

# **Managed Switch User's Manual**

---

**ETHERLINE ACCESS M05T/M08T**

**Version 1.0, June 2017**



© 2017 U.I Lapp GmH. All rights reserved.

# Managed Switch User's Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

## Copyright Notice

©2017 U.I. Lapp GmbH.

All rights reserved.

Reproduction without permission is prohibited.

## Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of LAPP.

LAPP provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. LAPP reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, LAPP assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

## Contact Information

U.I. Lapp GmbH

Schulze-Delitzsch-Straße 25

D-70565 Stuttgart

Tel.: +49 (711) 78 38-01

Fax: +49 (711) 78 38-2640

E-Mail: [info@lappkabel.de](mailto:info@lappkabel.de)

# Table of Contents

<b>1. About this Manual .....</b>	<b>1-1</b>
<b>2. Getting Started.....</b>	<b>2-1</b>
Serial Console Configuration (115200, None, 8, 1, VT100).....	2-2
Configuration by Telnet Console .....	2-4
Configuration by Web Browser .....	2-6
Disabling Telnet and Browser Access.....	2-7
<b>3. Featured Functions .....</b>	<b>3-1</b>
Configuring Basic Settings .....	3-2
System Identification .....	3-2
Password.....	3-3
Accessible IP List.....	3-4
Port Settings.....	3-5
Network Parameters .....	3-6
GARP Timer Parameters .....	3-9
System Time Settings .....	3-9
Turbo Ring DIP Switch .....	3-11
System File Update.....	3-11
Restart.....	3-13
Reset to Factory Default.....	3-13
Loop Protection .....	3-13
Configuring SNMP .....	3-14
SNMP Read/Write Settings.....	3-15
Trap Settings.....	3-16
Private MIB Information .....	3-16
Using Traffic Prioritization .....	3-17
The Traffic Prioritization Concept.....	3-17
Configuring Traffic Prioritization .....	3-19
Using Virtual LAN.....	3-21
The Virtual LAN (VLAN) Concept.....	3-21
Sample Applications of VLANs Using LAPP Switches .....	3-23
Configuring Virtual LAN .....	3-24
VLAN Table.....	3-26
Using Multicast Filtering.....	3-27
The Concept of Multicast Filtering .....	3-27
Configuring IGMP Snooping .....	3-29
Static Multicast MAC Addresses .....	3-32
Configuring GMRP.....	3-33
GMRP Table .....	3-33
Using Bandwidth Management.....	3-33
Configuring Bandwidth Management .....	3-34
Using Auto Warning .....	3-35
Configuring Email Warning .....	3-35
Configuring Relay Warning .....	3-38
Using Line-Swap-Fast-Recovery.....	3-39
Configuring Line-Swap Fast Recovery .....	3-39
Using Set Device IP.....	3-39
Configuring Set Device IP .....	3-40
Configuring DHCP Relay Agent .....	3-41
Using Diagnosis.....	3-43
Mirror Port.....	3-43
Ping.....	3-43
LLDP Function.....	3-44
Using Monitor.....	3-45
Bandwidth Utilization Mode.....	3-45
Packet Counter Mode .....	3-45
Using the MAC Address Table .....	3-47
Using Event Log .....	3-47
Using Syslog .....	3-48
<b>4. ETHERLINE ACCESS Configurator GUI .....</b>	<b>4-1</b>
Starting ETHERLINE ACCESS Configurator .....	4-2
Broadcast Search.....	4-2
Search by IP Address .....	4-3
Upgrade Firmware .....	4-4
Modify IP Address.....	4-5
Export Configuration .....	4-5
Import Configuration.....	4-6
Unlock Server .....	4-6

Set Default .....	4-8
<b>A. MIB Groups .....</b>	<b>A-1</b>

## About this Manual

---

Thank you for purchasing a LAPP managed switch. Read this user's manual to learn how to connect your LAPP switch to Ethernet-enabled devices used for industrial applications.

The following two chapters are covered in this user manual:

□ **Chapter 2: Getting Started**

This chapter explains the initial installation process for LAPP switches. There are three ways to access a LAPP switch's configuration settings: serial console, Telnet console, and web console.

□ **Chapter 3: Featured Functions**

This chapter explains how to access a LAPP switch's various configuration, monitoring, and administration functions. These functions can be accessed by serial, Telnet, or web console. The web console is the most user-friendly way to configure a LAPP switch. In this chapter, we use the web console interface to introduce the functions.

## Getting Started

---

In this chapter we explain how to install a LAPP switch for the first time. There are three ways to access the LAPP switch's configuration settings: serial console, Telnet console, or web console. If you do not know the LAPP switch's IP address, you can open the serial console by connecting the LAPP switch to a PC's COM port with a short serial cable. You can open the Telnet or web console over an Ethernet LAN or over the Internet.

The following topics are covered in this chapter:

- ❑ **Serial Console Configuration (115200, None, 8, 1, VT100)**
- ❑ **Configuration by Telnet Console**
- ❑ **Configuration by Web Browser**
- ❑ **Disabling Telnet and Browser Access**

# Serial Console Configuration (115200, None, 8, 1, VT100)

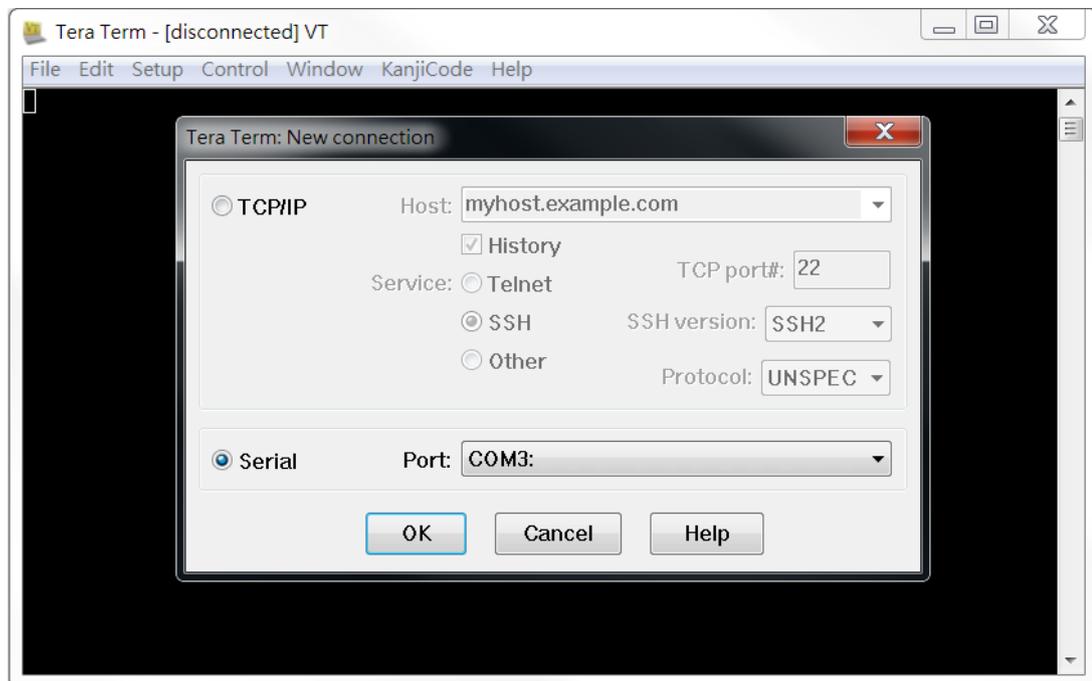
**NOTE**

- You cannot connect to the serial and Telnet console at the same time.
- You can connect to the web console and another console (serial or Telnet) at the same time. However, we strongly recommend that you do NOT do so. Following this advice will allow you to maintain better control over the LAPP switch's configuration.

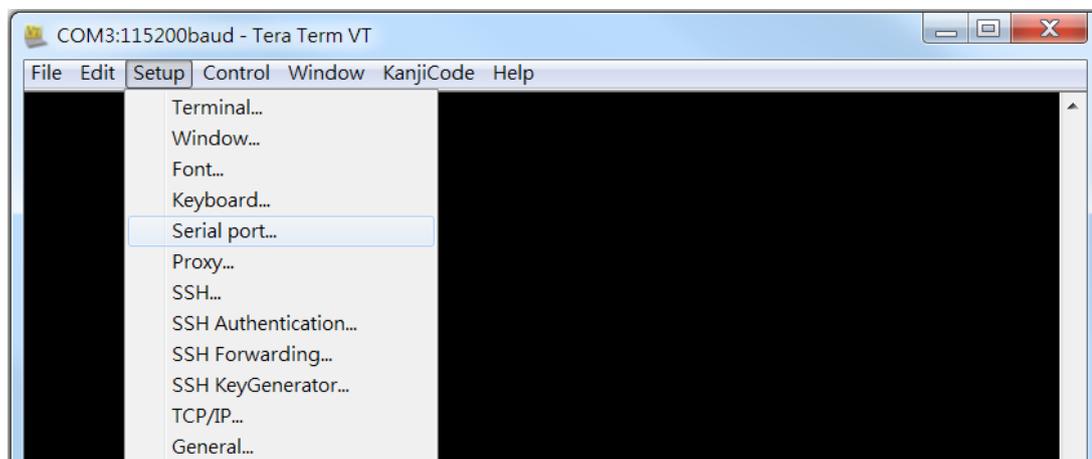
**NOTE** We recommend either using a commercial tool for serial communication or alternatively you can use a freeware tool like **PuTTY** or **Tera Term**.

Before running Tera Term, use an RJ45 to DB9-F (or RJ45 to DB25-F) cable to connect the LAPP switch's console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up).

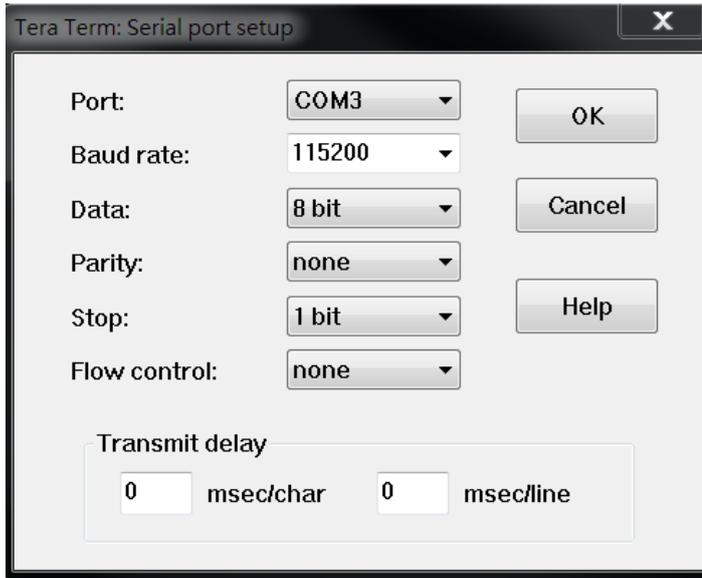
1. Open Tera Term and choose the serial port. Then click **OK**.



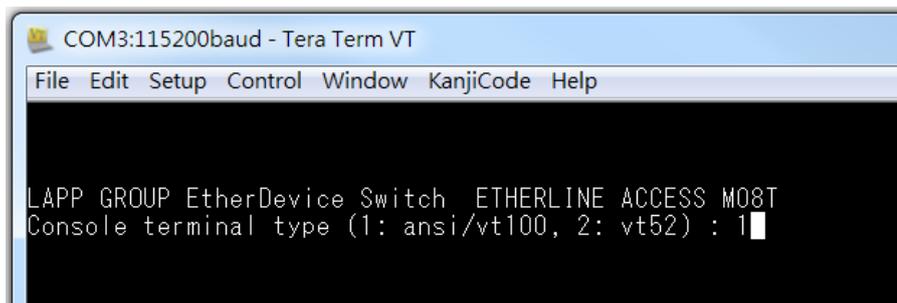
2. Select **Setup > Serial port....**



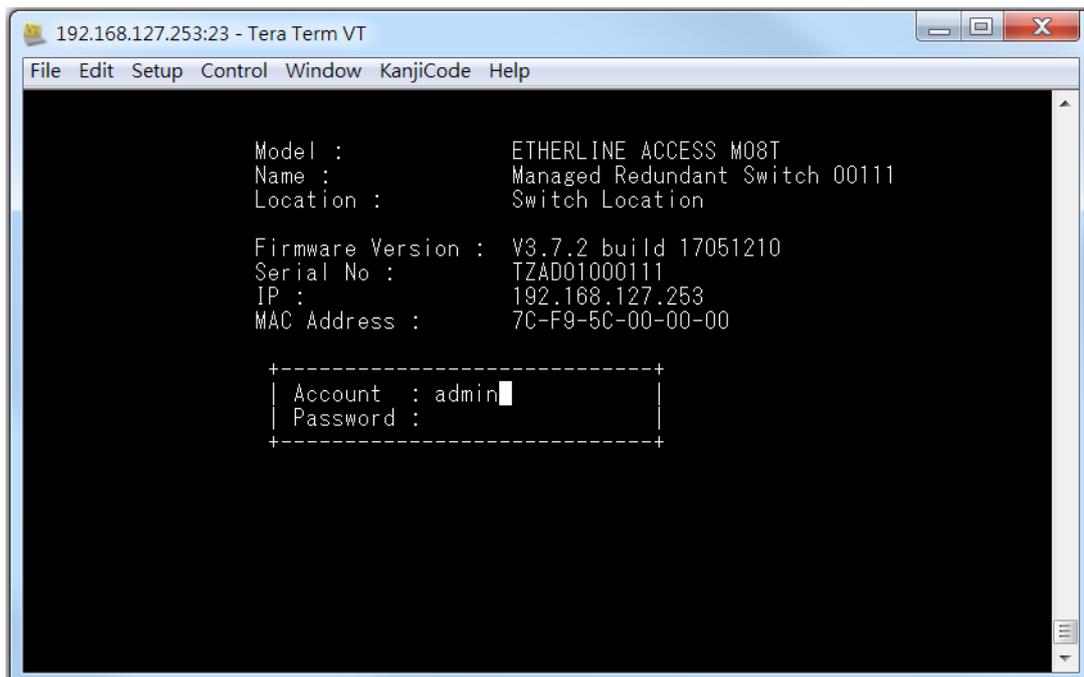
- The **Serial port setup** window should open. Set the fields as follows: **115200** for **Baud Rate**, **8** for **Data Bits**, **None** for **Parity**, and **1** for **Stop Bits**.



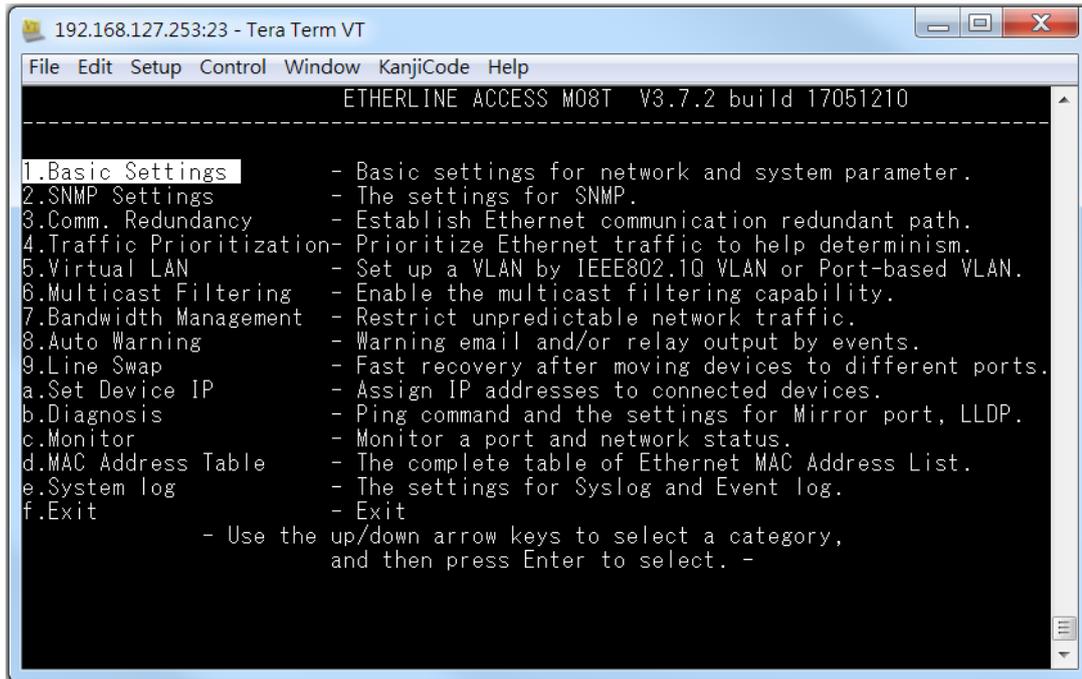
In the terminal window, the LAPP switch will prompt you to select a terminal type. Enter **1** to select **ansi/vt100** and then press **Enter**.



- The serial console will prompt you to log in. Press **Enter** and select **admin** or **user**. Use the down arrow key on your keyboard to select the **Password** field and enter a password if desired. This password will be required to access any of the consoles (web, serial, Telnet). If you do not wish to create a password, leave the **Password** field blank and press **Enter**.



5. The **Main Menu** of the LAPP switch’s serial console should appear.



6. Use the following keys on your keyboard to navigate the LAPP switch’s serial console:

Key	Function
Up, down, right, left arrow keys, Tab	Move the onscreen cursor
Enter	Display and select options
Space	Toggle options
Esc	Previous menu

## Configuration by Telnet Console

Opening the LAPP switch’s Telnet or web console over a network requires that the PC host and LAPP switch are on the same logical subnet. You may need to adjust your PC host’s IP address and subnet mask. By default, the LAPP switch’s IP address is 192.168.127.253 and the LAPP switch’s subnet mask is 255.255.255.0 (referred to as a Class B network). Your PC’s IP address must be set to 192.168.xxx.xxx if the subnet mask is 255.255.0.0, or to 192.168.127.xxx if the subnet mask is 255.255.255.0.

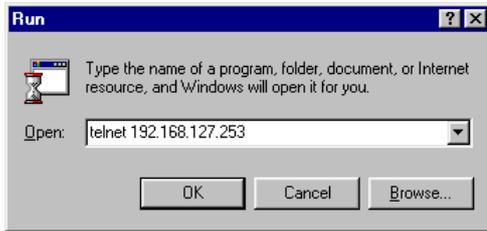
**NOTE** To connect to the LAPP switch’s Telnet or web console, your PC host and the LAPP switch must be on the same logical subnet.

**NOTE** When connecting to the LAPP switch’s Telnet or web console, first connect one of the LAPP switch’s Ethernet ports to your Ethernet LAN, or directly to your PC’s Ethernet port. You may use either a straight-through or cross-over Ethernet cable.

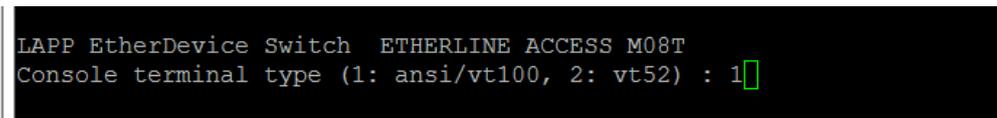
**NOTE** The LAPP switch’s default IP address is 192.168.127.253.

After making sure that the LAPP switch is connected to the same LAN and logical subnet as your PC, open the LAPP switch's Telnet console as follows:

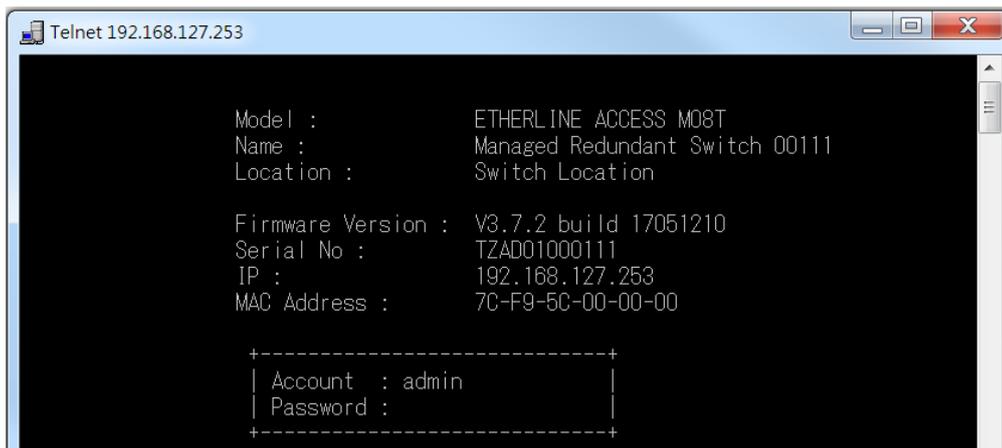
1. Click **Start** → **Run** from the Windows Start menu and then Telnet to the LAPP switch's IP address from the Windows **Run** window. You may also issue the Telnet command from a DOS prompt.



2. In the terminal window, the Telnet console will prompt you to select a terminal type. Type **1** to choose **ansi/vt100**, and then press **Enter**.



3. The Telnet console will prompt you to log in. Press **Enter** and then select **admin** or **user**. Use the down arrow key on your keyboard to select the **Password** field and enter a password if desired. This password will be required to access any of the consoles (web, serial, Telnet). If you do not wish to create a password, leave the **Password** field blank and press **Enter**.



4. The **Main Menu** of the LAPP switch's Telnet console should appear.



5. Use the following keys on your keyboard to navigate inside the LAPP switch’s Telnet console:

Key	Function
Up, down, right, left arrow keys, Tab	Move the onscreen cursor
Enter	Display and select options
Space	Toggle options
Esc	Previous menu

**NOTE** The Telnet console looks and operates in precisely the same manner as the serial console.

## Configuration by Web Browser

The LAPP switch’s web console is a convenient platform for modifying the configuration and accessing the built-in monitoring and network administration functions. You can open the LAPP switch’s web console using a standard web browser, such as Internet Explorer.

**NOTE** To connect to the LAPP switch’s Telnet or web console, your PC host and the LAPP switch must be on the same logical subnet.

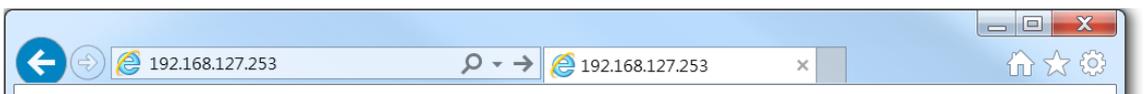
**NOTE** If the LAPP switch is configured for other VLAN settings, you must make sure your PC host is on the management VLAN.

**NOTE** When connecting to the LAPP switch’s Telnet or web console, first connect one of the LAPP switch’s Ethernet ports to your Ethernet LAN, or directly to your PC’s Ethernet port. You may use either a straight-through or cross-over Ethernet cable.

**NOTE** The LAPP switch’s default IP address is 192.168.127.253.

After making sure that the LAPP switch is connected to the same LAN and logical subnet as your PC, open the LAPP switch’s web console as follows:

1. Connect your web browser to the LAPP switch’s IP address by entering it in the **Address** or **URL** field.

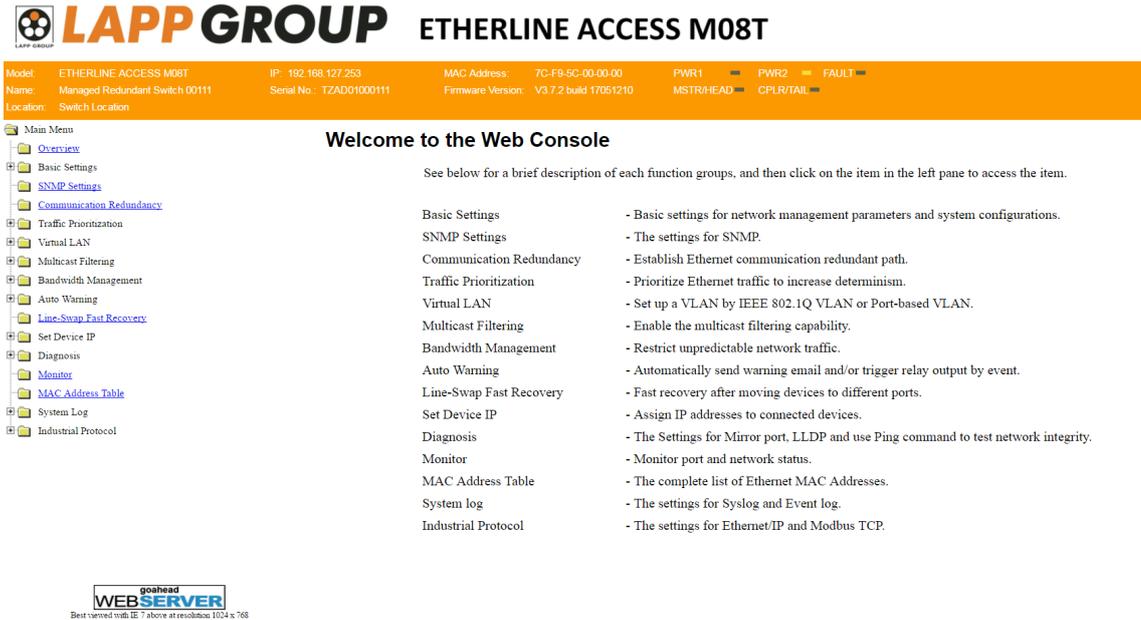


2. The LAPP switch’s web console will open, and you will be prompted to log in. Select the login account (admin or user) and enter the **Password**. This password will be required to access any of the consoles (web, serial, Telnet). If you do not wish to create a password, leave the **Password** field blank and press **Enter**.



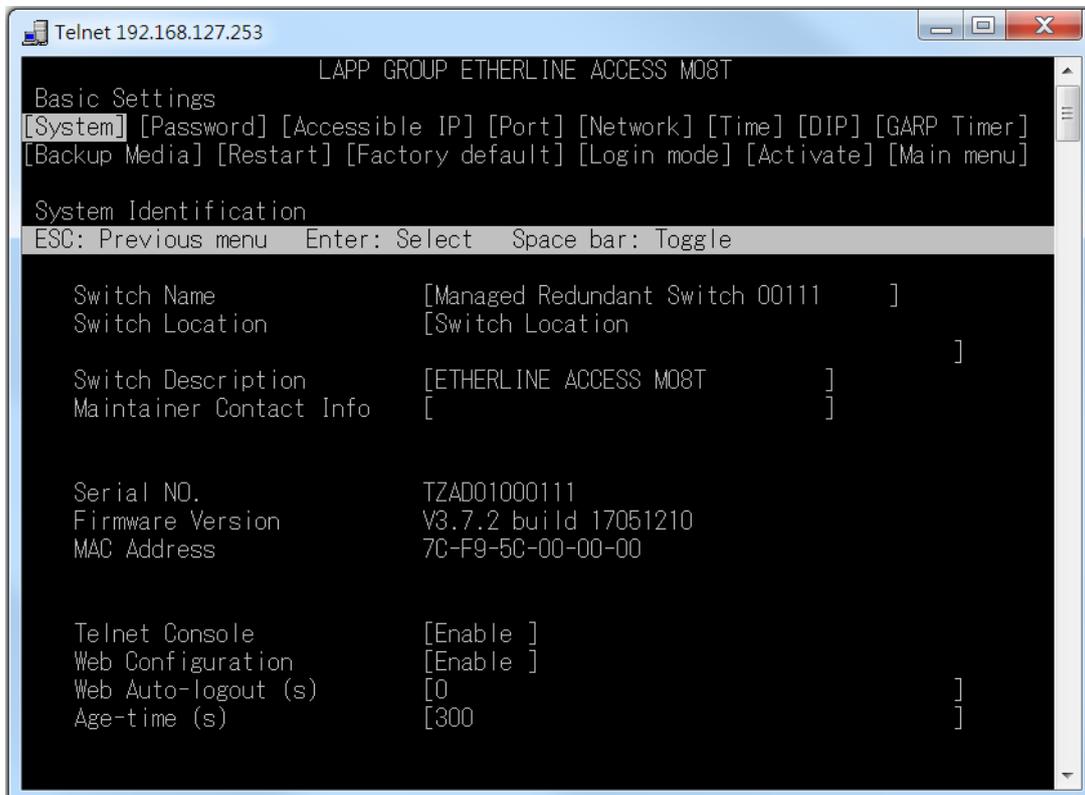
**NOTE** By default, no password is assigned to the LAPP switch’s web, serial, and Telnet consoles.

- After logging in, you may need to wait a few moments for the web console to appear. Use the folders in the left navigation panel to navigate between different pages of configuration options.



## Disabling Telnet and Browser Access

If you are connecting the LAPP switch to a public network but do not intend to manage it over the network, we suggest disabling both the Telnet and web consoles. This is done from the serial console by navigating to **System Identification** under **Basic Settings**. Disable or enable the **Telnet Console** and **Web Configuration** as shown below:



## Featured Functions

---

In this chapter, we explain how to access the LAPP switch's various configuration, monitoring, and administration functions. These functions can be accessed by serial, Telnet, or web console. The serial console can be used if you do not know the LAPP switch's IP address and requires that you connect the LAPP switch to a PC COM port. The Telnet and web consoles can be opened over an Ethernet LAN or the Internet.

The web console is the most user-friendly interface for configuring a LAPP switch. In this chapter, we use the web console interface to introduce the functions. There are only a few differences between the web console, serial console, and Telnet console.

The following topics are covered in this chapter:

- ❑ **Configuring Basic Settings**
- ❑ **Loop Protection**
- ❑ **Configuring SNMP**
- ❑ **Using Traffic Prioritization**
- ❑ **Using Virtual LAN**
- ❑ **Using Multicast Filtering**
- ❑ **Using Bandwidth Management**
- ❑ **Using Auto Warning**
- ❑ **Using Line-Swap-Fast-Recovery**
- ❑ **Using Set Device IP**
- ❑ **Using Diagnosis**
- ❑ **Using Monitor**
- ❑ **Using the MAC Address Table**
- ❑ **Using Event Log**
- ❑ **Using Syslog**

# Configuring Basic Settings

The **Basic Settings** section includes the most common settings required by administrators to maintain and control a LAPP switch.

## System Identification

**System Identification** items are displayed at the top of the web console and will be included in alarm emails. You can configure the System Identification items to make it easier to identify different switches that are connected to your network.

### System Identification

Switch Name	<input type="text" value="Managed Redundant Switch 00111"/>
Switch Location	<input type="text" value="Switch Location"/>
Switch Description	<input type="text" value="ETHERLINE ACCESS M08T"/>
Maintainer Contact Info	<input type="text"/>
Web Auto-logout (s)	<input type="text" value="0"/>
Age Time (s)	<input type="text" value="300"/>
CPU Loading (past 5 seconds)	<input type="text" value="1 %"/>
CPU Loading (past 30 seconds)	<input type="text" value="0 %"/>
CPU Loading (past 5 minutes)	<input type="text" value="0 %"/>
Free Memory	<input type="text" value="4929836"/>

**Activate**

#### Switch Name

Setting	Description	Factory Default
Max. 30 characters	This option is useful for differentiating between the roles or applications of different units. Example: Factory Switch 1.	Managed Redundant Switch [Serial no. of this switch]

#### Switch Location

Setting	Description	Factory Default
Max. 80 characters	This option is useful for differentiating between the locations of different units. Example: production line 1.	Switch Location

#### Switch Description

Setting	Description	Factory Default
Max. 30 characters	This option is useful for recording a more detailed description of the unit.	None

#### Maintainer Contact Info

Setting	Description	Factory Default
Max. 30 characters	This option is useful for providing information about who is responsible for maintaining this unit and how to contact this person.	None

**Web Auto-logout (S)**

Setting	Description	Factory Default
60 to 86400 (seconds)	Disable or extend the auto-logout time for the web management console.	0 (disabled)

**Age Time (S)**

Setting	Description	Factory Default
15 to 3825 (seconds)	The length of time that a MAC address entry can remain in the LAPP switch. When an entry reaches its aging time, it "ages out" and is purged from the switch, effectively cancelling frame forwarding to that specific port.	300

**CPU Loading**

Setting	Description	Factory Default
Read-only	The CPU usage volume in the past 5 seconds, 30 seconds, and 5 minutes.	None

**Free Memory**

Setting	Description	Factory Default
Read-only	The immediately free memory of the switch.	None

## Password

The LAPP switch provides two levels of configuration access. The **admin** account has read/write access of all configuration parameters, and the **user** account has read access only. A **user** account can view the configuration, but will not be able to make modifications.

### Password Setting

Account Name :

Old Password :

Type Old Password :

New Password :

Retype Password :



**ATTENTION**

By default, a password is not assigned to the LAPP switch's web, Telnet, and serial consoles. If a password is assigned, you will be required to enter the password when you open the serial console, Telnet console, or Web console.

**Account**

Setting	Description	Factory Default
Admin	This account can modify the LAPP switch's configuration.	admin
User	This account can only view the LAPP switch's configurations.	

**Password**

Setting	Description	Factory Default
Old password (max. 16 characters)	Enter the current password.	None
New password (Max. 16 characters)	Enter the desired new password. Leave it blank if you want to remove the password.	None
Retype password (Max. 16 characters)	Enter the desired new password again. Leave it blank if you want to remove the password.	None

## Accessible IP List

The LAPP switch uses an IP address-based filtering method to control access.

### Accessible IP List

Enable the accessible IP list ("Disable" will allow all IP's connection)

Index	IP	NetMask
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

**Activate**

You may add or remove IP addresses to limit access to the LAPP switch. When the accessible IP list is enabled, only addresses on the list will be allowed access to the LAPP switch. Each IP address and netmask entry can be tailored for different situations:

- Grant access to one host with a specific IP address**  
 For example, enter IP address 192.168.1.1 with netmask 255.255.255.255 to allow access to 192.168.1.1 only.
- Grant access to any host on a specific subnetwork**  
 For example, enter IP address 192.168.1.0 with netmask 255.255.255.0 to allow access to all IPs on the subnet defined by this IP address/subnet mask combination.
- Grant access to all hosts**  
 Make sure the accessible IP list is not enabled. Remove the checkmark from **Enable the accessible IP list**.

The following table shows additional configuration examples:

Hosts That Need Access	Input Format
Any host	Disable
192.168.1.120	192.168.1.120 / 255.255.255.255
192.168.1.1 to 192.168.1.254	192.168.1.0 / 255.255.255.0
192.168.0.1 to 192.168.255.254	192.168.0.0 / 255.255.0.0
192.168.1.1 to 192.168.1.126	192.168.1.0 / 255.255.255.128
192.168.1.129 to 192.168.1.254	192.168.1.128 / 255.255.255.128

# Port Settings

## Ethernet Port Settings

Port settings are included to give the user control over port access, port transmission speed, flow control, and port type (MDI or MDIX).

### Port Settings

Port	Enable	Description	Name	Speed	FDX Flow Ctrl	MDI/MDIX
1	<input checked="" type="checkbox"/>	100TX,RJ45.	<input type="text"/>	Auto ▾	Disable ▾	Auto ▾
2	<input checked="" type="checkbox"/>	100TX,RJ45.	<input type="text"/>	Auto ▾	Disable ▾	Auto ▾
3	<input checked="" type="checkbox"/>	100TX,RJ45.	<input type="text"/>	Auto ▾	Disable ▾	Auto ▾
4	<input checked="" type="checkbox"/>	100TX,RJ45.	<input type="text"/>	Auto ▾	Disable ▾	Auto ▾
5	<input checked="" type="checkbox"/>	100TX,RJ45.	<input type="text"/>	Auto ▾	Disable ▾	Auto ▾
6	<input checked="" type="checkbox"/>	100TX,RJ45.	<input type="text"/>	Auto ▾	Disable ▾	Auto ▾
7	<input checked="" type="checkbox"/>	100TX,RJ45.	<input type="text"/>	Auto ▾	Disable ▾	Auto ▾
8	<input checked="" type="checkbox"/>	100TX,RJ45.	<input type="text"/>	Auto ▾	Disable ▾	Auto ▾

Activate

#### Enable

Setting	Description	Factory Default
Checked	Allows data transmission through the port.	Enabled
Unchecked	Immediately shuts off port access.	



#### ATTENTION

If a connected device or sub-network is wreaking havoc on the rest of the network, the **Disable** option under **Advanced Settings/Port** gives the administrator a quick way to shut off access through this port immediately.

#### Description

Setting	Description	Factory Default
Media type	Displays the media type for each module's port	N/A

#### Name

Setting	Description	Factory Default
Max. 63 characters	Specifies an alias for the port to help administrators differentiate between different ports. Example: PLC 1	None

#### Speed

Setting	Description	Factory Default
Auto	Allows the port to use the IEEE 802.3u protocol to negotiate with connected devices. The port and connected devices will determine the best speed for that connection. Choose one of these fixed speed options if the connected Ethernet device has trouble auto-negotiating for line speed.	Auto
100M-Full		
100M-Half		
10M-Full		
10M-Half		

**FDX Flow Ctrl**

This setting enables or disables flow control for the port when the port’s Speed is set to Auto. The final result will be determined by the Auto process between the LAPP switch and connected devices.

Setting	Description	Factory Default
Enable	Enables flow control for this port when the port’s Speed is set to Auto.	Disabled
Disable	Disables flow control for this port when the port’s Speed is set to Auto.	

**MDI/MDIX**

Setting	Description	Factory Default
Auto	Allows the port to auto-detect the port type of the connected Ethernet device and change the port type accordingly.	Auto
MDI	Choose MDI or MDIX if the connected Ethernet device has trouble auto-negotiating for port type.	
MDIX		

## Network Parameters

Network configuration allows users to configure both IPv4 and IPv6 parameters for management access over the network. The LAPP switch supports both IPv4 and IPv6, and can be managed through either of these address types.

A brief explanation of each configuration item is given below.

### Network Parameters

**General Settings**

**IPv4**

Auto IP Configuration	<input type="text" value="Disable"/>
Switch IP Address	<input type="text" value="192.168.127.253"/>
Switch Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text"/>
1st DNS Server IP Address	<input type="text"/>
2nd DNS Server IP Address	<input type="text"/>
Dhcp Retry Periods	<input type="text" value="1"/> (1-30)
Dhcp Retry Times	<input type="text" value="0"/> (0-65535)

**IPv6**

Global Unicast Address Prefix	<input type="text"/>
Global Unicast Address	<input type="text" value="::"/>
Link-Local Address	<input type="text" value="fe80::290:e8ff:fe15:a97b"/>
	<input type="button" value="Activate"/>

## IP4

The IPv4 settings include the switch's IP address and subnet mask, as well as the IP address of the default gateway. In addition, input cells are provided for the IP addresses of a 1st and 2nd DNS server.

### **Auto IP Configuration**

Setting	Description	Factory Default
Disable	The LAPP switch's IP address must be set manually.	Disable
By DHCP	The LAPP switch's IP address will be assigned automatically by the network's DHCP server.	
By BootP	The LAPP switch's IP address will be assigned automatically by the network's BootP server.	

### **Switch IP Address**

Setting	Description	Factory Default
IP address for the LAPP switch	Assigns the LAPP switch's IP address on a TCP/IP network.	192.168.127.253

### **Switch Subnet Mask**

Setting	Description	Factory Default
Subnet mask for the LAPP switch	Identifies the type of network the LAPP switch is connected to (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network).	255.255.255.0

### **Default Gateway**

Setting	Description	Factory Default
IP address for gateway	Specifies the IP address of the router that connects the LAN to an outside network.	None

### **DNS IP Address**

Setting	Description	Factory Default
IP address for DNS server	Specifies the IP address of the DNS server used by your network. After specifying the DNS server's IP address, you can use the LAPP switch's URL (e.g., www.PT.company.com) to open the web console instead of entering the IP address.	None
IP address for 2nd DNS server	Specifies the IP address of the secondary DNS server used by your network. The LAPP switch will use the secondary DNS server if the first DNS server fails to connect.	None

### **DHCP Retry Periods**

Setting	Description	Factory Default
1 to 30	Users can configure the DHCP retry period manually	1

### **DHCP Retry Times**

Setting	Description	Factory Default
0 to 65535	Users can configure the times of DHCP retry manually	0

## IP6

The IPv6 settings include two distinct address types—Link-Local Unicast addresses and Global Unicast addresses. A Link-Local address makes the switch accessible over IPv6 for all devices attached to the same local subnet. To connect to a larger network with multiple segments, the switch must be configured with a Global Unicast address.

### **Global Unicast Address Prefix (Prefix Length: 64 bits) Default Gateway**

Setting	Description	Factory Default
Global Unicast Address Prefix	The prefix value must be formatted according to the RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.	None

### **Global Unicast Address**

Setting	Description	Factory Default
None	Displays the IPv6 Global Unicast address. The network portion of the Global Unicast address can be configured by specifying the Global Unicast Prefix and using an EUI-64 interface ID in the low order 64 bits. The host portion of the Global Unicast address is automatically generated using the modified EUI-64 form of the interface identifier (Switch's MAC address).	None

### **Link-Local Address**

Setting	Description	Factory Default
None	The network portion of the Link-Local address is FE80 and the host portion of the Link-Local address is automatically generated using the modified EUI-64 form of the interface identifier (Switch's MAC address)	None

## Neighbor Cache

IPv6 Address	Link Layer (MAC) Address	State
fe80::7ef9:5cff:fe00:0	7c-f9-5c-00-00-00	Reachable

### **Neighbor Cache**

Setting	Description	Factory Default
None	The information in the neighbor cache that includes the neighboring node's IPv6 address, the corresponding Link-Layer address, and the current state of the entry.	None

## GARP Timer Parameters

Generic Attribute Registration Protocol (GARP) was defined by the IEEE 802.1 working group to provide a generic framework. GARP defines the architecture, rules of operation, state machines, and variables for the registration and de-registration of attribute values.

The GARP Timer parameters are exchanged by creating the applications via GVRP (GARP VLAN Registration Protocol) to set the attributes of Timer.

Note that you need to set the same GARP timer values on all Layer 2 switches to ensure that the system works successfully.

### GARP Timer Parameters

Join Time (ms)	<input type="text" value="200"/>
Leave Time (ms)	<input type="text" value="600"/>
Leaveall Time (ms)	<input type="text" value="10000"/>

#### Join Time

Setting	Description	Factory Default
None	Specifies the period of the join time	200

#### Leave Time

Setting	Description	Factory Default
None	Specifies the period of leave time	600

#### Leaveall Time

Setting	Description	Factory Default
None	Specifies the period of leaveall time	10000

**NOTE** Leave Time should be at least two times more than Join Time, and Leaveall Time should be larger than Leave Time.

## System Time Settings

### System Time Settings

Current Time	<input type="text" value="--"/> : <input type="text" value="--"/> : <input type="text" value="--"/> (ex: 04:00:04)
Current Date	<input type="text" value="----"/> / <input type="text" value="--"/> / <input type="text" value="--"/> (ex: 2002/11/13)
Daylight Saving Time	<input type="text" value="Month"/> <input type="text" value="Week"/> <input type="text" value="Day"/> <input type="text" value="Hour"/>
Start Date	<input type="text" value="--"/> <input type="text" value="--"/> <input type="text" value="--"/>
End Date	<input type="text" value="--"/> <input type="text" value="--"/> <input type="text" value="--"/>
Offset	<input type="text" value="0"/> hour(s)

System Up Time	0d1h12m5s
Time Zone	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▾
1st Time Server IP/Name	<input type="text" value="time.nist.gov"/>
2nd Time Server IP/Name	<input type="text"/>
Time Server Query Period	600 secs
Time Protocol	Disable ▾
NTP/SNTP Server	<input type="checkbox"/> Enable

The LAPP switch has a time calibration function based on information from an NTP server or user specified time and date. Functions such as automatic warning emails can therefore include time and date stamp.

**NOTE** The LAPP switch does not have a real time clock. The user must update the Current Time and Current Date to set the initial time for the LAPP switch after each reboot, especially when there is no NTP server on the LAN or Internet connection.

**Current Time**

Setting	Description	Factory Default
User-specified time	Allows configuration of the local time in local 24-hour format.	None

**Current Date**

Setting	Description	Factory Default
User-specified date	Allows configuration of the local date in yyyy-mm-dd format.	None

**Daylight Saving Time**

The Daylight Saving Time settings are used to automatically set the LAPP switch’s time forward according to national standards.

**Start Date**

Setting	Description	Factory Default
User-specified date	Specifies the date that Daylight Saving Time begins.	None

**End Date**

Setting	Description	Factory Default
User-specified date	Specifies the date that Daylight Saving Time ends.	None

**Offset**

Setting	Description	Factory Default
User-specified hour	Specifies the number of hours that the time should be set forward during Daylight Saving Time.	None

**System Up Time**

Indicates how long the LAPP switch remained up since the last cold start. The up time is indicated in seconds.

**Time Zone**

Setting	Description	Factory Default
Time zone	Specifies the time zone, which is used to determine the local time offset from GMT (Greenwich Mean Time).	GMT (Greenwich Mean Time)

**NOTE** Changing the time zone will automatically correct the current time. Be sure to set the time zone before setting the time.

**Time Server IP/Name**

Setting	Description	Factory Default
IP address or name of time server	The IP or domain address (e.g., 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov).	None
IP address or name of secondary time server	The LAPP switch will try to locate the secondary NTP server if the first NTP server fails to connect.	

**Time Protocol**

Setting	Description	Factory Default
NTP	NTP (Network Time Protocol) is used to synchronize time with multiple time servers. The time accuracy is up to 50 ms.	-
SNTP	SNTP stands for Simple Network Time Protocol). The synchronization process of SNTP is simpler than NTP. The time accuracy is up to 1 second, which is suitable for low time accuracy requirements.	-

**Enable NTP/SNTP Server**

Setting	Description	Factory Default
Enable/Disable	Enables SNTP/NTP server functionality for clients	Disabled

## Turbo Ring DIP Switch

The **Turbo Ring DIP Switch** page allows users to disable the 4th DIP switch located on the device’s outer casing. The default is enabled with Turbo Ring v2 protocol. Once the user changes the 4th hardware DIP switch configuration to **ON**, the switch will start to initiate the Turbo Ring redundancy protocol based on the configuration. The detailed description is given below:

### Turbo Ring DIP Switch

Disable the Turbo Ring DIP Switch

1. To enable the entire set of Hardware DIP switches, uncheck the "Disable the Turbo Ring DIP Switch" option.
2. To disable the entire set of Hardware DIP switches, check the "Disable the Turbo Ring DIP Switch" option.

- Set DIP switch as Turbo Ring
- Set DIP switch as Turbo Ring V2

Activate

Setting	Description	Factory Default
Disable the Turbo Ring DIP switch	<b>Unchecked:</b> The Turbo Ring protocol will be activated automatically when the 4th DIP switch is moved to the ON position.	unchecked
	<b>Checked:</b> The Turbo Ring protocol will not be activated automatically, regardless of the position of the 4th DIP switch.	
Set DIP switch as Turbo Ring	If the DIP switch is enabled, Turbo Ring protocol will be enabled when the DIP switch is moved to the ON position.	Set DIP switch as Turbo Ring v2
Set DIP switch as Turbo Ring v2	If the DIP switch is enabled, Turbo Ring v2 protocol will be enabled when the DIP switch is moved to the ON position.	

**NOTE** If the 4th DIP switch (Turbo Ring) is configured to ON, you will not be able to disable the Turbo Ring DIP switch from the web interface, console, or Telnet.

**NOTE** If you would like to enable VLAN and/or port trunking on any of the last four ports, do not use the fourth DIP switch to activate Turbo Ring. In this case, you should use the Web, Telnet, or Serial console to activate Turbo Ring.

## System File Update

### Update System Files by Remote TFTP

The LAPP switch supports saving your configuration or log file to a remote TFTP server or local host. Other LAPP switches can also load the configuration at a later time. The LAPP switch also supports loading firmware or configuration files from the TFTP server or a local host.

### Update System Files by TFTP

TFTP Server IP/Name	<input type="text"/>		
Configuration Files Path and Name	<input type="text"/>	<input type="button" value="Download"/>	<input type="button" value="Upload"/>
Firmware Files Path and Name	<input type="text"/>	<input type="button" value="Download"/>	
Log Files Path and Name	<input type="text"/>		<input type="button" value="Upload"/>

#### TFTP Server IP/Name

Setting	Description	Factory Default
IP address of TFTP server	Specifies the IP address or name of the remote TFTP server. Must be specified before downloading or uploading files.	None

#### Configuration Files Path and Name

Setting	Description	Factory Default
Max. 40 characters	Specifies the path and file name of the LAPP switch's configuration file on the TFTP server.	None

#### Firmware Files Path and Name

Setting	Description	Factory Default
Max. 40 characters	Specifies the path and file name of the LAPP switch's firmware file.	None

#### Log Files Path and Name

Setting	Description	Factory Default
Max. 40 characters	Specifies the path and file name of the LAPP switch's log file.	None

After setting the desired paths and file names, click **Download** to download the prepared file from the remote TFTP server, or click **Upload** to upload the desired file to the remote TFTP server.

## Update System Files from Local PC

### Update System Files from Local PC

Configuration File	<input type="button" value="Export"/>		
Log File	<input type="button" value="Export"/>		
Upgrade Firmware	<input type="text"/>	<input type="button" value="Browse"/>	<input type="button" value="Import"/>
Upload Configure Data	<input type="text"/>	<input type="button" value="Browse"/>	<input type="button" value="Import"/>

#### Configuration File

Click **Export** to save the LAPP switch's configuration file to the local host.

#### Log File

Click **Export** to save the LAPP switch's log file to the local host.

**NOTE** Some operating systems will open the configuration file and log file directly in the web page. In such cases, right click the Export button to save the file.

#### Upgrade Firmware

To import a new firmware file into the LAPP switch, click **Browse** to select the firmware file that is saved on your computer. The upgrade procedure will proceed automatically after clicking **Import**.

**Upload Configure Data**

To import a configuration file into the LAPP switch, click **Browse** to select the configuration file already saved on your computer. The upgrade procedure will proceed automatically after clicking **Import**.

## Restart

This function provides users with a quick way to restart the system.

### Restart

This function will restart the system.

Activate

## Reset to Factory Default

### Reset to Factory Default

This function will reset all settings to their factory default values. Be aware that previous settings will be lost.

Activate

This function provides users with a quick way of restoring the LAPP switch's configuration to factory defaults. The function is available in the serial, Telnet, and web consoles.

**NOTE** After restoring the factory default configuration, you will need to use the default network settings to re-establish the web or Telnet console connection with the LAPP switch.

## Loop Protection

The switch is designed with a loop checking mechanism: Send a control BPDU from the Ethernet port and check if this control BPDU will be sent back to the switch again. If the looping occurs, the switch will automatically block the Ethernet port to prevent looping.

### Loop Protection

Enable

Activate

Check the Enable box and click Activate to enable the Loop protection.

# Configuring SNMP

The LAPP switch supports SNMP V1, V2c, and V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means that SNMP servers access all objects with read-only or read/write permissions using the community strings *public* and *private* by default. SNMP V3 requires that you select an authentication level of MD5 or SHA, and is the most secure protocol. You can also enable data encryption to enhance data security.

Supported SNMP security modes and levels are shown in the following table. Select the security mode and level that will be used to communicate between the SNMP agent and manager.

Protocol Version	UI Setting	Authentication	Encryption	Method
SNMP V1, V2c	V1, V2c Read Community	Community string	No	Uses a community string match for authentication.
	V1, V2c Write/Read Community	Community string	No	Uses a community string match for authentication.
SNMP V3	No-Auth	No	No	Uses an account with admin or user to access objects
	MD5 or SHA	Authentication based on MD5 or SHA	No	Provides authentication based on HMAC-MD5, or HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.
	MD5 or SHA	Authentication based on MD5 or SHA	Data encryption key	Provides authentication based on HMAC-MD5 or HMAC-SHA algorithms, and data encryption key. 8-character passwords and a data encryption key are the minimum requirements for authentication and encryption.

These parameters are configured on the SNMP page. A more detailed explanation of each parameter is given below the figure.

## SNMP

### SNMP Read/Write Settings

- SNMP Versions
- V1,V2c Read Community
- V1,V2c Write/Read Community
- Admin Auth. Type
- Admin Data Encryption Key
- User Auth. Type
- User Data Encryption Key

V1, V2c ▾  
  
  
 No-Auth ▾  
   
 No-Auth ▾

### Trap Settings

- 1st Trap Server IP/Name
- 1st Trap Community
- 2nd Trap Server IP/Name
- 2nd Trap Community

### Trap Mode

Trap ▾  
 Retries(1~99)   
 Timeout(1~300s)

### Private MIB information

Switch Object ID

enterprise.8691.7.7

## SNMP Read/Write Settings

### SNMP Versions

Setting	Description	Factory Default
V1, V2c, V3, or V1, V2c, or V3 only	Specifies the SNMP protocol version used to manage the switch.	V1, V2c

### V1, V2c Read Community

Setting	Description	Factory Default
Max. 30 characters	Specifies the community string to authenticate the SNMP agent for read-only access. The SNMP agent will access all objects with read-only permissions using this community string.	Public

### V1, V2c Write/Read Community

Setting	Description	Factory Default
Max. 30 characters	Specifies the community string to authenticate the SNMP agent for read/write access. The SNMP server will access all objects with read/write permissions using this community string.	Private

For SNMP V3, two levels of privilege are available accessing the LAPP switch. **Admin** privilege provides access and authorization to read and write the MIB file. **User** privilege allows reading of the MIB file only.

### Admin Auth. Type (for SNMP V1, V2c, V3, and V3 only)

Setting	Description	Factory Default
No-Auth	Allows the admin account to access objects without authentication.	No
MD5-Auth	Authentication will be based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	No
SHA-Auth	Authentication will be based on the HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	No

### Admin Data Encryption Key (for SNMP V1, V2c, V3, and V3 only)

Setting	Description	Factory Default
Enable	Enables data encryption using the specified data encryption key (between 8 and 30 characters).	No
Disable	Specifies that data will not be encrypted.	No

### User Auth. Type (for SNMP V1, V2c, V3 and V3 only)

Setting	Description	Factory Default
No-Auth	Allows the admin account and user account to access objects without authentication.	No
MD5-Auth	Authentication will be based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	No
SHA-Auth	Authentication will be based on the HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	No

### User Data Encryption Key (for SNMP V1, V2c, V3 and V3 only)

Setting	Description	Factory Default
Enable	Enables data encryption using the specified data encryption key (between 8 and 30 characters).	No
Disable	No data encryption	No

## Trap Settings

SNMP traps allow an SNMP agent to notify the NMS of a significant event. The switch supports two SNMP modes, **Trap** mode and **Inform** mode.

### SNMP Trap Mode—Trap

In Trap mode, the SNMP agent sends an SNMPv1 trap PDU to the NMS. No acknowledgment is sent back from the NMS so the agent has no way of knowing if the trap reached the NMS.

### SNMP Trap Mode—Inform

SNMPv2 provides an inform mechanism. When an inform message is sent from the SNMP agent to the NMS, the receiver sends a response to the sender acknowledging receipt of the event. This behavior is similar to that of the get and set requests. If the SNMP agent does not receive a response from the NMS for a period of time, the agent will resend the trap to the NMS agent. The maximum timeout time is 300 sec (default is 1 sec), and the maximum number of retries is 99 times (default is 1 time). When the SNMP agent receives acknowledgement from the NMS, it will stop resending the inform messages.

#### *1st Trap Server IP/Name*

Setting	Description	Factory Default
IP or name	Specifies the IP address or name of the primary trap server used by your network.	None

#### *1st Trap Community*

Setting	Description	Factory Default
Max. 30 characters	Specifies the community string to use for authentication.	Public

#### *2nd Trap Server IP/Name*

Setting	Description	Factory Default
IP or name	Specifies the IP address or name of the secondary trap server used by your network.	None

#### *2nd Trap Community*

Setting	Description	Factory Default
Max. 30 characters	Specifies the community string to use for authentication.	Public

## Private MIB Information

#### *Switch Object ID*

Setting	Description	Factory Default
Specific Switch ID	Indicates the switch's enterprise value.	Depends on switch model type

**NOTE:** The Switch Object ID cannot be changed.

# Using Traffic Prioritization

The LAPP switch's traffic prioritization capability provides Quality of Service (QoS) to your network by making data delivery more reliable. You can prioritize traffic on your network to ensure that high priority data is transmitted with minimum delay. Traffic can be controlled by a set of rules to obtain the required Quality of Service for your network. The rules define different types of traffic and specify how each type should be treated as it passes through the switch. The LAPP switch can inspect both IEEE 802.1p/1Q layer 2 CoS tags, and even layer 3 TOS information to provide consistent classification of the entire network. The LAPP switch's QoS capability improves the performance and determinism of industrial networks for mission critical applications.

## The Traffic Prioritization Concept

Traffic prioritization allows you to prioritize data so that time-sensitive and system-critical data can be transferred smoothly and with minimal delay over a network. The benefits of using traffic prioritization are:

- Improve network performance by controlling a wide variety of traffic and managing congestion.
- Assign priorities to different categories of traffic. For example, set higher priorities for time-critical or business-critical applications.
- Provide predictable throughput for multimedia applications, such as video conferencing or voice over IP, and minimize traffic delay and jitter.
- Improve network performance as the amount of traffic grows. Doing so will reduce costs since it will not be necessary to keep adding bandwidth to the network.

Traffic prioritization uses the four traffic queues that are present in your LAPP switch to ensure that high priority traffic is forwarded on a different queue from lower priority traffic. Traffic prioritization provides Quality of Service (QoS) to your network.

LAPP switch traffic prioritization depends on two industry-standard methods:

- **IEEE 802.1D**—a layer 2 marking scheme.
- **Differentiated Services (DiffServ)**—a layer 3 marking scheme.

### IEEE 802.1D Traffic Marking

The IEEE Std 802.1D, 1998 Edition marking scheme, which is an enhancement to IEEE Std 802.1D, enables Quality of Service on the LAN. Traffic service levels are defined in the IEEE 802.1Q 4-byte tag, which is used to carry VLAN identification as well as IEEE 802.1p priority information. The 4-byte tag immediately follows the destination MAC address and Source MAC address.

The IEEE Std 802.1D, 1998 Edition priority marking scheme assigns an IEEE 802.1p priority level between 0 and 7 to each frame. The priority marking scheme determines the level of service that this type of traffic should receive. Refer to the table below for an example of how different traffic types can be mapped to the eight IEEE 802.1p priority levels.

IEEE 802.1p Priority Level	IEEE 802.1D Traffic Type
0	Best Effort (default)
1	Background
2	Standard (spare)
3	Excellent Effort (business critical)
4	Controlled Load (streaming multimedia)
5	Video (interactive media); less than 100 milliseconds of latency and jitter
6	Voice (interactive voice); less than 10 milliseconds of latency and jitter
7	Network Control Reserved traffic

Even though the IEEE 802.1D standard is the most widely used prioritization scheme in the LAN environment, it still has some restrictions:

- It requires an additional 4-byte tag in the frame, which is normally optional for Ethernet networks. Without this tag, the scheme cannot work.
- The tag is part of the IEEE 802.1Q header, so to implement QoS at layer 2, the entire network must implement IEEE 802.1Q VLAN tagging.
- It is only supported on a LAN and not across routed WAN links, since the IEEE 802.1Q tags are removed when the packets pass through a router.

### Differentiated Services (DiffServ) Traffic Marking

DiffServ is a Layer 3 marking scheme that uses the DiffServ Code Point (DSCP) field in the IP header to store the packet priority information. DSCP is an advanced intelligent method of traffic marking that allows you to choose how your network prioritizes different types of traffic. DSCP uses 64 values that map to user-defined service levels, allowing you to establish more control over network traffic.

The advantages of DiffServ over IEEE 802.1D are:

- You can configure how you want your switch to treat selected applications and types of traffic by assigning various grades of network service to them.
- No extra tags are required in the packet.
- DSCP uses the IP header of a packet to preserve priority across the Internet.
- DSCP is backwards compatible with IPV4 TOS, which allows operation with existing devices that use a layer 3 TOS enabled prioritization scheme.

### Traffic Prioritization

LAPP switches classify traffic based on layer 2 of the OSI 7 layer model, and the switch prioritizes received traffic according to the priority information defined in the received packet. Incoming traffic is classified based upon the IEEE 802.1D frame and is assigned to the appropriate priority queue based on the IEEE 802.1p service level value defined in that packet. Service level markings (values) are defined in the IEEE 802.1Q 4-byte tag, and consequently traffic will only contain 802.1p priority markings if the network is configured with VLANs and VLAN tagging. The traffic flow through the switch is as follows:

- A packet received by the LAPP switch may or may not have an 802.1p tag associated with it. If it does not, then it is given a default 802.1p tag (which is usually 0). Alternatively, the packet may be marked with a new 802.1p value, which will result in all knowledge of the old 802.1p tag being lost.
- Because the 802.1p priority levels are fixed to the traffic queues, the packet will be placed in the appropriate priority queue, ready for transmission through the appropriate egress port. When the packet reaches the head of its queue and is about to be transmitted, the device determines whether or not the egress port is tagged for that VLAN. If it is, then the new 802.1p tag is used in the extended 802.1D header.
- The LAPP switch will check a packet received at the ingress port for IEEE 802.1D traffic classification, and then prioritize it based on the IEEE 802.1p value (service levels) in that tag. It is this 802.1p value that determines which traffic queue the packet is mapped to.

### Traffic Queues

The hardware of LAPP switches has multiple traffic queues that allow packet prioritization to occur. Higher priority traffic can pass through the LAPP switch without being delayed by lower priority traffic. As each packet arrives in the LAPP switch, it passes through any ingress processing (which includes classification, marking/re-marking), and is then sorted into the appropriate queue. The switch then forwards packets from each queue. LAPP switches support two different queuing mechanisms:

- **Weight Fair:** This method services all the traffic queues, giving priority to the higher priority queues. Under most circumstances, the Weight Fair method gives high priority precedence over low priority, but in the event that high priority traffic does not reach the link capacity, lower priority traffic is not blocked.
- **Strict:** This method services high traffic queues first; low priority queues are delayed until no more high priority data needs to be sent. The Strict method always gives precedence to high priority over low priority.

# Configuring Traffic Prioritization

Quality of Service (QoS) provides a traffic prioritization capability to ensure that important data is delivered consistently and predictably. The LAPP switch can inspect IEEE 802.1p/1Q layer 2 CoS tags, and even layer 3 TOS information, to provide a consistent classification of the entire network. The LAPP switch’s QoS capability improves your industrial network’s performance and determinism for mission critical applications.

## QoS Classification

### QoS Classification

Queuing Mechanism Weight Fair(8:4:2:1) ▼

Port	Inspect ToS	Inspect CoS	Port Priority
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3(Normal) ▼
2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3(Normal) ▼
3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3(Normal) ▼
4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3(Normal) ▼
5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3(Normal) ▼
6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3(Normal) ▼
7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3(Normal) ▼
8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3(Normal) ▼

**Activate**

The LAPP switch supports inspection of layer 3 TOS and/or layer 2 CoS tag information to determine how to classify traffic packets.

#### Queuing Mechanism

Setting	Description	Factory Default
Weight Fair	The LAPP switch has 4 priority queues. In the weight fair scheme, an 8, 4, 2, 1 weighting is applied to the four priorities. This approach prevents the lower priority frames from being starved of opportunity for transmission with only a slight delay to the higher priority frames.	Weight Fair
Strict	In the Strict-priority scheme, all top-priority frames egress a port until that priority’s queue is empty, and then the next lower priority queue’s frames egress. This approach can cause the lower priorities to be starved of opportunity for transmitting any frames but ensures that all high priority frames will egress the switch as soon as possible.	

#### Inspect TOS

Setting	Description	Factory Default
Enable/Disable	Enables or disables the LAPP switch for inspecting Type of Service (TOS) bits in the IPV4 frame to determine the priority of each frame.	Enabled

**Inspect COS**

Setting	Description	Factory Default
Enable/Disable	Enables or disables the LAPP switch for inspecting 802.1p COS tags in the MAC frame to determine the priority of each frame.	Enabled

**Inspect Port Priority**

Setting	Description	Factory Default
Port priority	The port priority has 4 priority queues. Low, normal, medium, high priority queue option is applied to each port.	3(Normal)

**NOTE** The priority of an ingress frame is determined in the following order:

1. Inspect TOS
2. Inspect CoS
3. Port Priority

**NOTE** The designer can enable these classifications individually or in combination. For instance, if a “hot” higher priority port is required for a network design, **Inspect TOS** and **Inspect CoS** can be disabled. This setting leaves only port default priority active, which results in all ingress frames being assigned the same priority on that port.

**CoS Mapping**

**Mapping Table of CoS Value and Priority Queues**

CoS	Priority Queue
0	Low
1	Low
2	Normal
3	Normal
4	Medium
5	Medium
6	High
7	High

**Activate**

**CoS Value and Priority Queues**

Setting	Description	Factory Default
Low/Normal/ Medium/High	Maps different CoS values to 4 different egress queues.	0: Low 1: Low 2: Normal 3: Normal 4: Medium 5: Medium 6: High 7: High

## TOS/DiffServ Mapping

### Mapping Table of ToS (DSCP) Value and Priority Queues

ToS	Level	ToS	Level	ToS	Level	ToS	Level
0x00(1)	Low	0x04(2)	Low	0x08(3)	Low	0x0C(4)	Low
0x10(5)	Low	0x14(6)	Low	0x18(7)	Low	0x1C(8)	Low
0x20(9)	Low	0x24(10)	Low	0x28(11)	Low	0x2C(12)	Low
0x30(13)	Low	0x34(14)	Low	0x38(15)	Low	0x3C(16)	Low
0x40(17)	Normal	0x44(18)	Normal	0x48(19)	Normal	0x4C(20)	Normal
0x50(21)	Normal	0x54(22)	Normal	0x58(23)	Normal	0x5C(24)	Normal
0x60(25)	Normal	0x64(26)	Normal	0x68(27)	Normal	0x6C(28)	Normal
0x70(29)	Normal	0x74(30)	Normal	0x78(31)	Normal	0x7C(32)	Normal
0x80(33)	Medium	0x84(34)	Medium	0x88(35)	Medium	0x8C(36)	Medium
0x90(37)	Medium	0x94(38)	Medium	0x98(39)	Medium	0x9C(40)	Medium
0xA0(41)	Medium	0xA4(42)	Medium	0xA8(43)	Medium	0xAC(44)	Medium
0xB0(45)	Medium	0xB4(46)	Medium	0xB8(47)	Medium	0xBC(48)	Medium
0xC0(49)	High	0xC4(50)	High	0xC8(51)	High	0xCC(52)	High
0xD0(53)	High	0xD4(54)	High	0xD8(55)	High	0xDC(56)	High

Activate

#### ToS (DSCP) Value and Priority Queues

Setting	Description	Factory Default
Low/Normal/ Medium/High	Maps different TOS values to 4 different egress queues.	1 to 16: Low 17 to 32: Normal 33 to 48: Medium 49 to 64: High

## Using Virtual LAN

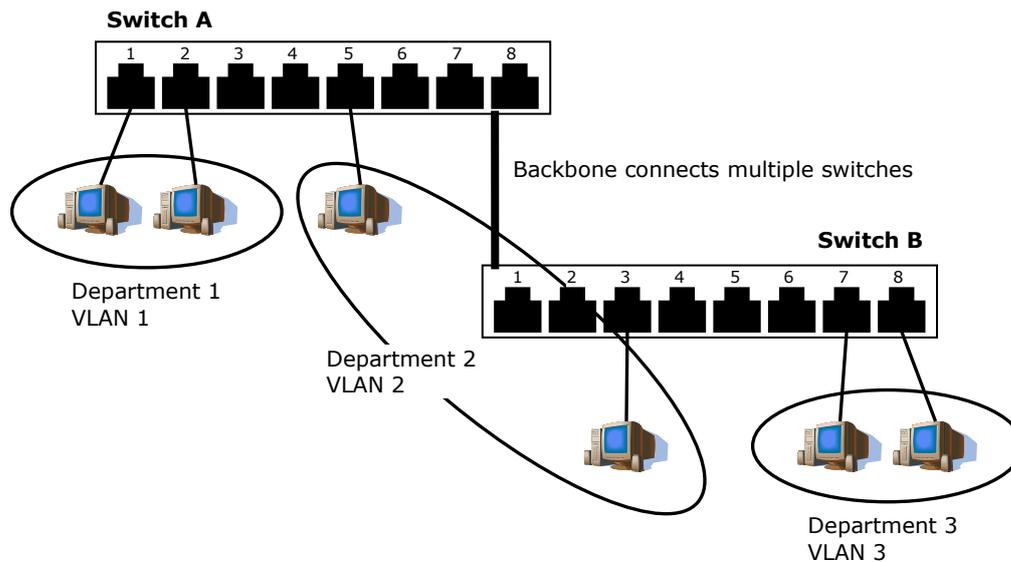
Setting up Virtual LANs (VLANs) on your LAPP switch increases the efficiency of your network by dividing the LAN into logical segments, as opposed to physical segments. In general, VLANs are easier to manage.

### The Virtual LAN (VLAN) Concept

#### What is a VLAN?

A VLAN is a group of devices that can be located anywhere on a network, but which communicate as if they are on the same physical segment. With VLANs, you can segment your network without being restricted by physical connections—a limitation of traditional network design. With VLANs you can segment your network according into:

- **Departmental groups**—You could have one VLAN for the marketing department, another for the finance department, and another for the product development department.
- **Hierarchical groups**—You could have one VLAN for directors, another for managers, and another for general staff.
- **Usage groups**—You could have one VLAN for email users and another for multimedia users.



### Benefits of VLANs

The main benefit of VLANs is that they provide a network segmentation system that is far more flexible than traditional networks. Using VLANs also provides you with three other benefits:

- **VLANs ease the relocation of devices on networks:** With traditional networks, network administrators spend much of their time dealing with moves and changes. If users move to a different subnetwork, the addresses of each host must be updated manually. With a VLAN setup, if a host originally on VLAN Marketing, for example, is moved to a port on another part of the network, and retains its original subnet membership, you only need to specify that the new port is on VLAN Marketing. You do not need to do any re-cabling.
- **VLANs provide extra security:** Devices within each VLAN can only communicate with other devices on the same VLAN. If a device on VLAN Marketing needs to communicate with devices on VLAN Finance, the traffic must pass through a routing device or Layer 3 switch.
- **VLANs help control traffic:** With traditional networks, congestion can be caused by broadcast traffic that is directed to all network devices, regardless of whether or not they need it. VLANs increase the efficiency of your network because each VLAN can be set up to contain only those devices that need to communicate with each other.

### VLANs and the Rackmount switch

Your LAPP switch provides support for VLANs using IEEE Std 802.1Q-1998. This standard allows traffic from multiple VLANs to be carried across one physical link. The IEEE Std 802.1Q-1998 standard allows each port on your LAPP switch to be placed as follows:

- On a single VLAN defined in the LAPP switch
- On several VLANs simultaneously using 802.1Q tagging

The standard requires that you define the *802.1Q VLAN ID* for each VLAN on your LAPP switch before the switch can use it to forward traffic:

### Managing a VLAN

A new or initialized LAPP switch contains a single VLAN—the Default VLAN. This VLAN has the following definition:

- *VLAN Name*—Management VLAN
- *802.1Q VLAN ID*—1 (if tagging is required)

All the ports are initially placed on this VLAN, and it is the only VLAN that allows you to access the management software of the LAPP switch over the network.

### Communication Between VLANs

If devices connected to a VLAN need to communicate to devices on a different VLAN, a router or Layer 3 switching device with connections to both VLANs needs to be installed. Communication between VLANs can only take place if they are all connected to a routing or Layer 3 switching device.

### VLANs: Tagged and Untagged Membership

The LAPP switch supports 802.1Q VLAN tagging, a system that allows traffic for multiple VLANs to be carried on a single physical link (backbone, trunk). When setting up VLANs you need to understand when to use untagged and tagged membership of VLANs. Simply put, if a port is on a single VLAN it can be an untagged member, but if the port needs to be a member of multiple VLANs, tagged membership must be defined.

A typical host (e.g., clients) will be untagged members of one VLAN, defined as an **Access Port** in a LAPP switch, while inter-switch connections will be tagged members of all VLANs, defined as a **Trunk Port** in a LAPP switch.

The IEEE Std 802.1Q-1998 defines how VLANs operate within an open packet-switched network. An 802.1Q compliant packet carries additional information that allows a switch to determine which VLAN the port belongs to. If a frame is carrying the additional information, it is known as a *tagged* frame.

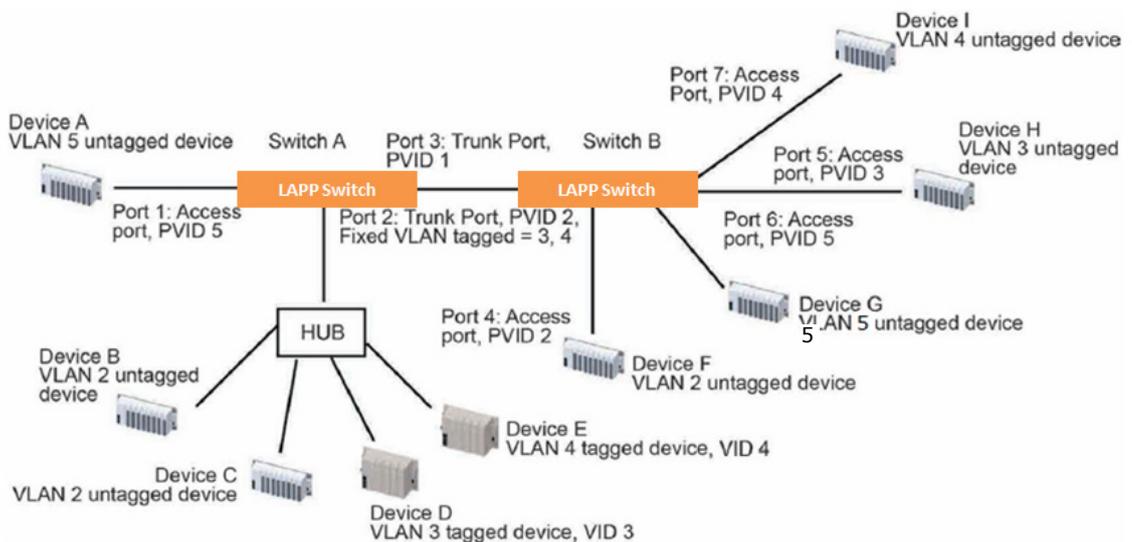
To carry multiple VLANs across a single physical link (backbone, trunk), each packet must be tagged with a VLAN identifier so that the switches can identify which packets belong in which VLAN. To communicate between VLANs, a router must be used.

The LAPP switch supports three types of VLAN port settings:

- **Access Port:** The port connects to a single device that is not tagged. The user must define the default port PVID that assigns which VLAN the device belongs to. Once the ingress packet of this Access Port egresses to another Trunk Port (the port needs all packets to carry tag information), the LAPP switch will insert this PVID into this packet so the next 802.1Q VLAN switch can recognize it.
- **Trunk Port:** The port connects to a LAN that consists of untagged devices, tagged devices and/or switches and hubs. In general, the traffic of the Trunk Port must have a Tag. Users can also assign a PVID to a Trunk Port. The untagged packet on the Trunk Port will be assigned the port default PVID as its VID.
- **Hybrid Port:** The port is similar to a Trunk port, except users can explicitly assign tags to be removed from egress packets.

The following section illustrates how to use these ports to set up different applications.

## Sample Applications of VLANs Using LAPP Switches



In this application,

- Port 1 connects a single untagged device and assigns it to VLAN 5; it should be configured as **Access Port** with PVID 5.
- Port 2 connects a LAN with two untagged devices belonging to VLAN 2. One tagged device with VID 3 and one tagged device with VID 4. It should be configured as **Trunk Port** with PVID 2 for untagged device and Fixed VLAN (Tagged) with 3 and 4 for tagged device. Since each port can only have one unique PVID, all untagged devices on the same port must belong to the same VLAN.
- Port 3 connects with another switch. It should be configured as **Trunk Port** GVRP protocol will be used through the Trunk Port.
- Port 4 connects a single untagged device and assigns it to VLAN 2; it should be configured as **Access Port** with PVID 2.
- Port 5 connects a single untagged device and assigns it to VLAN 3; it should be configured as **Access Port** with PVID 3.
- Port 6 connect a single untagged device and assigns it to VLAN 5; it should be configured as **Access Port** with PVID 5.
- Port 7 connects a single untagged device and assigns it to VLAN 4; it should be configured as **Access Port** with PVID 4.

After the application is properly configured:

- Packets from Device A will travel through **Trunk Port 3** with tagged VID 5. Switch B will recognize its VLAN, pass it to port 6, and then remove tags received successfully by Device G, and vice versa.
- Packets from Devices B and C will travel through **Trunk Port 3** with tagged VID 2. Switch B recognizes its VLAN, passes it to port 4, and then removes tags received successfully by Device F, and vice versa.
- Packets from Device D will travel through **Trunk Port 3** with tagged VID 3. Switch B will recognize its VLAN, pass to port 5, and then remove tags received successfully by Device H. Packets from Device H will travel through **Trunk Port 3** with PVID 3. Switch A will recognize its VLAN and pass it to port 2, but will not remove tags received successfully by Device D.
- Packets from Device E will travel through **Trunk Port 3** with tagged VID 4. Switch B will recognize its VLAN, pass it to port 7, and then remove tags received successfully by Device I. Packets from Device I will travel through **Trunk Port 3** with tagged VID 4. Switch A will recognize its VLAN and pass it to port 2, but will not remove tags received successfully by Device E.

## Configuring Virtual LAN

### VLAN Settings

To configure 802.1Q VLAN and port-based VLANs on the LAPP switch, use the **VLAN Settings** page to configure the ports.

#### VLAN Mode

Setting	Description	Factory Default
802.1Q VLAN	Set VLAN mode to 802.1Q VLAN	802.1Q VLAN
Port-based VLAN	Set VLAN mode to Port-based VLAN	

## 802.1Q VLAN Settings

### 802.1Q VLAN Settings

VLAN Mode

Management VLAN ID

Enable GVRP

Port	Type	PVID	Fixed VLAN (Tagged)	Fixed VLAN (Untagged)	Forbidden VLAN
1	Access ▼	1			
2	Access ▼	1			
3	Access ▼	1			
4	Access ▼	1			
5	Access ▼	1			
6	Access ▼	1			
7	Access ▼	1			
8	Access ▼	1			

Activate

#### Management VLAN ID

Setting	Description	Factory Default
VLAN ID from 1 to 4094	Assigns the VLAN ID of this switch.	1

#### Port Type

Setting	Description	Factory Default
Access	Port type is used to connect single devices without tags.	Access
Trunk	Select Trunk port type to connect another 802.1Q VLAN aware switch	
Hybrid	Select Hybrid port to connect another Access 802.1Q VLAN aware switch or another LAN that combines tagged and/or untagged devices and/or other switches/hubs.	



#### ATTENTION

For communication redundancy in the VLAN environment, set **Redundant Port Coupling Port** and **Coupling Control Port** as **Trunk Port** since these ports act as the **backbone** to transmit all packets of different VLANs to different switch units.

#### Port PVID

Setting	Description	Factory Default
VID ranges from 1 to 4094	Sets the default VLAN ID for untagged devices that connect to the port.	1

#### Fixed VLAN List (Tagged)

Setting	Description	Factory Default
VID ranges from 1 to 4094	This field will be active only when selecting the Trunk or Hybrid port type. Set the other VLAN ID for tagged devices that connect to the port. Use commas to separate different VIDs.	None

**Fixed VLAN List (Untagged)**

Setting	Description	Factory Default
VID range from 1 to 4094	This field will be active only when selecting the Hybrid port type. Set the other VLAN ID for tagged devices that connect to the port and tags that need to be removed in egress packets. Use commas to separate different VIDs.	None

**Forbidden VLAN List**

Setting	Description	Factory Default
VID ranges from 1 to 4094	This field will be active only when selecting the Trunk or Hybrid port type. Set the other VLAN IDs that will not be supported by this port. Use commas to separate different VIDs.	None

## Port-Based VLAN Settings

Check each specific port to assign its VLAN ID in the table. The maximum VLAN ID is the same as your number of switch ports.

**Port-based VLAN Settings**

VLAN Mode Port-based VLAN ▾

VLAN	Port							
	1	2	3	4	5	6	7	8
1	<input checked="" type="checkbox"/>							
2	<input type="checkbox"/>							
3	<input type="checkbox"/>							
4	<input type="checkbox"/>							
5	<input type="checkbox"/>							
6	<input type="checkbox"/>							
7	<input type="checkbox"/>							
8	<input type="checkbox"/>							

Activate

**NOTE** IGMP Snooping will be disabled when Port-Based VLAN is enabled.

## VLAN Table

**VLAN Table**

**VLAN Mode**  
 VLAN Mode 802.1Q VLAN

**Management VLAN**  
 Management VLAN 1

**Current 802.1Q VLAN List**

Index	VID	Joined Access Port	Joined Trunk Port	Joined Hybrid Port
1	1	1, 2, 3, 4, 5, 6, 7, 8,		

Use the **802.1Q VLAN table** to review the VLAN groups that were created, **Joined Access Ports**, **Trunk Ports**, and **Hybrid Ports**, and use the **Port-based VLAN table** to review the VLAN group and **Joined Ports**.

# Using Multicast Filtering

Multicast filtering improves the performance of networks that carry multicast traffic. This section explains multicasts, multicast filtering, and how multicast filtering can be implemented on your LAPP switch.

## The Concept of Multicast Filtering

### What is an IP Multicast?

A *multicast* is a packet sent by one host to multiple hosts. Only those hosts that belong to a specific multicast group will receive the multicast. If the network is set up correctly, a multicast can only be sent to an end-station or a subset of end-stations on a LAN or VLAN that belong to the multicast group. Multicast group members can be distributed across multiple subnets, so that multicast transmissions can occur within a campus LAN or over a WAN. In addition, networks that support IP multicast send only *one* copy of the desired information across the network until the delivery path that reaches group members diverges. To make more efficient use of network bandwidth, it is only at these points that multicast packets are duplicated and forwarded. A multicast packet has a multicast group address in the destination address field of the packet's IP header.

### Benefits of Multicast

The benefits of using IP multicast are:

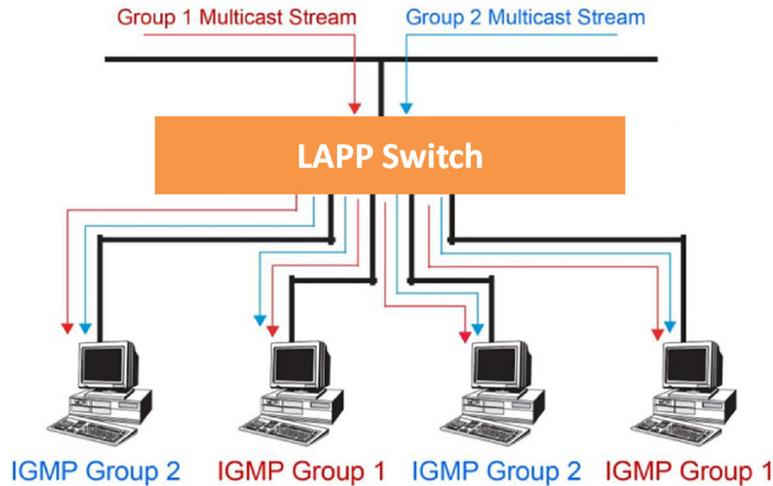
- It uses the most efficient, sensible method to deliver the same information to many receivers with only one transmission.
- It reduces the load on the source (for example, a server) since it will not need to produce several copies of the same data.
- It makes efficient use of network bandwidth and scales well as the number of multicast group members increases.
- Works with other IP protocols and services, such as Quality of Service (QoS).

Multicast transmission makes more sense and is more efficient than unicast transmission for some applications. For example, multicasts are often used for video-conferencing, since high volumes of traffic must be sent to several end-stations at the same time, but where broadcasting the traffic to all end-stations would cause a substantial reduction in network performance. Furthermore, several industrial automation protocols, such as Allen-Bradley, EtherNet/IP, Siemens Profibus, and Foundation Fieldbus HSE (High Speed Ethernet), use multicast. These industrial Ethernet protocols use publisher/subscriber communications models by multicasting packets that could flood a network with heavy traffic. IGMP Snooping is used to prune multicast traffic so that it travels only to those end destinations that require the traffic, reducing the amount of traffic on the Ethernet LAN.

### Multicast Filtering

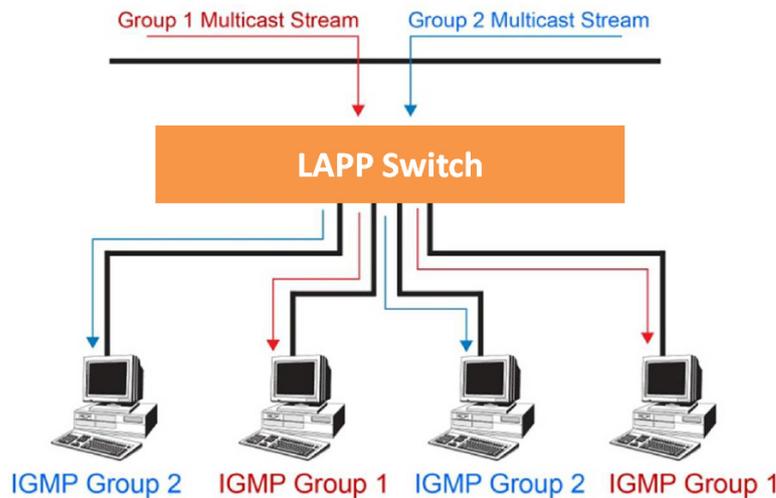
Multicast filtering ensures that only end-stations that have joined certain groups receive multicast traffic. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to registered end-stations. The following two figures illustrate how a network behaves without multicast filtering, and with multicast filtering.

**Network without multicast filtering**



All hosts receive the multicast traffic, even if they don't need it.

**Network with multicast filtering**



Hosts only receive dedicated traffic from other hosts belonging to the same group.

**Multicast Filtering and LAPP's Industrial Rackmount Switches**

The LAPP switch has three ways to achieve multicast filtering: IGMP (Internet Group Management Protocol) Snooping, GMRP (GARP Multicast Registration Protocol), and adding a static multicast MAC manually to filter multicast traffic automatically.

**Snooping Mode**

Snooping Mode allows your switch to forward multicast packets only to the appropriate ports. The switch **snoops** on exchanges between hosts and an IGMP device, such as a router, to find those ports that want to join a multicast group, and then configures its filters accordingly.

**IGMP Snooping Enhanced Mode**

Snooping Enhanced Mode allows your switch to forward multicast packets to the LAPP switch's member port only. If you disable Enhanced Mode, data streams will run to the querier port as well as the member port.

**Query Mode**

Query mode allows the LAPP switch to work as the Querier if it has the lowest IP address on the subnetwork to which it belongs.

IGMP querying is enabled by default on the LAPP switch to ensure proceeding query election. Enable query mode to run multicast sessions on a network that does not contain IGMP routers (or queriers). Query mode allows users to enable IGMP snooping by VLAN ID. LAPP switches support IGMP snooping version 1 and version 2.

### IGMP Multicast Filtering

IGMP is used by IP-supporting network devices to register hosts with multicast groups. It can be used on all LANs and VLANs that contain a multicast capable IP router, and on other network devices that support multicast filtering. LAPP switches support IGMP version 1 and 2. IGMP version 1 and 2 work as follows:

- The IP router (or querier) periodically sends query packets to all end-stations on the LANs or VLANs that are connected to it. For networks with more than one IP router, the router with the lowest IP address is the querier. A switch with IP address lower than the IP address of any other IGMP queriers connected to the LAN or VLAN can become the IGMP querier.
- When an IP host receives a query packet, it sends a report packet back that identifies the multicast group that the end-station would like to join.
- When the report packet arrives at a port on a switch with IGMP Snooping enabled, the switch knows that the port should forward traffic for the multicast group, and then proceeds to forward the packet to the router.
- When the router receives the report packet, it registers that the LAN or VLAN requires traffic for the multicast groups.
- When the router forwards traffic for the multicast group to the LAN or VLAN, the switches only forward the traffic to ports that received a report packet.

#### IGMP version comparison

IGMP Version	Main Features	Reference
V1	a. Periodic query	RFC-1112
V2	Compatible with V1 and adds: a. Group-specific query b. Leave group messages c. Resends specific queries to verify leave message was the last one in the group d. Querier election	RFC-2236

### GMRP (GARP Multicast Registration Protocol)

LAPP switches support IEEE 802.1D-1998 GMRP (GARP Multicast Registration Protocol), which is different from IGMP (Internet Group Management Protocol). GMRP is a MAC-based multicast management protocol, whereas IGMP is IP-based. GMRP provides a mechanism that allows bridges and end stations to register or de-register Group membership information dynamically. GMRP functions similarly to GVRP, except that GMRP registers multicast addresses on ports. When a port receives a **GMRP-join** message, it will register the multicast address to its database if the multicast address is not registered, and all the multicast packets with that multicast address are able to be forwarded from this port. When a port receives a **GMRP-leave** message, it will de-register the multicast address from its database, and all the multicast packets with this multicast address will not be able to be forwarded from this port.

### Static Multicast MAC

Some devices may only support multicast packets, but not support either IGMP Snooping or GMRP. The LAPP switch supports adding multicast groups manually to enable multicast filtering.

### Enabling Multicast Filtering

Use the serial console or web interface to enable or disable IGMP Snooping and IGMP querying. If IGMP Snooping is not enabled, then IP multicast traffic is always forwarded, flooding the network.

## Configuring IGMP Snooping

**NOTE** IGMP Snooping will be disabled when Port-Based VLAN is enabled.

IGMP Snooping provides the ability to prune multicast traffic so that it travels only to those end destinations that require that traffic, thereby reducing the amount of traffic on the Ethernet LAN.

Layer 2 switch setting page

## IGMP Snooping Setting

Current VLAN List

IGMP Snooping Enable

Query Interval  (s)

IGMP Snooping Enhanced Mode

Index	VID	IGMP Snooping	Querier	Static Multicast Querier Port							
1	1	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/> 6	<input type="checkbox"/> 7	<input type="checkbox"/> 8

Activate

### IGMP Snooping Enable

Setting	Description	Factory Default
Enable/Disable	Checkmark the <b>IGMP Snooping Enable</b> checkbox near the top of the window to enable the IGMP Snooping function globally.	Disabled

NOTE: You should enable IGMP Snooping if the network also uses non-LAPP 3rd party switches.

### Query Interval

Setting	Description	Factory Default
Numerical value, input by the user	Sets the query interval of the Querier function globally. Valid settings are from 20 to 600 seconds.	125 seconds

### IGMP Snooping Enhanced Mode

Setting	Description	Factory Default
Enable	IGMP Multicast packets will be forwarded to: <ul style="list-style-type: none"> <li>• Auto-Learned Multicast Querier Ports</li> <li>• Member Ports</li> </ul>	Disable
Disable	IGMP Multicast packets will be forwarded to: <ul style="list-style-type: none"> <li>• Auto-Learned Multicast Router Ports</li> <li>• Static Multicast Querier Ports</li> <li>• Querier Connected Ports</li> <li>• Member Ports</li> </ul>	

NOTE: IGMP Snooping Enhanced Mode in networks composed entirely of LAPP switches.

### IGMP Snooping

Setting	Description	Factory Default
Enable/Disable	Enables or disables the IGMP Snooping function on that particular VLAN.	Enabled if IGMP Snooping is enabled globally

**Querier**

Setting	Description	Factory Default
Enable/Disable	Enables or disables the LAPP switch's querier function.	Enabled if IGMP Snooping is enabled globally
V1/V2 and V3 checkbox	V1/V2: Enables switch to send IGMP snooping version 1 and 2 queries V3: Enables switch to send IGMP snooping version 3 queries	V1/V2

**Static Multicast Querier Port**

Setting	Description	Factory Default
Select/Deselect	Select the ports that will connect to the multicast routers. These ports will receive all multicast packets from the source. This option is only active when IGMP Snooping is enabled.	Disabled

**NOTE**

If a router or layer 3 switch is connected to the network, it will act as the Querier, and consequently this Querier option will be disabled on all LAPP layer 2 switches.

If all switches on the network are LAPP layer 2 switches, then only one layer 2 switch will act as Querier.

**IGMP Table**

The LAPP switch displays the current active IGMP groups that were detected. View IGMP group setting per VLAN ID on this page.

**Current Active IGMP Groups**

VID	Auto Learned Multicast Querier Port	Static Multicast Querier Port	Querier Connected Port	Act as Querier	Active IGMP Groups		
					IP	MAC	Members Port

The information shown in the table includes:

- Auto-learned Multicast Router Port: This indicates that a multicast router connects to/sends packets from these port(s)
- Static Multicast Router Port: Displays the static multicast querier port(s)
- Querier Connected Port: Displays the port which is connected to the querier.
- Act as a Querier: Displays whether or not this VLAN is a querier (winner of a election).

## Static Multicast MAC Addresses

### Static Multicast MAC Address

#### Current Static Multicast MAC Address List

All	Index	MAC Address	Join Port
-----	-------	-------------	-----------

Remove Select

#### Add New Static Multicast MAC Address to the List

MAC Address  -  -  -  -  -

Join Port  1  2  3  4  5  6  7  8

Activate

#### Add New Static Multicast Address to the List

Setting	Description	Factory Default
MAC Address	Input the multicast MAC address of this host.	None

#### MAC Address

Setting	Description	Factory Default
Integer	Input the number of the VLAN that the host with this MAC address belongs to.	None

#### Join Port

Setting	Description	Factory Default
Select/Deselect	Checkmark the appropriate check boxes to select the join ports for this multicast group.	None

## Configuring GMRP

GMRP is a MAC-based multicast management protocol, whereas IGMP is IP-based. GMRP provides a mechanism that allows bridges and end stations to register or un-register Group membership information dynamically.

### GMRP Settings

Port	GMRP
1	<input type="checkbox"/> Enable
2	<input type="checkbox"/> Enable
3	<input type="checkbox"/> Enable
4	<input type="checkbox"/> Enable
5	<input type="checkbox"/> Enable
6	<input type="checkbox"/> Enable
7	<input type="checkbox"/> Enable
8	<input type="checkbox"/> Enable

Activate

#### GMRP enable

Setting	Description	Factory Default
Enable/Disable	Enables or disables the GMRP function for the port listed in the Port column	Disable

## GMRP Table

The LAPP switch displays the current active GMRP groups that were detected

### GMRP Status

Multicast Address	Fixed Ports	Learned Ports
-------------------	-------------	---------------

Setting	Description
Fixed Ports	This multicast address is defined by static multicast.
Learned Ports	This multicast address is learned by GMRP.

## Using Bandwidth Management

In general, one host should not be allowed to occupy unlimited bandwidth, particularly when the device malfunctions. For example, so-called "broadcast storms" could be caused by an incorrectly configured topology, or a malfunctioning device. LAPP industrial Ethernet switches not only prevents broadcast storms, but can also be configured to a different ingress rate for all packets, giving administrators full control of their limited bandwidth to prevent undesirable effects caused by unpredictable faults.

# Configuring Bandwidth Management

## Traffic Rate Limiting Settings

### Traffic Rate Limiting Settings

Control Mode Normal ▼

Port	Policy	Ingress Priority Queue Rate			
		Low	Normal	Medium	High
1	<span style="border: 1px solid black; padding: 2px;">Limit Broadcast ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>
2	<span style="border: 1px solid black; padding: 2px;">Limit Broadcast ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>
3	<span style="border: 1px solid black; padding: 2px;">Limit Broadcast ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>
4	<span style="border: 1px solid black; padding: 2px;">Limit Broadcast ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>
5	<span style="border: 1px solid black; padding: 2px;">Limit Broadcast ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>
6	<span style="border: 1px solid black; padding: 2px;">Limit Broadcast ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>
7	<span style="border: 1px solid black; padding: 2px;">Limit Broadcast ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>
8	<span style="border: 1px solid black; padding: 2px;">Limit Broadcast ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>	<span style="border: 1px solid black; padding: 2px;">8M ▼</span>

Control Mode	Description	Factory Default
Normal	Set the max. ingress rate limit for different packet types	Normal
Port Disable	When the ingress multicast and broadcast packets exceed the ingress rate limit, the port will be disabled for a certain period. During this period, all packets from this port will be discarded.	

#### Ingress Rate Limit - Normal

Policy	Description	Factory Default
Limit All	Select the ingress rate limit for different packet types from the following options: Not Limited, 128K, 256K, 512K, 1M, 2M, 4M, 8M	Limit Broadcast 8M
Limit Broadcast, Multicast, Flooded Unicast		
Limit Broadcast, Multicast		
Limit Broadcast		

### Traffic Rate Limiting Settings

Control Mode Port Disable ▼

Port Disable Duration (1~65535s) 30

#### Port Ingress (fps of multicast and broadcast packets.)

- 1 Not Limited ▼
- 2 Not Limited ▼
- 3 Not Limited ▼
- 4 Not Limited ▼
- 5 Not Limited ▼
- 6 Not Limited ▼
- 7 Not Limited ▼
- 8 Not Limited ▼

Activate

**Ingress Rate Limit – Port Disable**

Setting	Description	Factory Default
Port disable duration (1~65535 seconds)	When the ingress multicast and broadcast packets exceed the ingress rate limit, the port will be disabled for this period of time. During this time, all packets from this port will be discarded.	30 second
Ingress (fps)	Select the ingress rate (fps) limit for all packets from the following options: Not Limited, 4464, 7441, 14881, 22322, 37203, 52084, 74405	Not Limited

**Egress Rate Limit**

Port	Egress
1	Not Limited ▼
2	Not Limited ▼
3	Not Limited ▼
4	Not Limited ▼
5	Not Limited ▼
6	Not Limited ▼
7	Not Limited ▼
8	Not Limited ▼

Activate

Setting	Description	Factory Default
Egress rate	Select the ingress rate limit (% of max. throughput) for all packets from the following options: Not Limited, 3%, 5%, 10%, 15%, 25%, 35%, 50%, 65%, 85%	Not Limited

## Using Auto Warning

Since industrial Ethernet devices are often located at the endpoints of a system, these devices will not always know what is happening elsewhere on the network. This means that an industrial Ethernet switch that connects to these devices must provide system maintainers with real-time alarm messages. Even when control engineers are out of the control room for an extended period of time, they can still be informed of the status of devices almost instantaneously when exceptions occur. The LAPP switch supports different approaches to warn engineers automatically, such as email and relay output. It also supports two digital inputs to integrate sensors into your system to automate alarms by email and relay output.

## Configuring Email Warning

The Auto Email Warning function uses e-mail to alert the user when certain user-configured events take place. Three basic steps are required to set up the Auto Warning function:

### Configure Email Event Types

Select the desired **Event types** from the Console or Web Browser Event type page (a description of each event type is given later in the *Email Alarm Events setting* subsection).

### Configure Email Settings

To configure a LAPP switch’s email setup from the serial, Telnet, or web console, enter your Mail Server IP/Name (IP address or name), Account Name, Account Password, Retype New Password, and the email address to which warning messages will be sent.

### Activate your settings and if necessary, test the email

After configuring and activating your LAPP switch’s Event Types and Email Setup, you can use the **Test Email** function to see if your e-mail addresses and mail server address have been properly configured.

## Configuring Event Types

### Email Warning Events Settings

#### System Events

- Switch Cold Start
- Switch Warm Start
- Power Transition(On->Off)
- Power Transition(Off->On)
- Config. Change
- Auth. Failure
- Comm. Redundancy Topology Changed

#### Port Events

Port	Link-ON	Link-OFF	Traffic-Overload	Rx-Threshold(%)	Traffic-Duration(s)
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	1
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	1
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	1
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	1
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	1
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	1
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	1
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	1

**Activate**

Event Types can be divided into two basic groups: **System Events** and **Port Events**. System Events are related to the overall function of the switch, whereas Port Events are related to the activity of a specific port.

System Events	Warning e-mail is sent when...
Switch Cold Start	Power is cut off and then reconnected.
Switch Warm Start	LAPP switch is rebooted, such as when network parameters are changed (IP address, subnet mask, etc.).
Power Transition (On→Off)	LAPP switch is powered down.
Power Transition (Off→On)	LAPP switch is powered up.
Configuration Change Activated	Any configuration item has been changed.
Authentication Failure	An incorrect password was entered.
Comm. Redundancy Topology Changed	If any Spanning Tree Protocol switches have changed their position (applies only to the root of the tree). If the Master of the Turbo Ring has changed or the backup path is activated.

Port Events	Warning e-mail is sent when...
Link-ON	The port is connected to another device.
Link-OFF	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).
Traffic-Overload	The port's traffic surpasses the Traffic-Threshold for that port (provided this item is Enabled).
Traffic-Threshold (%)	Enter a nonzero number if the port's Traffic-Overload item is Enabled.
Traffic-Duration (sec.)	A Traffic-Overload warning is sent every Traffic-Duration seconds if the average Traffic-Threshold is surpassed during that time period.

**NOTE** The Traffic-Overload, Traffic-Threshold (%), and Traffic-Duration (sec.) Port Event items are related. If you Enable the Traffic-Overload event, then be sure to enter a nonzero Traffic-Threshold percentage, as well as a Traffic-Duration between 1 and 300 seconds.

**NOTE** The sender of warning e-mail messages will have the following form:  
 Managed-Redundant-Switch-00000@Switch\_Location  
 where Managed-Redundant-Switch-00000 is the default Switch Name, 00000 is the LAPP switch's serial number, and Switch\_Location is the default Server Location. Refer to the Basic Settings section to see how to modify Switch Name and Switch Location.

## Configuring Email Settings

### Email Warning Events Settings

Mail Server IP/Name:

SMTP Port:

Account Name :

Account Password :

Change Account Password

Old Password :

New Password :

Retype Password :

1st email address :

2nd email address :

3rd email address :

4th email address :

#### Mail Server IP/Name

Setting	Description	Factory Default
IP address	The IP Address of your email server.	None

#### SMTP Port

Setting	Description	Factory Default
SMTP port	Display the SMTP port number	25

#### Account Name

Setting	Description	Factory Default
Max. 45 of characters	Your email account.	None

#### Password Setting

Setting	Description	Factory Default
Disable/Enable to change password	To reset the password from the Web Browser interface, click the Change password check-box, type the Old password, type the New password, retype the New password, and then click Activate (Max. of 45 characters).	Disable
Old password	Type the current password when changing the password	None
New password	Type new password when enabled to change password; Max. 45 characters.	None
Retype password	If you type a new password in the Password field, you will be required to retype the password in the Retype new password field before updating the new password.	None

#### Email Address

Setting	Description	Factory Default
Max. of 30 characters	You can set up to 4 email addresses to receive alarm emails from the LAPP switch.	None

#### Send Test Email

After you complete the email settings, you should first click **Activate** to activate those settings, and then press the **Send Test Email** button to verify that the settings are correct.

## Configuring Relay Warning

The Auto Relay Warning function uses relay output to alert the user when certain user-configured events take place. There are two basic steps required to set up the Relay Warning function:

### Configure Relay Event Types

Select the desired **Event types** from the Console or Web Browser Event type page (a description of each event type is given later in the *Relay Alarm Events setting* subsection).

### Activate your settings

After completing the configuration procedure, you will need to activate your LAPP switch’s Relay Event Types.

## Configuring Event Types

### Relay Warning Events Settings

#### System Events

**Override Relay Warning Settings**

Power Input 1 failure(On->Off) Disable ▾

Power Input 2 failure(On->Off) Disable ▾

Turbo Ring Break Disable ▾

#### Port Events

Port	Link	Traffic-Overload	Rx-Threshold(%)	Traffic-Duration(s)
1	<span>Ignore ▾</span>	<span>Disable ▾</span>	<input type="text" value="1"/>	<input type="text" value="1"/>
2	<span>Ignore ▾</span>	<span>Disable ▾</span>	<input type="text" value="1"/>	<input type="text" value="1"/>
3	<span>Ignore ▾</span>	<span>Disable ▾</span>	<input type="text" value="1"/>	<input type="text" value="1"/>
4	<span>Ignore ▾</span>	<span>Disable ▾</span>	<input type="text" value="1"/>	<input type="text" value="1"/>
5	<span>Ignore ▾</span>	<span>Disable ▾</span>	<input type="text" value="1"/>	<input type="text" value="1"/>
6	<span>Ignore ▾</span>	<span>Disable ▾</span>	<input type="text" value="1"/>	<input type="text" value="1"/>
7	<span>Ignore ▾</span>	<span>Disable ▾</span>	<input type="text" value="1"/>	<input type="text" value="1"/>
8	<span>Ignore ▾</span>	<span>Disable ▾</span>	<input type="text" value="1"/>	<input type="text" value="1"/>

Activate

Event Types can be divided into two basic groups: **System Events** and **Port Events**. System Events are related to the overall function of the switch, whereas Port Events are related to the activity of a specific port.

The LAPP switch supports two relay outputs. You can configure which relay output is related to which events, which helps administrators identify the importance of the different events.

System Events	Warning Relay output is triggered when...
Power Transition (On -> Off)	LAPP switch is powered down
Power Transition (Off -> On)	LAPP switch is powered up
Turbo Ring Break	The Turbo Ring is broken. Only the MASTER switch of Turbo Ring will output warning relay.

Port Events	Warning e-mail is sent when...
Link-ON	The port is connected to another device.
Link-OFF	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).
Traffic-Overload	The port’s traffic surpasses the Traffic-Threshold for that port (provided this item is Enabled).
Traffic-Threshold (%)	Enter a nonzero number if the port’s Traffic-Overload item is Enabled.
Traffic-Duration (sec.)	A Traffic-Overload warning is sent every Traffic-Duration seconds if the average Traffic-Threshold is surpassed during that time period.

### Override relay alarm settings

Check the checkbox to override the relay warning setting temporarily. Releasing the relay output will allow administrators to fix any problems with the warning condition

**NOTE** The Traffic-Overload, Traffic-Threshold (%), and Traffic-Duration (sec) Port Event items are related. If you Enable the Traffic-Overload event, then be sure to enter a nonzero Traffic-Threshold percentage, as well as a Traffic-Duration between 1 and 300 seconds.

## Warning List

Use this table to see if any relay alarms have been issued.

### Current Warning List

Index	Event	Relay
-------	-------	-------

## Using Line-Swap-Fast-Recovery

The Line-Swap Fast Recovery function, which is enabled by default, allows the LAPP switch to return to normal operation extremely quickly after devices are unplugged and then re-plugged into different ports. The recovery time is on the order of a few milliseconds (compare this with standard commercial switches for which the recovery time could be on the order of several minutes). To disable the Line-Swap Fast Recovery function, or to re-enable the function after it has already been disabled, access either the Console utility’s **Line-Swap recovery** page, or the Web Browser interface’s **Line-Swap fast recovery** page, as shown below.

## Configuring Line-Swap Fast Recovery

### Line Swap Fast Recovery

Enable All Ports

Activate

#### Enable Line-Swap-Fast-Recovery

Setting	Description	Factory Default
Enable/Disable	Checkmark the checkbox to enable the Line-Swap-Fast-Recovery function	Enable

## Using Set Device IP

To reduce the effort required to set up IP addresses, the LAPP switch comes equipped with DHCP/BootP server and RARP protocol to set up IP addresses of Ethernet-enabled devices automatically.

When enabled, the **Set device IP** function allows the LAPP switch to assign specific IP addresses automatically to connected devices that are equipped with *DHCP Client* or *RARP* protocol. In effect, the LAPP switch acts as a DHCP server by assigning a connected device with a specific IP address stored in its internal memory. Each time the connected device is switched on or rebooted, the LAPP switch sends the device the desired IP address.

Take the following steps to use the **Set device IP** function:

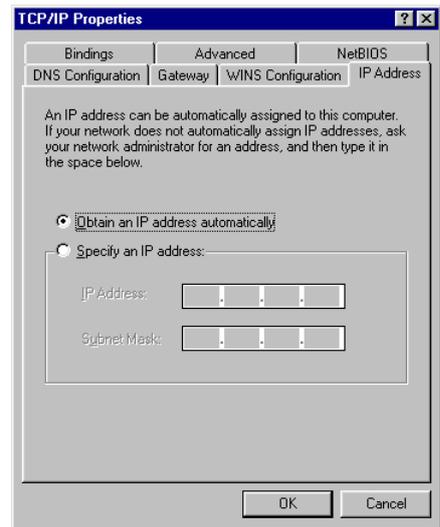
**STEP 1—Set up the connected devices**

Set up those Ethernet-enabled devices connected to the LAPP switch for which you would like IP addresses to be assigned automatically. The devices must be configured to obtain their IP address automatically.

The devices' configuration utility should include a setup page that allows you to choose an option similar to the *Obtain an IP address automatically* option.

For example, Windows' TCP/IP Properties window is shown at the right. Although your device's configuration utility may look quite a bit different, this figure should give you some idea of what to look for.

You also need to decide which of the LAPP switch's ports your Ethernet-enabled devices will be connected to. You will need to set up each of these ports separately, as described in the following step.



**STEP 2**

Configure the LAPP switch's **Set device IP** function, either from the Console utility or from the Web Browser interface. In either case, you simply need to enter the **Desired IP** for each port that needs to be configured.

**STEP 3**

Be sure to activate your settings before exiting.

- When using the Web Browser interface, activate by clicking on the Activate button.
- When using the Console utility, activate by first highlighting the **Activate** menu option, and then press **Enter**. You should receive the **Set device IP settings are now active! (Press any key to continue)** message.

## Configuring Set Device IP

### Automatic "Set Device IP" by DHCP/BootP/RARP

#### Automatic Set Device IP by DHCP/BootP/RARP

Port	Device's current IP	Active function	Desired IP address
1	NA	--	<input type="text"/>
2	NA	--	<input type="text"/>
3	NA	--	<input type="text"/>
4	NA	--	<input type="text"/>
5	NA	--	<input type="text"/>
6	NA	--	<input type="text"/>
7	NA	--	<input type="text"/>
8	NA	--	<input type="text"/>

**Activate**

**Desired IP Address**

Setting	Description	Factory Default
IP Address	Set the desired IP of connected devices.	None

# Configuring DHCP Relay Agent

The DHCP Relay Agent makes it possible for DHCP broadcast messages to be sent over routers. The DHCP Relay Agent enables DHCP clients to obtain IP addresses from a DHCP sever on a remote subnet, or those that are not located on the local subnet.

## DHCP Relay Agent (Option 82)

Option 82 is used by the relay agent to insert additional information into the client’s DHCP request. The Relay Agent Information option is inserted by the DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server. Servers can recognize the Relay Agent Information option and use the information to implement IP addresses to Clients.

When Option 82 is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified.

The Option 82 information contains 2 sub-options, Circuit ID and Remote ID, which define the relationship between the end device IP and the DHCP Option 82 server. The **Circuit ID** is a 4-byte number generated by the Ethernet switch—a combination of physical port number and VLAN ID. The format of the **Circuit ID** is shown below:

### FF-VV-VV-PP

This is where the first byte “FF” is fixed to “01”, the second and the third byte “VV-VV” is formed by the port VLAN ID in hex, and the last byte “PP” is formed by the port number in hex. For example:

01-00-0F-03 is the “Circuit ID” of port number 3 with port VLAN ID 15.

The “Remote ID” identifies the relay agent itself and can be one of the following:

1. The IP address of the relay agent.
2. The MAC address of the relay agent.
3. A combination of IP address and MAC address of the relay agent.
4. A user-defined string.

## DHCP Relay Agent

**Server IP Address**

1st Server	
2nd Server	
3rd Server	
4th Server	

**DHCP Option 82**

Enable Option 82

Type: IP

Value: 192.168.127.253

Display: C0A87FFD

**DHCP Function Table**

Port	Circuit-ID	Option 82
1	01000101	<input type="checkbox"/> Enable
2	01000102	<input type="checkbox"/> Enable
3	01000103	<input type="checkbox"/> Enable
4	01000104	<input type="checkbox"/> Enable
5	01000105	<input type="checkbox"/> Enable
6	01000106	<input type="checkbox"/> Enable
7	01000107	<input type="checkbox"/> Enable
8	01000108	<input type="checkbox"/> Enable

Activate

## Server IP Address

### 1st Server

Setting	Description	Factory Default
IP address for the 1st DHCP server	Assigns the IP address of the 1st DHCP server that the switch tries to access.	None

### 2nd Server

Setting	Description	Factory Default
IP address for the 2nd DHCP server	Assigns the IP address of the 2nd DHCP server that the switch tries to access.	None

### 3rd Server

Setting	Description	Factory Default
IP address for the 3rd DHCP server	Assigns the IP address of the 3rd DHCP server that the switch tries to access.	None

### 4th Server

Setting	Description	Factory Default
IP address for the 4th DHCP server	Assigns the IP address of the 4th DHCP server that the switch tries to access.	None

## DHCP Option 82

### Enable Option 82

Setting	Description	Factory Default
Enable or Disable	Enable or disable the DHCP Option 82 function.	Disable

### Type

Setting	Description	Factory Default
IP	Uses the switch's IP address as the remote ID sub.	IP
MAC	Uses the switch's MAC address as the remote ID sub.	IP
Client-ID	Uses a combination of the switch's MAC address and IP address as the remote ID sub.	IP
Other	Uses the user-designated ID sub.	IP

### Value

Setting	Description	Factory Default
Max. 12 characters	Displays the value that was set. Complete this field if type is set to Other.	Switch IP address

### Display

Setting	Description	Factory Default
<i>read-only</i>	The actual hexadecimal value configured in the DHCP server for the Remote-ID. This value is automatically generated according to the Value field. Users cannot modify it.	COA87FFD

## DHCP Function Table

### Enable

Setting	Description	Factory Default
Enable or Disable	Enable or disable the DHCP Option 82 function for this port.	Disable

# Using Diagnosis

The LAPP switch provides three important tools for administrators to diagnose network systems.

## Mirror Port

The **Mirror Port** function can be used to monitor data being transmitted through a specific port. This is done by setting up another port (the mirror port) to receive the same data being transmitted from, or both to and from, the port under observation. Using a mirror port allows the network administrator to **sniff** the observed port to keep tabs on network activity.

### Mirror Port Settings

Monitored port

Watch direction

Mirror port

**Activate**

#### Mirror Port Settings

Setting	Description
Monitored Port	Select the number of one port whose network activity will be monitored.
Watch Direction	Select one of the following two watch direction options: Input data stream: Select this option to monitor only those data packets coming into the LAPP switch's port. Output data stream: Select this option to monitor only those data packets being sent out through the LAPP switch's port. Bi-directional: Select this option to monitor data packets both coming into, and being sent out through, the LAPP switch's port.
Mirror Port	Select the number of the port that will be used to monitor the activity of the monitored port.

## Ping

### Use Ping Command to test Network Integrity

IP address/Name

**Ping**

The **Ping** function uses the *ping* command to give users a simple but powerful tool for troubleshooting network problems. The function's most unique feature is that even though the ping command is entered from the user's PC keyboard, the actual ping command originates from the LAPP switch itself. In this way, the user can essentially sit on top of the LAPP switch and send ping commands out through its ports.

To use the Ping function, type in the desired IP address, and then press **Enter** from the Console utility, or click **Ping** when using the Web Browser interface.

# LLDP Function

## Overview

LLDP is an OSI Layer 2 protocol defined by IEEE 802.11AB. LLDP standardizes the self-identification advertisement method, and allows each networking device, such as a LAPP managed switch, to periodically send its system and configuration information to its neighbors.

From the switch’s web interface, you can enable or disable LLDP, and set the LLDP transmit interval. In addition, you can view each switch’s neighbor-list, which is reported by its network neighbors.

## Configuring LLDP Settings

### LLDP Settings

#### General Settings

LLDP Enable ▾  
 Message Transmit Interval  (5~32768secs)

**Activate**

#### LLDP Table

Port	Neighbor ID	Neighbor Port	Neighbor Port Description	Neighbor System
------	-------------	---------------	---------------------------	-----------------

## General Settings

### LLDP

Setting	Description	Factory Default
Enable or Disable	Enables or disables the LLDP function.	Enable

### Message Transmit Interval

Setting	Description	Factory Default
5 to 32768 sec.	Sets the transmit interval of LLDP messages, in seconds.	30 (seconds)

## LLDP Table

The LLDP Table displays the following information:

- Port** The port number that connects to the neighbor device.
- Neighbor ID** A unique entity (typically the MAC address) that identifies a neighbor device.
- Neighbor Port** The port number of the neighbor device.
- Neighbor Port Description** A textual description of the neighbor device’s interface.
- Neighbor System** Hostname of the neighbor device.

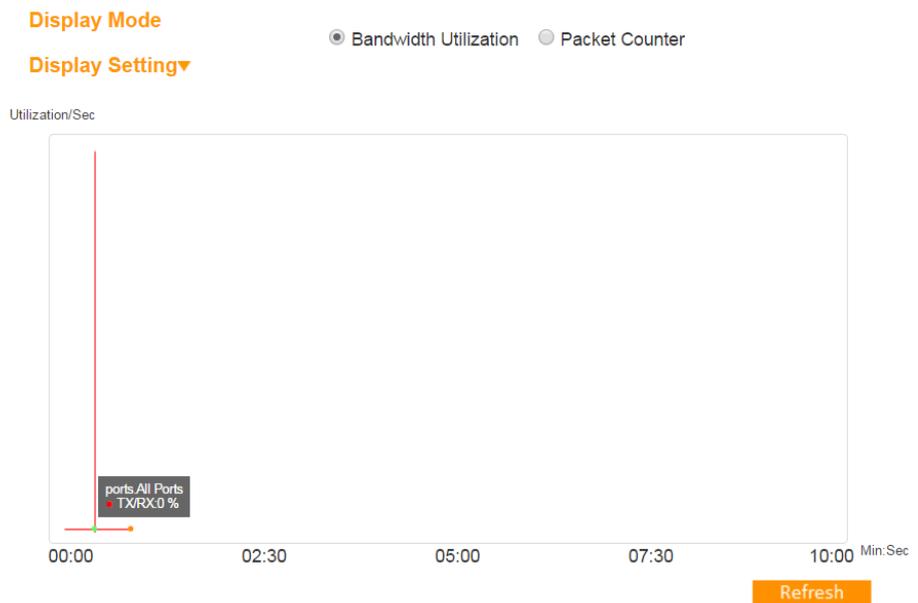
# Using Monitor

Access the monitoring page by selecting **Monitor** from the left selection bar. This feature allows the user to view a graph that shows the combined data transmission activity of all of the LAPP switch's ports. Click one of the two display modes - Bandwidth Utilization or Packet Counter—to view transmission activity of all or specific ports graphically.

## Bandwidth Utilization Mode

The graph displays the utilization of the bandwidth of the switch. While moving the mouse pointer to the graph, it will show the utilization rate of a specific time.

### Monitor



Add different ports' information in **Display Setting**. Choose the information you want in **Port Selection** and **Sniffer Mode** then click **Add**. The added information will be showed in the graph in a different color.

### Display Type

Port Selection

Sniffer Mode

Ports

All Ports	▼
TX/RX	▼

Add	Reset
-----	-------

## Packet Counter Mode

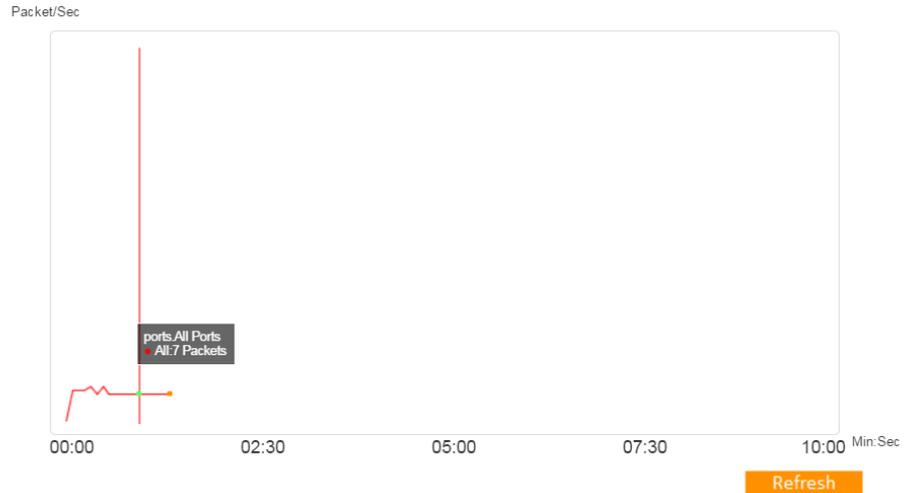
The graph displays the packet count of the switch's ports. While moving the mouse pointer to the graph, it will show the packet count of a specific time.

## Monitor

### Display Mode

Bandwidth Utilization  Packet Counter

### Display Setting



Add different ports' information in **Display Setting**. Choose the information you want in **Port Selection**, **Sniffer Mode** and **Packet Type** then click **Add**. The added information will be showed in the graph in a different color.

### Display Type

Ports

Port Selection

All Ports ▼

Sniffer Mode

TX/RX ▼

Packet Type

All ▼

Add

Reset

In the summary table below, one of four options can be chosen —**Total Packets, TX Packets, RX Packets**, or **Error Packets**. Users can view the transmission activity of specific types of packets on all or specific ports. Recall that TX Packets are packets sent out from the LAPP switch, RX Packets are packets received from connected devices, and Error Packets are packets that did not pass TCP/IP's error checking algorithm.

Refresh

Port : All Ports ▼

Packet: Total Packets ▼

[Format] Total Packets + Packets in past 5 secs

Update Interval: every 5 secs

Port	Tx	Tx Error	Rx	Rx Error
1	0+0	0+0	0+0	0+0
2	0+0	0+0	0+0	0+0
3	0+0	0+0	0+0	0+0
4	0+0	0+0	0+0	0+0
5	0+0	0+0	0+0	0+0
6	10835+20	0+0	11589+23	0+0
7	0+0	0+0	0+0	0+0
8	0+0	0+0	0+0	0+0

# Using the MAC Address Table

This section explains the information provided by the LAPP switch’s MAC address table.

## All MAC Address List

All ▾

Page 1/1 ▾

Index	MAC	Type	Port
1	28-d2-44-d3-e7-09	ucast(l)	6

The MAC Address table can be configured to display the following LAPP switch MAC address groups, which are selected from the drop-down list:

<b>ALL</b>	Select this item to show all of the LAPP switch’s MAC addresses.
<b>ALL Learned</b>	Select this item to show all of the LAPP switch’s Learned MAC addresses.
<b>ALL Static Lock</b>	Select this item to show all of the LAPP switch’s Static Lock MAC addresses.
<b>ALL Static</b>	Select this item to show all of the LAPP switch’s Static, Static Lock, and Static Multicast MAC addresses.
<b>ALL Static Multicast</b>	Select this item to show all of the LAPP switch’s Static Multicast MAC addresses.
<b>Port x</b>	Select this item to show all of the MAC addresses dedicated ports.

The table displays the following information:

<b>MAC</b>	This field shows the MAC address.
<b>Type</b>	This field shows the type of this MAC address.
<b>Port</b>	This field shows the port that this MAC address belongs to.

# Using Event Log

## Event Log Table

Page 67/67 ▾

Index	Bootup	Date	Time	System Startup Time	Event
991	141	--	--	1d6h34m53s	Authentication fail
992	141	--	--	1d6h34m54s	Authentication fail
993	141	--	--	1d6h34m55s	Authentication fail
994	141	--	--	1d6h34m59s	Authentication fail
995	141	--	--	1d6h35m0s	Authentication fail
996	141	--	--	1d6h35m0s	Authentication fail
997	141	--	--	1d6h35m0s	192.168.127.100 admin Auth. ok
998	142	--	--	0d0h0m0s	Cold start
999	142	--	--	0d0h0m2s	Port 6 link on
1000	142	--	--	0d0h0m14s	192.168.127.100 admin Auth. ok

Clear

The Event Log Table displays the following information:

<b>Bootup</b>	This field shows how many times the LAPP switch has been rebooted or cold started.
<b>Date</b>	The date is updated based on how the current date is set in the Basic Setting page.
<b>Time</b>	The time is updated based on how the current time is set in the Basic Setting page.
<b>System Startup Time</b>	The system startup time related to this event.
<b>Events</b>	Events that have occurred.

**NOTE** The following events will be recorded into the LAPP switch’s Event Log Table:

- Cold start
- Warm start
- Configuration change activated
- Power 1/2 transition (Off ( On), Power 1/2 transition (On ( Off))
- Authentication fail
- Topology changed
- Master setting is mismatched
- Port traffic overload
- Port link off/on

## Using Syslog

The Syslog function provides the event logs for the syslog server. The function supports 3 configurable syslog servers and syslog server UDP port numbers. When an event occurs, the event will be sent as a syslog UDP packet to the specified syslog servers.

### Syslog Settings

Syslog Server 1	<input type="text"/>
Port Destination	514 (1~65535)
Syslog Server 2	<input type="text"/>
Port Destination	514 (1~65535)
Syslog Server 3	<input type="text"/>
Port Destination	514 (1~65535)

Activate

#### Syslog Server 1/2/3

Setting	Description	Factory Default
IP Address	Enter the IP address of Syslog server 1/2/3, used by your network.	None
Port Destination (1 to 65535)	Enter the UDP port of Syslog server 1/2/3.	514

**NOTE** The following events will be recorded into the LAPP switch's Event Log table, and will then be sent to the specified Syslog Server:

- Cold start
- Warm start
- Configuration change activated
- Power 1/2 transition (Off (On), Power 1/2 transition (On (Off))
- Authentication fail
- Topology changed
- Master setting is mismatched
- Port traffic overload
- Port link off/on

# ETHERLINE ACCESS Configurator GUI

---

ETHERLINE ACCESS Configurator is a comprehensive Windows-based GUI that is used to configure and maintain multiple LAPP switches. A suite of useful utilities is available to help you locate LAPP switches attached to the same LAN as the PC host (regardless of whether or not you know the IP addresses of the switches), connect to a LAPP switch whose IP address is known, modify the network configurations of one or multiple LAPP switches, and update the firmware of one or more LAPP switch. ETHERLINE ACCESS Configurator is designed to provide you with instantaneous control of *all* of your LAPP switches, regardless of location. You may download the ETHERLINE ACCESS Configurator software from LAPP's website free of charge.

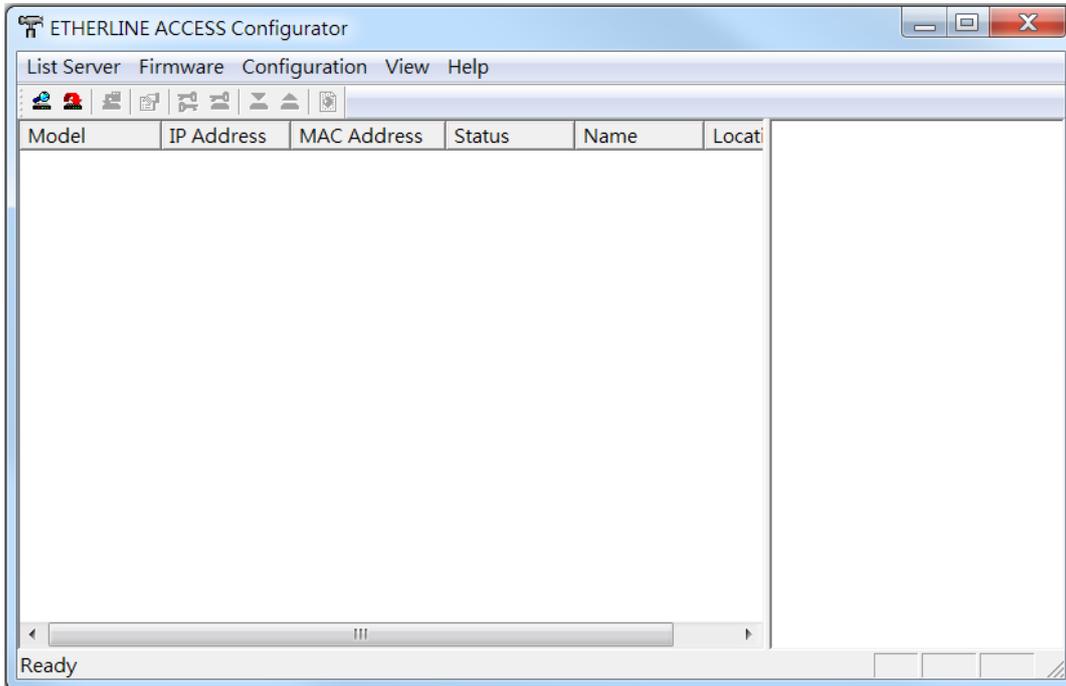
The following topics are covered in this chapter:

- Starting ETHERLINE ACCESS Configurator**
- Broadcast Search**
- Search by IP Address**
- Upgrade Firmware**
- Modify IP Address**
- Export Configuration**
- Import Configuration**
- Unlock Server**
- Set Default**

# Starting ETHERLINE ACCESS Configurator

To start ETHERLINE ACCESS Configurator, locate and run the executable file.

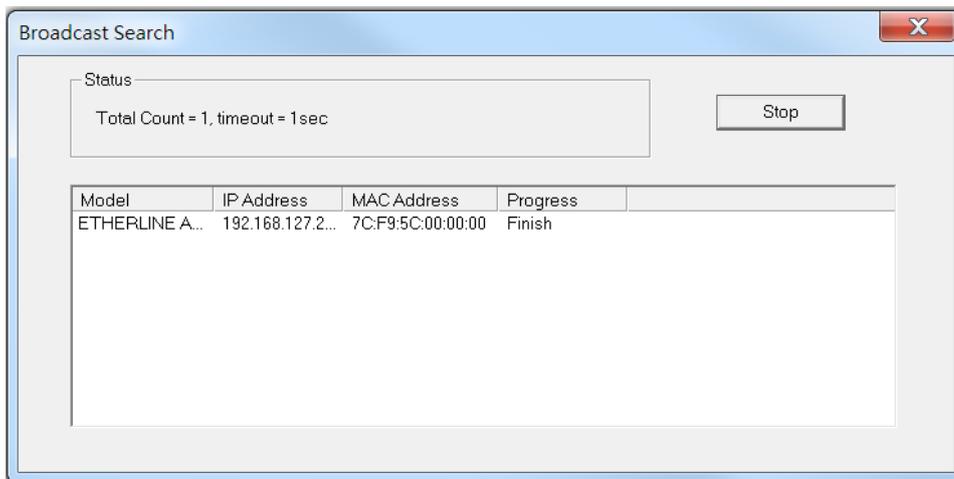
The ETHERLINE ACCESS Configurator window will open, as shown below.



## Broadcast Search

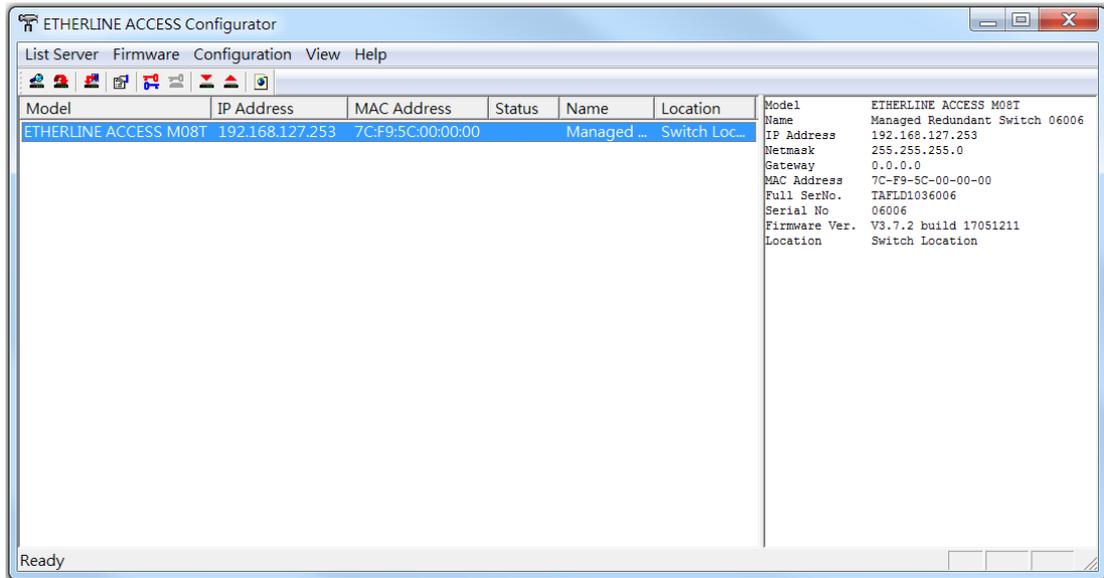
Use the **Broadcast Search** utility to search the LAN for all LAPP switches that are connected to the LAN. Note that since the search is done by MAC address, **Broadcast Search** will not be able to locate LAPP switches connected outside the PC host's LAN.

1. Start by clicking the Broadcast Search icon , or select **Broadcast Search** under the **List Server** menu. The Broadcast Search window will open and display a list of all switches located on the network. Look in the **Progress** column to see the progress of the search.



**NOTE** If you can't complete the Broadcast Search, please close the anti-virus software and try it again.

- Once the search is complete, the Configurator window will display a list of all switches that were located.



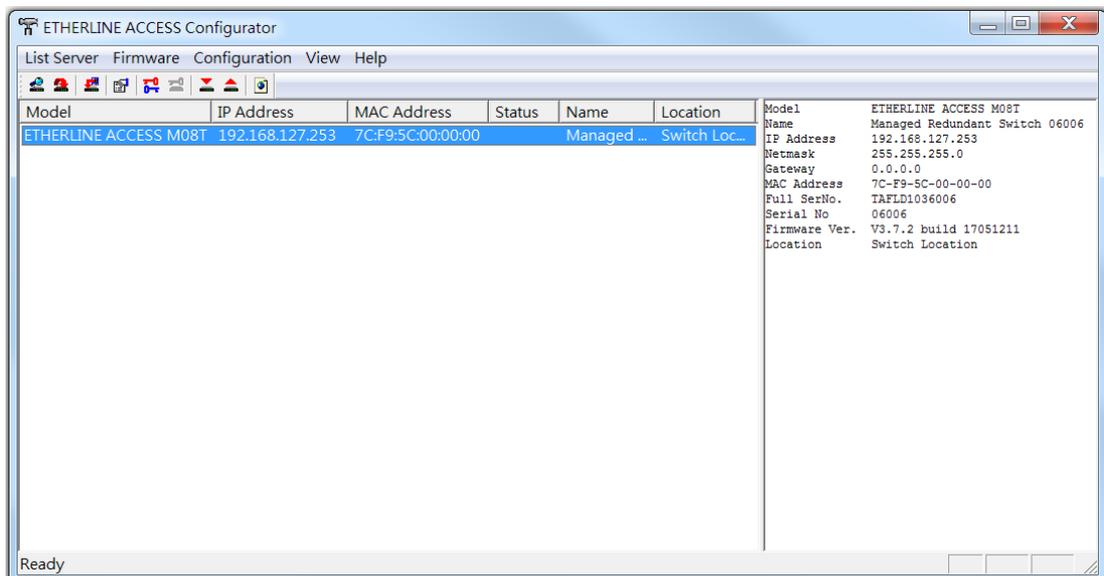
## Search by IP Address

Use the **Search by IP Address** utility to search for LAPP switches one at a time. Note that the search is conducted by IP address, so you should be able to locate any LAPP switch that is properly connected to your LAN, WAN, or the Internet.

- Start by clicking the **Specify by IP address** icon , or by selecting **Specify IP address** under the **List Server** menu. The **Search Server with IP Address** window will open. Enter the IP address of the switch you wish to search for, and then click **OK**.



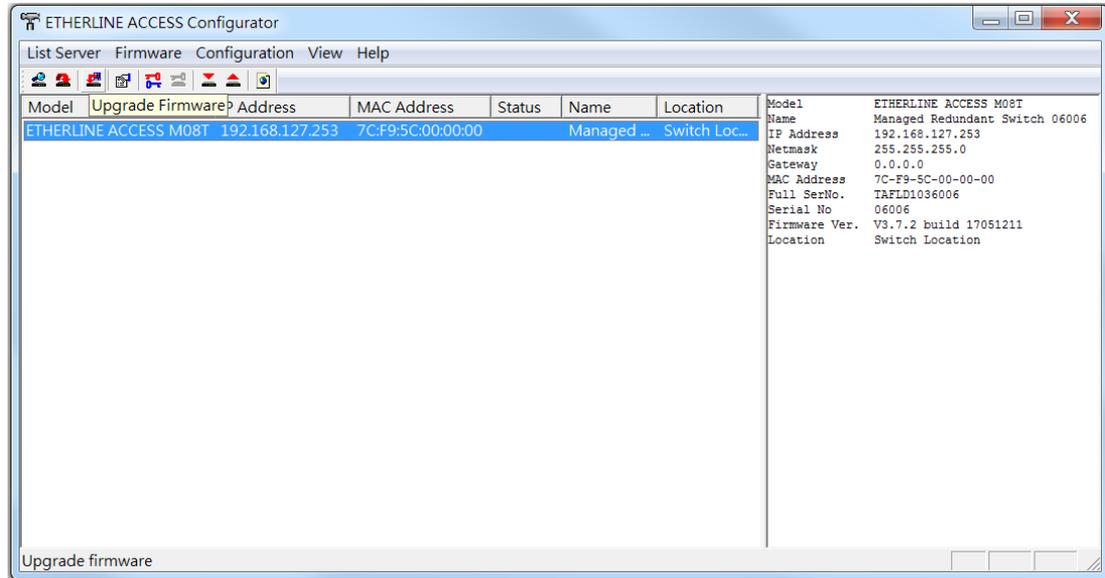
- Once the search is complete, the Configurator window will add the switch to the list of switches.



# Upgrade Firmware

Keep your LAPP switch up to date with the latest firmware from LAPP. Perform the following steps to upgrade the firmware:

1. Download the updated firmware (\*.rom) file from LAPP's website.
2. Click the switch (from the **ETHERLINE ACCESS Configurator** window) whose firmware you wish to upgrade to highlight it.

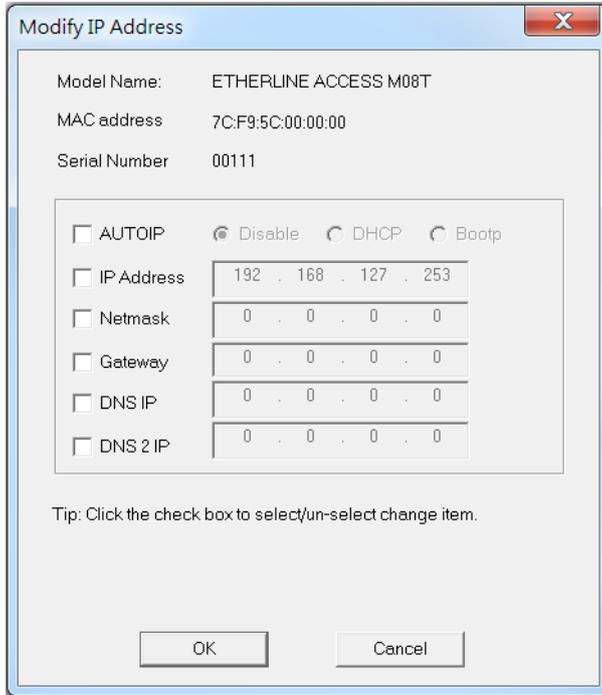


3. Click the **Upgrade Firmware** toolbar icon , or select **Upgrade** under the **Firmware** menu. If the switch is Locked, you will be prompted to input the switch's User Name and Password.
4. Use the **Open** window to navigate to the folder that contains the firmware upgrade file, and then click the correct "\*.rom" file to select the file. Click **Open** to activate the upgrade process.

# Modify IP Address

You may use the **Modify IP Address** function to reconfigure the LAPP switch's network settings.

1. Start by clicking the Modify IP address icon , or by selecting **Modify IP address** under the **Configuration** menu.
2. The **Setup Configuration** window will open. Checkmark the box to the left of those items that you wish to modify, and then Disable or Enable DHCP, and enter the IP Address, Subnet mask, Gateway, and DNS IP. Click **OK** to accept the changes to the configuration.



Modify IP Address

Model Name: ETHERLINE ACCESS M08T  
 MAC address: 7C:F9:5C:00:00:00  
 Serial Number: 00111

AUTOIP   
  Disable   
  DHCP   
  Bootp

IP Address    192 . 168 . 127 . 253  
 Netmask        0 . 0 . 0 . 0  
 Gateway         0 . 0 . 0 . 0  
 DNS IP            0 . 0 . 0 . 0  
 DNS 2 IP         0 . 0 . 0 . 0

Tip: Click the check box to select/un-select change item.

OK    Cancel

# Export Configuration

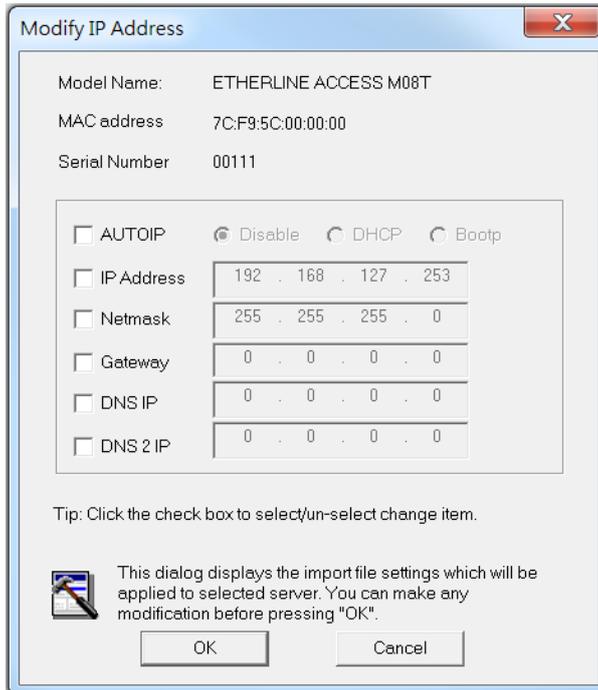
The **Export Configuration** utility is used to save the entire configuration of a particular LAPP switch to a text file. Take the following steps to export a configuration:

1. Highlight the switch (from the Server list in the Configurator window's left pane), and then click the **Export** toolbar icon  or select **Export Configuration** from the **Configuration** menu. Use the **Open** window to navigate to the folder in which you would like to store the configuration, and then type the name of the file in the **File name** input box. Click **Save** to continue.
2. Click **OK** when the **Export configuration to file OK** message appears.
3. You may use a standard text editor, such as Notepad under Windows, to view and modify the newly created configuration file.

# Import Configuration

The **Import Configuration** function is used to import an entire configuration from a text file to the LAPP switch. The utility can be used to transfer the configuration from one LAPP switch to another, by first using the Export Configuration function (described in the previous section) to save a switch configuration to a file, and then using the Import Configuration function. Perform the following steps to import a configuration:

1. Highlight the server (from the Configurator window's left pane), and then click the **Import** toolbar icon , or select **Import Configuration** from the **Configuration** menu.
2. Use the **Open** window to navigate to the text file that contains the desired configuration. Once the file is selected, click **Open** to initiate the import procedure.
3. The **Setup Configuration** window will be displayed, with a special note attached at the bottom. Parameters that have been changed will be indicated with a checkmark. You may make more changes if necessary, and then click **OK** to accept the changes.



Modify IP Address

Model Name: ETHERLINE ACCESS M08T

MAC address: 7C:F9:5C:00:00:00

Serial Number: 00111

AUTOIP   
 Disable   
 DHCP   
 Bootp

IP Address    192 . 168 . 127 . 253

Netmask    255 . 255 . 255 . 0

Gateway    0 . 0 . 0 . 0

DNS IP    0 . 0 . 0 . 0

DNS 2 IP    0 . 0 . 0 . 0

Tip: Click the check box to select/un-select change item.

 This dialog displays the import file settings which will be applied to selected server. You can make any modification before pressing "OK".

OK    Cancel

# Unlock Server

The **Unlock Server** function is used to open a password protected switch so that the user can modify its configuration, import/export a configuration, and perform other procedures. There are six possible responses under the **Status** column. The **Status** of a LAPP switch indicates how ETHERLINE ACCESS Configurator located the switch, and what type of password protection it has.

The types are:

- **Locked**  
The switch is password protected, **Broadcast Search** was used to locate it, and the password has not yet been entered from within the current Configurator session.
- **Unlocked**  
The switch is password protected, **Broadcast Search** was used to locate it, and the password was entered from within the current Configurator session. Henceforth during this Configurator session, activating various utilities for this switch will not require re-entering the server password.
- **Blank**  
The LAPP switch is not password protected, and **Broadcast Search** was used to locate it.

Follow the steps given below to unlock a locked LAPP switch (i.e., LAPP switch with Status “Locked” or “Locked Fixed”). Highlight the server (from the EHTERLINE ACCESS Configurator window’s left pane), and then click the **Unlock** toolbar icon , or select **Unlock** from the **Configuration** menu.

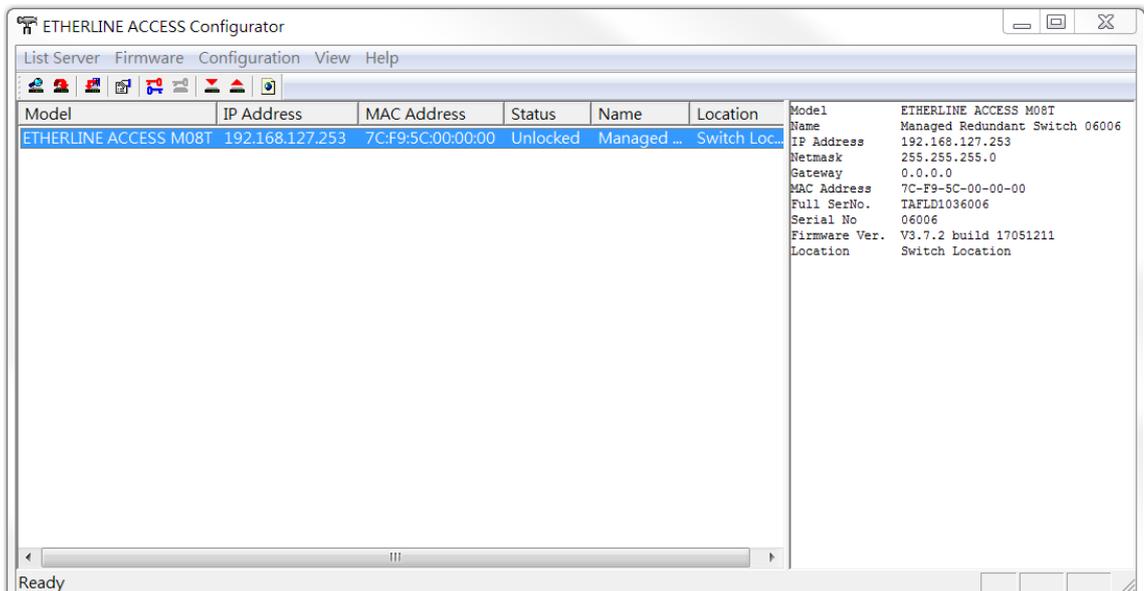
1. Enter the switch’s **User Name** and **Password** when prompted, and then click **OK**.



2. When the **Unlock status** window indicates the Progress as **OK**, click the **Close** button in the upper right corner of the window.

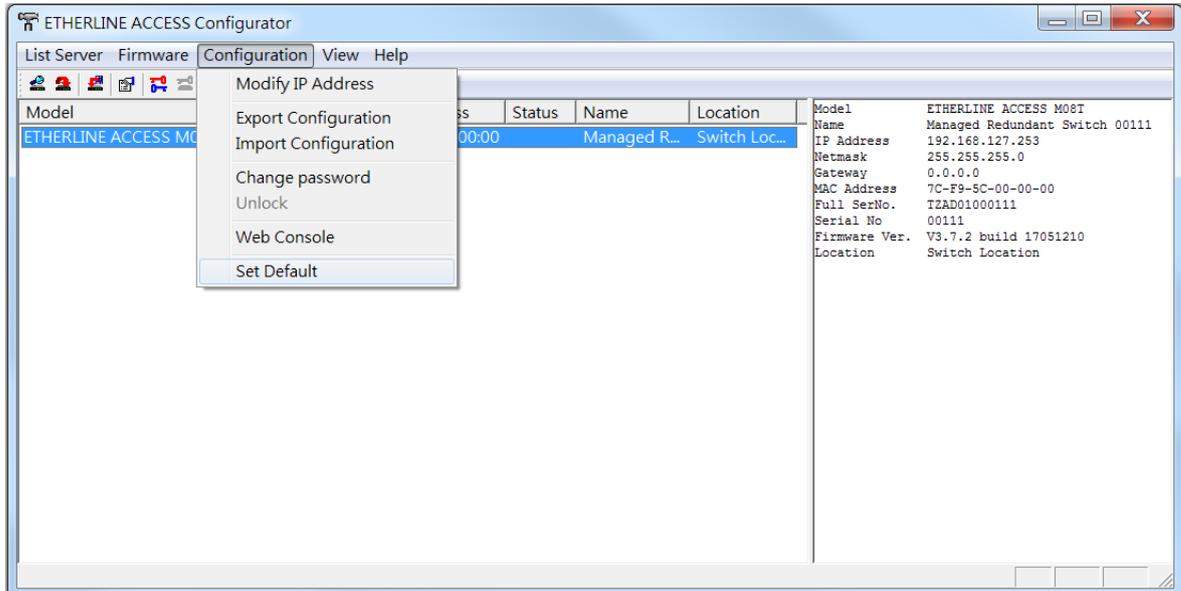


3. The status of the switch will now be shown as **Unlocked**.



# Set Default

The **Set Default** function is used to reset the chosen device to factory default settings. The device will restart itself and return to the default settings after you trigger this function.



# MIB Groups

---

The LAPP switch comes with built-in SNMP (Simple Network Management Protocol) agent software that supports cold/warm start trap, line up/down trap, and RFC 1213 MIB-II.

The standard MIB groups that the LAPP switch supports are as follows:

## **MIB II.1—System Group**

sysORTable

## **MIB II.2—Interfaces Group**

ifTable

## **MIB II.4 – IP Group**

ipAddrTable  
ipNetToMediaTable  
IpGroup  
IpBasicStatsGroup  
IpStatsGroup

## **MIB II.5—ICMP Group**

IcmpGroup  
IcmpInputStatus  
IcmpOutputStats

## **MIB II.6—TCP Group**

tcpConnTable  
TcpGroup  
TcpStats

## **MIB II.7—UDP Group**

udpTable  
UdpStats

## **MIB II.10—Transmission Group**

dot3  
dot3StatsTable

## **MIB II.11—SNMP Group**

SnmpBasicGroup  
SnmpInputStats  
SnmpOutputStats

## **MIB II.17—dot1dBridge Group**

dot1dBase  
dot1dBasePortTable  
dot1dStp  
dot1dStpPortTable  
dot1dTp  
dot1dTpFdbTable  
dot1dTpPortTable

```
dot1dTpHCPortTable
dot1dTpPortOverflowTable
pBridgeMIB
dot1dExtBase
dot1dPriority
dot1dGarp
qBridgeMIB
dot1qBase
dot1qTp
dot1qFdbTable
dot1qTpPortTable
dot1qTpGroupTable
dot1qForwardUnregisteredTable
dot1qStatic
dot1qStaticUnicastTable
dot1qStaticMulticastTable
dot1qVlan
dot1qVlanCurrentTable
dot1qVlanStaticTable
dot1qPortVlanTable
```

The LAPP switch also provides a private MIB file, located in the file **LAPP-[switch's model name]-MIB.my**.

### Public Traps

- Cold Start
- Link Up
- Link Down
- Authentication Failure
- dot1dBridge New Root
- dot1dBridge Topology Changed

### Private Traps

- Configuration Changed
- Power On
- Power Off
- Traffic Overloaded
- Turbo Ring Topology Changed
- Turbo Ring Coupling Port Changed
- Turbo Ring Master Mismatch