detected, the switch security only blocks unauthorized traffic without disabling the port. This feature enables you to apply the security configuration to ports on which hubs, switches, or other devices are connected and maintain security while also maintaining network access to authorized users.

5.6.3 Planning For Port Security

1.Plan your port security configuration and monitoring according to the following:

a. On which ports do you want to configure port security?

b. Which devices (MAC addresses) are authorized on each port?

c. For each port, what security actions do you want? (The switch automatically blocks intruders detected on that port from transmitting to the network.) The switch can be configured to

(i) Send intrusion alarms to the event Log and

(ii) optionally disable the port on which the intrusion was detected.

d. How do you want to learn of the security violation attempts the switch detects? You can use the Event Log (through the CLI **show log** command) to see the intrusion.

2. Use the CLI commands to configure port security operating and address controls.

5.7 CLI: Port Security Command Options and Operation

5.7.1 Configuring Port Security

Syntax: **configure port-security**

LE2425MNS# **configure port-security**

It will take you to the configuration mode to configure the port security.

Adding an Authorized Device to a Port.

Syntax: **allow mac=**<address|list|range> **port=**<num|list|range>

To simply add a device (MAC address) to a port's existing Authorized Addresses list, enter the port number with the **mac-address** parameter and the device's MAC address.

LE2425MNS(port-security)## **allow mac=00:c1:00:7f:ec: 00 00:60:b0:88:9e:00 port=18**

In above example, two authorized devices are allowed for port number 18.

To enable and disable Port Security

Syntax: **ps <enable|disable>**

LE2425MNS(port-security)## **ps enable**

This command enables the port security and switch is now ready to learn the MAC addresses.

To See the Authorized Devices

Syntax: **show port-security**

LE2425MNS# **show port-security port=18**

After executing the above command, the security configuration for port 18 would be:

```
Port            :18
Action          :Disable
Signal          :Log
Learn Mode      :Enable
MAC_Addresses: 00:c1:00:7f:ec:00  00:60:b0:88:9e:00
```

To see all the Ports,

LE2425MNS# **show port-security**

```
Status: Port-security Disabled
Port Action      Signal    Learn_Mode Mac_Address
1    None        None      Disable    None
2    None        None      Disable    None
3    None        None      Disable    None
4    None        None      Disable    None
5    None        None      Disable    None
6    None        None      Disable    None
7    None        None      Disable    None
8    None        None      Disable    None
9    None        None      Disable    None
10   None        None      Disable    None
11   None        None      Disable    None
12   None        None      Disable    None
13   None        None      Disable    None
14   None        None      Disable    None
15   None        None      Disable    None
16   None        None      Disable    None
17   Drop        Log       Enable     None
18   Drop        Log       Enable00:c1:00:7f:ec:00  00:60:b0:88:9e:00
19   Drop        Log       Enable     None
20   Drop        Log       Enable     None
21   Drop        Log       Enable     None
22   Drop        Log       Enable     None
23   Disable     Log       Enable     00:e0:29:6c:a4:fd
24   Drop        Log       Enable     None
25   None        None      Disable    None
```

Ports can also learn the MAC addresses with the help of the following command.

Syntax: **learn port=<number-list> <enable|disable>**

LE2425MNS(port-security)## **learn port=17,18 enable**

In the above example, Port 17 and 18 start learn the MAC addresses of connected devices.

Note: 1. Only when the ACTION is set to NONE will the MAC ADDRESS be learned
2. 25 MAC addresses can be learned per port.

Removing a Device From the " Authorized" List for a Port.

This command option removes unwanted devices (MAC addresses) from the Authorized Addresses list. (An Authorized Address list is available for each port where Learn Mode is set to " Static"

To use the CLI to remove a device that is no longer authorized:

Example: suppose port 18 is configured as shown below and you want to remove 00c100-123456 from the Authorized Address list:

LE2425MNS# **show port-security port=18**

```
Port            :18
Action          :Disable
Signal          :Log
Learn Mode      :Disable
MAC_Addresses: 00:c1:00:7f:ec:00  00:60:b0:88:9e:00
```

The following command serves this purpose by removing
00:c1:00:7f:ec:00

```
LE2425MNS(port-security)## remove mac=00:c1:00:7f:ec:00 port=18
```

The above command sequence results in the following configuration for port 18:

```
LE2425MNS# show port-security port=18
Port            :18
Action          :Disable
Signal          :Log
Learn Mode      :Disable
MAC_Addresses:00:60:b0:88:9e:00
```

5.8 Reading Intrusion Alerts and Resetting Alert Flags

5.8.1 Notice of Security Violations

When the switch detects an intrusion on a port, it sets an “ alert flag” for that port and makes the intrusion information available as described below. When a security violation occurs on a port configured for Port Security, the switch logs the intruder activity in the event log.

– The show log command displays the Intrusion Log and the Event Log with different options.

5.8.2 How the Intrusion Log Operates

When the switch detects an intrusion attempt on a port, it enters a record of this event in the event Log. The event Log lists the most recently detected security violation attempts. This gives you a history of past intrusion attempts also.

Example:

```
S Date          Time            Log Description
A 01-01-2001 12:05:52 AM PS:INTRUDER 00:e0:29:6c:a4:fd@port19, packet dropped
A 01-01-2001 12:07:04 AM PS:INTRUDER 00:50:0f:02:33:b6@port17, packet dropped
A 01-01-2001 12:07:16 AM PS:INTRUDER 00:e0:29:2a:f0:3a@port17, packet dropped
A 01-01-2001 12:07:16 AM PS:INTRUDER 00:01:03:e2:27:89@port17, packet dropped
A 01-01-2001 12:07:30 AM PS:INTRUDER 00:e0:29:08:d7:e9@port17, packet dropped
A 01-01-2001 12:07:32 AM PS:INTRUDER 00:10:dc:6e:52:95@port17, packet dropped
A 01-01-2001 12:07:34 AM PS:INTRUDER 00:e0:29:08:d6:43@port17, packet dropped
```

The above is an example of Multiple Intrusion Log Entries for the Same Port

The log shows the most recent intrusion at the top of the listing. Instead, if the log is filled when the switch detects a new intrusion, the oldest entry is dropped off the listing and the newest entry appears at the top of the listing.

5.8.3 CLI: Checking for Intrusions, Listing Intrusion Alerts

The following commands display port status including, whether there are intrusion alerts for any port(s), a list of the intrusions, and which specific ports had the intrusions.

```
LE2425MNS# show log
S Date       Time        Log Description
A 01-01-2001 12:05:18 AM PS:INTRUDER 00:50:0f:02:33:b6@port17, packet dropped
A 01-01-2001 12:05:26 AM PS:INTRUDER 00:02:b3:1d:05:dc@port17, packet dropped
A 01-01-2001 12:05:36 AM PS:INTRUDER 00:01:03:e2:27:89@port17, packet dropped
A 01-01-2001 12:05:40 AM PS:INTRUDER 00:e0:29:11:1b:af@port17, packet dropped
A 01-01-2001 12:05:44 AM PS:INTRUDER 00:02:b3:64:d8:cf@port17, packet dropped
A 01-01-2001 12:05:44 AM PS:INTRUDER 00:e0:29:09:5d:be@port17, packet dropped
A 01-01-2001 12:05:48 AM PS:INTRUDER 00:02:b3:08:d2:22@port17, packet dropped
A 01-01-2001 12:05:48 AM PS:INTRUDER 00:e0:29:2a:f0:3a@port17, packet dropped
A 01-01-2001 12:05:56 AM PS:INTRUDER 00:10:dc:40:57:95@port17, packet dropped
A 01-01-2001 12:06:02 AM PS:port 18 disabled, INTRUDER 00:e0:29:2a:f1:bd
```

This log shows the intrusion at the port 17 and 18. You can always clear the log with clear command.

```
LE2425MNS# clear log
```

It clears the complete log.

You can also clear the specific part of the Log.

Syntax: **clear log <informational|debug|activity|critical|fatal>**

```
LE2425MNS# clear log activity
```

It clears the ‘activity’ log only.

6.0 Using Authorized IP Managers to Protect Against Unauthorized Access

6.1 Authorized IP Manager Features

This feature enables you to enhance security on the switch by using IP addresses to authorize which stations (PCs or workstations) can access the switch. Thus, having the correct passwords is not sufficient for accessing the switch through the network unless the station attempting access is also included in the switch's Authorized IP Managers configuration. Access controls cover:

Telnet (CLI)
SNMP (network management)
Web (Web Interface)
Up to 25 authorized manager addresses, where each address applies to
either a single management station or a group of stations

Note This feature does not protect access to the switch through a modem or direct connection to the Console (RS-232) port. Also, if the IP address assigned to an authorized management station is configured in another station, the other station can gain management access to the switch even though a duplicate IP address condition exists. For these reasons, you should enhance your network's security by keeping physical access to the switch restricted to authorized personnel, using the password features built into the switch, and preventing unauthorized access to data on your management stations.

6.2 Access Levels

For each authorized manager address, you can configure either of these access levels:

6.2.1 Authorizing Single Stations:

The table entry authorizes a single management station to have IP access to the switch. To use this method, just enter the IP address of an authorized management station in the Authorized Manager IP column, and leave the IP Mask set to **255.255.255.255**. This is the easiest way to use the Authorized Managers feature.

6.2.2 Authorizing Multiple Stations:

The table entry uses the IP Mask to authorize access to the switch from a defined group of stations. This is useful if you want to easily authorize several stations to have access to the switch without typing in an entry for every station. All stations in the group are defined by the one Authorized Manager IP table entry and its associated IP mask and will have the same access level.

To configure the switch for authorized manager access, enter the appropriate *Authorized Manager IP* value and specify an *IP Mask*. The IP Mask determines how the Authorized Manager IP value is used for allowing or denying access to the switch by a management station.

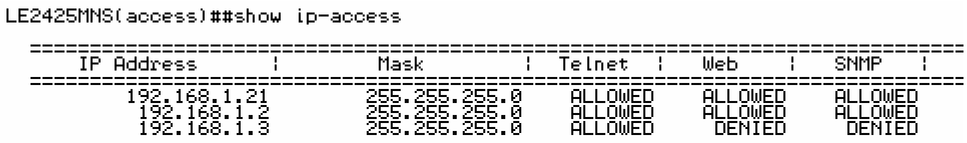
6.3 Overview of IP Mask Operation

The default IP Mask is 255.255.255.255 and allows switch access only to a station having an IP address that is identical to the Authorized Manager IP parameter value. ("255" in an octet of the mask means that only the exact value in the corresponding octet of the Authorized Manager IP parameter is allowed in the IP address of an authorized management station.) However, you can alter the mask and the Authorized Manager IP parameter to specify ranges of authorized IP addresses. For example, a mask of **255.255.255.*0*** and any value for the Authorized Manager IP parameter allows a range of 0 through 255 in the 4th octet of the authorized IP address. This enables a block of up to 254 IP addresses for IP management access (excluding 0 for the network and 255 for broadcasts). A mask of **255.255.255.25*2*** uses the 4th octet of a given Authorized Manager IP address to authorize four IP addresses (252,253,254,and 255) for management station access.

Note The IP Mask is a method for recognizing whether a given IP address is authorized for management access to the switch. This mask serves a different purpose than IP subnet masks and is applied in a different manner.

6.4 CLI: Viewing and Configuring Authorized IP Managers

Listing the Switch's Current Authorized IP Manager(s) Use the show ip authorized-managers command to list IP stations authorized to access the switch. For example:



```
LE2425MNS(access)##show ip-access

  ==========================================================================
      IP Address      ¦         Mask         ¦  Telnet  ¦   Web    ¦   SNMP   ¦
  ==========================================================================
           192.168.1.21        255.255.255.0    ALLOWED    ALLOWED    ALLOWED
            192.168.1.2        255.255.255.0    ALLOWED    ALLOWED    ALLOWED
            192.168.1.3        255.255.255.0    ALLOWED     DENIED     DENIED
```

Example of the Show IP Authorized-Manager Display
The above example shows an Authorized IP Manager List that allows stations
to access the switch for a specific service.

Configuring IP Authorized Managers for the Switch
Syntax: allow ip=<ipaddress> mask=<netmask> service=<name|list>

To Authorize Manager Access. This command authorizes access for any station having an IP address of 10.28.227.0 through 10.28.227.255for Telnet service:
LE2425MNS(access)## allow ip=10.28.227.101 mask = 255.255.255.0 service=telnet

Similarly, the next command authorizes access for any station having an IP address of 10.28.227.101 through 103 for snmp service:
LE2425MNS(access)##allow ip=10.28.227.101 mask=255.255.255.252 service=snmp,telnet

You can deny a service(s) for a specific IP/Net mask also as shown below.
Syntax: deny=<ipaddress> mask=<netmask> service=<name|list>
LE2425MNS(access)## deny ip=10.28.227.101 mask = 255.255.255.0 service=telnet

To Edit an Existing Access Entry. To change the mask or access level for an existing entry, use the entry's IP address and enter the new value(s).

LE2425MNS(access)## deny ip=10.28.227.101 mask = 255.255.255.0 service=web
The above command replaces the existing mask and access level for IP address 10.28.227.101 with 255.255.255.0 and web denied service.

LE2425MNS(access)## allow ip=10.28.227.101 mask = 255.255.0.0 service=web
The above command replaces the existing mask and access level for IP address 10.28.227.101 with 255.255.0.0 and allowed web service.

6.5 Building IP Masks

The IP Mask parameter controls how the switch uses an Authorized Manager IP value to recognize the IP addresses of authorized manager stations on your network.

6.5.1 Configuring One Station Per Authorized Manager IP Entry

This is the easiest way to apply a mask. If you have ten or fewer management and/or operator stations, you can configure them quickly by simply adding the address of each to the Authorized Manager IP list with **255.255.255.255** for the corresponding mask. For example, if you configure an IP address of **10.28.227.125** with an IP mask of 2**55.255.255.255**, only a station having an IP address of **10.28.227.125** has management access to the switch.

	1st Octet	2nd Octet	3rd Octet	4th Octet	Device Access
IP Mask	255	255	255	255	The "255" in each octet of the mask specifies that only the exact value in that octet of the corresponding IP address is allowed. This mask allows management access only to a station having an IP address of 10.33.248.5.
Authorized Manager IP	10	28	227	125	

Table . Analysis of IP Mask for Single-Station Entries

6.5.2 Configuring Multiple Stations Per Authorized Manager IP

The mask determines whether the IP address of a station on the network meets the criteria you specify. That is, for a given Authorized Manager entry, the switch applies the IP mask to the IP address you specify to determine a range of authorized IP addresses for management access. As described above, that range can be as small as one IP address (if **255** is set for all octets in the mask), or can include multiple IP addresses (if one or more octets in the mask are set to less than **255**).

If a bit in an octet of the mask is "on" (set to 1), then the corresponding bit in the IP address of a potentially authorized station must match the same bit in the IP address you entered in the Authorized Manager IP list. Conversely, if a bit in an octet of the mask is "off' (set to 0), then the corresponding bit in the IP address of a potentially authorized station on the network does not have to match its counterpart in the IP address you entered in the Authorized Manager IP list. Thus, in the example shown above, a "255" in an IP Mask octet (*all* bits in the octet are "on") means only one value is allowed for that octet—the value you specify in the corresponding octet of the Authorized Manager IP list. A "0" (all bits in the octet are "off") means that any value from 0 to 255 is allowed in the corresponding octet in the IP address of an authorized station. You can also specify a series of values that are a subset of the 0-255 range by using a value that is greater than 0, but less than 255.

	1st Octet	2nd Octet	3rd Octet	4th Octet	Device Access
IP Mask	255	255	0	255	This combination specifies an authorized IP address of 10.33.*xxx*.1. It could be applied, for example, to a subnetted network where each subnet is defined by the third octet and includes a management station defined by the value of "1" in the fourth octet of the station's IP address.
Authorized Manager IP	10	33	248	1	
IP Mask	255	238	0	255	Allows 230, 231, 246, and 247 in the 2nd octet, and 194, 195, 198, 199 in the 4th octet.
Authorized Manager IP	10	247	100	195	

Table . Analysis of IP Mask for Multiple-Station Entries

NOTE: User can set maximum 25 rules (Allow/Deny). 26th rule will overwrite the first rule.

6.6 Operating and Troubleshooting Notes:

6.6.1 Network Security Precautions:

You can enhance your network's security by keeping physical access to the switch restricted to authorized personnel, using the password features built into the switch, and preventing unauthorized access to data on your management stations.

Modem and Direct Console Access: Configuring authorized IP managers does not protect against access to the switch through a modem or direct Console (RS-232) port connection.

6.6.2 Duplicate IP Addresses:

If the IP address configured in an authorized management station is also configured in another station, the other station can gain management access to the switch even though a duplicate IP address condition exists.

6.6.3 Web Proxy Servers:

If you use the web browser interface to access the switch from an authorized IP manager station, it is recommended that you avoid the use of a web proxy server in the path between the station and the switch. This is because switch access through a web proxy server requires that you first add the web proxy server to the Authorized Manager IP list. This reduces security by opening switch access to anyone who *uses the web proxy server*. The following two options outline how to eliminate a web proxy server from the path between a station and the switch:

Even if you need proxy server access enabled in order to use other applications, you can still eliminate proxy service for web access to the switch. To do so, add the IP address or DNS name of the switch to the non-proxy, or "Exceptions" list in the web browser interface you are using on the authorized station. (e.g. in Microsoft Explorer go to tools, internet options, connections, lan settings, use a proxy server check, and advanced and enter it there).
If you don't need proxy server access at all on the authorized station, then just disable the proxy server feature in the station's web browser interface.

6.6.4 Global Access

User can authorize the services globally. Here is the list of commands.

```
snmp <enable|disable>
dhcp <enable|disable>
telnet <enable|disable>
```

For example,

```
LE2425MNS(access)##snmp disable
```

It disables the SNMP Access to everyone.

7.0 Configuration for Network Management Applications (SNMP)

This chapter includes:

- An overview of SNMP management for the switch
- Bitview and Hubview through SNMPc.
- Configuring the Series 6K switch for:
- SNMP management
- SNMP Communities
- Traps Configuration
- Information on advanced management through RMON

To implement SNMP management, you must configure the switch with an appropriate IP address.

7.1 Overview

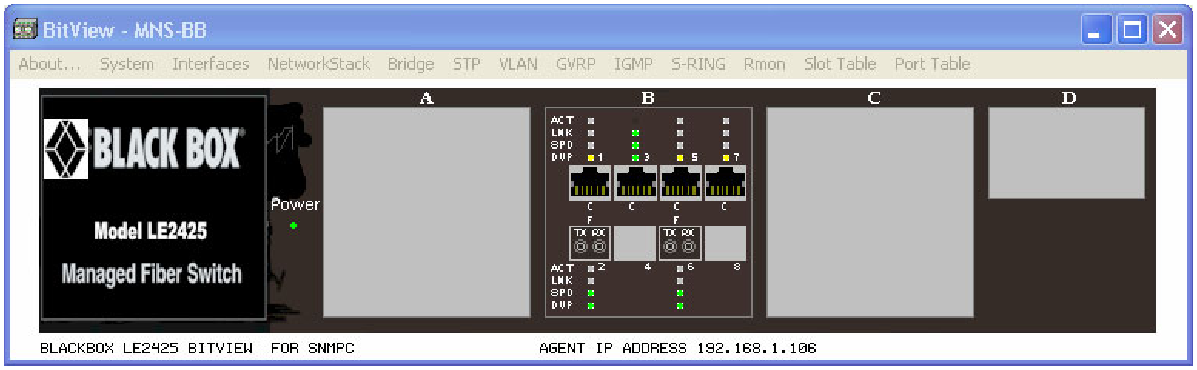
You can manage the switch via SNMP from a network management station.

For this purpose, Black Box recommends the **SNMPc**, an easy-to-install and use network management platform that runs on Windows based PC's. It uses the SNMP and RMON agents statistical sampling software that is included in the switch to provide powerful, but easy-to-use traffic monitoring and network activity analysis tools.

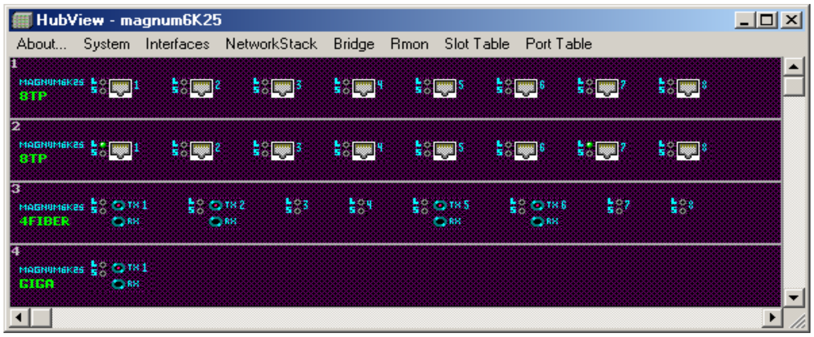
7.2 BitView and HubView

The BitView and HubView can be seen through SNMPc (Management PC Software).

LE2425's that have BitView and HubView definitions can be managed graphically. BitView displays a bitmap image that matches the faceplate of the device, whereas HubView is a more generic view that shows the layout of the device, but always uses the same picture elements.
BitView is functionally similar to HubView, but displays a more realistic image of supported devices. Generally, all the LEDs and other graphical elements available on the device front panel can be displayed with BitView. As with HubView, you can select a device slot or port, and then a menu to operate on the selected item.


BitView - MNS-BB
About... System Interfaces NetworkStack Bridge STP VLAN GVRP IGMP S-RING Rmon Slot Table Port Table
BLACK BOX
Model LE2425
Managed Fiber Switch
Power
A
B
C
D
ACT LNK SPD DUP
TX RX
BLACKBOX LE2425 BITVIEW FOR SNMPC
AGENT IP ADDRESS 192.168.1.106

LE2425MNS: Bitview



LE2425MNS: Hubview

7.3 SNMP Management Features

SNMP management features on the switch include:

SNMP version 1
Security via configuration of SNMP communities
Event reporting via SNMP
Managing the switch with an SNMP network management tool Supported *Standard* MIBs include:
• SNMP MIB-II (RFC 1213)
• Bridge MIB (RFC 1493)
ifGeneralGroup, ifRcvAddressGroup, ifStackGroup
• RMON MIB (RFC 1757)
• RMON: groups 1, 2, 3, and 9
(Statistics, Events, Alarms, and History)
• Version 1 traps (Warm Start, Cold Start, Link Up, Link Down, Authentication Failure, Rising Alarm, Falling Alarm)

• *Black Box Proprietary* MIB

7.4 Configuring for SNMP Access to the Switch

SNMP access requires an IP address and subnet mask configured on the switch. In other words, Network stacks should be configured with an IP address and subnet mask. Once an IP address has been configured, we can follow the same steps as configuring the CLI (see CLI section 6.5) to configure the SNMP Access.

To authenticate the SNMP Manager station, you need to add the IP Address of the Manager station.

This is a security feature of 6K Switches to authenticate the SNMP console station.

Go to SNMP configuration mode. (i.e., LE2425MNS(SNMP)##) and assign the following command.

Syntax: **mgrip <add|delete> ip=<ipaddress>**

Note: If SNMP console is not added to the 6K switch, then user will not be able to access the SNMP agent.

To configure and add the appropriate traps please see the CLI section of this chapter.

7.5 CLI: Viewing and Configuring Community Names

7.5.1 Listing Community Names

This command lists the data for currently configured SNMP community names.

Syntax: **show snmp**

LE2425MNS# **show snmp**

This example lists the data for all communities in a switch; that is, both the default "public" community name and another community named "private".
The configured community values are

```
SNMP CONFIGURATION INFORMATION
 ------------------------------------------------------
 SNMP Get Community Name  :  public
 SNMP Set Community Name  :  private
 SNMP Trap Community Name :  public
 AuthenTrapsEnableFlag    :  enabled
 SNMP Access Status       :  enabled
 SNMP MANAGERS INFO
 ---------------------------------
 SNMP TRAP STATIONS INFO
 ---------------------------------------
```

SNMP Manager and Traps are not yet configured.

7.6 Configuring Community Names and Values

If you do not specify restricted or unrestricted for the read/write MIB access, the switch automatically restricts the community to read access for the MIB.

7.6.1 Adding SNMP Communities in the Switch

The following SNMP command add *new* SNMP communities:

Syntax: community [write=<string>] [read=<string>] [trap=<string>]

LE2425MNS(snmp)## **community write="private" read="public" trap="netman"**

7.6.2 Adding SNMP Traps in the Switch

The following SNMP command adds a new SNMP Trap:

Syntax: **traps add type=rmon|snmp|rmon,snmp|snmp,rmon|all ipaddress=<ipaddr>**

LE2425MNS(snmp)## **traps add type=all ipaddress=192.168.1.2**

7.6.3 Add or Modify system parameters

The following command to add or modify the system Name, System Contact or System Location.

Syntax: setvar [sysname|syscontact|syslocation]=<string>

LE2425MNS(snmp)## **setvar sysname=LE2425**

LE2425MNS(snmp)## **setvar syscontact=support@blackbox.com**

7.7 Using the CLI To List Current SNMP Trap Receivers

This command lists the currently configured trap receivers along with the current SNMP community name data.

*Synta*x: **show snmp**

In the next example, the **show snmp** command shows that the switch has been previously configured to send SNMP traps to management stations belonging to the "public" and "private" communities.

LE2425MNS(snmp)## **show snmp**

```
SNMP CONFIGURATION INFORMATION
 -----------------------------------------------------
 SNMP Get Community Name  :  public
 SNMP Set Community Name  :  private
 SNMP Trap Community Name :  public
 AuthenTrapsEnableFlag    :  enabled
 SNMP Access Status       :  enabled
 SNMP MANAGERS INFO
 ---------------------------------
  IP=192.168.1.10
 SNMP TRAP STATIONS INFO
 ---------------------------------------
  IP=192.168.1.11
```

7.8 RMON

The switch supports RMON (Remote Monitoring) on all connected network segments. This allows for troubleshooting and optimizing your network.

The LE2425 switches provides hardware-based RMON counters in the switch chipset. The switch manager CPU polls these counters periodically to collect the statistics in a format that compiles with the RMON MIB definition.

The following RMON groups are supported:

- Ethernet Statistics Group - maintains utilization and error statistics for the switch port being monitored.
- History Group – gathers and stores periodic statistical samples from previous Statistics Group.
- Alarm Group – allows a network administrator to define alarm thresholds for any MIB variable.
- Log and Event Group – allows a network administrator to define actions based on alarms. SNMP Traps are generated when RMON Alarms are triggered.

The RMON agent automatically runs in the switch. Use the RMON management station on your network to enable or disable specific RMON traps and events.

7.8.1 Adding RMON Communities in the Switch

The following RMON commands add *new RMON* communities:

```
history def-owner = <string>
statistics def-owner = <string>
alarm def-owner = <string>
event def-owner = <string>
```

e.g.,

```
LE2425MNS(rmon)## event def-owner = “test”
```

The **show** command lists the RMON data of specified type.

*Synta*x: **show rmon <stats|hist|event|alarm>**

```
LE2425MNS(snmp)##show rmon event

RMON Event Default Owner        :  monitor
RMON Event Default Community:  public
```

8.0 Monitoring and Analyzing Switch Operation

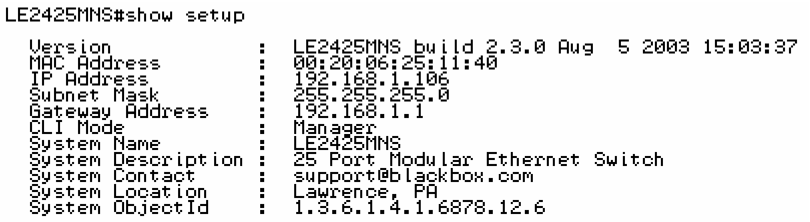
8.1 Overview

The LE2425 Switches have several built-in tools for monitoring, analyzing, and troubleshooting switch and network operations:

Status: Includes options for displaying general Switch information, management address data, and MAC addresses.
Event Log: Lists Switch operating events and Alert events.
Configurable trap receivers: Uses SNMP to enable management stations on your network to receive SNMP traps from the Switch.
Port monitoring (mirroring): Copies all traffic from the specified ports to a designated monitoring port.

8.2 CLI Access

Syntax: **show setup**



```
LE2425MNS#show setup

  Version            :  LE2425MNS build 2.3.0 Aug  5 2003 15:03:37
  MAC Address        :  00:20:06:25:11:40
  IP Address         :  192.168.1.106
  Subnet Mask        :  255.255.255.0
  Gateway Address    :  192.168.1.1
  CLI Mode           :  Manager
  System Name        :  LE2425MNS
  System Description :  25 Port Modular Ethernet Switch
  System Contact     :  support@blackbox.com
  System Location    :  Lawrence, PA
  System ObjectId    :  1.3.6.1.4.1.6878.12.6
```

8.3 Port Monitoring (Mirroring) Features

You can designate a port for monitoring traffic of one or more ports on the Switch. The Switch monitors the network activity by copying all traffic from the specified monitoring sources (ports or VLAN) to the designated monitoring (mirror) port, to which a network analyzer can be attached.

8.3.1 CLI: Configuring Port Monitoring

You must use the following configuration sequence to configure port monitoring in the CLI:

1. Assign a monitoring (mirroring) port.
2. Designate the port to monitor.

To list the ports assigned to mirror (receive monitored traffic) and the ports being monitored you need to use the command below:
Syntax: **show port-mirror**
For example, if you assign port 12 as the monitoring port and configure the Switch to monitor port 3, **show port-mirror** displays the following:

LE2425MNS> **show port-mirror**
Port mirroring is Enabled
Monitor Port is : 3
Sniffer Port is : 12

Configuring the monitor port assigns or removes a monitoring port. This must be executed from the configuration level. Removing the monitor port disables port monitoring and resets the monitoring parameters to their factory-default settings.
Syntax:
setport monitor=<number> sniffer=<number>
For example, to assign port 12 as the monitoring port and 3 as the monitored port, *type syntax*:
LE2425MNS## **setport monitor=3 sniffer=12**
To turn off port monitoring *type syntax*:
LE2425MNS# **prtmr disable**

9.0 Optimizing Port Usage

9.1 Overview

This chapter includes:

- Configuring port, status, mode (speed and duplex), and flow control parameters.
- Configuration screens corresponding to the port numbers on the front of the switch.

9.2 CLI: Viewing Port Status and Configuring Port Parameters

From the CLI commands, you can configure and view all port parameter settings and view all port status indicators.

9.2.1 Port Status and Configuration Features

Status or Parameter **Description**

---------------------------------- --------------------

Status

Enable (default): The port is ready for a network connection.
Disable: The port will not operate even when properly connected in a network. Use this setting if the port needs to be shut down for diagnostic purposes or while you are making topology changes.

Link

Up: The port senses a linkbeat.
Down: The port is not enabled, has no cables connected, or is experiencing a network error. For troubleshooting information, see the installation manual you received with the switch. See also chapter 9, “ Troubleshooting” (in this manual).

Mode

The port’s speed and duplex (data transfer operation) setting.
10/100Base-T ports:
• **Auto** (default): Senses speed and negotiates with the port at the other end of the link for data transfer operation (half-duplex or full-duplex).
Note: Ensure that the device attached to the port is configured for the same setting that you selected here. Also, if “ Auto” is used, the device to which the port is connected must operate in compliance with the IEEE 802.3u “Auto Negotiation” standard for 100Base-T networks. If the other device does not comply with the 802.3u standard, or is not set to “Auto”, then the port configuration on the switch must be manually set to match the port configuration on the other device.
To see what the switch negotiated for the Auto setting, use the CLI **show port** command.

Possible port setting combinations for copper ports.

- ✓ 10HDx: 10 Mbps, Half-Duplex
- ✓ 10FDx: 10 Mbps, Full-Duplex
- ✓ 100HDx: 100 Mbps, Half-Duplex
- ✓ 100FDx: 100 Mbps, Full-Duplex

Possible port settings for 100FX ports:

- ✓ 100FDx (default): 100 Mbps, Full-Duplex
- ✓ 100HDx: 100 Mbps, Half-Duplex

Possible port settings for 10FL ports:

- ✓ 10HDx (default): 10 Mbps, Half-Duplex
- ✓ 10FDx: 10 Mbps, Full-Duplex

100/1000Base-T ports:
• **Auto** (default): Senses speed and negotiates with the port at the other end of the link for port operation (MDI-X or MDI).
To see what the switch negotiated for the Auto setting, use the

CLI **show port** command.

- ✓ 1000Fdx: 1000 Mbps (1Gbps), Full-Duplex only
- ✓ 100Fdx: 100 Mbps, Full-Duplex

Notes:

• To change the port speed on a transceiver port you are required to reboot the switch.

• Ensure that the device attached to the port is configured for the same setting that you selected here.

Also, if “ Auto” is used, the device the port is connected to must also be configured to “ Auto” and operate in compliance with the IEEE 802.3ab “ Auto Negotiation” standard for 1000Base-T networks.

Gigabit fiber-optic ports (Gigabit-SX and Gigabit-LX):

- ✓ 1000FDx (default): 1000 Mbps (1 GBPS), Full Duplex only

• **Auto**: The port operates at 1000FDx and auto-negotiates flow control with the device connected to the port.

Flow Control

• **Disabled** (default): The port will not generate flow control packets and drops received flow control packets.

• **Enabled**: The port uses 802.3x Link Layer Flow Control, generates flow control packets, and processes received flow control packets.

With the port mode set to “Auto” (the default) and “Flow Control” set to enabled, the switch negotiates Flow Control on the indicated port. If the port mode is not set to “Auto”, or if “Flow Control” is disabled on the port, then Flow Control is not used.

9.2.2 Port Status and Configuration Commands

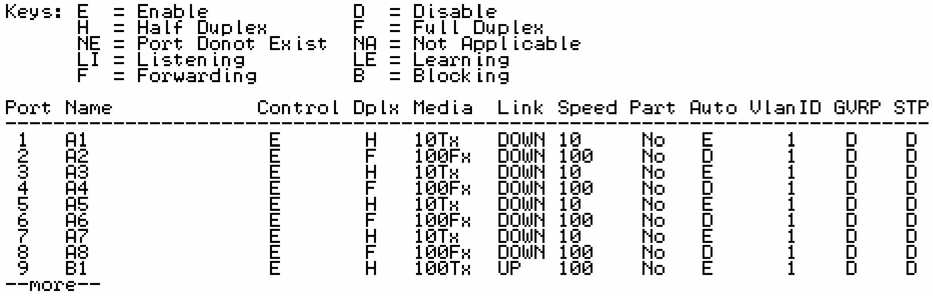
From the CLI, you can configure and view all port parameter settings and all port status indicators.

9.2.3 Using the CLI to View Port Status

Use the following commands to display port status and configuration:

show port: Lists the full status and configuration for all ports on the switch.

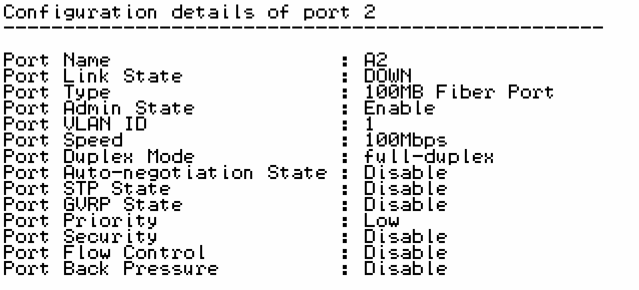
Syntax: **show port**



```
Keys: E  = Enable            D  = Disable
      H  = Half Duplex       F  = Full Duplex
      NE = Port Donot Exist  NA = Not Applicable
      LI = Listening         LE = Learning
      F  = Forwarding        B  = Blocking

Port Name            Control Dplx Media  Link Speed Part Auto VlanID GVRP STP
-----------------------------------------------------------------------------
 1   A1               E       H    10Tx   DOWN 10     No   E      1    D    D
 2   A2               E       F    100Fx  DOWN 100    No   D      1    D    D
 3   A3               E       H    10Tx   DOWN 10     No   E      1    D    D
 4   A4               E       F    100Fx  DOWN 100    No   D      1    D    D
 5   A5               E       H    10Tx   DOWN 10     No   E      1    D    D
 6   A6               E       F    100Fx  DOWN 100    No   D      1    D    D
 7   A7               E       H    10Tx   DOWN 10     No   E      1    D    D
 8   A8               E       F    100Fx  DOWN 100    No   D      1    D    D
 9   B1               E       H    100Tx  UP   100    No   E      1    D    D
--more--
```

show port=<Port number>: Lists the status of the specific port.

Syntax: **show port=2**



```
Configuration details of port 2
--------------------------------------------------

Port Name                   : A2
Port Link State             : DOWN
Port Type                   : 100MB Fiber Port
Port Admin State            : Enable
Port VLAN ID                : 1
Port Speed                  : 100Mbps
Port Duplex Mode            : full-duplex
Port Auto-negotiation State : Disable
Port STP State              : Disable
Port GVRP State             : Disable
Port Priority               : Low
Port Security               : Disable
Port Flow Control           : Disable
Port Back Pressure          : Disable
```

9.2.4 Using the CLI To Configure Ports

You can configure one or more of the following port parameters. For details on each option, see Table above.

Syntax: **setport port**=<port-list> **status**=<enable|disable> **speed**=<10|100> **duplex**=<half|full> **auto**=<enable|disable>

For example, to configure ports 1 through 4 and port 7 for 100Mbps full-duplex, you would enter this command:
Note: Before changing the port setting, you have to 'disable' the auto- negotiation.

LE2425MNS(device)## **setport port=1- 4,7 speed=100 duplex=full**

Similarly, to configure a single port with the settings in the above command, you could enter the same command with only the one port identified.

LE2425MNS(device)## **setport port=7 speed=100 duplex=full**

If port 8 was disabled, and you wanted to enable it and configure it for 100FDx you could do so with the following command.

LE2425MNS(device)## **setport port=8 status=enable speed=100 duplex=full**

To set the Age Time
LE2425MNS(device)## **setage time=<timeout-period>**
Note: Default value is 300 secs

9.3 Broadcast Storm Protection

One of the best features of the LE2425 is its ability to keep broadcast storms from spreading throughout a network. Network storms are characterized by an excessive number of broadcast packets being sent over the network. These storms can occur if network equipment is configured incorrectly, network software is not properly functioning, or poorly designed programs (including some network games) are used. Storms can reduce network performance and cause bridges, routers, workstations, servers and PC's to slow down or even crash.

9.3.1 How does it works

The LE2425 is capable of detecting and limiting storms on each interface (Port) or through each Ethernet address. A network administrator can set the maximum number of broadcast frames (Threshold value) that are permitted from a particular interface every second. If that maximum number is exceeded, a storm condition is declared. Once it is determined that a storm is occurring on an interface, any additional broadcast packets received on that interface will be dropped until the storm is determined to be over. The storm is determined to be over when a one-second period elapses with no broadcast packets received on that interface.
A network administrator can also limit the number of broadcast packets allowed from a particular

Ethernet address (host) every second. Once it is determined that a storm is occurring, any additional broadcast packets from that host address will be dropped until the storm is determined to be over. The storm is determined to be over when thirty seconds have passed in which the host sends less than one-half the stated threshold of broadcast packets in every one-second period.

9.3.2 CLI: To Enable/Disable the broadcast Protection

Syntax: broadcast-protect <enable|disable>

9.3.3 To set the Filter

Syntax: broadcast-filter port=<port> <enable|disable>

9.3.4 To set the Threshold value

Syntax: rate-threshold port=<port|list|range> rate=<frms/sec>

In most situations, you will not need to set the Storm Thresholds. However, if intensive broadcast messaging is typical to the network protocols used in your network environment, you may wish to control the maximum number of broadcast messages or frames per second that will be bridged from a particular host. If the maximum value of broadcast per second is exceeded, the Access Point will drop all subsequent messages of that type from that source address.

9.3.5 How to Protect against Broadcast Storms

```
LE2425MNS(device)##broadcast-protect enable
LE2425MNS#show broadcast-protect
=====================================================================
 PORT |  STATUS  | THRESHOLD (frms/sec) | CURR RATE (frms/sec) | ACTIVE
=====================================================================
   1  Enabled     4294967295        0                  NO
   2  Enabled     4294967295        0                  NO
   3  Enabled     4294967295        0                  NO
   4  Enabled     4294967295        0                  NO
   5  Enabled     4294967295        0                  NO
   6  Enabled     4294967295        0                  NO
   7  Enabled     4294967295        0                  NO
   8  Enabled     4294967295        0                  NO
   9  Enabled     4294967295        0                  NO
  10  Enabled     4294967295        0                  NO
  11  Enabled     4294967295        0                  NO
  12  Enabled     4294967295        0                  NO
  13  Enabled     4294967295        0                  NO
  14  Enabled     4294967295        0                  NO
  15  Enabled     4294967295        0                  NO
  16  Enabled     4294967295        0                  NO
  17  Enabled     4294967295        0                  NO
  18  Enabled     4294967295        0                  NO
  19  Enabled     4294967295        0                  NO
  20  Enabled     4294967295        4000               YES
  21  Enabled     4294967295        0                  NO
  22  Enabled     4294967295        0                  NO
  23  Enabled     4294967295        0                  NO
  24  Enabled     4294967295        0                  NO
  25  Enabled     4294967295        0                  NO
```

In this example Port 20 has broadcast packets To avoid the packet storm you need to set up the threshold value. Threshold value should be less than the current rate.

```
LE2425MNS(Device)## rate-threshold port=20 rate= 3500
```

```
LE2425MNS(Device)## show broadcast-protect
=================================================================
 PORT |  STATUS  | THRESHOLD (frms/sec) | CURR RATE (frms/sec) | ACTIVE
=================================================================
    1  Enabled         4294967295          0                  NO
    2  Enabled         4294967295          0                  NO
    3  Enabled         4294967295          0                  NO
    4  Enabled         4294967295          0                  NO
    5  Enabled         4294967295          0                  NO
    6  Enabled         4294967295          0                  NO
    7  Enabled         4294967295          0                  NO
    8  Enabled         4294967295          0                  NO
    9  Enabled         4294967295          0                  NO
   10  Enabled         4294967295          0                  NO
   11  Enabled         4294967295          0                  NO
   12  Enabled         4294967295          0                  NO
   13  Enabled         4294967295          0                  NO
   14  Enabled         4294967295          0                  NO
   15  Enabled         4294967295          0                  NO
   16  Enabled         4294967295          0                  NO
   17  Enabled         4294967295          0                  NO
   18  Enabled         4294967295          0                  NO
   19  Enabled         4294967295          0                  NO
   20  Enabled         3500                4000               YES
   21  Enabled         4294967295          0                  NO
   22  Enabled         4294967295          0                  NO
   23  Enabled         4294967295          0                  NO
   24  Enabled         4294967295          0                  NO
   25  Enabled         4294967295          0                  NO
```

User can also disable/enable a particular port or a set of ports for broadcast storm protection.

```
LE2425MNS(Device)## broadcast-filter port= 24,25 enable
LE2425MNS#show broadcast-protect

=================================================================
 PORT |  STATUS  | THRESHOLD (frms/sec) | CURR RATE (frms/sec) | ACTIVE
=================================================================
    1  Disabled        4294967295          0                  NO
    2  Disabled        4294967295          0                  NO
    3  Disabled        4294967295          0                  NO
    4  Disabled        4294967295          0                  NO
    5  Disabled        4294967295          0                  NO
    6  Disabled        4294967295          0                  NO
    7  Disabled        4294967295          0                  NO
    8  Disabled        4294967295          0                  NO
    9  Disabled        4294967295          0                  NO
   10  Disabled        4294967295          0                  NO
   11  Disabled        4294967295          0                  NO
   12  Disabled        4294967295          0                  NO
   13  Disabled        4294967295          0                  NO
   14  Disabled        4294967295          0                  NO
   15  Disabled        4294967295          0                  NO
   16  Disabled        4294967295          0                  NO
   17  Disabled        4294967295          0                  NO
   18  Disabled        4294967295          0                  NO
   19  Disabled        4294967295          0                  NO
   20  Disabled        4294967295          0                  NO
   21  Disabled        4294967295          0                  NO
   22  Disabled        4294967295          0                  NO
   23  Disabled        4294967295          0                  NO
   24  Enabled         4294967295          4500               YES
   25  Enabled         4294967295          4500               YES
```

Note: User can enable or disable this feature at any point of time.

10.0 QoS (Quality of Service)

10.1 Overview

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic over various technologies, including Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet and 802.1 networks, SONET, and IP-routed networks that may use any or all of these underlying technologies. The primary goal of QoS is to provide priority including dedicated bandwidth.

10.2 QoS Concepts

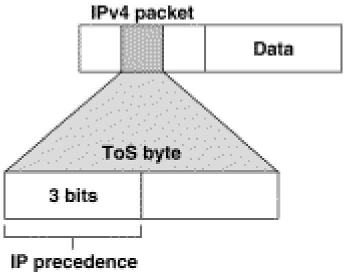
Fundamentally, QoS enables you to provide better service to certain flows. This is accomplished by either raising the priority of a flow or limiting the priority of another flow. When using congestion-management tools, you try to raise the priority of a flow by queuing and servicing queues in different ways. The queue management tool used for congestion avoidance raises priority by dropping lower-priority flows before higher-priority flows. Policing and shaping provide priority to a flow by limiting the throughput of other flows.

The LE2425 switch supports QoS as specified in the IEEE 802.1p and 802.1Q standards. QoS can be important in network environments where there are time-critical applications, such as voice transmission or video conferencing, which can be adversely effected by packet transfer delays.
QoS was designed to address this problem. The 802.1p standard outlines eight levels of priority, 0 to 7, with 0 the lowest priority and 7 the highest. The LE2425 switch has two priority queues, 1 (low) and 0 (high).When a tagged packet enters a switch port, the switch responds by placing the packet into one of the two queues

10.3 IP Precedence: Differentiated QoS

IP precedence utilizes the 3 precedence bits in the IPv4 header's Type of Service (ToS) field to specify class of service for each packet. You can partition traffic in up to eight classes of service using IP precedence. The queuing technologies throughout the network can then use this signal to provide the appropriate expedited handling.

This Diagram Shows the IP Precedence ToS Field in an IP Packet Header



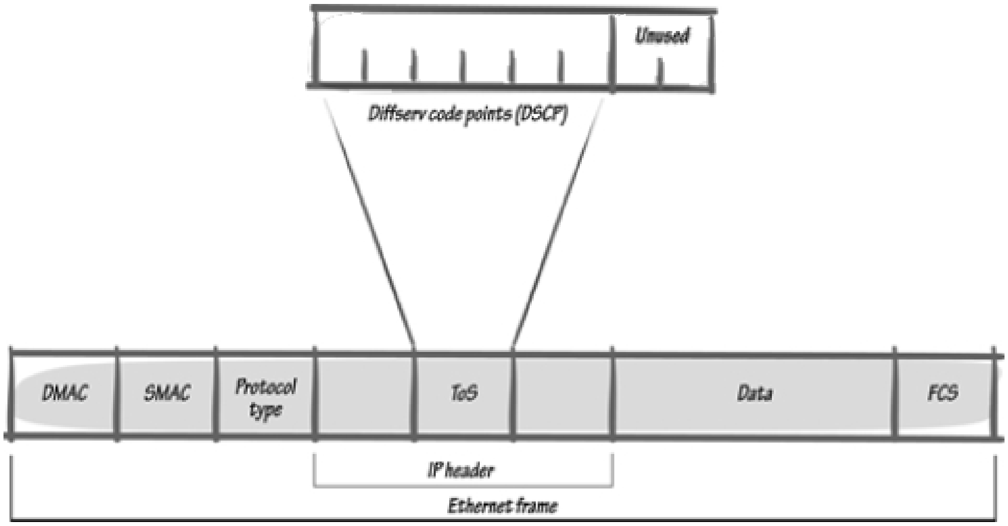
The 3 most significant bits (correlating to binary settings 32, 64, and 128) of the Type of Service (ToS) field in the IP header constitute the bits used for IP precedence. These bits are used to provide a priority from 0 to 7 for the IP packet.

Because only 3 bits of the ToS byte are used for IP precedence, you need to differentiate these bits from the rest of the ToS byte.

10.4 DiffServ

QoS (quality of service) refers to the level of preferential treatment a packet receives when it is being sent through a network. QoS allows time sensitive packets, such as voice and video, to be given priority over time insensitive packets, such as data. Differentiated services (DiffServ or DS) is a set of technologies defined by the IETF (Internet Engineering Task Force) to provide quality of service for traffic on IP networks.

DiffServ is designed for use at the edge of the enterprise where corporate traffic enters the service provider environment. DiffServ is a layer-3 protocol and requires no specific layer-2 capability, allowing it to be used in the LAN, MAN, and WAN. DiffServ works by tagging each packet (at the originating device or an intermediate switch) for the requested level of service it requires across the network.



DiffServ inserts a 6-bit DiffServ code point (DSCP) in the TOS (type of service) field of the IP header, as shown in the picture above. Information in the DSCP allows nodes to determine the per hop behavior (PHB), which is an observable forwarding behavior for each packet. Per hop behaviors are defined in according to:

- Resources required (e.g., bandwidth, buffer size)
- Priority (based on application or business requirements)
- Traffic characteristics (e.g., delay, jitter, packet loss)

Nodes implement PHBs through buffer management and packet scheduling mechanisms. This hop-by-hop allocation of resources is the basis by which DiffServ provides quality of service for different types of communications traffic.

10.5 PQ: Priority Queuing

PQ ensures that important traffic gets the fastest handling at each point where it is used.
It was designed to give strict priority to important traffic. Priority queuing can flexibly prioritize according to network protocol (for example IP, IPX, or AppleTalk), incoming interface, packet size, source/destination address, and so on. In PQ, each packet is placed in one of two queues—high or low—based on an assigned priority. Packets that are not classified by this priority list mechanism fall into the normal queue.
Note: LE2425 Switches support two priority queues, 1 (low) and 0 (high). During transmission, the algorithm gives higher-priority queues absolute preferential treatment over low-priority queues.

10.6 QoS Management

The introduction discussed a common method (but by no means the only method) for QoS management. For baselining a network, you can use RMON probes and an application (such as Traffic Director) to develop a good understanding of traffic characteristics. RMON probes provide more complete information. In addition, targeted applications should be baselined (this is commonly measured by response time). This information helps to validate any QoS deployment. From this data, QoS policy is set and deployed.

Once deployed, it is important to evaluate the QoS policies and deployment and to decide whether additional services are needed. In addition, RMON probes should still continue to monitor the network because the traffic characteristics likely will change. A constant look at network traffic will help with changing trends and allow a network administrator to address new network requirements more expeditiously.

10.7 QoS on Ethernet

The LE2425 Switches have the capability to provide QoS at Layer 2. At Layer 2, the frame uses type of service (ToS) as specified in IEEE 802.1p . ToS uses 3 bits, just like IP precedence, and maps well from Layer 2 to layer 3, and vice versa.

The switches have the capability to differentiate frames based on ToS settings. When two queues are present (high or low), frames can be placed in either and serviced via the weight set on all ports. This placement of queues, added to the weight set plus the particular tag setting on a packet allows each queue to have different service levels.

LE2425 QoS implementations provided mapping of ToS (or IP precedence) to CoS (class of service). In this instance, an Ethernet frame CoS setting can be mapped to the ToS byte of the IP packet, and vice versa. A ToS level of 1 equals a CoS level of 1. This provides end-to-end priority for the traffic flow.

10.8 CLI

LE2425 Switches support three types of QoS; Port based, Tag based and ToS based (Layer 3).

10.8.1 To set the QoS type on the switch.

Note: QoS is disabled by default on the switch.
Set QoS <*type*> [*ports*] [*priority*] [*tos*] [*tag*] : Sets the QOS for a particular port. The following types of QOS are supported:

a. Port QOS
b. Tag QOS
c. Tos QOS (Layer 3)
d. None.

Note: Not all packets received on a port have high priority. IGMP and BPDU packets have high priority by default.

10.8.2 Functions of QoS settings:

Port QOS: If we set a port to high priority all the packets received on that port will be assigned high priority regardless of the type of the packet.

TAG QOS: If a packet contains a tag, the port (if tag QoS is enabled) on which the packet was received then looks to see at which level that tag value is set. Regardless of the tag value, if there is a tag, that packet is automatically assigned high priority.

TOS QOS: (Layer 3) When a port is set to TOS QOS, the most significant 6-bits of the IPv4 packet (which has 64 bits) are used. If the 6 bits are set to TOS QOS for the specific port number the packet went to, that packet is assigned high priority by that port.

Syntax: **setqos type=<port|tag|tos|none> [port=<port|list|range>] [priority=<high|low>] [tos=<0-63|list|range>][tag=<0-7|list|range>]**

Depending on the type of QOS, the corresponding field has to be set. For example, for QOS type tag, the tag levels have to be set, and for QOS type ToS, the ToS levels have to be set. If the priority field is not set, it then defaults to low priority. ToS has 64 levels and the valid values are 0-63 and a tagged packet has 8 levels and the valid values are 0-7.

Note: Setting type to none will clear the QOS (***Disable***) for all the ports.

Set port weight: Sets the port priority weight for **All** the ports. Once the weight is set, all the ports will be the same weight across the switch. The valid value for *weight* is 0-7.

Note A weight is a number calculated from the IP precedence setting for a packet in flow. This weight is used in an algorithm to determine when the packet will be serviced.

Weight settings can be viewed using the **show-portweight** command.

As mentioned previously, the switch is capable of detecting higher-priority packets marked with precedence by the IP forwarder and can schedule them faster, providing superior response time for this traffic. The IP Precedence field has values between 0 (the default) and 7. As the precedence value increases, the algorithm allocates more bandwidth to that traffic to make sure that it is served more quickly when congestion occurs. We can assign a weight to each flow, which determines the transmit order for queued packets. In this scheme, lower weights (set on all ports) are provided more service. IP precedence serves as a divisor to this weighting factor. For instance, traffic with an IP Precedence field value of 7 gets a lower weight than traffic with an IP Precedence field value of 3, and thus has priority in the transmit order.

Syntax: **set-weight weight=<0-7>**

One you set the Port weight, the hardware will interpret the weight setting for all ports as outlined below:

Setting	Hardware Interpretation
0 -	1 packet transmitted from HIGH, 1 packet from LOW
1 -	2 packet transmitted from HIGH, 1 packet from LOW
2 -	4 packet transmitted from HIGH, 1 packet from LOW
3 -	6 packet transmitted from HIGH, 1 packet from LOW
4 -	8 packet transmitted from HIGH, 1 packet from LOW
5 -	10 packet transmitted from HIGH, 1 packet from LOW
6 -	12 packet transmitted from HIGH, 1 packet from LOW
7 -	All packets transmitted from HIGH, 0 packets from LOW.

show portweight : Shows the global port priority weight.
Syntax: **show-portweight**

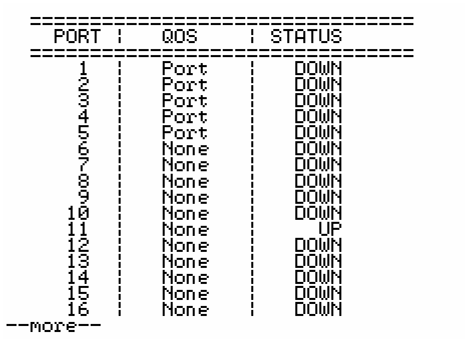
Note: Port weight can be assign only globally (the whole switch has the same setting)

LE2425MNS(qos)##**show-portweight**
Port priority Weight set to 1 High : 1 Low.

Show qos : It shows the QoS information.
Syntax: **show qos [type=<port|tag|tos>] [port=<port|list|range>]**

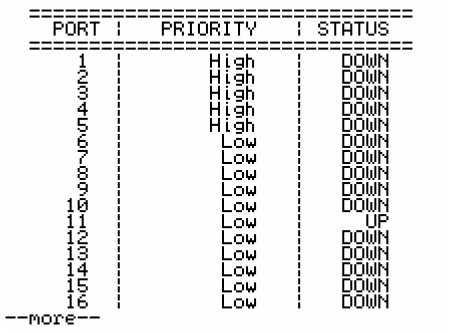
For example,
To set the QoS type as "Port" and set particular ports (1-5) with high priority.
LE2425MNS(qos)##**setqos type=port port=1-5 priority=high**

To see just the QoS status.
LE2425MNS(qos)##**show qos**



```
 ================================
   PORT |    QOS    | STATUS
 ================================
      1 |   Port    |   DOWN
      2 |   Port    |   DOWN
      3 |   Port    |   DOWN
      4 |   Port    |   DOWN
      5 |   Port    |   DOWN
      6 |   None    |   DOWN
      7 |   None    |   DOWN
      8 |   None    |   DOWN
      9 |   None    |   DOWN
     10 |   None    |   DOWN
     11 |   None    |     UP
     12 |   None    |   DOWN
     13 |   None    |   DOWN
     14 |   None    |   DOWN
     15 |   None    |   DOWN
     16 |   None    |   DOWN
--more--
```

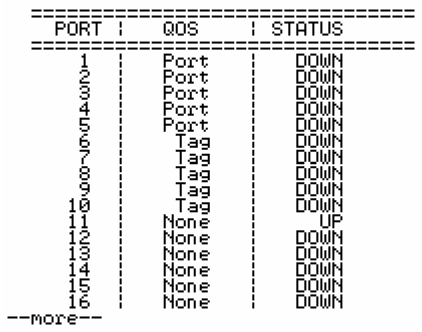
To see the QoS type.
LE2425MNS(qos)##**show qos type=port**



```
 ================================
   PORT |    PRIORITY   | STATUS
 ================================
     1  |        High   |   DOWN
     2  |        High   |   DOWN
     3  |        High   |   DOWN
     4  |        High   |   DOWN
     5  |        High   |   DOWN
     6  |         Low   |   DOWN
     7  |         Low   |   DOWN
     8  |         Low   |   DOWN
     9  |         Low   |   DOWN
    10  |         Low   |   DOWN
    11  |         Low   |     UP
    12  |         Low   |   DOWN
    13  |         Low   |   DOWN
    14  |         Low   |   DOWN
    15  |         Low   |   DOWN
    16  |         Low   |   DOWN
--more--
```

To set QoS type Tag,
This command will set the bits making tag levels 0, 4 and 7 high priority**.**
LE2425MNS(qos)##**setqos type=tag port=6-10 tag=0,4,7 priority=high**

To show the tag level (0-7)
LE2425MNS(qos)##**show qos type=tag**



```
 ================================
   PORT |    QOS    | STATUS
 ================================
     1  |   Port    |   DOWN
     2  |   Port    |   DOWN
     3  |   Port    |   DOWN
     4  |   Port    |   DOWN
     5  |   Port    |   DOWN
     6  |     Tag   |   DOWN
     7  |     Tag   |   DOWN
     8  |     Tag   |   DOWN
     9  |     Tag   |   DOWN
    10  |     Tag   |   DOWN
    11  |   None    |     UP
    12  |   None    |   DOWN
    13  |   None    |   DOWN
    14  |   None    |   DOWN
    15  |   None    |   DOWN
    16  |   None    |   DOWN
--more--
```

Note: The default setting for traffic class is the low priority queue.

All tagged frames will be directed to either the low or high priority queue as specified.

10.9 To tag untagged packets.

When a packet is received untagged and has to be transmitted, with an addition of 802.1Q tag on transmit, then 802.1p priority tag is assigned depending on the untag value set. Hence if you set untag port=1 tag=2 priority=low, untagged packets received on that port will be tagged with a priority low upon transmit.

set-untag : The 802.1p user priority assigned to untagged received packets to be transmitted as tagged from the priority queue 1/0.
Syntax: **set-untag port=<port|list|range> priority=<high|low> tag=<0-7>**

11.0 IGMP

11.1 Overview

In a network where IP multicast traffic is transmitted for various multimedia applications, you can use the switch to reduce unnecessary bandwidth usage on a per-port basis by configuring IGMP (Internet Group Management Protocol controls). In the factory default state (IGMP disabled), the switch forwards all IGMP traffic to all ports, which can cause unnecessary bandwidth usage on ports not belonging to multicast groups. Enabling IGMP allows the ports to detect IGMP queries, report packets and manage IP multicast traffic through the switch.

11.2 Purpose

The purpose of IGMP Snooping is to limit multicast traffic to only those LAN segments that are interested in receiving the messages. In normal switch operations without IGMP, IP multicast traffic is flooded through out the whole LAN. It is flooded because a switch usually learns MAC address by looking in to the source address field of all the frames it receives. However, since a multicast address is never used as a source address for a packet (it has several false addresses which are not unique) and since they do not appear in the MAC address table (because they are not real), the switch has no method for learning them. The most efficient method to weed them out is to use IGMP Snooping. With IGMP Snooping the switch intercepts the IGMP messages (multicast messages only) from the host itself and updates its MAC table accordingly.

IGMP is useful in multimedia applications such as LAN TV, desktop conferencing, and collaborative computing, where there is multipoint communication; that is, communication from one to many hosts, or communication originating from many hosts and destined for many other hosts. In such multipoint applications, IGMP will be configured on the hosts, and multicast traffic will be generated by one or more servers (inside or outside of the local network). Switches in the network (that support IGMP) can then be configured to direct the multicast traffic to only the ports where needed.

Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch. If no other querier is detected, the switch will then also function as the querier. (If you need to disable the querier feature, you can do so through the IGMP configuration MIB. Refer to “Changing the Querier Configuration Setting”)

11.3 IGMP Operating Features

In the factory default configuration, IGMP is disabled. IGMP works only on default VLAN (DEFAULT_VLAN; VID = 1). When you use either the CLI or the Telnet interface to enable IGMP on the switch, the switch forwards IGMP traffic only to ports belonging to multicast groups.

- **Auto/Blocked/Forward:** You can use the console to configure individual ports to any of the following states:

- **Auto** (the default): Causes the switch to interpret IGMP packets and to filter IP multicast traffic based on the IGMP packet information for ports belonging to a multicast group. This means that IGMP traffic will be forwarded on a specific port only if an IGMP host or multicast router is connected to the port.
- **Blocked:** Causes the switch to drop all IGMP transmissions received from a specific port and to block all outgoing IP Multicast packets for that port. This has the effect of preventing IGMP traffic from moving through specific ports.
- **Forward:** Causes the switch to forward all IGMP and IP multicast transmissions through the port.

- **Querier**: In the default state (enabled), eliminates the need for a multicast router. In most cases, Black Box recommends that you leave this parameter in the default “enabled” state even if you have a multicast router performing the querier function in your multicast group.

11.4 Benefit

The IGMP Snooping feature enables the switch to monitor the flow of queries from the router and reports from the host nodes to build its own multicast membership lists. It uses the lists to forward multicast packets only to switch ports where there are host nodes that are members of multicast groups. This improves switch performance and network security by further restricting the flow of multicast packets only to those switch ports connected to host nodes.
Without IGMP Snooping, the switch would flood all multicast packets out all of its ports, except the

port on which it received the packet. Such flooding of packets can negatively impact switch and network performance.

11.5 How IGMP Operates

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, multicast routers, and hosts that support IGMP. (In the LE2425 Switches implementation of IGMP, a multicast router is not necessary as long as a switch is configured to support IGMP with the **querier** feature enabled.) A set of hosts, routers, and/or switches that send or receive multicast data streams to or from the same source(s) is termed a *multicast group*, and all devices in the group use the same multicast group address. The multicast group running version 2 of IGMP uses three fundamental types of messages to communicate:

- **Query:** A message sent from the querier (multicast router or switch) asking for a response from each host belonging to the multicast group. If a multicast router supporting IGMP is not present, then the switch must assume this function in order to elicit group membership information from the hosts on the network. (If you need to disable the querier feature, you can do so through the CLI, using the IGMP configuration MIB. See "Changing the Querier Configuration Setting" on page "Configuring the Querier Function")
- **Report:** A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
- **Leave Group:** A message sent by a host to the querier to indicate that the host has ceased to be a member of a specific multicast group. Thus, IGMP identifies members of a multicast group (within a subnet) and allows IGMP-configured hosts (and routers) to join or leave multicast groups.

11.6 IGMP Data.

To display data showing active group addresses, reports, queries, querier access port, and active group address data (port, type, and access), see "CLI Section".

11.7 Role of the Switch

When IGMP is enabled on the switch, it examines the IGMP packets it receives:

- To learn which of its ports are linked to IGMP hosts and multicast routers/ queriers belonging to any multicast group.
- To become a querier if a multicast router/querier is not discovered on the network.

Once the switch learns the port location of the hosts belonging to any particular multicast group, it can direct group traffic to only those ports, resulting in bandwidth savings on ports where group members do not reside. The following example illustrates this operation.

Figure (below) shows a network running IGMP.

- PCs 1 and 4, switch 2, and all of the routers are members of an IP multicast group. (The routers operate as queriers.)
- Switch 1 ignores IGMP traffic and does not distinguish between IP multicast group members and non-members. Thus, it is sending large amounts of unwanted multicast traffic out the ports to PCs 2 and 3.
- Switch 2 is recognizing IGMP traffic and learns that PC 4 is in the IP multicast group receiving multicast data from the video server (PC X). Switch 2 then sends the multicast data only to the port for PC 4, thus avoiding unwanted multicast traffic on the ports for PCs 5 and 6.

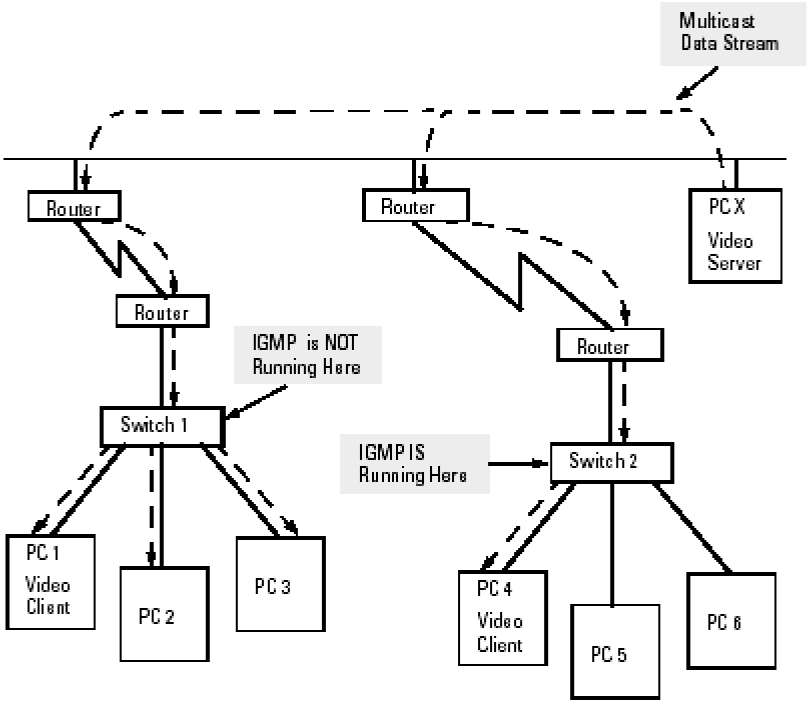


Figure: The Advantage of Using IGMP

The next figure (below) shows a network running IP multicasting using IGMP without a multicast router. In this case, the IGMP-configured switch runs as a querier.
PCs 2, 5, and 6 are members of the same IP multicast group. IGMP is configured on switches 3 and 4. Either of these switches can operate as querier because a multicast router is not present on the network. (If an IGMP switch does not detect a querier, it automatically assumes this role, assuming the querier feature is enabled—the default—within IGMP.)

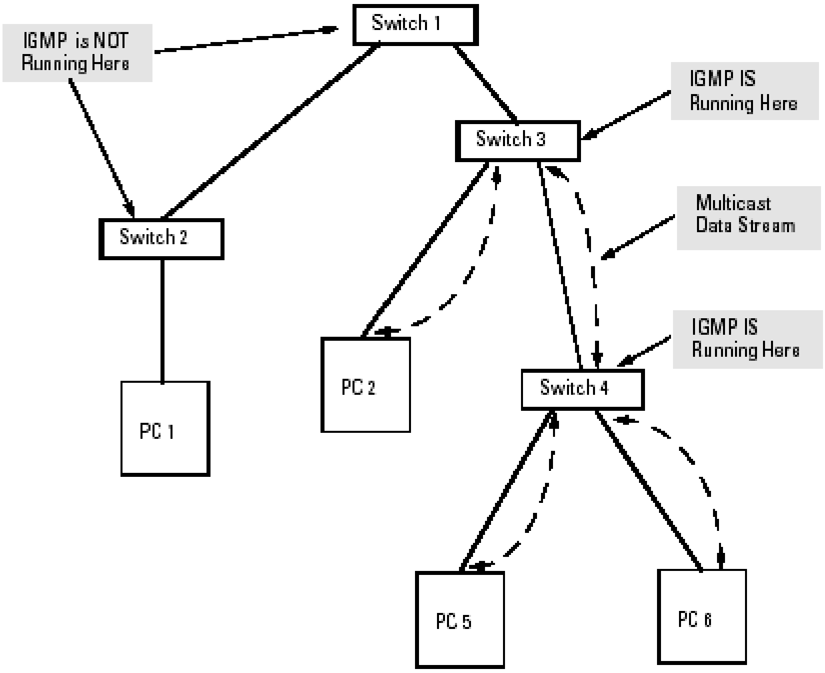


Figure: Isolating IP Multicast Traffic in a Network

- In the above figure, the multicast group traffic does not go to switch 1 and beyond because either the port on switch 3 that connects to switch 1 has been configured as blocked or there are no hosts connected to switch 1 or switch 2 that belong to the multicast group.

- For PC 1 to become a member of the same multicast group without flooding IP multicast traffic on all ports of switches 1 and 2, IGMP must be configured on both switches 1 and 2, and the port on Switch 3 that connects to Switch 1 must be unblocked.

11.8 IP Multicast Filters

IP multicast addresses occur in the range from 224.0.0.0 through 239.255.255.255 (which corresponds to the Ethernet multicast address range of 01005e-000000 through 01005e-7fffff). Devices such as the Magnum Switch 6K having static Traffic/Security filters configured with a "Multicast" filter type and a "Multicast Address" in this range will continue in effect unless IGMP learns of a multicast group destination in this range. In that case, IGMP takes over the filtering function for the multicast destination address(es) for as long as the IGMP group is active. If the IGMP group subsequently deactivates, the static filter resumes control over traffic to the multicast address formerly controlled by IGMP.

11.9 Reserved Addresses Excluded from IP Multicast (IGMP) Filtering.

Traffic to IP multicast groups in the IP address range of 224.0.0.0 to 224.0.0.255 will always be flooded because addresses in this range are "well known" or "reserved" addresses. Thus, if IP Multicast is enabled and there is an IP multicast group within the reserved address range, traffic to that group will be flooded instead of filtered by the switch.

11.10 IGMP Support

LE2425 support IGMP version 1 and version 2. The switch can act either as a querier or a nonquerier. The querier router periodically sends general query messages to solicit group membership information. Hosts on the network that are members of a multicast group send report messages. When a host leaves a group, it sends a leave group message. The difference between Version 1 and Version 2 is that version 1 does not have a "Leave" mechanism for the host.

LE2425 does pruning when there is a leave message or a time expires on a port, we prune the multicast group membership on that port.

The LE2425 supports only the default VLAN. It can be enabled within a port VLAN, tagged VLAN, or no VLAN. It can snoop up to 256 Multicast Groups.

11.11 CLI

11.11.1 Enable/disable IGMP

Syntax: **igmp <enable/disable>**
Note: By default IGMP is disable.

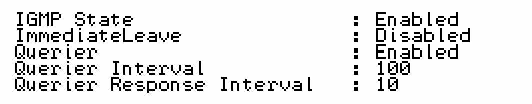
To enable and disable IGMP in the switch, first go to IGMP context using the command "igmp" or "configure igmp".

```
LE2425MNS##igmp

LE2425MNS(igmp)##igmp disable

 IGMP is disabled

LE2425MNS(igmp)##igmp enable

IGMP is enabled
```

11.11.2 Showing IGMP Configuration

To show current IGMP operation, use the command "show igmp" available globally in the command line. For example:

LE2425MNS#**show igmp**



```
IGMP State                  : Enabled
ImmediateLeave              : Disabled
Querier                     : Enabled
Querier Interval            : 100
Querier Response Interval   : 10
```

IGMP State shows if IGMP is turned on (Enable) or off (Disable).

Immediate Leave provides a mechanism for a particular host that wants to leave a multicast group. It disables the port (where the leave message is received) ability to transmit multicast traffic.

Querier shows where the switch is acting a querier or a non-querier.

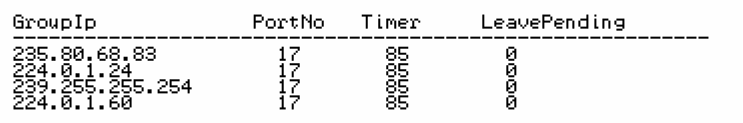
Querier interval shows the time period in seconds on which the switch sends general host-query messages.

Querier response interval specifies maximum amount of time in seconds that can elapse between when the querier sends a host-query message and when it receives a response from a host.

11.11.3 Showing Snooped Multicast Groups

Using the command "show-group" in IGMP command context will show the multicast groups being snooped. For example:

LE2425MNS(igmp)##**show-group**



```
GroupIp              PortNo   Timer     LeavePending
--------------------------------------------------------
235.80.68.83           17       85        0
224.0.1.24             17       85        0
239.255.255.254        17       85        0
224.0.1.60             17       85        0
```

The *GroupIp* column shows the multicast groups. *PortNo* shows the port where the multicast group is being detected. *Timer* shows the amount of time left in seconds before the group port will be deleted (will not be able to route multicast traffic) if the switch does not receive a membership report. *Leave pending* column shows the number of leave messages received from this port.

11.11.4 Showing Detected Router Ports

To view detected IGMP-enabled router ports, use the command "show-router" in the IGMP command context. For example:

LE2425MNS(igmp)##**show-router**

```
RouterIp        PortNo   Timer
-------------------------------------
10.21.1.250        9        25
```

11.11.5 Enable/Disable Immediate Leave Processing

To enable or disable the switch to immediately process a host sending a leave message rather that wait for the timer to expire, use the command "set-leave" in the IGMP command context.

Syntax: **set-leave <enable|disable>**

LE2425MNS(igmp)##**set-leave enable**

IGMP immediate leave status is enabled

```
LE2425MNS(igmp)##show igmp

 IGMP State                   : Enabled
 ImmediateLeave               : Enabled
 Querier                      : Enabled
 Querier Interval             : 125
 Querier Response Interval : 10

LE2425MNS(igmp)##set-leave disable
IGMP immediate leave status is disabled

LE2425MNS(igmp)##show igmp

 IGMP State                    : Enabled
 ImmediateLeave                : Disabled
 Querier                       : Enabled
 Querier Interval              : 125
 Querier Response Interval  : 10
```

11.11.6 Enable/Disable Switch as Querier

To enable or disable a switch as IGMP querier, use the command “set-querier” in the IGMP command context.

Syntax: **set-querier <enable|disable>**

```
LE2425MNS(igmp)##set-querier enable
 IGMP querier status is enabled

LE2425MNS(igmp)##show igmp

IGMP State                    : Enabled
ImmediateLeave              : Disabled
Querier                : Enabled
Querier Interval              : 125
Querier Response Interval : 10

LE2425MNS(igmp)##set-querier disable
IGMP querier status is disabled

LE2425MNS(igmp)##show igmp

 IGMP State                   : Enabled
 ImmediateLeave               : Disabled
 Querier                      : Disabled
 Querier Interval             : 125
 Querier Response Interval : 10
```

11.12 Setting the Host Membership Query Interval

The IGMP querier router periodically sends general host-query messages. These messages are sent to ask for group membership information. This is sent to the all-system multicast group address, `224.0.0.1`.

Note: The default value is 125 seconds. The valid range can be from 60 to 127 seconds.
To set the value, use the command “set-qi” in the IGMP command context.

Syntax: **set-qi interval=<value>**

```
LE2425MNS(igmp)##set-qi interval=127

Query interval successfully set
```

```
LE2425MNS(igmp)##show igmp

IGMP State                   : Enabled
ImmediateLeave               : Disabled
Querier                      : Disabled
Querier Interval             : 127
Querier Response Interval    : 10
```

11.13 Setting the Query Response Interval

The query response interval is the maximum amount of time that can elapse between when the querier router sends a host-query message and when it receives a response from a host.
Note: The Default value is 10 seconds. The Range can be from 2 to 270 seconds. Restrictions apply to the maximum value because of an internal calculation that is dependent on the value of the Query Interval.
Syntax: **set-qri interval=<value>**

```
LE2425MNS(igmp)##set-qri interval=11
Query response interval successfully set

LE2425MNS(igmp)##show igmp

IGMP State                   : Enabled
ImmediateLeave             : Disabled
Querier                      : Disabled
Querier Interval             : 125
Querier Response Interval   : 11
```

Every port can be individually set to three different IGMP modes (please see section “Showing IGMP Port Mode”). To set port mode, you use the command “set-port” in the IGMP command context.

User can use the console to configure individual ports to any of the following states:
Auto/Blocked/Forward (As described above in IGMP Operating Features).

- Auto – lets IGMP control whether the port should or should not participate sending multicast traffic
- Block – manually configures the port to always block multicast traffic
- Forward – manually configures the port to always forward multicast traffic

11.14 Configure IGMP Port Mode

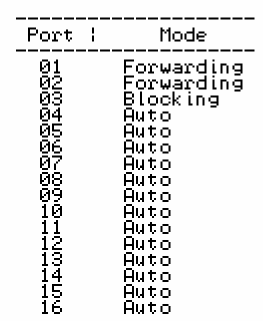
Syntax: **set-port port=< port|list|range>> mode=<auto|forward|block>**

```
LE2425MNS(igmp)##set-port port=1-2 mode=forward
Port mode is set.
```

11.14.1 Showing Port Configuration

To view the current setting of Ports in respect of IGMP.
Syntax: **show-port**

```
LE2425MNS(igmp)## show-port
```



```
--------------------
 Port |     Mode
--------------------
   01     Forwarding
   02     Forwarding
   03     Blocking
   04     Auto
   05     Auto
   06     Auto
   07     Auto
   08     Auto
   09     Auto
   10     Auto
   11     Auto
   12     Auto
   13     Auto
   14     Auto
   15     Auto
   16     Auto
```

Note: The default mode is **Auto**.

12.0 Spanning Tree Protocol (STP)

12.1 STP Features

The switch uses the IEEE 802.1D Spanning Tree Protocol (STP). When this STP is enabled, it ensures that only one path at a time is active between any two nodes on the network. In networks where more than one physical path exists between two nodes, STP ensures only a single path is active by blocking all redundant paths. Enabling STP is necessary in such networks because having more than one path between a pair of nodes causes loops in the network which can result in duplication of messages. This duplication leads to a " broadcast storm" that can bring down the network.

Note: You should enable STP in any switch that is part of a redundant physical link (loop topology). (It is recommended that you enable STP on all switches belonging to a loop topology.)

As recommended in the IEEE 802.1Q VLAN standard, the Magnum Switches use **single-instance STP**. This means a single spanning tree is created to make sure there are no network loops associated with any of the connections to the switch. This works regardless of whether VLANs are configured on the switch. Thus, these switches do not distinguish between VLANs when identifying redundant physical links.

12.2 Feature Default

enable/disable STP disabled

reconfiguring general operation priority: 32768

max age: 20 s

hello time: 2 s

fwd. delay: 15 s

reconfiguring per-port STP path cost: var

priority: 128

mode: norm

monitoring STP n/a

In the factory default configuration, STP is off. If a redundant link (loop) exists between nodes in your network, you should enable Spanning Tree.

Note STP retains its current parameter settings when disabled. Thus, if you disable STP, then later re-enable it, the parameter settings will be the same as before STP was disabled.

Caution Because the switch automatically gives faster links a higher priority, the default STP parameter settings are usually adequate for spanning tree operation. Also because incorrect STP settings can adversely affect network performance, you should not make changes unless you have a strong understanding of how STP operates. For more on STP, see the IEEE 802.1D standard.

12.3 Viewing the Current STP Configuration.

Regardless of whether STP is disabled (the default), this command lists the switch's full STP configuration, including general settings and port settings.

Syntax: **show stp <config | port | age>**

```
LE2425MNS# show stp config
STP Bridge Configuration:
```

In the default configuration, STP appears as shown here

```
Spanning Tree Enabled(Global)     :NO
Spanning Tree Enabled(Ports)      :YES, 9,10,11,12,13,14,15,16,17,18,19,20,21,22
Bridge Priority                   :32768
Bridge Forward Delay              :15
Bridge Hello Time                 :2
Bridge Max Age                    :20
Root Port                         :0
Root Path Cost                    :0
Designated Root                   :80:00:00:20:06:25:00:11
Designated Root Priority          :32768
Root Bridge Forward Delay         :15
Root Bridge Hello Time            :2
Root Bridge Max Age               :20
```

12.3.1 Explaining Parameters in Detail

The following parameters are explained in detail.

Spanning Tree Enabled(Global): This field indicates whether STP is enabled or disabled globally i.e. if the values is YES, all ports have STP enabled, otherwise, all ports have STP disabled.

Spanning Tree Enabled(Ports): This field indicates which ports have STP enabled.

Bridge Priority: This field specifies the switch (bridge) priority value which is used along with the switch MAC address to determine the root device. Lower values mean higher priority. Value ranges from 0 to 65535. Default value is 32768.

Bridge Forward Delay: This field indicates the time duration the switch will wait from listening to learning states and from learning to forwarding states. The value ranges from 4 to 30 seconds. Default value is 15.

Bridge Hello Time: When the switch is the root device, this is the time between messages being transmitted. The value is from 1 to 10 seconds. Default value is 2 seconds.

Bridge Max Age: This is the maximum age a received message with STP information is allowed by the switch before the switch checks all messages and updates the address table again. Value ranges from 6 to 40 seconds with default value of 20 seconds.

Root Port: This field indicates the port number, which is elected as the root port of the switch.

Root Path Cost: This field indicates the root ports path cost. A path cost is assigned to individual ports for the switch to determine which ports are the forwarding points. A higher cost means more loops, a lower cost means fewer loops. More loops equal more traffic and a slower system.

Designated Root: This field shows the MAC address of the bridge in the network elected or designated as the root bridge.

Designated Root Priority: This field shows the designated root bridge’s priority.

Root Bridge Forward Delay: This field indicates the designated root bridge’s forward delay. This is the time the switch waits from the listening to the forwarding state. The default is 15 seconds. Can be set between 4-30 seconds.

Root Bridge Hello Time: This field indicates the designated root bridge’s hello time.

Root Bridge Max Age: This field indicates the designated root bridge’s Max Age.

12.3.2 Showing STP Configuration by Port

To show STP configuration by ports, an example shows below

```
LE2425MNS#show stp ports

STP Port Configuration:
-----------------------------------------------------------------------------------------
Port#  Type     Priority  Path Cost    State    Des. Bridge           Des. Port
-----------------------------------------------------------------------------------------
01   TP(10/100)  128      100  Forwarding  80:00:00:20:06:25:00:62  80:01
02   TP(10/100)  128      100  Disabled  80:00:00:20:06:25:00:62  80:02
03   TP(10/100)  128      100  Disabled  80:00:00:20:06:25:00:62  80:03
04   TP(10/100)  128      100  Disabled  80:00:00:20:06:25:00:62  80:04
05   TP(10/100)  128      100  Forwarding  80:00:00:20:06:25:00:62  80:05
06   TP(10/100)  128      100  Disabled  80:00:00:20:06:25:00:62  80:06
07   TP(10/100)  128      100  Forwarding  80:00:00:20:06:25:00:62  80:07
08   TP(10/100)  128      100  Disabled  80:00:00:20:06:25:00:62  80:08
```

The command above outputs the result in tabular format. The explanation of each column in the table is shown below:

Port#: This field indicates the port number. Value ranges from 01 to max number of ports in the switch.

Type: This field indicates the type of port.

Priority: STP uses this to determine which ports are used for forwarding. Lower the number means higher priority. Value ranges from 0 to 255. Default is 128.

Path Cost: This is the assigned port cost value used for the switch to determine the forwarding points. Values range from 1 to 65535.

State: This indicates the STP state of individual ports. Values can be Listening, Learning, Forwarding, Blocking and Disabled.

Des. Bridge: This is the port's designated root bridge.

Des. Port: This is the port's designated root port.

12.4 Enabling or Disabling STP.

Enabling STP implements the spanning-tree protocol for all physical ports on the switch, regardless of whether multiple VLANs are configured. Disabling STP removes protection against redundant loops that can significantly slow or halt a network.

Syntax: stp <enable|disable>
Default: Disabled
This command enables STP with the current parameter settings or disables STP without losing the most recently configured parameter settings. (To learn how the switch handles parameter changes, how to test changes without losing the previous settings, and how to replace previous settings with new settings, see appendix C, " Switch Memory and Configuration".) When
enabling STP, you can also include the STP general and per-port parameters described in the next two sections. When you use the "no" form of the command, you can do so only to disable STP. (STP parameter settings are not changed when you disable STP, and cannot be included with the no spanning-tree command.

Caution Because incorrect STP settings can adversely affect network performance, Black Box recommends that you use the default STP parameter settings. You should not change these settings unless you have a strong understanding of how STP operates. For more on STP, see the IEEE 802.1D standard.

```
LE2425MNS(stp)# stp  enable
```

12.5 Reconfiguring General STP Operation on the Switch.

This command enables STP (if it is not already enabled) and configures one or more of the following parameters:

General STP Operating Parameters

Name	Default	Range	Function
priority	32768	0 - 65535	Specifies the priority value used along with the switch MAC address to determine which device is root. The lower a priority value, the higher the priority.
maximum-age	20 seconds	6 – 40 sec	Maximum received message age the switch allows for STP info before discarding messages and receiving new messages.
hello-time	2 seconds	1 - 10 sec	Time between message transmission when switch is the root.
forward-delay	15 seconds	4 – 30 sec	Time the switch waits before transitioning from the listening to the learning state, and between the learning state to the forwarding state.

Syntax to set the above-mentioned parameters:

```
priority port=<number|list|range> value=<0-255 / 0-65535>
cost port=<number|list|range> value=<0-65535>
time forward-delay=<4-30> hello=<1-10> age=<6-40>
```

Default: See table above.

For example, to enable STP with a maximum-age of 30 seconds and a hello-time of 3 seconds with forward delay of 15 secs:

```
LE2425MNS(stp)# time forward-delay=15 hello= 3 age= 30
```

12.6 Globally Enabling or Disabling STP

To globally enable or disable STP on the switch, one must be in the STP context in CLI. The following command sequence shows enabling and disabling STP globally.

```
LE2425MNS(stp)##show stp config
STP Configuration:
Spanning Tree Enabled(Global)      :NO
Spanning Tree Enabled(Ports)       :YES, 1,2,3,4,5,6,7,8
Bridge Priority                    :32768
Bridge Forward Delay               :15
Bridge Hello Time                  :2
Bridge Max Age                     :20
Root Port                          :1
Root Path Cost                     :100
Designated Root                    :80:00:00:01:96:ed:a7:80
Designated Root Priority           :32768
Root Bridge Forward Delay          :15
Root Bridge Hello Time             :2
Root Bridge Max Age                :20
```

```
LE2425MNS(stp)##stp enable
Successfully set the STP status

LE2425MNS(stp)##show stp config

STP Configuration:
Spanning Tree Enabled(Global)      :YES
Spanning Tree Enabled(Ports)       :YES, 1,2,3,4,5,6,7,8
Bridge Priority                    :32768
Bridge Forward Delay               :15
Bridge Hello Time                  :2
Bridge Max Age                     :20
Root Port                          :1
Root Path Cost                     :100
Designated Root                    :80:00:00:01:96:ed:a7:80
Designated Root Priority           :32768
Root Bridge Forward Delay          :15
Root Bridge Hello Time             :2
Root Bridge Max Age                :20
```

To disable STP, just issue the command *stp disable* under the STP CLI context.

To enable/disable STP by ports, the *port port=<number|list|range> status=<enable/disable>* is used. An example shows below.

```
LE2425MNS(stp)##show stp config
STP Configuration:
Spanning Tree Enabled(Global)      :YES
Spanning Tree Enabled(Ports)       :NO
Bridge Priority                    :32768
Bridge Forward Delay               :15
Bridge Hello Time                  :2
Bridge Max Age                     :20
Root Port                          :0
Root Path Cost                     :0
Designated Root                    :80:00:00:20:06:25:00:62
Designated Root Priority           :32768
Root Bridge Forward Delay          :15
Root Bridge Hello Time             :2
Root Bridge Max Age                :20


LE2425MNS(stp)##port port=1-8 status=enable
Successfully set the STP status for port 1
Successfully set the STP status for port 2
Successfully set the STP status for port 3
Successfully set the STP status for port 4
Successfully set the STP status for port 5
Successfully set the STP status for port 6
Successfully set the STP status for port 7
Successfully set the STP status for port 8

LE2425MNS(stp)##show stp config

STP Configuration:
Spanning Tree Enabled(Global)      :YES
Spanning Tree Enabled(Ports)       :YES, 1,2,3,4,5,6,7,8
Bridge Priority                    :32768
Bridge Forward Delay               :15
Bridge Hello Time                  :2
Bridge Max Age                     :20
```

```
Root Port                       :1
Root Path Cost                  :100
Designated Root                 :80:00:00:01:96:ed:a7:80
Designated Root Priority        :32768
Root Bridge Forward Delay       :15
Root Bridge Hello Time          :2
Root Bridge Max Age             :20
```

12.7 Changing STP Bridge Parameter Values

To change bridge priority parameters, the user must be in STP CLI context. Using the command *priority value=<0-65535>*.

```
LE2425MNS#stp

LE2425MNS(stp)##show stp config

STP Configuration:

Spanning Tree Enabled(Global)   :YES
Spanning Tree Enabled(Ports)    :YES, 1,2,3,4,5,6,7,8
Bridge Priority                 :32768
Bridge Forward Delay            :15
Bridge Hello Time               :2
Bridge Max Age                  :20
Root Port                       :1
Root Path Cost                  :100
Designated Root                 :80:00:00:01:96:ed:a7:80
Designated Root Priority        :32768
Root Bridge Forward Delay       :15
Root Bridge Hello Time          :2
Root Bridge Max Age             :20
LE2425MNS(stp)##priority value=65535

Successfully set the bridge priority
```

To change bridge STP timing parameters, use the command *time forward-delay=<4-30> hello=<1-10> age=<6-40>*.

```
LE2425MNS(stp)##time forward-delay=4 hello=1 age=6
Successfully set the bridge time parameters

LE2425MNS(stp)##show stp config

STP Configuration:
Spanning Tree Enabled(Global)   :YES
Spanning Tree Enabled(Ports)    :YES, 1,2,3,4,5,6,7,8
Bridge Priority                 :65535
Bridge Forward Delay            :4
Bridge Hello Time               :1
Bridge Max Age                  :6
Root Port                       :1
Root Path Cost                  :100
Designated Root                 :80:00:00:01:96:ed:a7:80
Designated Root Priority        :32768
Root Bridge Forward Delay       :15
Root Bridge Hello Time          :2
Root Bridge Max Age             :20
```

12.8 Changing STP Port Parameter Values

To change the STP port priority, use the command *priority port=<number|list|range> value=<0-255>* under the STP CLI context.

```
LE2425MNS(stp)##show stp ports

STP Port Configuration:
---------------------------------------------------------------------------
Port#  Type      Priority  Path Cost   State    Des. Bridge          Des. Port
---------------------------------------------------------------------------
01    TP(10/100)  128      100  Forwarding  80:00:00:01:96:ed:a7:80  80:20
02    TP(10/100)  128      100  Disabled  ff:ff:00:20:06:25:00:62  80:02
03    TP(10/100)  128      100  Disabled  ff:ff:00:20:06:25:00:62  80:03
04    TP(10/100)  128      100  Disabled  ff:ff:00:20:06:25:00:62  80:04
05    TP(10/100)  128       19  Forwarding  ff:ff:00:20:06:25:00:62  80:05
06    TP(10/100)  128      100  Disabled  ff:ff:00:20:06:25:00:62  80:06
07    TP(10/100)  128       19  Forwarding  ff:ff:00:20:06:25:00:62  80:07
08    TP(10/100)  128      100  Disabled  ff:ff:00:20:06:25:00:62  80:08

LE2425MNS(stp)##priority port=01 value=50
Successfully set the priority for port 1
```

To change STP port cost, use the command, use the *cost port=<number|list|range> value=<0-65535>* .

```
LE2425MNS(stp)##cost port=1 value=200
Successfully set the path cost for port 1

LE2425MNS(stp)##show stp ports

STP Port Configuration:
---------------------------------------------------------------------------
Port#  Type      Priority  Path Cost   State    Des. Bridge          Des. Port
---------------------------------------------------------------------------
01    TP(10/100)   50     200  Forwarding  80:00:00:01:96:ed:a7:80  80:20
02    TP(10/100)  128      100  Disabled  ff:ff:00:20:06:25:00:62  80:02
03    TP(10/100)  128      100  Disabled  ff:ff:00:20:06:25:00:62  80:03
04    TP(10/100)  128      100  Disabled  ff:ff:00:20:06:25:00:62  80:04
05    TP(10/100)  128       19  Forwarding  ff:ff:00:20:06:25:00:62  80:05
06    TP(10/100)  128      100  Disabled  ff:ff:00:20:06:25:00:62  80:06
07    TP(10/100)  128       19  Forwarding  ff:ff:00:20:06:25:00:62  80:07
08    TP(10/100)  128      100  Disabled  ff:ff:00:20:06:25:00:62  80:08
```

12.9 How STP Operates

The switch automatically senses port identity and type, and automatically defines port cost and priority for each type. The console interface allows you to adjust the Cost and Priority for each port. It also allows you to adjust the mode for each port and the global STP parameter values for the switch.
While allowing only one active path through a network at any time, STP retains any redundant physical path to serve as a backup (blocked) path in case the existing active path fails. Thus, if an active path fails, STP automatically activates (unblocks) an available backup to serve as the new active path for as long as the original active path is down.

13.0 Port-Based Virtual LANs (Static VLANs)

A VLAN is a group of ports designated by the switch as belonging to the same broadcast domain. (That is, all ports carrying traffic for a particular subnet address would normally belong to the same VLAN.)
Note This section describes *static* VLANs, which are VLANs you manually configure with a name, VLAN ID (VID), and port assignments. Using a VLAN, you can group users by logical function instead of physical location. This helps to control bandwidth usage by allowing you to group high-bandwidth users on low-traffic segments and to organize users from different LAN segments according to their need for common resources.

By default, the Series 6K switches are VLAN (Port based) enabled and allow up to 32 port-based VLANs. The port-based nature of the configuration allows interoperation with older switches that require a separate port for each VLAN.

13.1 General Use and Operation.

Port-based VLANs are typically used to enable broadcast traffic reduction and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs that may be configured on a switch. Packets are forwarded only between ports that are designated for the same VLAN. Thus, all ports carrying traffic for a particular subnet address should be configured to the same VLAN. Cross-domain broadcast traffic in the switch is eliminated and bandwidth is saved by not allowing packets to flood out all ports. An external router is required to enable separate VLANs on a switch to communicate with each other.

13.2 VLAN Support and the Default VLAN

In the factory default configuration, VLAN support is enabled and all ports on the switch belong to the default VLAN (named DEFAULT-VLAN). This places all ports in the switch into one physical broadcast domain.
You can partition the switch into multiple virtual broadcast domains by adding one or more additional VLANs and moving ports from the default VLAN to the new VLANs. (The switch supports up to 32 VLANs.) You can change the name of the default VLAN, but you cannot change the default VLAN's VID (which is always " 1"). Although you can remove all ports from the default VLAN, this VLAN is always present.

To display the current VLAN, use the CLI **show vlan** command.
Syntax: **show vlan type=port**

13.3 General Steps for Using VLANs

1.Plan your VLAN strategy and create a map of the logical topology that will result from configuring VLANs. Include consideration for the interaction between VLANs .

2. Configure at least one VLAN in addition to the default VLAN.

3. Assign the desired switch ports to the new VLAN(s).

Notes on Using VLANs

- You can rename the default VLAN, but you cannot change its VID (1) or delete it from the switch.
- Any ports *not* specifically assigned to another VLAN will remain assigned to the DEFAULT-VLAN.
- Changing the number of VLANs supported on the switch requires the SAVE command.

13.4 CLI: Configuring VLAN Parameters

In the factory default state, all ports on the switch belong to the default VLAN (DEFAULT-VLAN) and are in the same broadcast/multicast domain. You can configure up to 31 additional static VLANs by adding new VLAN names, and then assigning one or more ports to each VLAN.
(The switch accepts a maximum of 32 VLANs, including the default VLAN).
NOTE: LE2425 support one type of VLAN at a time. The user has to set the VLAN type before configuration.

Steps:

To set the type of Vlan that you are going to use.

Syntax: **set vlan type=<port|tag|mac|none>**

Go to Configuration mode

Syntax: **configure vlan type=port OR vlan type=port**

Add VLAN

Syntax: **add id=<vlan Id> [name=<vlan name>] port=<number|list|range>**

Start Vlan

Syntax: **start vlan=<name|number|list|range>**

Save the configuration

Syntax: **save**

13.4.1 Displaying the Switch's VLAN Configuration.

The next command lists the VLANs currently running in the switch, with VID, VLAN name, and VLAN status.

LE2425MNS# **show vlan type=port**

```
VLAN ID    :  1
Name       :  Default VLAN
Status     :  Active

=========================
 PORT |     STATUS
=========================
    1 |       DOWN
    2 |       DOWN
    3 |       DOWN
    4 |       DOWN
    5 |       DOWN
    6 |       DOWN
    7 |       DOWN
    8 |       DOWN
   25 |       DOWN

VLAN ID    :  2
Name       :  Engg
Status     :  Active

=========================
 PORT |     STATUS
=========================
    9 |        UP
   10 |       DOWN
   11 |       DOWN
   12 |       DOWN
   13 |       DOWN
   14 |       DOWN
   15 |       DOWN
   16 |       DOWN
   17 |       DOWN
   18 |       DOWN


VLAN ID    :  3
Name       :  Mktg
Status     :  Active

=========================
 PORT |     STATUS
=========================
   18 |       DOWN
   19 |       DOWN
   20 |       DOWN
   21 |       DOWN
   22 |       DOWN
   23 |       DOWN
   24 |       DOWN
```

13.4.2 Displaying the Configuration for a Particular VLAN

This command uses the VID to identify and display the data for a specific static VLAN.
Syntax: **show vlan type=port [<id=vlanid>]**
LE2425MNS# **show vlan type=port id=2**

```
VLAN ID    :  2
Name       :  Engg
Status      :  Active

========================
  PORT |     STATUS
========================
     9 |        UP
    10 |      DOWN
    11 |      DOWN
    12 |      DOWN
    13 |      DOWN
    14 |      DOWN
    15 |      DOWN
    16 |      DOWN
    17 |      DOWN
    18 |      DOWN
```

13.5 Creating a New Static VLAN

13.5.1 Changing the VLAN Context Level.

With this command, entering a new VID creates a new static VLAN. Entering the VID or name of an existing static VLAN places you in the context level for that VLAN.

Syntax: **add id=<vlan Id> [name=<vlan name>] port=<number|list|range>**

This command creates a new static VLAN (if a VLAN with that VID does not already exist) and places you in that VLAN's context level. If you do not use the name option, the switch uses " VLAN" and the new VID to automatically name the VLAN. If the VLAN already exists, the switch places you in the context level for that VLAN.
For example, to create a new static VLAN with a VID of 32:
LE2425MNS(vlan-port)## **add id=32 name=Fin port=10,11,12**
Port vlan added successfully

LE2425MNS# **show vlan type=port id=32**

```
VLAN ID    :  32
Name       :  Fin
Status      :  Pending

========================
  PORT |     STATUS
========================
    10 |      DOWN
    11 |      DOWN
    12 |      DOWN
```

To enable the new VLAN type the following:
LE2425MNS(vlan-port)## **start vlan =<ID or port list>**
For example, LE2425MNS(vlan-port)## **start vlan = 32**
Resulting,

```
VLAN ID    :  32
Name       :  Fin
Status      :  Active

========================
  PORT |     STATUS
========================
    10 |      DOWN
    11 |      DOWN
    12 |      DOWN
```

13.6 Effect of VLANs on Other Switch Features

13.6.1 VLAN Restrictions

- A port must be a member of at least one VLAN. In the factory default configuration, all ports are assigned to the default VLAN (DEFAULT-VLAN; VID = 1).
- Before you can delete a VLAN, you can optionally re-assign all ports in the VLAN to another VLAN. Ports that are members of other VLANs will retain these memberships while all other ports will fall back into the default VLAN.
- The LE2425 switches support port based VLANs. Each port is configured to be member of one or more VLANs. A port can communicate with another port only if both the ports share membership in the same VLAN. A specific port can be a member of more than one VLAN.
- The LE2425 Switches Port Based VLAN operates by restricting broadcast traffic between the ports. When a packet with a broadcast address or with an unknown destination address, it is forwarded only to ports that share VLAN membership with the source port. Un necessary repeating of broadcast packets is thus avoided, conserving bandwidth. Packets destined to known addresses are forwarded normally.

  Note: Since the higher-level network protocols rely upon broadcasts to discover network addresses of other stations, normal communication will not be possible between ports with no common VLAN membership. However, it is sometimes possible to send a frame to another port if the destination address is known. This happens since the switching hardware filters packets that are to be broadcast.

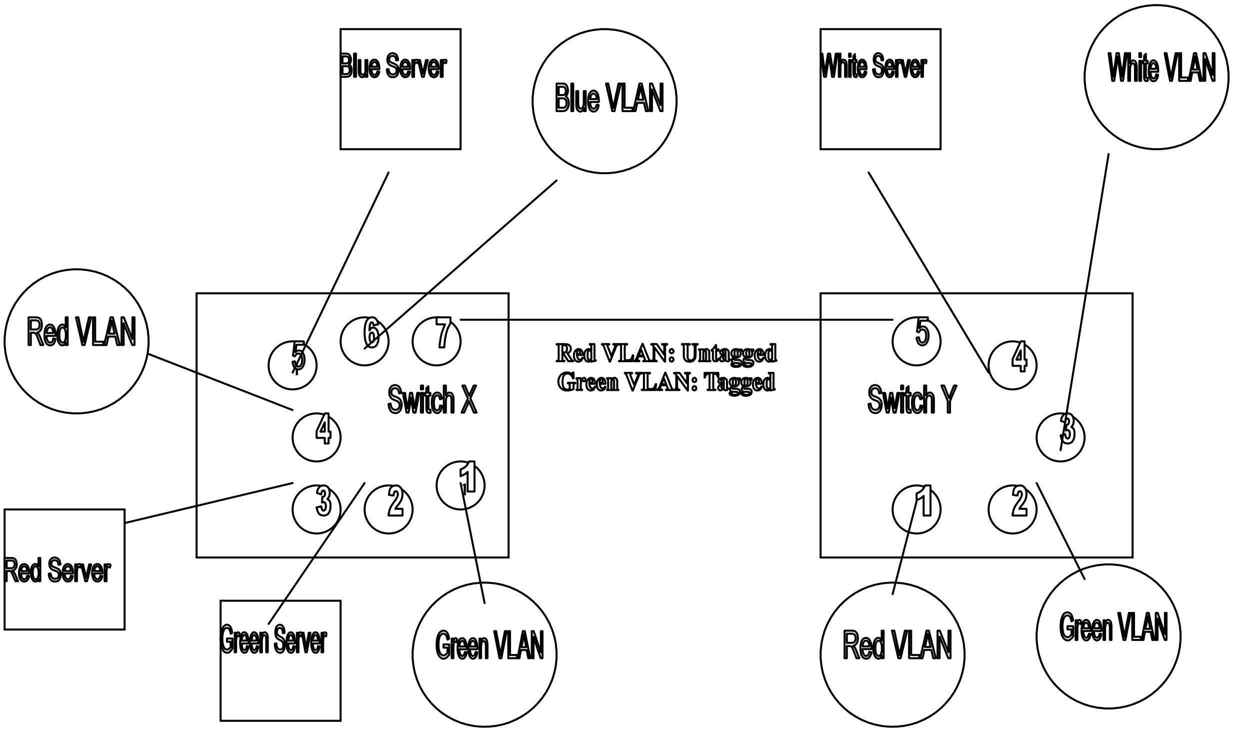
14.0 TAG Based VLAN

14.1 Introduction

TAG based VLANs are used to filter packets arriving at a particular port or set of ports. The filtering is based on the TAG information contained in the packet. Hence, we can drop or allow through packets arriving on a set of ports based on the source TAG information contained in the packets.

14.2 VLAN Tagging Information

VLAN tagging enables traffic from more than one VLAN to use the same port. (Even when two or more VLANs use the same port they remain as separate domains and cannot receive traffic from each other without going through an external router.) As mentioned earlier, a "tag" is simply a unique VLAN identification number (VLAN ID, or VID) assigned to a VLAN at the time that you configure the VLAN name in the switch. In the LE2425 switches, the tag can be any number from 1 to 4095 that is not already assigned to a VLAN. When you subsequently assign a port to a given VLAN, you must implement the VLAN tag (VID) if the port will carry traffic for more than one VLAN. Otherwise, the port VLAN assignment can remain "untagged" because the tag is not needed. On a given switch, this means you should use the "Untagged" designation for a port VLAN assignment where the port is connected to a non 802.1Q-compliant device or is assigned to only one VLAN. Use the "Tagged" designation on at least one of the VLAN's when the port is assigned to more than one VLAN or the port is connected to a device that *does* comply with the 802.1Q standard.



Ports 1-6: Untagged
Port 7: Red VLAN Untagged
Ports 1-4: Untagged

Green VLAN Tagged
Port 5: Red VLAN Untagged

Example of Tagged and Untagged VLAN Port Assignments

For example, if port 7 on an 802.1Q-compliant switch is assigned to only the Red VLAN, the assignment can remain "untagged" because the port will forward traffic only for the Red VLAN. However, if both the Red and Green VLANs are assigned to port 7, then at least one of those VLAN assignments must be "tagged" so that Red VLAN traffic can be distinguished from Green VLAN traffic. The above illustration shows this concept.

- ➢ In switch X:
- Suppose the ports X1 - X6 each only have one VLAN per port. The VLANs assigned can all be untagged. Red VLAN traffic will go out only the Red ports; Green VLAN traffic will go out only the

Green ports, and so on. Devices connected to these ports do not have to be 802.1Qcompliant.

- However, if both the Red VLAN and the Green VLAN are assigned to port X7, at least one of the VLANs must be tagged for this port.

➢ In switch Y:

- VLANs assigned to ports Y1 - Y4 can all be untagged if there is only one VLAN assignment per port. Devices connected to these single VLAN ports do not have to be 802.1Q-compliant.
- If both the Red VLAN and the Green VLAN are assigned to port Y5, at least one of the VLANs must be tagged for this port. In both switches: The ports on the link between the two switches must be configured the same. Referring to figure 9-54 (above), the Red VLAN can be untagged on port X7 and Y5 and the Green VLAN can be tagged on port X7 and Y5, or vice-versa if the Red and Green VLAN's are both on the link.

Note Each 802.1Q-compliant VLAN must have its own unique VID number, and that VLAN *must* be given the same VID in every device in which it is configured. That is, if the Red VLAN has a VID of 10 in switch X, then 10 must also be used for the Red VID in switch Y.

VLAN tagging gives you several options:

- Since the purpose of VLAN tagging is to allow multiple VLANs on the same port, any port that has only one VLAN assigned to it can be configured as "Untagged" (the default).
- Any port that has two or more VLANs assigned to it can have one VLAN assignment for that port as "Untagged". All other VLANs assigned to the same port must be configured as "Tagged". (There can be no more than one Untagged VLAN on a port.)
- If all end nodes on a port comply with the 802.1Q standard and are configured to use the correct VID, then, you can configure all VLAN assignments on a port as "Tagged" if doing so makes it easier to manage your VLAN assignments, or for security reasons.

14.3 Rules of Tag Vlan Operation

After you select a VLAN mode for the system and create VLAN interfaces with VLAN characteristics such as IEEE 802.1Q or no tagging and port membership, the system determines the details of VLAN operation by observing two main types of rules:

- **Ingress rules** - Assign an incoming frame to a specific VLAN.
- **Egress rules** - Use standard bridging rules to determine whether the frame is forwarded, flooded, or filtered. These rules also determine the tag status of the transmitted frame.

These rules are classified in the IEEE 802.1Q standard. In addition, the system relies on some system-specific rules.

14.3.1 Ingress Rules

These rules determine the VLAN to which an *incoming* frame belongs. The frame is assigned to the VLAN that matches most closely. A protocol match hierarchy is used to find the most specific match. The ingress rules, which are classified according to your VLAN mode, use the following process to determine the most specific match:

1. IEEE 802.1Q tag VID value
2. The default VLAN (an untagged VLAN with all ports and a VID of 1), or any port-based VLAN

Ingress Rules for VLANs

- If the frame is an IEEE 802.1Q tagged frame, the frame is assigned to the VLAN if the VID of the frame matches that of the VLAN. If there is no VID match, the frame is dropped.

- If the frame is not tagged, the frame is assigned to the VLAN if the receive port is untagged (that is, if tagging is set to none) and if the receive port of the frame matches that of the VLAN. If there is no match, the frame is dropped.

14.3.2 Egress Rules

These rules determine whether the *outgoing* frame is forwarded, filtered (dropped), or flooded; they also determine the frame's tag status. The frame is forwarded out of the port in the VID 2 VLAN (where the address is known) and with the tag status of that port.

Standard Bridging Rules for Outgoing Frames

The frame is handled according to these bridging rules:

If the transmit port is tagged and is not a member of the assigned VLAN, the frame is dropped.

If the frame's destination address matches an address that was learned on the receive port, it is *filtered* (dropped).

If the frame's destination address matches an address that was learned on a port other than the receive port, it is *forwarded* to that port.

If a frame with an unknown, multicast, or broadcast destination address is received, then it is *flooded* (that is, forwarded to all ports on the VLAN that is associated with the frame, except the port on which it was received).

If the frame's destination address matches a MAC address of one of the bridge's ports, it is further processed, not forwarded immediately. This type of frame is a management/configuration frame, such as a SNMP get/set PDU, Administration Console Telnet packet, or a Web Management Interface http packet.

Tag Status Rules

After the VLAN and the transmit ports are determined for the frame, the tag status rules determine whether the frame is transmitted with an IEEE 802.1Q tag:

- For each port on which a frame is to be transmitted, if that port is tagged for the VLAN that is associated with the frame, transmit the frame as a tagged frame.
- For each port on which a frame is to be transmitted, if that port is *not* tagged for the VLAN that is associated with the frame, transmit the frame as an untagged frame

14.4 CLI

LE2425 Switches support one type of VLAN at a time. The user has to set the VLAN type before configuration.

LE2425MNS# **set vlan type=<port|mac|tag|none>**

For Tag VLAN,

LE2425MNS# **set vlan type=tag**

Than, go to Vlan configuration mode by typing,

LE2425MNS# **vlan type=tag**

To **add** a TAG based VLAN we use the following command:

LE2425MNS(tag-vlan)##***id*=<vlan Id> [*name*=<vlan name>] *port*=<number|list|range>** where,

id is a valid VLAN ID. Its value has to be between 1 and 4095.

name is an optional field which is used to name a VLAN.

port is a valid range/list of ports or a single port which is to be added to the VLAN.

Note: When a new TAG VLAN is added, the VLAN's state is set to 'pending', to activate the VLAN, use the start command described below.

To **delete** a TAG VLAN use the following command:

LE2425MNS(tag-vlan)## **delete *vlan*=<name|number|list|range>** where,

vlan is the name or VLAN ID which is to be deleted.

This field also accepts range of VLAN ID values.

Note: An active VLAN cannot be deleted. The VLAN has to be stopped before it can be deleted. Only VLAN's in pending state can be deleted.

To **edit/change** the VLAN settings use the following command:

LE2425MNS(tag-vlan)##

edit*id*=<vlanId>[*name*=<vlanname>]*port*=<number|list|range> where,

id is an exisiting VLAN ID.

name is an optional field which is the name of the VLAN.

port is valid range/list of ports or a single port.

Note: An active VLAN cannot be edited. The VLAN has to be stopped before it can be edited. Only VLAN's in pending state can be edited.

To **start/activate** a VLAN use the following command:

```
LE2425MNS(tag-vlan)## start vlan=<all|name|number|list|range> where,
```

vlan is the name or VLAN ID which is to be started/activated.
This field also accepts range of VLAN ID values. To activate all the 'pending' VLAN's, use 'all' instead of VLAN ID's or VLAN name.

Note: Starting VLAN(s) will put them in active state.

To **stop** a VLAN use the following command:

```
LE2425MNS(tag-vlan)##stop vlan=<all|name|number|list|range> where,
```

vlan is the name or VLAN ID which is to be stopped.
This field also accepts range of VLAN ID values. To stop all the 'active' VLAN's, use 'all' instead of VLAN ID's or VLAN name.

Note: Stopping VLAN(s) will put them in pending state.

To **set the ingress** for a set of ports use the following command:

Note: If you are setting Ingress or Egress rules remotely (Telnet, SNMP etc), then please start the Vlan first. Otherwise, you would lock out yourself from the Vlan.

```
LE2425MNS(tag-vlan)## set-ingress port=<number|list|range>
                      pvid=<number> action=<enable|disable> where,
```

port is valid range/list of ports or a single port.
pvid is the valid Port VLAN ID. Its value can be between 1 and 4095.
action is used to enable or disable ingress on that set of ports.

To **set the egress** rules for a set of ports in a particular TAG VLAN use the following command:

```
LE2425MNS(tag-vlan)## set-egress vlan=<number> port=<number|list|range>
                      status=<tagged|untagged> where,
```

vlan is the VLAN ID whose ports egress value has to be changed.
port is the port or list/range of ports who are members of the VLAN ID mentioned above.
status is the egress status for the ports. It can be either enable or disable.

To **see the list** of VLAN's use the following command.

```
LE2425MNS(tag-vlan)##show vlan type=<port|tag|mac> [<id=vlanid>] where,
```

type is the type of VLAN, here it has to be tag.
Id is optional, and is used to see information about a particular VLAN, if this field is not entered, the entire list of TAG based VLAN's is shown.

Note: VLAN's that are still pending don't have their egress setting set in the hardware. Only when the VLAN is activated, the egress settings are set in the hardware. Hence to see the list of ports which are set to tagged use the '**show-egress**' command because show vlan will only show ports whose egress settings are set in the hardware.

To **see the ports and their ingress** values use the following command:

```
LE2425MNS(tag-vlan)## show-ingress [ports=<number|list|range>]
```

ports is the port or list/range of ports whose ingress value has to be shown. This field is optinal and if it is not entered, the entire list of ports and their respective ingress values are shown.

To **see the ports which are tagged** (whose egress values are set or to be set) use the following command:

```
LE2425MNS(tag-vlan)## show-egress
```

Note: Egress settings are updated only when the VLAN is set to active state; hence, this command shows the list of ports, which are set to egress, and their corresponding VLAN state. VLAN's that are still in pending state do not have their egress set in the hardware.

15.0 GVRP

15.1 GVRP (GARP VLAN Registration Protocol)

The above is an application of the Generic Attribute Registration Protocol (GARP). GVRP is defined in the IEEE 802.1Q standard, and GARP is defined in the IEEE 802.1P standard.

Note: To understand and use GVRP you must have a working knowledge of 802.1Q VLAN tagging. (See “Tag-Based Virtual LANs (Static VLANs)”). GVRP uses “GVRP Bridge Protocol Data Units” (“GVRP BPDUs”) to “advertise” static VLANs. In this manual, a GVRP BPDU is termed an *advertisement*.

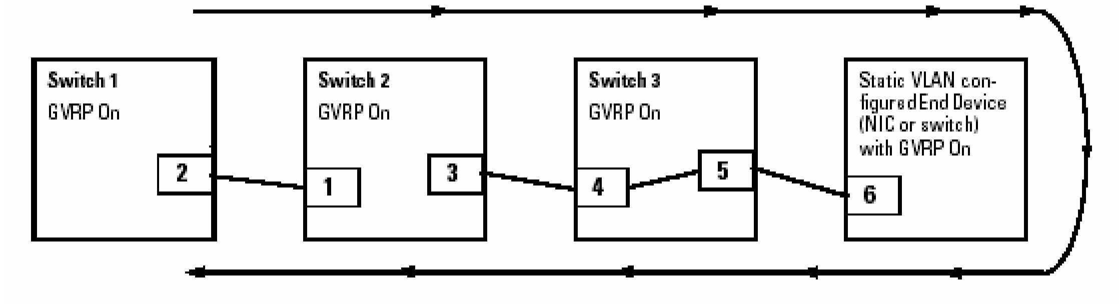
GVRP enables the 6K Switch to dynamically create 802.1Q-compliant VLANs on links with other devices running GVRP. This enables the switch to automatically create VLAN links between GVRP-aware devices. (A GVRP link can include intermediate devices that are not GVRP-aware.) This operation reduces the chances for errors in VLAN configuration by automatically providing VLAN ID (VID) consistency across the network. That is, you can use GVRP to propagate VLANs to other GVRP-aware devices instead of manually having to set up VLANs across your network. After the switch creates a dynamic, you can also use GVRP to dynamically enable port membership in static VLANs configured on a switch.

Note: There must be one common VLAN (that is, one common VID) connecting all of the GVRP-aware devices in the network to carry GVRP packets. Black Box recommends the default VLAN (DEFAULT_VLAN; VID = 1), which is automatically enabled and configured as untagged on every port of the LE2425 switches). That is, on ports used for GVRP links, leave the default VLAN set to **Untagged** and configure other static VLANs on the same ports as either **Tagged**, **Forbid**. (**Forbid** option described under “Per-Port Options for Dynamic VLAN Advertising and Joining”.

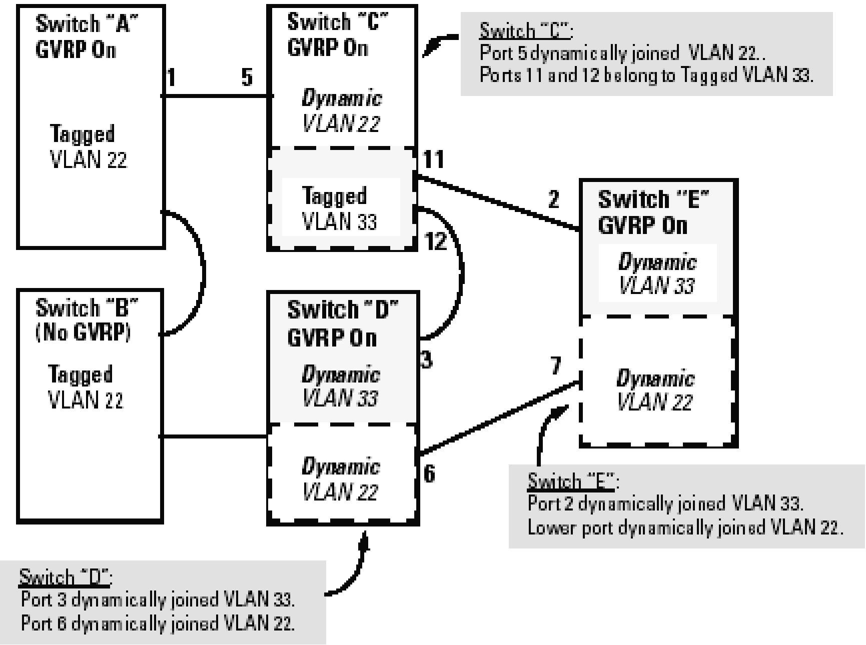
15.2 General Operation

A GVRP-enabled port with a Tagged or Untagged static VLAN sends advertisements (BPDUs, or Bridge Protocol Data Units) advertising the VLAN (actually, its VID). Another GVRP-aware port receiving the advertisements over a link can dynamically join the advertised VLAN. *All dynamic VLANs operate as Tagged VLANs*. Also, a GVRP-enabled port can forward an advertisement for a VLAN it learned about from other ports on the same switch. However, the forwarding port will not itself join that VLAN until an advertisement for that VLAN is received on that specific port.

Core switch with static VLANs (VID= 1, 2, & 3). Port 2 is a member of VIDs 1, 2, & 3.
1. Port 2 advertises VIDs 1, 2,& 3.
2. Port 1 receives advertisement of VIDs 1, 2, & 3 AND becomes a member of VIDs 1, 2, & 3.
3. Port 3 advertises VIDs 1, 2, & 3, but port 3 is NOT a member of VIDs 1, 2, & 3 at this point.
4. Port 4 receives advertisement of VIDs 1, 2, & 3 AND becomes a member of VIDs 1, 2, & 3.
5. Port 5 advertises VIDs 1, 2,& 3, but port 5 is NOT a member of VIDs 1, 2, & 3 at this point.
Port 6 is statically configured to be a member of VID 3.
6. Port 6 advertises VID 3.
7. Port 5 receives advertisement
8. Port 4 advertises VID 3.
9. Port 3 receives advertisement of VID 3 AND becomes a member of VID 3. (Still not a member of VIDs 1 & 2.)
10. Port 1 advertises VID 3 of VID 3 AND becomes a member of VID 3. (Still not a member of VIDs 1 & 2.)
11. Port 2 receives advertisement of VID 3. (Port 2 is already statically configured for VID 3.


Switch 1
GVRP On
2
Switch 2
GVRP On
1
3
Switch 3
GVRP On
4
5
Static VLAN con-figured End Device (NIC or switch) with GVRP On
6

Note that if a static VLAN is configured on at least one port of a switch, and that port has established a link with another device, then all other ports of that switch will send advertisements for that VLAN. For example, in the following figure, Tagged VLAN ports on switch "A" and switch "C", below advertise VLANs 22 and 33 to ports on other GVRP-enabled switches that can dynamically join the VLANs.



Switch "C":
Port 5 dynamically joined VLAN 22..
Ports 11 and 12 belong to Tagged VLAN 33.

Switch "E":
Port 2 dynamically joined VLAN 33.
Lower port dynamically joined VLAN 22.

Switch "D":
Port 3 dynamically joined VLAN 33.
Port 6 dynamically joined VLAN 22.

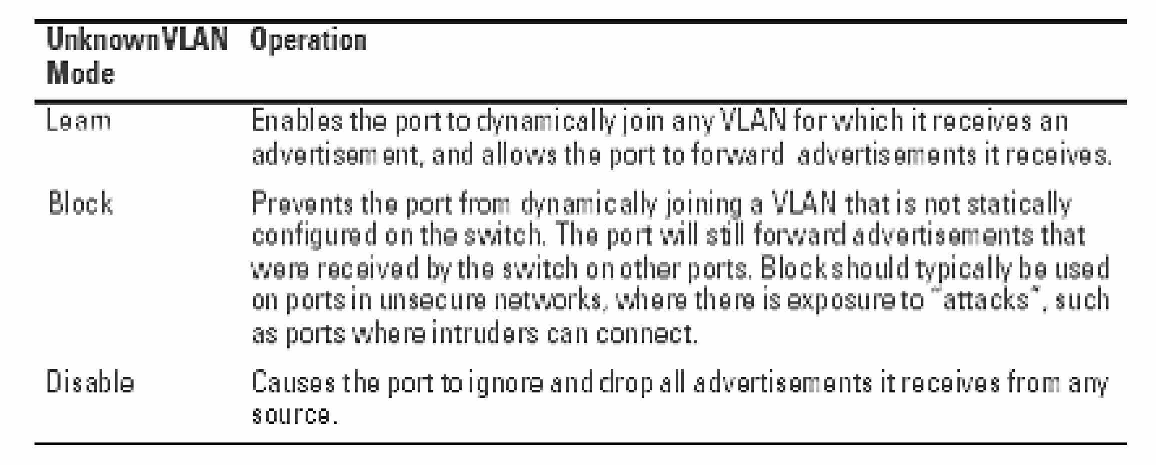
A port can learn of a dynamic VLAN through devices that are not aware of GVRP (Switch "B", above). VLANs must be disabled in GVRP-unaware devices to allow tagged packets to pass through. A GVRP-aware port receiving advertisements has these options:

If there is not already a static VLAN with the advertised VID on the receiving port, then dynamically create a VLAN with the same VID as in the advertisement, and begin moving that VLAN's traffic.
If the switch already has a static VLAN assignment with the same VID as in the advertisement, and the port is configured to **Learn** for that VLAN, then the port will dynamically join the VLAN and begin moving that VLAN's traffic. (For more detail on **Leran**, see "Per-Port Options for Dynamic VLAN Advertising and Joining".)
Ignore the advertisement for that VID and drop all GVRP traffic with that VID.
Don't participate in that VLAN.

Note also that a port belonging to a Tagged or Untagged static VLAN has these configurable options:
Send VLAN advertisements, and also receive advertisements for VLANs on other ports and dynamically join those VLANs.
Send VLAN advertisements, but ignore advertisements received from other ports.
Avoid GVRP participation by not sending advertisements and dropping any advertisements received from other devices.

15.3 Per-Port Options for Handling GVRP "Unknown VLANs"

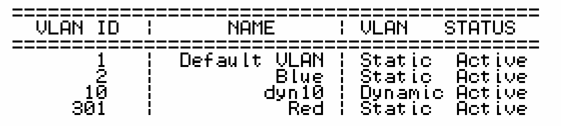
An "unknown VLAN" is a VLAN that the switch learns of by GVRP. For example, suppose that port 1 on switch "A" is connected to port 5 on switch "C". Because switch "A" has VLAN 22 statically configured, while switch "C" does not have this VLAN statically configured, VLAN 22 is handled as an "Unknown VLAN" on port 5 in switch "C". Conversely, if VLAN 22 was statically configured on switch C, but port 5 was not a member, port 5 would become a member when advertisements for VLAN 22 were received from switch "A". When you enable GVRP on a switch, you have the per-port join-request options



Unknown VLAN Mode	Operation
Learn	Enables the port to dynamically join any VLAN for which it receives an advertisement, and allows the port to forward advertisements it receives.
Block	Prevents the port from dynamically joining a VLAN that is not statically configured on the switch. The port will still forward advertisements that were received by the switch on other ports. Block should typically be used on ports in unsecure networks, where there is exposure to "attacks", such as ports where intruders can connect.
Disable	Causes the port to ignore and drop all advertisements it receives from any source.

The CLI **show-vlan (**command line interface VLAN Support screen) shows a switch's current GVRP configuration, including the Unknown VLAN settings.

LE2425MNS(GVRP)## **show-vlan**



```
===========================================
  VLAN ID   |      NAME      | VLAN   STATUS
===========================================
        1   |  Default VLAN  | Static  Active
        2   |          Blue  | Static  Active
       10   |         dyn10  | Dynamic Active
      301   |           Red  | Static  Active
```

15.4 Per-Port Options for Dynamic VLAN Advertising and Joining

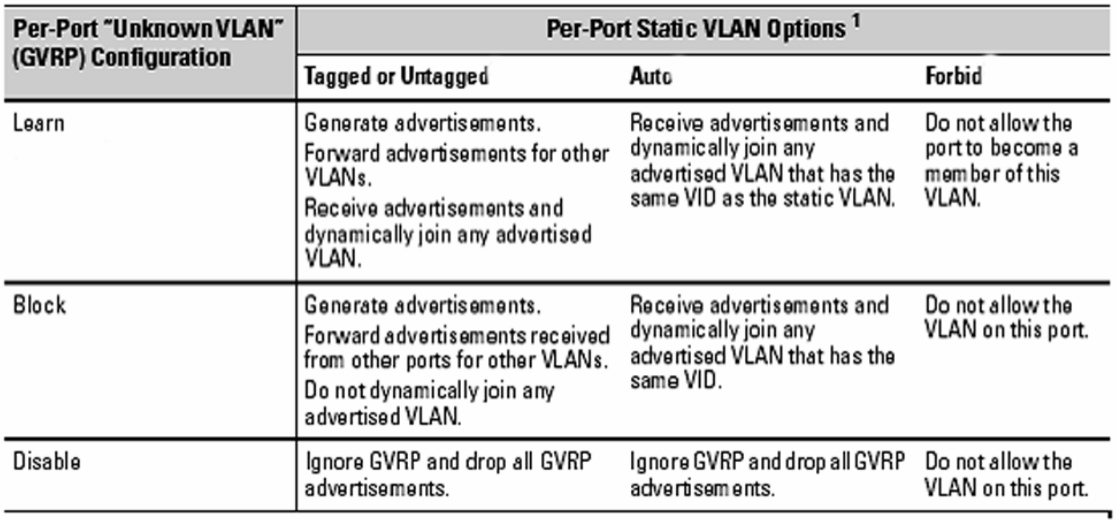
Initiating Advertisements. As described in the preceding section, to enable dynamic joins, GVRP must be enabled and a port must be configured to Learn (the default). However, to send advertisements in your network, one or more Tagged or Untagged static VLANs must be configured on one or more switches (with GVRP enabled), depending on your topology.

15.4.1 Enabling a Static VLAN for Dynamic Joins.

You can configure a port to dynamically join a static VLAN (that shares the same VID) if that port subsequently receives an advertisement for the static VLAN. (This is done by using the **Learn** option described in table, below.

15.4.2 Parameters for Controlling VLAN Propagation Behavior.

On an individual port, you can configure an existing static VLAN to actively or passively participate in dynamic VLAN propagation or to ignore dynamic VLAN (GVRP) operation. These options are controlled by the GVRP "Unknown VLAN" and the static VLAN configuration parameters, as described in the following table:



Per-Port "Unknown VLAN" (GVRP) Configuration	Per-Port Static VLAN Options [1]		
	Tagged or Untagged	Auto	Forbid
Learn	Generate advertisements. Forward advertisements for other VLANs. Receive advertisements and dynamically join any advertised VLAN.	Receive advertisements and dynamically join any advertised VLAN that has the same VID as the static VLAN.	Do not allow the port to become a member of this VLAN.
Block	Generate advertisements. Forward advertisements received from other ports for other VLANs. Do not dynamically join any advertised VLAN.	Receive advertisements and dynamically join any advertised VLAN that has the same VID.	Do not allow the VLAN on this port.
Disable	Ignore GVRP and drop all GVRP advertisements.	Ignore GVRP and drop all GVRP advertisements.	Do not allow the VLAN on this port.

As the above table indicates, when you enable GVRP, a port that has a Tagged or Untagged static VLAN has the option for both generating advertisements and dynamically joining other VLANs. **Note** In table , above, the Unknown VLAN parameters are configured on a per interface basis using the CLI. The Tagged, Untagged, Auto, and Forbid options are configured in the VLAN context using either the menu interface or the CLI. Because dynamic VLANs operate as Tagged VLANs, and because a tagged port on one device cannot communicate with an untagged port on another device, Black Box recommends that you use Tagged VLANs for the static VLANs you will use to generate advertisements.

15.5 GVRP and VLAN Access Control

When you enable GVRP on a switch, the default GVRP parameter settings allow all of the switch's ports to transmit and receive dynamic VLAN advertisements (GVRP advertisements) and to dynamically join VLANs. The two preceding sections describe the per-port features you can use to control and limit VLAN propagation. To summarize, you can:
Allow a port to advertise and/or join dynamic VLANs (the default).
Allow a port to send VLAN advertisements, but not receive them from other devices; that is, the port cannot dynamically join a VLAN but other devices can dynamically join the VLANs it advertises.
Prevent a port from sending dynamic VLAN advertisements for specific VLANs
Prevent a port from participating in GVRP operation.

15.6 Port-Leave From a Dynamic VLAN

A dynamic VLAN continues to exist on a port for as long as the port continues to receive advertisements of that VLAN from another device connected to that port or until you:
Convert the VLAN to a static VLAN (See "Converting a Dynamic VLAN to a Static VLAN".)
Reconfigure the port to **Block** or **Disable**
Disable GVRP
Reboot the switch

The time-to-live for dynamic VLANs is 10 seconds. That is, if a port has not received an advertisement for an existing dynamic VLAN during the last 10 seconds, the port removes itself from that dynamic VLAN.

Converting a Dynamic VLAN to a Static VLAN.

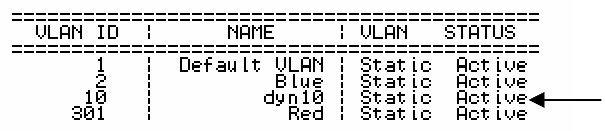
If GVRP is running on the switch and a port dynamically joins a VLAN, you can use the next command to convert the dynamic VLAN to a static VLAN. This is necessary if you want to make the VLAN permanent.
Note: After you convert a dynamic VLAN to static, you must configure the switch's per-port participation in the VLAN in the same way that you would for any static VLAN.
Syntax: static vlan=<**dynamic vlanid**>

If you need a VID reference, use **show vlan type=tag** to list the switch's currently existing VLANs.

For example, suppose a dynamic VLAN with a VID of 10 exists on the switch.
The following command converts the VLAN to a static VLAN.

LE2425MNS(gvrp)# **static vlan=10**
Once dynamic Vlan converted into static, it needs to configure as a normal static Vlan.

LE2425MNS(gvrp)# **show-vlan**



```
=========================================
  VLAN ID  |      NAME      | VLAN   STATUS
=========================================
       1   |  Default VLAN  | Static  Active
       2   |          Blue  | Static  Active
      10   |         dyn10  | Static  Active
     301   |           Red  | Static  Active
```

15.7 Planning for GVRP Operation

These steps outline the procedure for setting up dynamic VLANs for a segment.

1. Determine the VLAN topology you want for each segment (broadcast domain) on your network.
2. Determine the VLANs that must be static and the VLANs that can be dynamically propagated.
3. Determine the device or devices on which you must manually create static VLANs in order to propagate VLANs throughout the segment.
4. Determine security boundaries and how the individual ports in the segment will handle dynamic VLAN advertisements. (See tables above.)
5. Enable GVRP on all devices you want to use with dynamic VLANs and configure the appropriate "Unknown VLAN" parameter (**Learn**, **Block**, or **Disable**) for each port.
6. Configure the static VLANs on the switch(es) where they are needed, along with the per-VLAN parameters (**Tagged**, **Untagged**, and **Forbid**—see table on the appropriate ports.
7. Dynamic VLANs will then appear automatically, according to the configuration options you have chosen.
8. Convert dynamic VLANs to static VLANs where you want dynamic VLANs to become permanent.

15.8 Configuring GVRP On a Switch

The procedures in this section describe how to:
View the GVRP configuration on a switch
Enable and disable GVRP on a switch
Specify how individual ports will handle advertisements
To view or configure static VLANs for GVRP operation, refer to "Port-Based Virtual LANs (Static VLANs)"

CLI: Viewing and Configuring GVRP
Displaying the Switch's Current GVRP Configuration.

This command shows whether GVRP is disabled, along with the current settings for the maximum number of VLANs and the current Primary VLAN. (For more on the last two parameters, see "Port-Based Virtual LANs (Static VLANs)")
Syntax: show gvrp

LE2425MNS#**show gvrp**
GVRP Status : Enabled

15.9 Enabling and Disabling GVRP on the Switch.

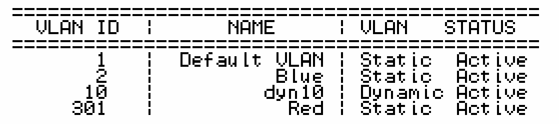
This command enables GVRP on the switch.
Syntax: gvrp <enable/disable>

LE2425MNS(gvrp)##**gvrp enable**
  GVRP enabled
LE2425MNS(gvrp)##**gvrp disable**
 GVRP is now disabled

15.10 Displaying the Static and Dynamic VLANs Active on the Switch.

The **show-vlan** command lists all VLANs present in the switch.

*Syntax***:** **show-vlan**

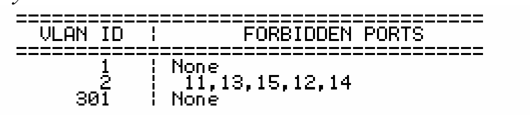


```
=============================================
  VLAN ID  |       NAME      | VLAN    STATUS
=============================================
       1   |   Default VLAN  | Static   Active
       2   |           Blue  | Static   Active
      10   |          dyn10  | Dynamic  Active
     301   |            Red  | Static   Active
```

Specify the individual ports to handle advertisements
To set the state of the port
Syntax: **set-ports port**=<port|list|range> **state**=<learn|block|disable>
Note: Default state of the port is 'disable'.

To set the forbid ports or VLAN's
Syntax: **set-forbid vlan**=<tag vlanid> **forbid**=<port number|list|range>

To see the forbidden Ports
Syntax : **show-forbid**



```
======================================
  VLAN ID  |        FORBIDDEN PORTS
======================================
       1   | None
       2   |  11,13,15,12,14
     301   | None
```

LE2425MNS(gvrp)# **show-port**

```
1  | Block
2  | Block
3  | Disable
4  | Disable
5  | Disable
6  | Disable
7  | Disable
8  | Disable
9  | Disable
10  | Learn
11  | Learn
12  | Learn
13  | Disable
14  | Disable
15  | Disable
```

15.11 GVRP Operating Notes

A dynamic VLAN must be converted to a static VLAN before it can have an IP address. Converting a dynamic VLAN to a static VLAN and then executing the **save** command saves the VLAN in the startup-config file and makes it a permanent part of the switch's VLAN configuration. Within the same broadcast domain, a dynamic VLAN can pass through a device that is not GVRP-aware. This is because a hub or a switch that is not GVRP-aware will flood the GVRP (multicast) advertisement packets out all ports.

GVRP assigns dynamic VLANs as Tagged VLANs. To configure the VLAN as Untagged, you must first convert it to a static VLAN.

Rebooting a switch on which a dynamic VLAN exists deletes that VLAN. However, the dynamic VLAN re-appears after the reboot if GVRP is enabled and the switch again receives advertisements for that VLAN through a port configured to add dynamic VLANs.
By receiving advertisements from other devices running GVRP, the switch learns of static VLANs on those other devices and dynamically (automatically) creates tagged VLANs on the links to the advertising devices. Similarly, the switch advertises its static VLANs to other GVRP-aware devices.
A GVRP-enabled switch does not advertise any GVRP-learned VLANs out of the port(s) on which it originally learned of those VLANs.

16.0 Troubleshooting

16.1 Overview

This chapter addresses performance-related network problems that can be caused by topology, Switch configuration, and the effects of other devices or their configurations on Switch operation. (For Switch-specific information on hardware problems indicated by LED behavior, cabling requirements, and other potential hardware-related problems, refer to the LE2425 Switches User Manual.)

This chapter includes:

- Troubleshooting Approaches
- Console Interface Problems
- Unusual Network Activity
- General Problems
- VLAN-Related Problems
- Using the Event Log To Identify Problem Sources
- Diagnostics and Management Tools, including:
- Ping test
- Command prompt
- Restoring the factory default configuration

For information on support and warranty provisions, see the LE2425 Switches User Manual

16.2 Troubleshooting Approaches

Use these approaches to diagnose Switch problems:

- Check the Switch LEDs for indications of proper Switch operation:
- Each Switch port has a Link LED that should light whenever an active network device is connected to the port.

See the *Hardware User Guide* shipped with the Switch for a description of the LED behavior and information on using the LEDs for trouble-shooting.

- Check the network topology/installation. See the *Hardware User Guide* shipped with the Switch for topology information.
- Check cables for visible damage, correct type, and proper connections. See the *Hardware User Guide* shipped with the Switch for correct cable types and connectopin-outs.
- For help in isolating problems, use the easy-to-access console port built into the Switch. See chapter 2, “Using the Console Interface” for operating information.

These tools are available through the console port.

- Status and Counters screens
- Event Log
- Diagnostics tools (Ping test, and advanced user commands)

16.3 Console Access Problems

The Switch may not have the correct IP address, subnet mask, or gateway. Verify the problem by connecting a console to the Switch’s Console port and check the IP configuration.

16.4 Unusual Network Activity

Network activity that exceeds accepted norms may indicate a hardware problem with one or more of the network components, possibly including the Switch. Unusual network activity is indicated by the light patterns of the LEDs on the front of the Switch. This unusual activity can be measured with the Switch console interface or with a network management tool. Refer to the *Hardware User Guide* you received with the Switch for information on using LEDs to identify unusual network activity.

A topology loop can also cause excessive network activity. The event log messages can be indicative of this type of problem. Please see Using the Event Log To Identify Problem Sources section of this chapter for more detail.

16.5 General Problems

If you experience problems such as “the network runs slow; processes fail; or users cannot access servers or other devices” then Broadcast storms may be occurring in the network. These may be due to redundant links between nodes.

16.5.1 Duplicate IP Addresses

This is indicated by this Event Log message:

TCP/IP: duplicate IP Addresses [IP address] *sent from Ethernet address [*MAC address*]*.

The IP Address above is the same IP address of both devices, indicating the Switch’s IP address has been duplicated somewhere on the network.

16.5.2 SNTP or Gateway Problems

If problems such as “The Switch Cannot Find the SNTP Server or the Configured Gateway” occur then your primary VLAN to the ports may have moved.   SNTP and Gateway access are through the VLAN (If VLAN **enable**), which in the default configuration is the DEFAULT-VLAN. If the primary VLAN has been moved to another VLAN, it may be disabled or does not have ports assigned to it.

16.6 Using the Event Log To Identify Problem Sources

The Event Log records operating events as single-line entries listed in chronological order, and serves as a tool for isolating problems. Each Event Log entry is composed of four fields:

Severity   Date   Time   Description

Severity is one of the following levels:
I (Information) indicates routine events.
A (Activity) indicates the activity on Switch.
D (Debug). reserved for Magnum internal diagnostic information.
C (Critical) indicates that a severe Switch error has occurred.
F (Fatal). indicates that a service has behaved unexpectedly.

Date is the date in *mm/dd/yy* format (as per configured) that the entry was placed in the log.
Time is the time in *hh:mm:ss* format (as per configured) that the entry was placed in the log.
Source Name is the name of the node, computer, device or the user.
Description is a brief description of the operating event.

The event log holds up to 1000 lines in chronological order, from the oldest to the newest. Each line consists of one complete event message. Once the log has received 1000 entries, it discards the current oldest line (with information level severity only) each time a new line is received. The event log window contains 22 log entry lines and can be positioned to any location in the log.
The event log is *not* erased by using the “Reboot Command” in the Main CLI.

CLI Command to see the Event Log
*Type Syntax**:*** **show log** <option>

```
-----------------------------------------------------------------------------------------------
Severity    Date            Time                      Log   Description
-----------------------------------------------------------------------------------------------
   D        21-09-2001  11:18:18 AM    System X    System is resetted
   I        21-09-2001  11:18:18 AM    Rajesh      Rajesh is now on line
   I        21-09-2001  11:18:18 AM    Server1      network enabled on  192.168.1.16
  A         22-09-2001   12:00:03PM    Device       Port 17 disabled
-----------------------------------------------------------------------------------------------
```

The output can be filtered with the help of “Show Commands”.
E.g., *Type Syntax*: **show log informational** where “informational” is the <option> will show only informational log entries.

```
-----------------------------------------------------------------------------------------------
Severity    Date            Time                      Log   Description
-----------------------------------------------------------------------------------------------
   I        21-09-2001  11:18:18 AM    Rajesh      Rajesh is now on line
   I        21-09-2001  11:18:18 AM    Server1      network enabled on  192.168.1.16
```

Here is the List of System Events:

Subsystem	Description	Severity
SNTP	client started	I
SNTP	client stopped..disabled by user	I
SNTP	client stopped..server not configured	I
SNTP	Request timed out	I
SNTP	Retrying..	I
DEVICE	System started	I
DEVICE	Network Stack not yet configured	I
SNMP	Snmp.snmpEnableAuthenTraps is set to enabled	A
SNMP	Snmp.snmpEnableAuthenTraps is set to disabled	A
PRTMR	Enabled by user monitor = x , sniffer = y	I
PRTMR	Disabled by user	I
VLAN	Type set to port	I
VLAN	Type set to mac	I
VLAN	Type set to tag	I
VLAN	Type set to none	I
VLAN	Pvlan: port based vlan started	I
VLAN	Pvlan: default vlan is modified	I
VLAN	Tvlan: Tag based vlan started	I
TCP/IP	Failed to initialize the interface x	F
BRIDGE	Bridge init failed for ethx	F
BRIDGE	Bridge enable for ethx failed	F
DEVICE	IP address a.b.c.d configured	I
DEVICE	subnetmask a.b.c.d configured	I
DEVICE	Default gateway a.b.c.d configured	I
DEVICE	Switch rebooted by user	I
SNMP	System.sysName configured	A
SNMP	System.sysLocation configured	A
SNMP	System.sysContact configured	A
DEVICE	Port x enabled	A
DEVICE	Port x disabled	A
CLI	Manager login at console	I
CLI	Operator login at console	I
CLI	Manager password changed	I
CLI	Operator password changed	I
SNMP	read community string changed	I
SNMP	write community string changed	I
SNMP	trap community string changed	I
RMON	rising alarm trap sent to a.b.c.d by alarm entry X	I
RMON	falling alarm trap sent to a.b.c.d by alarm entry X	I
SNMP	authentication failure trap sent to a.b.c.d	I
SNMP	Trap receiver a.b.c.d added	I
SNMP	Trap receiver a.b.c.d deleted	I
DEVICE	No saved system logs	I
DEVICE	Failed to read saved system logs	D
SNMP	Coldstart trap sent to a.b.c.d	I
SNMP	Warmstart trap sent to a.b.c.d	I
SNMP	Port X link up trap sent to a.b.c.d	A
SNMP	Port X Link down trap sent to a.b.c.d	A
SNMP	Configuring IP address in trap receivers list failed	D
DEVICE	Timezone set to x	I
DEVICE	Country set to x (no DST)	I
DEVICE	Country set to x (DST valid)	I

DEVICE	Time set to x : y : z (HH:MM:SS) tz = a	I
DEVICE	Date set to x : y : z (HH:MM:YYYY)	I
RMON	RMON init is done	I
BRIDGE	Bridge MIB init is done	I
TCP/IP	Duplicate IP a.b.c.d sent from MAC address XXXXXX	C
TCP/IP	IP packet of version X is dropped	I
TCP/IP	IP packet from a.b.c.d , with checksum error dropped	D
TCP/IP	Bad IP fragments from a.b.c.d dropped	D
TCP/IP	UDP checksum error in the received packet a.b.c.d	D
TCP/IP	TCP checksum error in the received packet a.b.c.d	D
TCP/IP	Unable to allocate memory for an ICMP packet	C
TCP/IP	ICMP checksum error in the received packet	D
SNTP	Time synchronized through SNTP	I
RMON	history : control entry X is set to valid	I
RMON	history : control entry X is set to invalid	I
RMON	Event : entry X is set to valid	I
RMON	Event : entry X is set to invalid	I
RMON	Alarm : entry X is set to valid	I
RMON	Alarm : entry X is set to invalid	I
RMON	Alarm : internal error , unable to get memory	F
RMON	Alarm : internal error, unable to get memory for alarm entry	F
RMON	History : internal error, unable to get memory for history control entry	F
RMON	History : internal error, unable to get memory for history data entry	F
RMON	History : internal error, unable to get memory	F
RMON	Event : unable to get memory for event entry	F
RMON	Alarm : unable to get memory for RMON logs	F
DEVICE	Ethernet DMA init failure	F
DEVICE	Ethernet hardware error	F
DEVICE	Ethernet interrupt init failure	F
DEVICE	Ethernet counters init failure	C
BRIDGE	Unable to delete MAC address from FDB	D
BRIDGE	Unable to insert MAC address to FDB	D
DEVICE	Unable to access ethernet counters	C
DEVICE	Unable to allocate ethernet memory	F
DEVICE	Port X link down	A
DEVICE	Port X link up	A
PS	INTRUDER a:b:c:d:e:f @ port X , port disabled	A
PS	INTRUDER a:b:c:d:e:f @ port X , port disabled	A
PS	Resetting MAC a:b:c:d:e:f at port X failed	C
PS	Unable to delete learnt MACs in hardware	D
PS	Port security enabled	A
PS	port security disabled	A
VLAN	pvlan:vlan X enabled	I
VLAN	pvlan:vlan X disabled	I
VLAN	pvlan:vlan X deleted	I
VLAN	pvlan:port based VLAN started	I
VLAN	pvlan:port based VLAN stopped	I
VLAN	pvlan:default vlan is modified	I
VLAN	tvlan:vlan X deleted	I
VLAN	tvlan:vlan X enabled	I
VLAN	tvlan:vlan X disabled	I
VLAN	tvlan:tag based VLAN stopped	I
VLAN	tvlan:tag based VLAN started	I

16.7 Diagnostic Tools

16.7.1 Ping Test

The Ping test is a point-to-point test between your Switch and another IEEE 802.3-compliant device on your network. These tests can tell you whether the Switch is communicating properly with another device.

Note: To respond to a Ping test or a Link test, the device you are trying to reach must be IEEE 802.3-compliant.

This is a test of the path between the Switch and another device on the same or another IP network that can respond to IP packets (ICMP Echo Requests).

16.7.2 CLI: Ping Test

Ping Test. You can issue single or multiple ping tests with varying repetitions or counts and timeout periods. The defaults and ranges are:

_ Count: 1 (1 - 999)
_ Timeout: 5 seconds (1 - 256 seconds)
Syntax: ping <*ip-address*> [count <1 - 999>] [timeout <1 - 256>]

Example: LE2425MNS> **ping 192.168.1.10**
Your response will be 192.168.1.10 is alive, time=15ms

Example 2: LE2425MNS> **ping 192.168.1.10 count=3**

```
Your response will be      192.168.1.10 is alive, time=15ms
                           192.168.1.10 is alive, time=15ms
                           192.168.1.10 is alive, time=15ms
```

You can do any combination of the above IP address, count, and timeout commands.

To halt a ping test before it concludes, press [Ctrl] [C].

16.8 CLI Administrative and Troubleshooting Commands

These commands provide information or perform actions that you may find helpful in troubleshooting operating problems with the Switch.

Note For more on the CLI, refer to chapter 2, "Using the Command Line Reference (CLI).

Type Syntax: **show version** shows the software version currently running on the Switch.
Similarly *Type Syntax*: **show history** Displays the current command history.
Type Syntax: **show setup** Displays the Switch Setup screen.
Type Syntax: **!!** Repeatedly executes the previous command.

16.9 Restoring the factory default configuration

To erase the current configuration
Syntax: **kill config**
Note: This is a hidden command. It erases the current configuration and loads the factory default configuration. It is highly recommended to use this command only if you really need to erase the current configuration.
For More information please refer *chapter 4.*

APPENDIX A

Daylight Savings Time on LE2425 Switch

LE2425 Switches provide a way to automatically adjust the system clock for Daylight Savings Time (DST) changes. The

user defines the month and date to begin and end the change from standard time. In addition to the value "none" (no time changes), there are fifteen pre-defined settings, a few examples are:

- Alaska
- Canada and Continental US
- Middle Europe and Portugal
- Southern Hemisphere
- Western Europe

The pre-defined settings follow these rules:

Alaska:

• Begin DST at 2am the first Sunday on or after April 24th.
• End DST at 2am the first Sunday on or after October 25th.

Canada and Continental US:

• Begin DST at 2am the first Sunday on or after April 1st.
• End DST at 2am the first Sunday on or after October 25th.

Middle Europe and Portugal:

• Begin DST at 2am the first Sunday on or after March 25th.
• End DST at 2am the first Sunday on or after September 24th.

Southern Hemisphere:

• Begin DST at 2am the first Sunday on or after October 25th.
• End DST at 2am the first Sunday on or after March 1st.

Western Europe:

• Begin DST at 2am the first Sunday on or after March 23rd.
• End DST at 2am the first Sunday on or after October 23rd.

A sixth option named "User defined" allows the user to customize the DST configuration by entering the beginning month and date plus the ending month and date for the time change.

Before configuring a "User defined" Daylight Time Rule, it is important to understand how the Switch treats the entries. The Switch knows which dates are Sundays, and uses an algorithm to determine on which date to change the system clock, given the configured "Beginning day" and "Ending day":

- If the configured day is a Sunday, the time changes at 2am on that day.
- If the configured day is not a Sunday, the time changes at 2am on the first Sunday after the configured day.

This is true for both the "Beginning day" and the "Ending day".

Here is the list of valid country codes to set daylight settings.

- Egypt
- Namibia
- USSR
- Iraq
- Lebanon
- Syria
- Australia
- London
- Belgium
- Italy
- Greece
- Cuba
- USA
- Falklands
- Chile

APPENDIX B
How to Upgrade

LE2425 Managed Network Software (MNS-BB) can be obtained from Black Box FTP site (ftp.blackbox.com)
Username: m6kuser, Password: m6kuser and uploaded to the LE2425 Switch unit. The upgrade feature of the LE2425 is provided for facilitating periodic MNS Software upgrades.

MNS Software Download from FTP site

Downloading LE2425 software (MNS) from Black Box's FTP site (ftp.blackbox.com

a. Use browser (Microsoft Internet Explorer or Netscape Navigator) or any FTP tools to download the MNS Software.
b. If you use browser interface, use the following URL to access the files: ftp://ftp.blackbox.com
c. If you are using an FTP client program, connect to **ftp.blackbox.com**
d. User: m6kuser ; password: m6kuser
e. Download the MNS Software on your Desktop PC (Chosen to be used as a console terminal)

Assumptions:

- The responsible person configuring this switch is well versed with Hyper Terminal (Windows 98, 2000, XP) or Minicom (Linux).

Note: For Linux/Unix Minicom Configuration instructions, please refer to page g below.

- The 6K Switch must be connected via the console RS-232 port (located on the right rear of the unit as shown in Fig 1.0) to a serial port of a Desktop PC operating as a console terminal.

Note:(*The DB-9 (Null Modem) connecting cable is required for the connection. It is not supplied along with the LE2425 unit*). It can be purchased from any Electronic Store.

Connecting the Console Terminal to LE2425

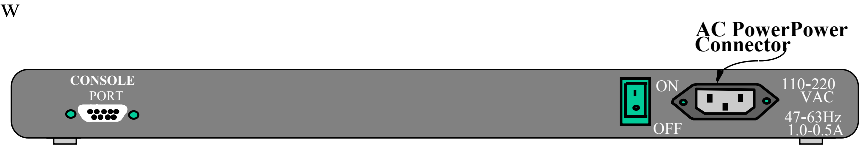
Use the DB-9 cable to connect the LE2425 Switch Console (RS-232) port to the Desktop PC (Console Terminal).

Caution: While connecting the DB9 cable to the LE2425 unit, the unit must be switched off.

On Desktop PC (Windows Console)

Follow these steps to connect the Desktop PC or terminal to the LE2425 Switch:

Step 1: Using the DB9 cable, connect to the LE2425 console port, as shown in the Fig. 1.0 below



Rear View of LE2425

Fig 1.0

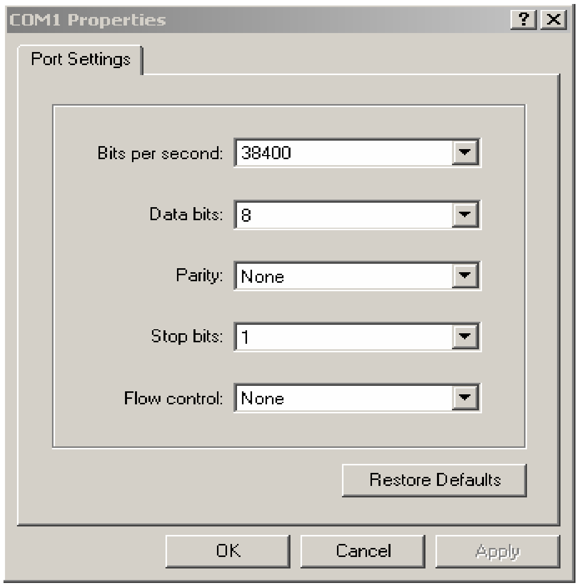
Step 2: Attach the other end of the DB-9 female adapter to the Desktop PC (COM1, COM2 or COM3 Port).

Step 3: Run Hyper Terminal on the Desktop PC.

Step 4: Provide an appropriate name and Press **OK** then connect to the serial port using COM1, COM2 or COM3 (as provided on Desktop PC) and Press **OK.**

Step 5: Configure the following parameters as shown in the Fig 1.0:

- 38400 baud
- 8 data bits
- 1 stop bit
- No parity
- None



COM1 Properties

Bits per second: 38400

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

Fig 2.0

Step 6: Power on the LE2425 Switch and obtain the
LE2425MNS# prompt on the *Hyper Terminal* window.

Step 7: Invoke the **upgrade** command by typing "upgrade" without any arguments and press enter key as shown below.

LE2425MNS# **upgrade mode=serial** <*enter*>

Step 8: From the *Hyper Terminal Menu*, Select **Transfer -> Send File** -> a small popup window opens... use **Browse** button to locate your path to the MNS Software file (Rel2.x.x.bin) location, and select the protocol as **Xmodem** from the drop down list, then **click Ok.**

Step 9: The download starts and proceeds to download the file. You will get the message " Upgrade is Successful. Please reboot LE2425 now to start the application" at the end. If there is any error in the file transfer, you will get the error message " Upgrade failed " and the program will abort back to the (boot) prompt.
NOTE: Please do not interrupt the LE2425 unit or the Desktop PC during the download process. If for any reason the download is not complete, please follow steps 6 through 9 again to complete the upgrade process.

<u>**On Linux Console**</u>

Step 1: Run Minicom.

Step 2: To set the baud rate of the COM Port. Press <ctrl> A …Z…P…G and <Enter>

Step 3: Power on the LE2425 Switch. You will get the Prompt LE2425MNS#

Step 4: Invoke the **upgrade** command by typing "upgrade" without any arguments and press enter key as shown below.

LE2425MNS# **upgrade mode=serial** <*enter*>

Step 5: Press <ctrl>A…S, Select *xmodem* from the Popup window and press <enter>. Select [Go To] Tab and <Enter>

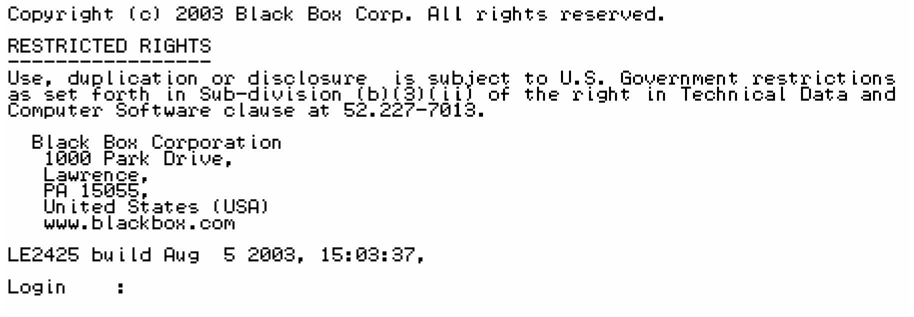
Step 6: You will get the window asking for the Directory. Give the full path of the directory where you have copied the Image file to upload and press <enter>.

Step 7: Select the file with the help of the spacebar and Press <Enter>. The download starts and proceeds to download the file. At the end of the transfer close the progress indicator window.

Step 8: The download starts and proceeds to download the file. You will get the message " Upgrade is Successful. Please reboot LE2425 now to start the application" at the end. If there is any error in the file transfer, you will get the error message " Upgrade failed " and the program will abort back to the (boot) prompt.

To Check the Successful Upgrade:

Once you restart the switch, you will get the **login** prompt on the Hyper Terminal (as shown below).



```
Copyright (c) 2003 Black Box Corp. All rights reserved.

RESTRICTED RIGHTS
-----------------
Use, duplication or disclosure  is subject to U.S. Government restrictions
as set forth in Sub-division (b)(3)(ii) of the right in Technical Data and
Computer Software clause at 52.227-7013.

  Black Box Corporation
   1000 Park Drive,
   Lawrence,
   PA 15055,
   United States (USA)
   www.blackbox.com

LE2425 build Aug  5 2003, 15:03:37,

Login    :
```

Upgrade over the Network

You can upgrade the software over the Network using **TFTP** or **FTP** protocol.

Syntax: **upgrade mode = <serial|tftp|ftp> [<ipaddress>] [file=<filename>]**