DLM-3500
User Guide

Version DLM-3500-1.0 July 13, 2007

Trademarks

Statement of Conditions

In the interest of improving internal design, operation function, and/or reliability, D-Link Corporation reserves the right to make changes to products described in this document without notice. D-Link Corporation does not assume any liability that may occur due to the use or application of the product(s) described herein.

Table of Contents

Chapter 1. Before You Start

1.1 Audience

This manual is intended for use by system integrators, field engineers and network administrators to help them set up DLM-3500 Intelligent WAN Link Manager in their network environments. It contains step by step procedures and pictures to guide users with basic network system knowledge to complete the installation.

1.2 Document Conventions

The following information provides the details of conventions used in this manual.

For cautionary statements or warning requiring special attention by readers, a text box with italic font will be used.

Example:

Warning: *For security purposes, you should immediately change the Administrator's password.*

When any of the button symbol shown below is selected, the following action will be executed accordingly:

After modifying the parameters of specific menu page, click this button to save your changes to memory, the old settings will also be saved.

Click the Help button to display the on-line help of the current page. The on-line help information will automatically swap when you change the function page or language.

Click Hide Help to hide the on-line help information.

Please Note: *Screen captures and pictures used in this manual may be displayed in part or in whole, and may vary or differ slightly from the actual product, depending on versioning and menu accessed.*

Chapter 2. Overview

2.1 Introduction of DLM-3500

The DLM-3500 is a WAN Link Manager designed for medium to large network environments to provide network **“manageability”, “efficiency”** and a **“friendly interface”** suitable for campuses, libraries, gymnasiums, small and middle enterprises, factories, hotspots and community hospitals.

2.2 System Concept

DLM-3500 is a network device that combines the features of WAN load balancing, link fault tolerance, multihoming, bandwidth management and firewall into an integrated unit to maximize the performance and reliability potentials of your broadband Internet setup.

DLM-3500 is suitable for environments with multiple access lines to the Internet. With its load balancing feature, user can direct packets to route through a specified link for outbound Internet traffic by means of Auto Routing. In addition, if there should be a failed link, DLM-3500 can speedily detect it and dynamically adjust Packet Route to prevent future traffic from going to that link. This achieves the function of fault tolerance. However, when there are public websites sitting inside an internal network of a corporation, fault tolerance alone is not enough to ensure uptime. DLM-3500’s proprietary PromptDNS technology has the ability to make proper adjustments based on results of DNS queries, achieving the function of multihoming. With these combined features, enterprise websites will now be able to provide services with continuous uptimes.

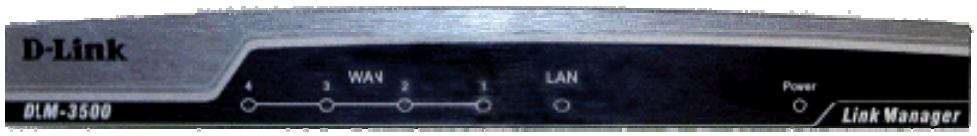
The flexibility of the Bandwidth Management feature of DLM-3500 can satisfy the user’s various management needs. It can be set to target a particular protocol such as FTP, HTTP, or a particular time period (e.g., peak hours) by variably adjusting the size of allowable bandwidth. This will increase the network QoS (Quality of Service). DLM-3500 also makes provisions for network security with the features of Firewall and DMZ (Demilitarized Zone). These features will be able to prevent malicious attacks from entering from the outside.

DLM-3500 targets a wide range of users, including small to mid-size businesses and schools. It easily fits into any environment, and comes with an easy-to-use administration interface. DLM-3500 also provides very comprehensive features, set to satisfy the most demanding network environments.

Chapter 3. Hardware Installation

3.1 Panel Function Descriptions

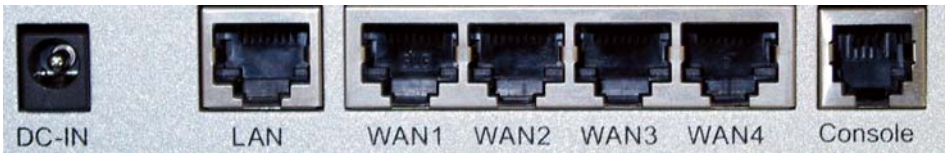
Front Panel



LED's:

1. **WAN1/WAN2/WAN3/WAN4**: OFF indicates the line is not connected, and ON indicates the line is connected.
2. **LAN**: OFF indicates the line is not connected, and ON indicates the line is connected.
3. **Power**: ON indicates power on, and OFF indicates power off.

Rear Panel



DC-IN: The power cord is attached here.

LAN: The LAN port is connected to internal private network for users to access Internet. Default LAN port IP is 192.168.0.1. By connecting to LAN port, user can access the web management interface to configure DLM-3500.

WAN1/WAN2/WAN3/WAN4: The four WAN ports are connected to a network which is not managed by the DLM-3500 system. This port can be used to connect the ATU-Router of ADSL, the Cable Modem, or the Switch or Hub on the LAN of a company. Default WAN1/WAN2/WAN3/WAN4 port IPs are 192.168.1.1, 192.168.2.1, 192.168.3.1 and 192.168.4.1 respectively. An example in the next chapter will show you how to configure WAN ports to correspond to your network environment.

Console Port: The system can be configured via HyperTerminal. The terminal's configuration must be 9600bps, 8, N, 1, flow control - none.

3.2 Package Contents

The standard package of the DLM-3500 includes:

- DLM-3500 x 1
- CD-ROM x 1
- Quick Installation Guide x 1
- Console Cable x 1
- Ethernet Cable (Crossover) x 1
- Switching US Power Adapter x 1
- Power Translator (for EU/UK/AU only) x 1

3.3 System Requirement

- Standard 10/100BaseT including network cables with RJ-45 connectors
- All PCs need to install the TCP/IP network protocol

3.4 Installation Steps

Please follow the steps mentioned below to install the DLM-3500:

1. Connect the power cord to the power socket on the rear panel. The Power LED will light up.
2. Connect one end of an Ethernet cable to the WAN1 Port on the rear panel, and the other end to the WAN connection of the Internet.
3. Connect a cross-over Ethernet cable to LAN Port on the rear panel. The ***LAN*** port is referred to as ***Private LAN*** and the administrator can enter the web management interface to perform configurations via this ***Private LAN***. Connect the other end of the Ethernet cable to a client's PC.

Attention: *Usually a straight RJ-45 can be applied if the DLM-3500 is connected to a hub/computer which supports automatic crossover, such as the Access Point. However, after the Access Point hardware resets, the DLM-3500 may not be able to connect to the Access Point using a straight cable the next time, unless the cable is pulled out and plugged-in again. This scenario does NOT occur while using a crossover cable.*

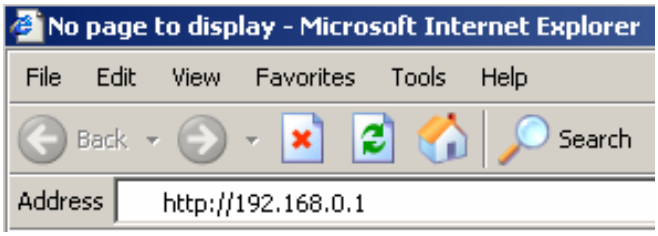
After the hardware of the DLM-3500 is installed completely, the system is ready to be configured in the following sections. This manual will guide you step by step to set up the system using a single DLM-3500 to manage the network.

Chapter 4. Web Interface Configuration

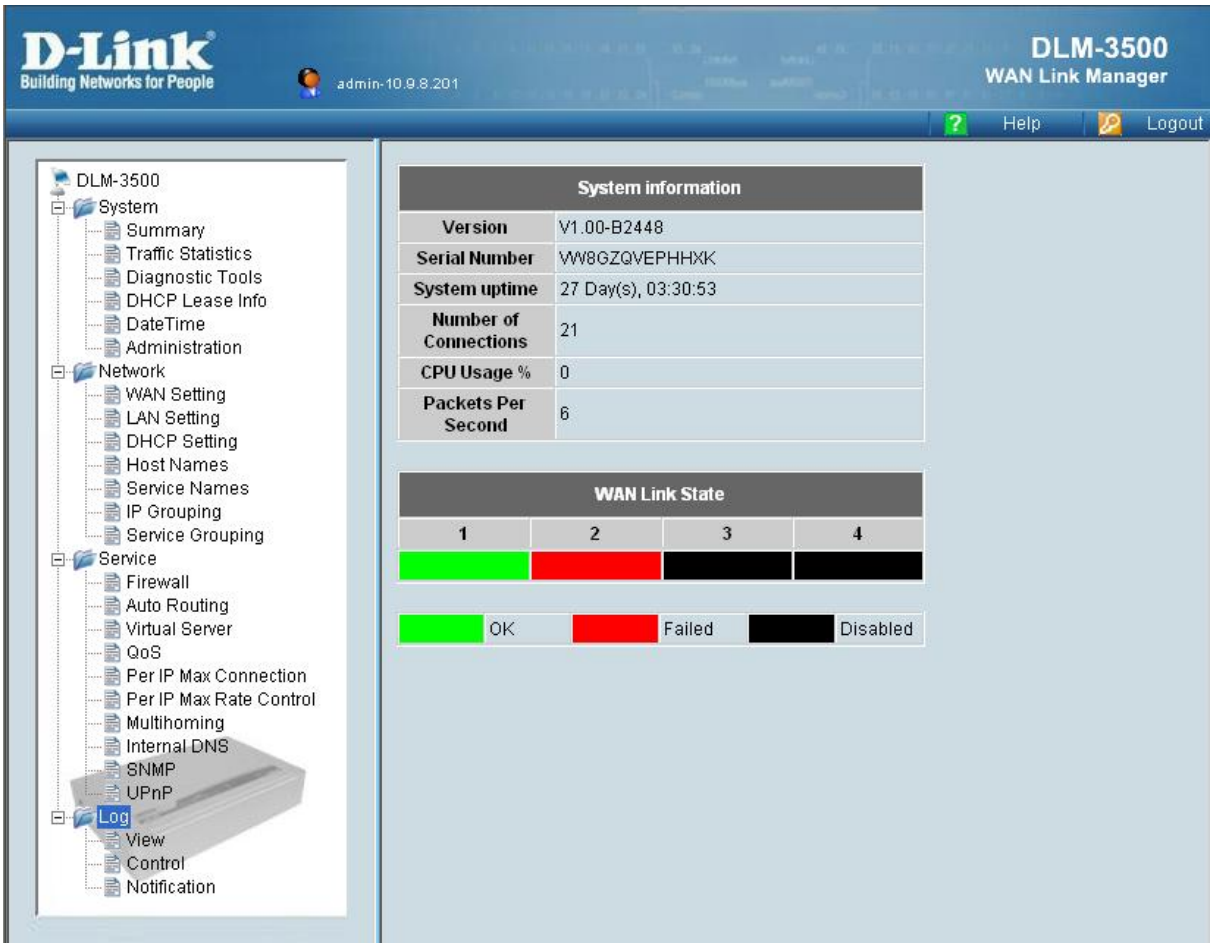
This chapter provides further detailed information on setting up the DLM-3500.

After the basic installation has been completed according to the instructions of the previous chapter, the DLM-3500 can further be configured with the following steps:

1. Use the network cable of the 10/100BaseT to connect a PC to the LAN port, and start a browser (such as Microsoft IE). Next, enter the gateway address for that port in the opened webpage, the default which is http://192.168.0.1. A login screen will then appear. Enter ***"admin"*** for the default username and password and click ***Enter*** to log in.



2. After successfully logging in to the DLM-3500, enter the web management interface and you should see the screen as below:



The following table shows all the functions of DLM-3500.

Option	Function
System	Summary
	Traffic Statistics
	Diagnostic Tools
	DHCP Lease Info
	Date Time
	Administration
Network	WAN Setting
	LAN Setting
	DHCP Setting
	Host Names
	Service Names
	IP Grouping
	Service Grouping
Service	Firewall
	Auto Routing
	Virtual Server

	QoS
	Per IP Max Connection
	Per IP Max Rate Control
	Multihoming
	Internal DNS
	SNMP
	UPnP
Log	View
	Control
	Notification

Apply, **Help**/**Hide Help** and **Logout** buttons are always displayed on the operating menu, the functions are as described below:

After modifying the parameters of specific menu page, click this button to save your changes to memory, the old settings will also be saved.

Click the Help button to display the on-line help of the current page, the on-line help information will automatically swap when you change the function page or language.

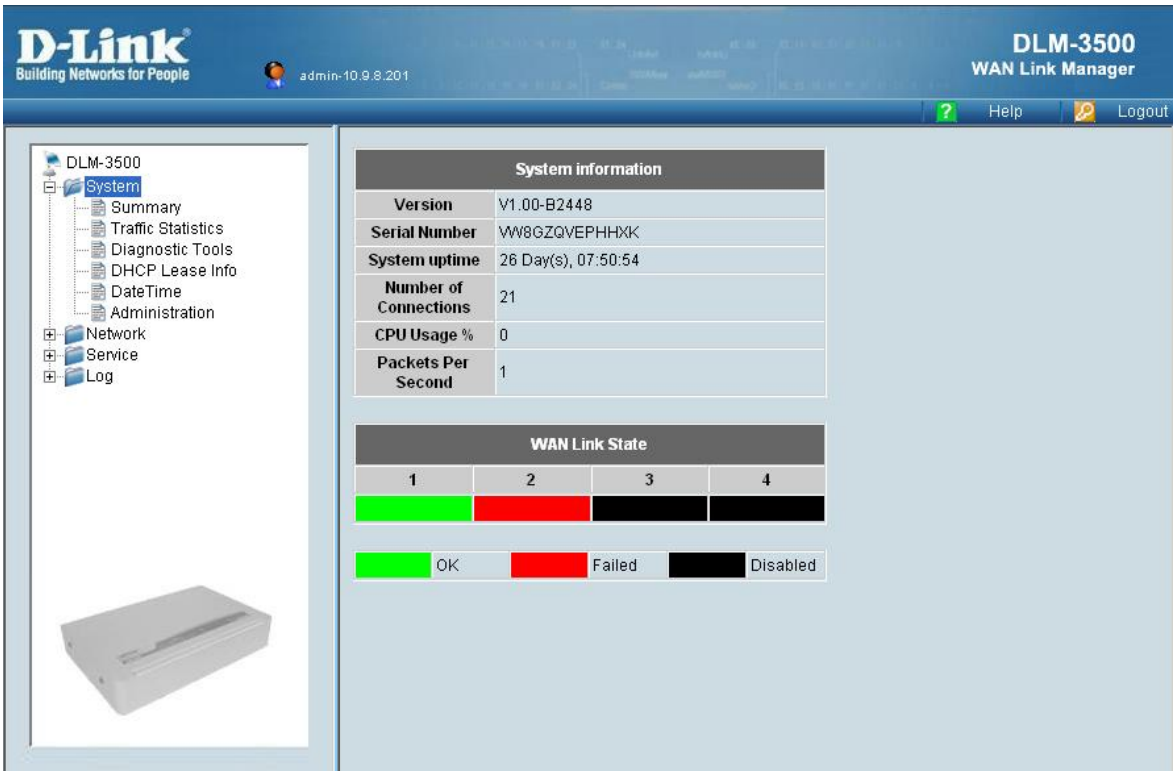
Click Hide Help to hide the on-line help information.

Logout of the system when completed

Caution: *After finishing the configuration, please click* ***Apply*** *and pay attention to see if a restart message appears on the screen. If the message appears, the system must be restarted to allow the settings to take effect. All on-line users will be disconnected during restart.*

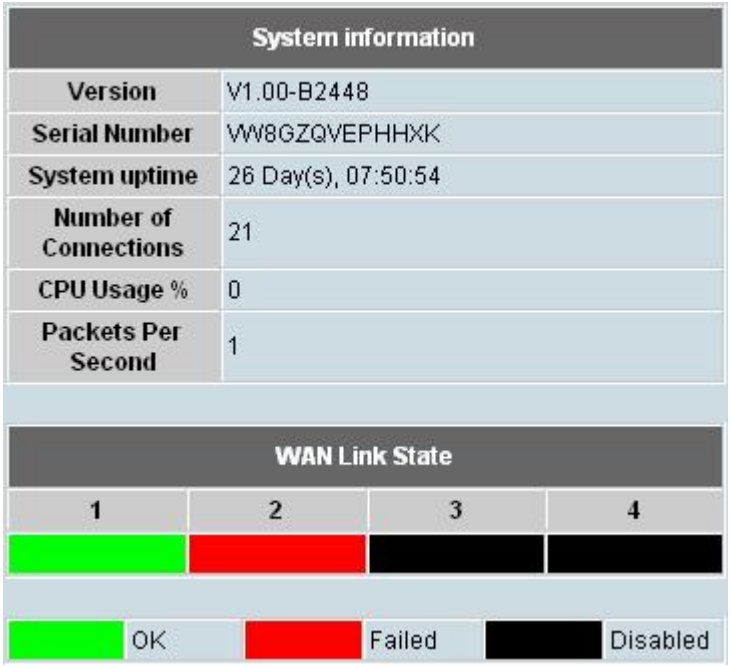
4.1 System

This section provides information on the following functions: **Summary**, **Traffic Statistics**, **Diagnostic Tools**, **DHCP Lease Info**, **Date&Time**, and **Administration**.



4.1.1 Summary

The picture below is what you will see when you first login to DLM-3500's web-based UI. There are two sections on the **Summary** page: **System Information** and **WAN Link State**.



- **System Information**

  This displays the following information of the system:

Category	Field	Description
System Information	Version	The Firmware Version
	Serial Number	The Serial number
	System uptime	The uptime since the last reboot
	Number of Connections	The number of total connections
	CPU Usage %	CPU usage in percentage
	Packets Per Second	Number of packets served per second

Note: *Connections may jump up to over 100 when DLM-3500 is starting up. This is due to many ICMP packets sent out DLM-3500 to test the network. It will revert to normal thereafter.*

- **WAN Link State**

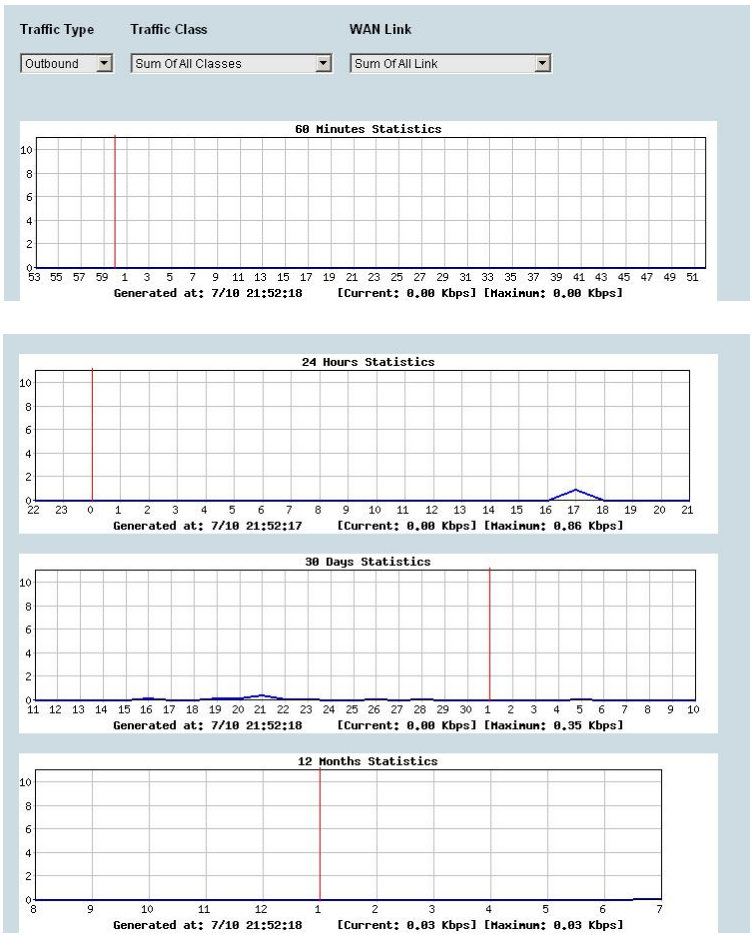
  Show the current status of each WAN link. Each WAN link is represented as a color-coded block with the following color coding scheme to indicate its status:

  - **Green:** Active WAN link
  - **Red:** Broken WAN link
  - **Black:** WAN link not in use

Note: *When you put the mouse on the color-coded block of WAN Link, the IP address will appears.*

4.1.2 Traffic Statistics

In the traffic statistics page, you can inspect real-time traffic information sorted by traffic classes over each WAN link. The statistics of the traffic classes in the table is adjusted accordingly by your selection of **Traffic Type** - either **Inbound** or **Outbound** traffic.



Field	Value	Descriptions
Traffic Type	Inbound Outbound	The direction of traffic flow – either inbound or outbound.
Traffic Class		The names of the traffic classes defined on the QoS page. The rest of the unclassified information is labelled as “Default Class”.
WAN Link	1, 2…	The index number of WAN link you want to inspect.

4.1.3 Diagnostic Tools

There are three sections on this page: **ARP Enforcement, IP Conflict Test,** and **Ping & Trace Route**.

- **ARP Enforcement:**

  ARP Enforcement updates ARP tables of servers and network devices around DLM-3500. When the **Enforce** button is pushed, DLM-3500 sends out ARP packets to the surrounding servers or network devices to update their ARP tables. This is necessary only if certain equipments in DMZ cannot connect to the Internet properly after initial setup.

- **IP Conflict Test:**

  IP Conflict Test helps you to detect if the location of any machine on the network conflicts with the DMZ or WAN settings of the Network Setting category on DLM-3500. Push **Test** button to begin the test. The result of the test is one of the following:

  - Everything is ok.
  - DLM-3500 discovers a machine in DMZ conflicts with Network Setting on DLM-3500. For example, a public IP address should be in WAN but is used by a machine in DMZ. In this case, an error message with the conflicting IP address and MAC address of the machine will be displayed.
  - DLM-3500 discovers a machine in WAN conflicts with Network Setting on DLM-3500. For example, a public IP address should be in DMZ but is used by a machine in WAN. In this case, an error message with the conflicting IP address and MAC address of the machine will be displayed.

- **Ping and Trace Route:**

  Ping is used to detect network condition by sending ICMP packets to a target device. You may specify a target device in the Target IP field. Either IP address or host name is acceptable. Select a network interface, WAN or LAN. If it is WAN, select WAN link number in Index field. For error messages relating to ICMP, please refer to the relevant document.

Caution: *If a domain name is used to ping, a DNS server has to be specified in* ***Network→Host Names****.*

Trace Route: Trace route is used to detect network condition by showing the routing path from DLM-3500 to the target device.

You may specify a target device in the Target IP field. It accepts either an IP address or a host name. Select a network interface, WAN or LAN. If it is WAN, select WAN link number in Index field. For ICMP related error messages, please refer to other relevant materials.

You may specify a target device in the Target IP field. It accepts either an IP address or FQDN. Select a network interface, WAN or LAN. If it is WAN, select WAN link number in Index field.

Caution: *If a domain name is used to traceroute, a DNS server has to be specified in* ***Network→Host Names****.*

Arping: Arping is used to detect the MAC address of a computer.

You may specify a target device in the Target IP field. It accepts either an IP address or a host name. Select a network interface (WAN, LAN). If it is WAN, select WAN link number in Index field. For ARP related error messages, please refer other relevant materials.

Caution: *If a host name is used in Target IP field, then a DNS server has to be specified in* ***Network→Host Names****.*

4.1.4 DHCP Lease Info

This page shows the information regarding data assigned through a DHCP lease, such as IP address and its corresponding MAC address, client-hostnames, and expiration date. DHCP Lease Info contains for items:

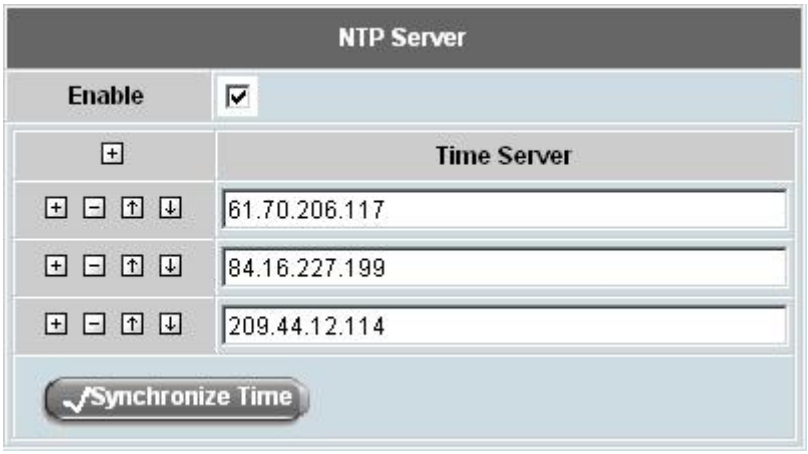
- **Address:** the MAC address of the client's machine
- **IP:** the IP address assigned to client's machine
- **Hostname:** the name of the client's machine
- **Time:** the time period during which the IP address is valid

4.1.5 Date&Time

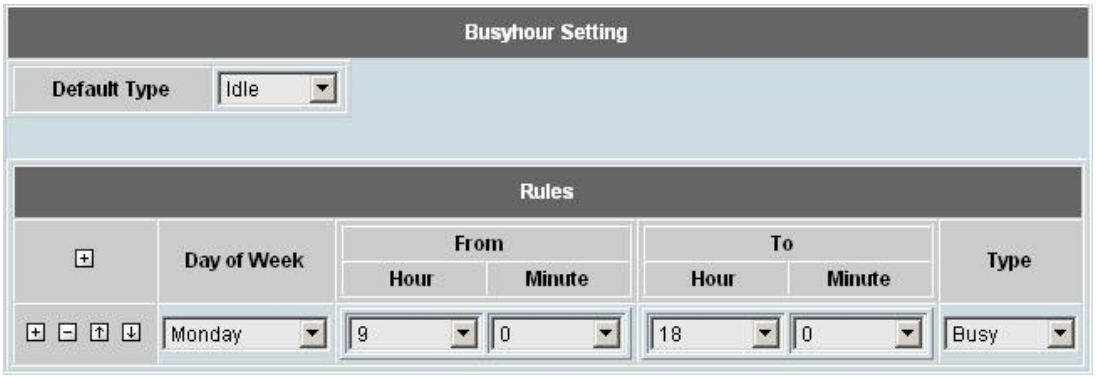
In this page, you can set up time related configurations. There are four sections on this page: **Date&Time Setting**, **NTP Server**, **Busyhour Setting**, and **Rules**.

- **Date&Time Setting:** For time zone information, you should pick the region first and then the city you are located in (or a city of the same time zone as you). For example, if you are located in Hawaii, select US in the left list and then choose Hawaii in the right list.

- **NTP Server:** DLM-3500 can use the NTP protocol to get time from the Internet. You can select a time server from the list or add your preferred time server to the list. With NTP, DLM-3500 automatically adjusts its time when necessary. You can also push the Synchronize Time button to adjust time immediately.



- **Busyhour Setting:** Busyhour Setting is very important from a MIS manager's point of view. It provides a tool for you to define two time segments: busy-hour and idle-hour. All other rule-based services such as bandwidth management and auto-routing can take advantage of this function. For example, you can define 9:00 am to 5:00 pm, Monday through Friday to be busy-hour. This will help reserve bandwidth to business-related network traffic during busy-hour and relax the rule on idle-hour.
-



Field	Value	Description
Default Type	Idle Busy	Define default type to be either Idle or Busy hour.
Rules	-	You set the time segment rules in this table. They are matched in sequence on a first-match basis. If none of the rules match, the default type is used.
Day of Week	Sunday Monday Tuesday Wednesday Thursday Friday Saturday Any Day	Day of the week.
From	<Hour/Minute>	The start time.
To	<Hour/Minute>	The end time.
Type	Busy Idle	If the current time matches the day of the week and in between From and To time, then Type field applies.

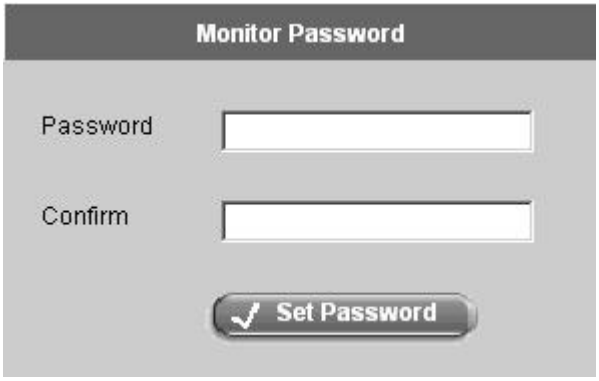
4.1.6 Administration

You can do a few administrative tasks on this page: **Administrator Password**, **Monitor Password**, **Firmware Update**, **Configuration File**, and **Maintenance**.

- **Administrator Password:** You can add, delete, or modify the administrator's account and password.

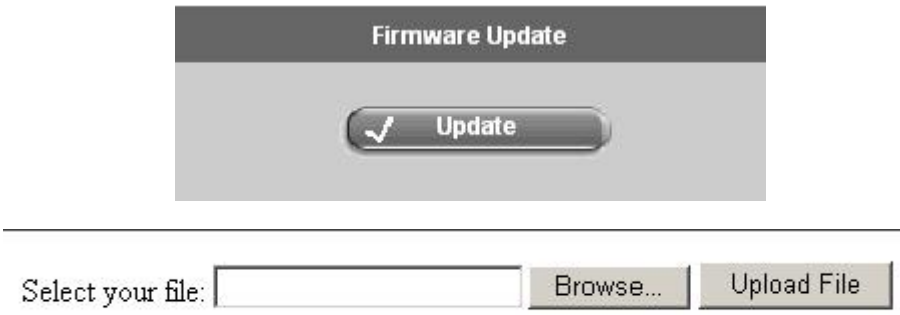
Field	Value	Description
New Password		Enter the new password here.
Confirm		Enter the new password here again.
Set Password		Click this button to enable the new password.

- **Monitor Password:** You can add, delete, or modify the monitor's account and password.



Field	Value	Descreption
New Password		Enter the new password here.
Confirm		Enter the new password here again.
Set Password		Click this button to enable the new password.

- **Firmware Update:** Push the **Update** button and follow the instructions below to start the firmware update process:
    1. Obtain the latest firmware pack.
    2. Log on to Web UI as the Administrator and go to function **System→ Administration**.
    3. Use **Browse...** to select the path to the new firmware image, and then select **Upload.**
    4. Update is successfully completed when the **Update succeeded** message appears. Power off and on the system to restart DLM-3500 with the new firmware.



Caution: *The firmware update takes a while to complete, so please be patient. During the update processes, BE SURE not to turn off the system or pull the power plug. You should also NOT click the* ***Upload*** *button.*

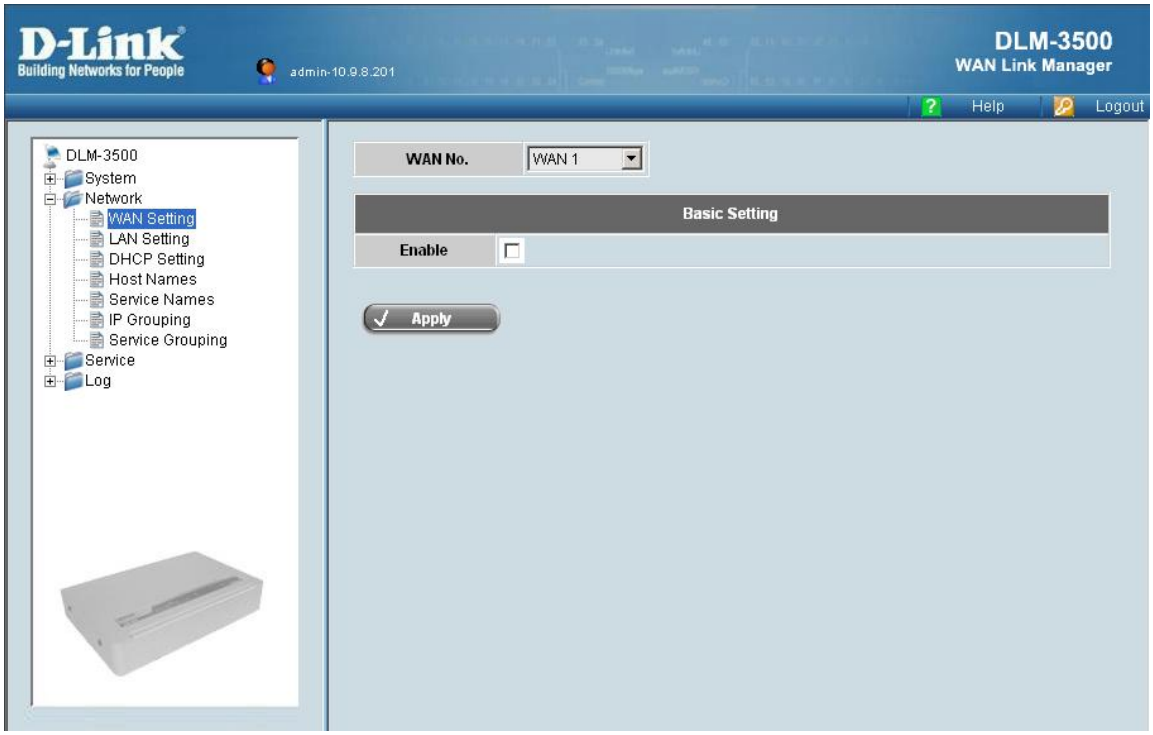
- **Configuration File:** Push the **Save** button to save current configurations into a file. Push **Restore** button to restore a previously saved configuration file.
    1. Login to DLM-3500 as the Administrator. In the Web UI, go to **System→ Administration** and select **Configuration File → Save** to backup the configuration file to your local machine/notebook.
    2. To restore to the previously saved configuration file, go to **Configuration File→ Restore**, select **Browse...** to choose the required saved configuration file and select **Upload.**
    3. Restart DLM-3500 to effect the configuration.

Caution: *DO NOT turn off the power during the config file upload process, or repetitively select the* ***Upload*** *button.*

- **Maintenance:** Push **Factory Default** button to reset DLM-3500 configurations to its factory default. You can do the same operation using **resetconfig** command in console. Push **Reboot** button to reboot DLM-3500.

4.2 Network

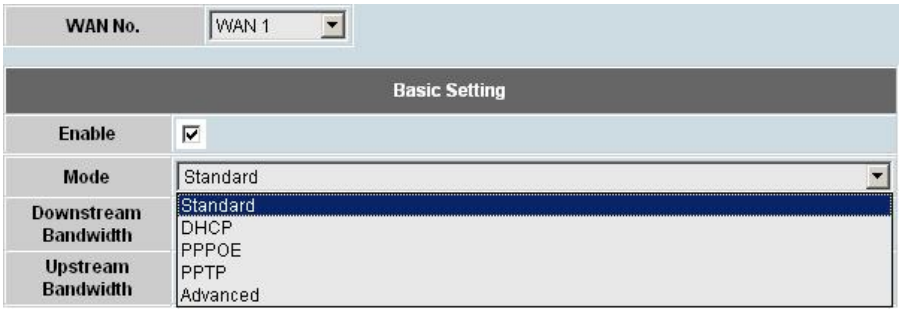
This section provides information on the following functions: **WAN Setting**, **LAN Setting**, **DHCP Setting**, **Host Names**, **Service Names**, **IP Grouping**, and **Service Grouping**.



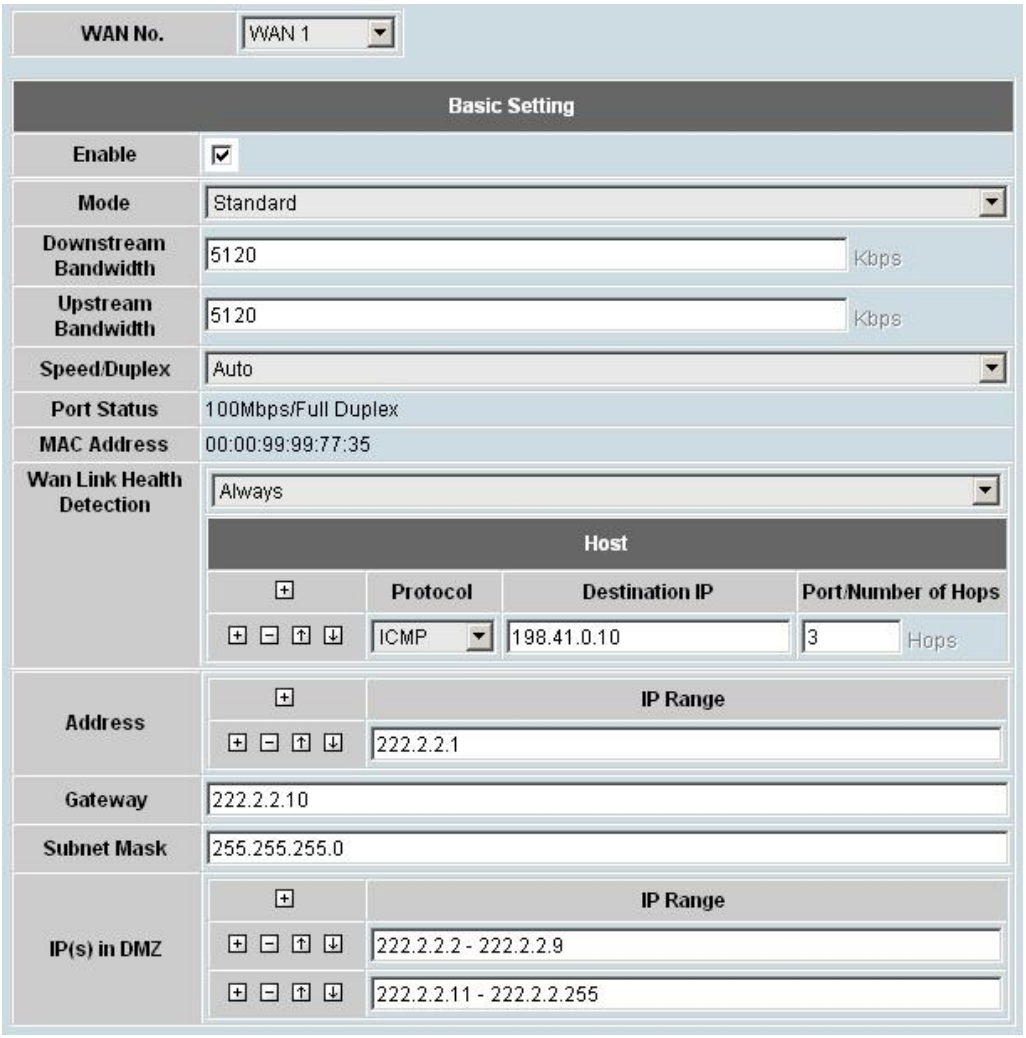
4.2.1 WAN Setting

WAN Setting is important for DLM-3500. The relevant parameters for configuring WAN are defined in this chapter. The configuration is to be done on one WAN link at a time. You can however apply all the changes at once at the end. There are two steps to complete the WAN setting:

- **WAN No.:** Select a WAN link by selecting the link number in the WAN No. drop-down box.
  Basic Setting: For each WAN link, you will fill out a few parameters with correct information from the ISP.
  Enable: Tick the checkbox to enable the basic setting of the selected WAN link.
  Mode: Select the WAN mode from the drop-down menu. Options available are **Standard**, **DHCP**, **PPPOE**, **PPTP** and **Advanced**. The rest of the settings will change based on the WAN mode you have selected.



4.2.1.1 Standard Mode



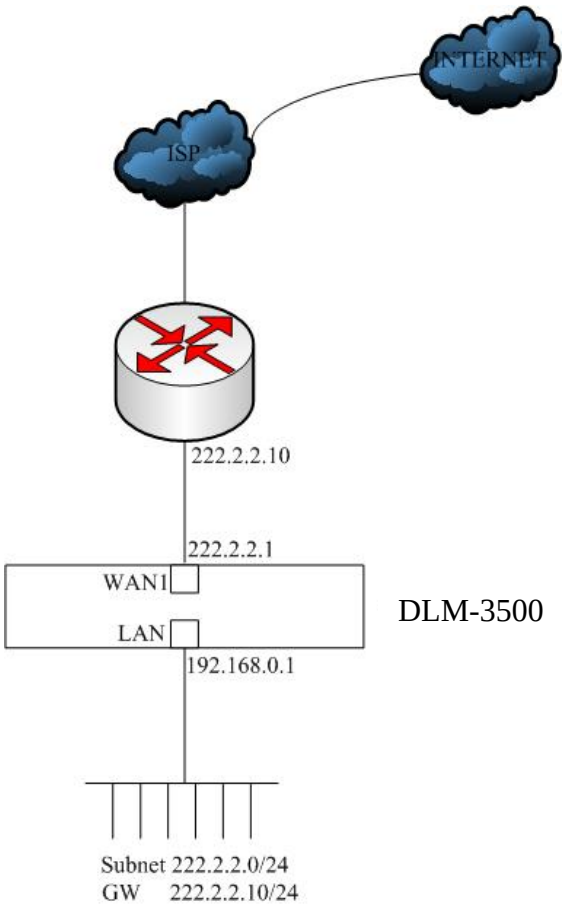
When you select **Standard** mode, you need to fill the parameters as shown below in the **Basic Setting** table.

- **Basic Setting:**

Field	Value	Description
Downstream Bandwidth		The down stream (inbound) bandwidth of the WAN link, for example 25600 (Kbps).
Upstream Bandwidth		The up stream (outbound) bandwidth of the WAN link, for example 25600 (Kbps).
Speed Duplex	Auto 10Mbps/Half duplex 10Mbps/Full duplex 100Mbps/Half duplex 100Mbps/Full duplex	The speed and duplex of WAN Port. You can set it manually or let the system obtain it automatically.

Port Status	10Mbps/Half duplex 10Mbps/Full duplex 100Mbps/Half duplex 100Mbps/Full duplex	Self-detected by device.
MAC Address	xx-xx-xx-xx-xx-xx	Self-detected by device.
WAN Link Health Detection	Never Always Only when no packet is received	This function is for configuring the WAN link health detection mechanism for the specific WAN link.
Address	IP Address IP Range	Input the IP Address of DLM-3500 in WAN. It can be: ▪ IP Address ▪ IP Range
Gateway		Input the predefined Gateway, e.g.: 211.21.40.254.
Subnet Mask		Input the Subnet Mask.
IP(s) in DMZ *	IP Address IP Range	Input the IP Address of DLM-3500 in DMZ. It can be: ▪ IP Address ▪ IP Range

Caution: If ISP provides user with multiple public IPs or a subnet public IPs beside the WAN IP, other IPs can be assigned to DMZ. Servers such as Web servers can be positioned at DMZ with public IPs. Physically, DLM-3500 has no DMZ port, and servers with public DMZ IP are located in LAN. This configuration however will let these servers be logically treated as within the DMZ.*



- **Wan Link Health Detection:**

Wan Link Health Detection	Always			
	Host			
	Protocol	Destination IP	Port/Number of Hops	
	ICMP	222.34.56.78	5	Hops
	TCP	211.11.33.56	25	Port
	ICMP	202.99.96.68	8	Hops
	TCP	168.95.1.1	110	Port
	ICMP	222.96.2.4	4	Hops
	TCP	202.99.92.13	80	Port

This function allows MIS to configure how WAN link health detection is performed. By fine-tuning certain parameters, an MIS can adjust DLM-3500 to match a particular network structure and/or a particular ISP.

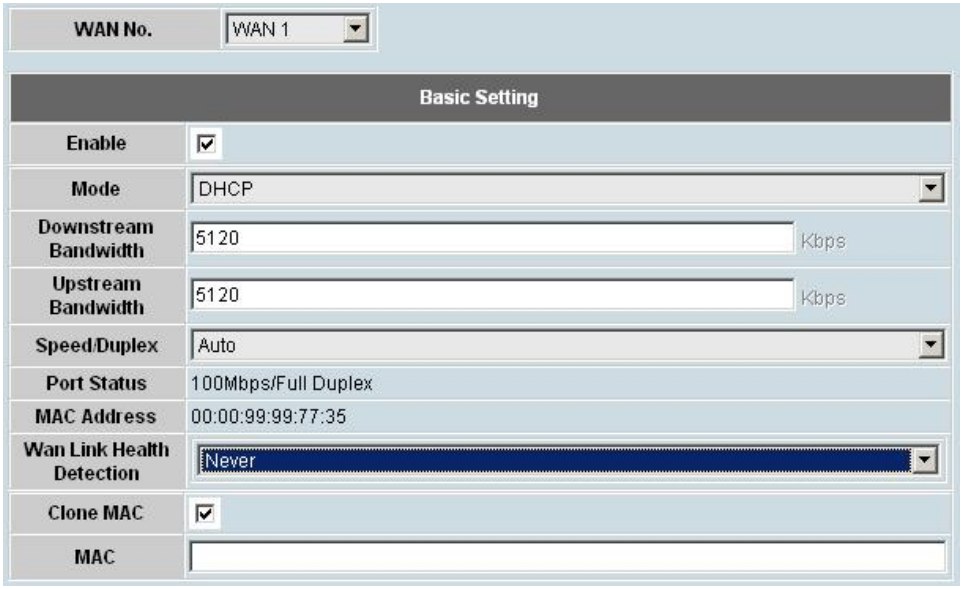
For WAN link health detection, DLM-3500 sends out ICMP or TCP packets and monitors responses to determine the statuses of the links. In the WAN Link Health Detection page, the following parameters are available:

Field	Description
Never	DLM-3500 assumes a healthy WAN and stop monitoring ICMP and TCP packets.
Always	DLM-3500 will always do the health detection according to the rules.
Only when no packet is received	If DLM-3500 detects no inbound WAN traffic, it will start the health detection.
Protocol	Choose either ICMP or TCP as methods for WAN health detection.
Destination	Input the destination IP Address.
Port/Number of Hops	Set the Hops* if ICMP is selected. Set the Port number if TCP is selected.

Caution: If ICMP is selected to do health detection, user can define the number of hops respond of ICMP packet for the WAN link to be considered as healthy. For example, a user configures the number of hops as 5, and after the health detection packet has been sent out from the DLM-3500, if the DLM-3500 receives ICMP respond packet with 5 hops between source and destination site, this WAN link is considered healthy. The default number of hops is 3. You can assign any number above 0.*

4.2.1.2 DHCP Mode

This mode is enabled when DLM-3500 is a client using DHCP to acquire a dynamic IP address from an ISP's DHCP server. You will need to fill in the following parameters:

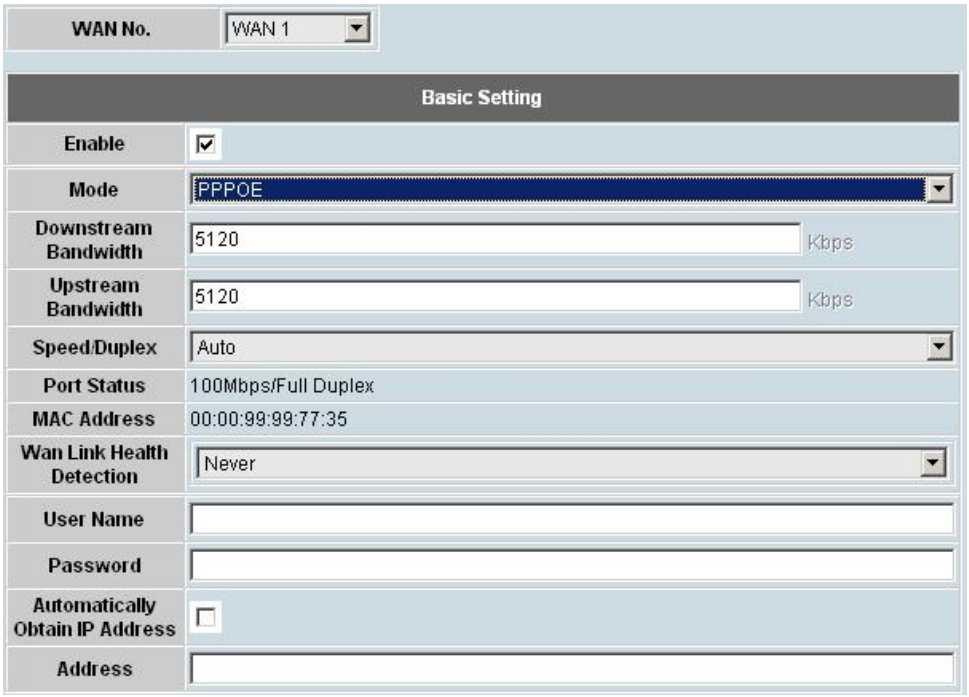


Field	Value	Description
Downstream Bandwidth		The down stream (inbound) bandwidth of the WAN link, for example 25600 (Kbps).
Upstream Bandwidth		The up stream (outbound) bandwidth of the WAN link, for example 25600 (Kbps).
Speed/Duplex	Auto 10Mbps/Half duplex 10Mbps/Full duplex 100Mbps/Half duplex 100Mbps/Full duplex	The speed and duplex of WAN Port. You can set it manually or let the system obtain it automatically.
Port Status	10Mbps/Half duplex 10Mbps/Full duplex 100Mbps/Half duplex 100Mbps/Full duplex	Self-detected by device.
MAC Address	xx-xx-xx-xx-xx-xx	Self-detected by device.
WAN Link Health Detection	Never Always Only when no packet is received	This function is for configuring the WAN link health detection mechanism for the specific WAN link. Please refer to Chapter 4.2.1.1 WAN Link Health Detection.

Clone MAC		Normally the DHCP will assign IP dynamically. Static IP, however, can be assigned to the WAN link via the DHCP server with MAC address binding. You can enable the 'Mac Cloning' option to force the DHCP server to assign the static IP according to the DLM-3500's MAC address. MAC address format: xx-xx-xx-xx-xx-xx

4.2.1.3 PPPOE Mode

PPPoE is a popular bridging mode protocol for ADSL. You need to specify the PPPoE account information to obtain IPs from the ISP PPPoE server.



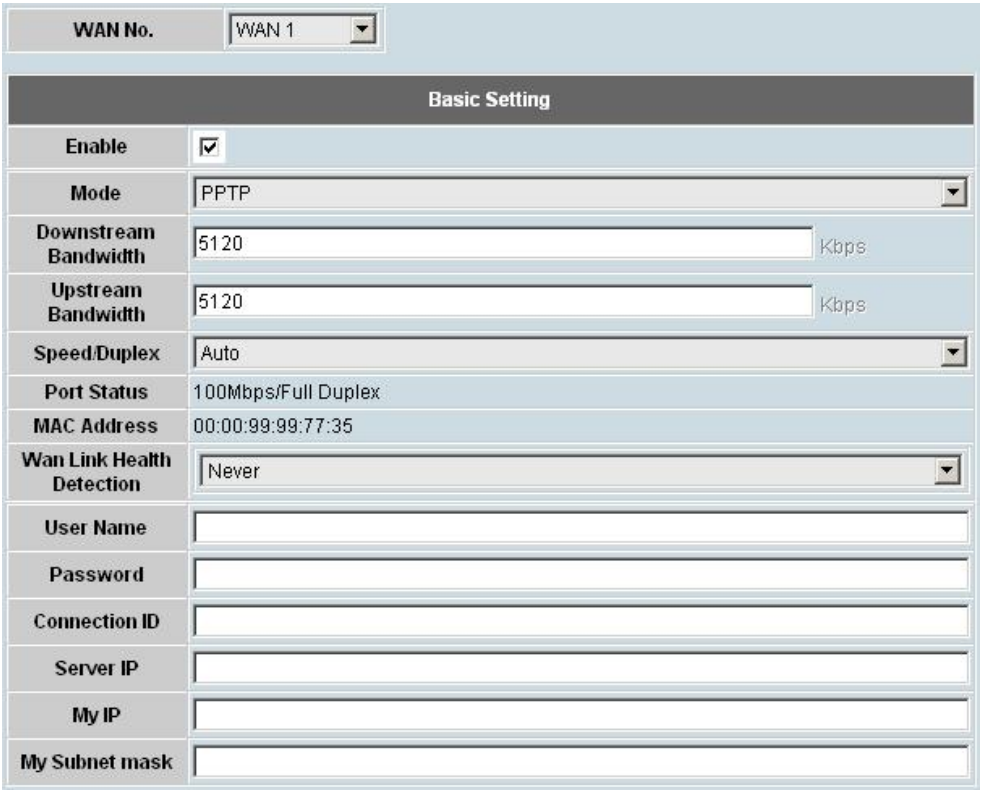
Field	Value	Description
Downstream Bandwidth		The down stream (inbound) bandwidth of the WAN link, for example 25600 (Kbps).
Upstream Bandwidth		The up stream (outbound) bandwidth of the WAN link, for example 25600 (Kbps).
Speed/Duplex	Auto 10Mbps/Half duplex 10Mbps/Full duplex 100Mbps/Half duplex 100Mbps/Full duplex	The speed and duplex of WAN Port. You can set it manually or let the system obtain it automatically.
Port Status	10Mbps/Half duplex 10Mbps/Full duplex 100Mbps/Half duplex 100Mbps/Full duplex	Self-detected by device.
MAC Address	xx-xx-xx-xx-xx-xx	Self-detected by device.

WAN Link Health Detection	Never Always Only when no packet is received	This function is for configuring the WAN link health detection mechanism for the specific WAN link. Please refer to Chapter 4.2.1.1 WAN Link Health Detection.
User Name		Input the user's account assigned by ISP.
Password		Enter the password of the account.
Automatically Obtain IP Address		Enable this function, and ISP will provide IP Address, Gateway and Netmask. Note: If your ADSL is using dynamic IP, check the checkbox. If it is using static IP, please do not.
Address	x.x.x.x	Input the IP Address assigned by ISP.

Caution**:** *If your ADSL is using dynamic IP, check the checkbox. If it is using static IP, DO NOT check the checkbox. Input the IP address assigned by the ISP in the field of* ***Address****, which only appears when the checkbox is unchecked.*

4.2.1.4 PPTP Mode

This mode is enabled when DLM-3500 accesses to the PPTP server. You will need to fill in the following parameters:



Field	Value	Description
Downstream Bandwidth		The down stream (inbound) bandwidth of the WAN link, for example 25600 (Kbps).
Upstream Bandwidth		The up stream (outbound) bandwidth of the WAN link, for example 25600 (Kbps).
Speed/Duplex	Auto 10Mbps/Half duplex 10Mbps/Full duplex 100Mbps/Half duplex 100Mbps/Full duplex	The speed and duplex of WAN Port. You can set it manually or let the system obtain it automatically.
Port Status	10Mbps/Half duplex 10Mbps/Full duplex 100Mbps/Half duplex 100Mbps/Full duplex	Self-detected by device.
MAC Address	xx-xx-xx-xx-xx-xx	Self-detected by device.

WAN Link Health Detection	Never Always Only when no packet is received	This function is for configuring the WAN link health detection mechanism for the specific WAN link. Please refer to Chapter 4.2.1.1 WAN Link Health Detection.
User Name		Input the user name for VPN login.
Password		Input the password for VPN login.
Connection ID		Input the ID for Connection through VPN.
Server IP	x.x.x.x	Input the PPTP Sever IP Address for VPN dialing.
My IP	x.x.x.x	Input the IP Address used to connect to PPTP server, this IP will be assigned to the wan link. ISP should provide this IP.
My subnet mask		Input the Subnet Mask of “My IP”. ISP provides it.

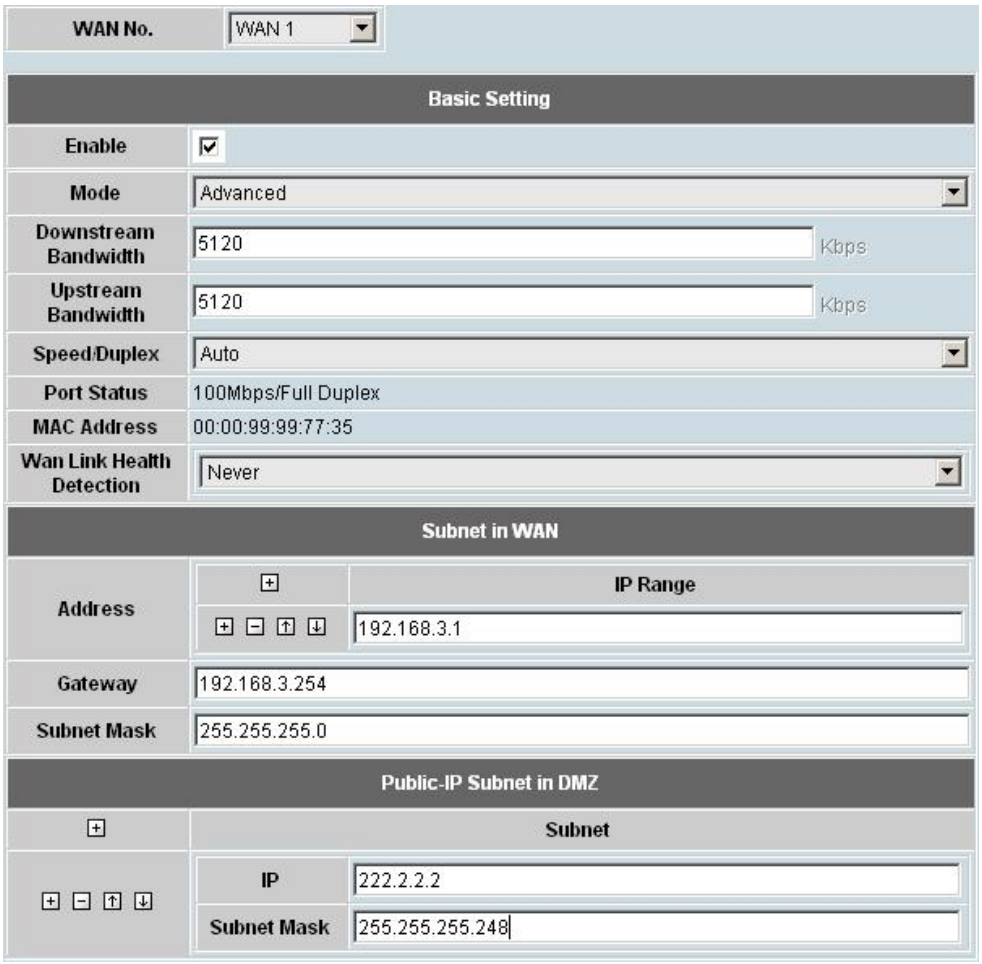
Caution:

Connection ID is provided by your ISP. If your ISP does not use this, leave it blank.

My IP and **My subnet mask** are provided by the ISP. if your ISP did not provide you the information, you may do the following: Set My IP in the same subnet with the routers IP and place the corresponding subnet mask with it. The ISP will assign a new IP for you when you establish the PPTP connection.

4.2.1.5 Advanced Mode

In the advanced mode, you will need to fill in the information for three settings: **Basic Setting**, **Subnet in WAN** and **Public-IP Subnet in DMZ**.



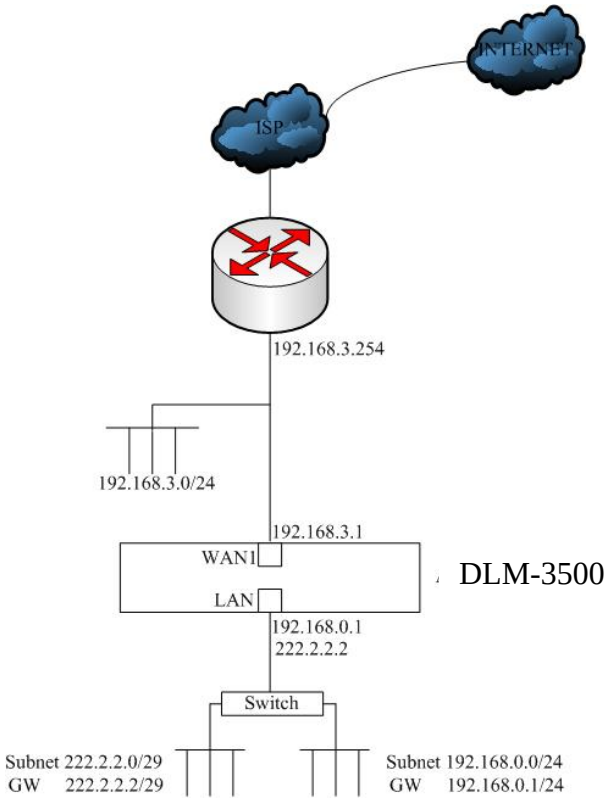
Field	Value	Description
Downstream Bandwidth		The down stream (inbound) bandwidth of the WAN link, for example 25600 (Kbps).
Upstream Bandwidth		The up stream (outbound) bandwidth of the WAN link, for example 25600 (Kbps).
Speed/Duplex	Auto 10Mbps/Half duplex 10Mbps/Full duplex 100Mbps/Half duplex 100Mbps/Full duplex	The speed and duplex of WAN Port. You can set it manually or system can get it automatically.

Port Status	10Mbps/Half duplex 10Mbps/Full duplex 100Mbps/Half duplex 100Mbps/Full duplex	Self-detected by device.
MAC Address	xx-xx-xx-xx-xx-xx	Self-detected by device.
Wan Link Health Detection	Never Always Only when no packet is received	This function is for configuring the WAN link health detection mechanism for the specific WAN link. Please refer to Chapter 4.2.1.1 WAN Link Health Detection.
Subnet in WAN		
Address	IP Address IP Range	Input the private IP address of DLM-3500 connected with the router. There are two options available: IP Address IP Range
Gateway		Input the predefined Gateway, e.g.: 192.168.99.1.
Subnet Mask		Input the Subnet Mask.
Public-IP Subnet in DMZ		
IP *		Input the public IP of DLM-3500 in DMZ
Subnet Mask		Input the Subnet Mask.

Caution: **The difference between "Public-IP Subnet in DMZ" in the Advanced Mode, and "IP(s) in DMZ" in the Standard Mode, are as follows:*

If the IP address in DMZ and the IP address in WAN are in the same subnet, then you have to use the Standard Mode; if they are in the different subnet, then you have to use the Advanced Mode.

Take the figure below as the example. The administrator sets the subnet of WAN1 as 192.168.3.0/24; meanwhile, he wants to set a public subnet 222.2.2.0/29 in the DMZ. In this case, the administrator will need to set the Gateway and Subnet Mask of the subnet in the DMZ using 222.2.2.2 and 255.255.255.248 respectively.


INTERNET
ISP
192.168.3.254
192.168.3.0/24
192.168.3.1
WAN1
LAN
DLM-3500
192.168.0.1
222.2.2.2
Switch
Subnet 222.2.2.0/29
GW 222.2.2.2/29
Subnet 192.168.0.0/24
GW 192.168.0.1/24

4.2.2 LAN Setting

There are two sections on this page: **Basic Subnet** and **Static Routing Subnet.**

- **Basic Subnet:** Basic Subnet allows you to specify one or more private subnets connecting to the DLM-3500 directly.

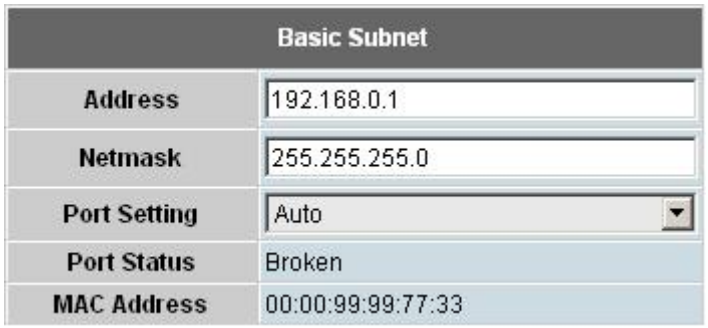
  Address: Input the IP address of LAN Port

  Netmask: input the corresponding subnet mask

  Port Setting: Select the corresponding Speed/Duplex

  Port Status: Self-detected by device

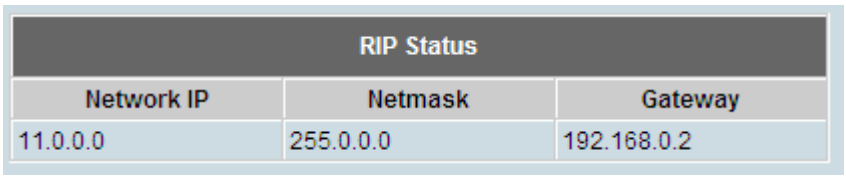
  MAC Address: Self-detected by device



- **RIP:** DLM-3500 supports RIP (Routing Information Protocols) for both version 1 and 2. Please refer to IETF's official documents for the complete definition of RIP. If your private LAN subnet supports RIP, you need to also enable DLM-3500's RIP function, by doing as follows:

  If the router in LAN enables RIP v1, check the checkbox in front of RIP v1. If the router in LAN enables RIP v2, check the checkbox in front of RIP v2. DLM-3500 supports the transmission of RIP packets. If the authentication is enabled on RIP V2, password must be entered in Authentication Password field. If there is no predefined password, just leave the field blank.

A **RIP Status** table will show on the screen if **RIP** is enabled.

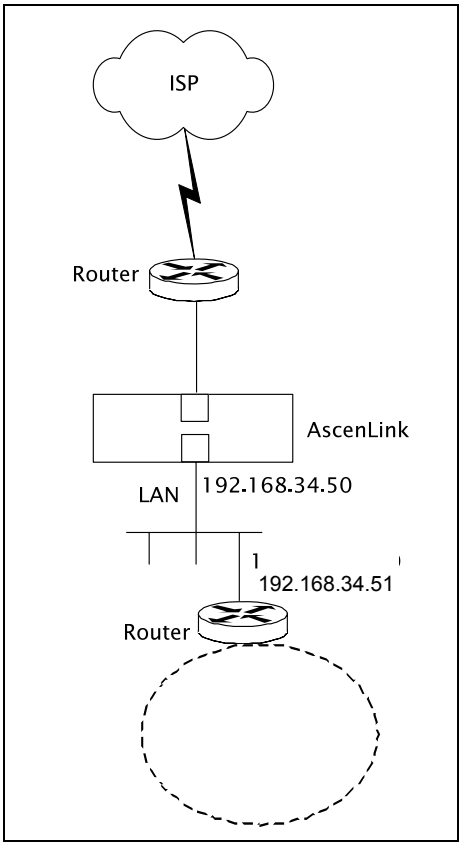


Static Routing Subnet: If there is static routing subnet in the LAN, you will need to specify the Static Routing Subnet in the configuration. When Static Routing Subnet is used, the router will route through the subnet from LAN to a destination not connected to the DLM-3500 directly.

Static Routing Subnet			
⊞	Subnet	Subnet Mask	Gateway

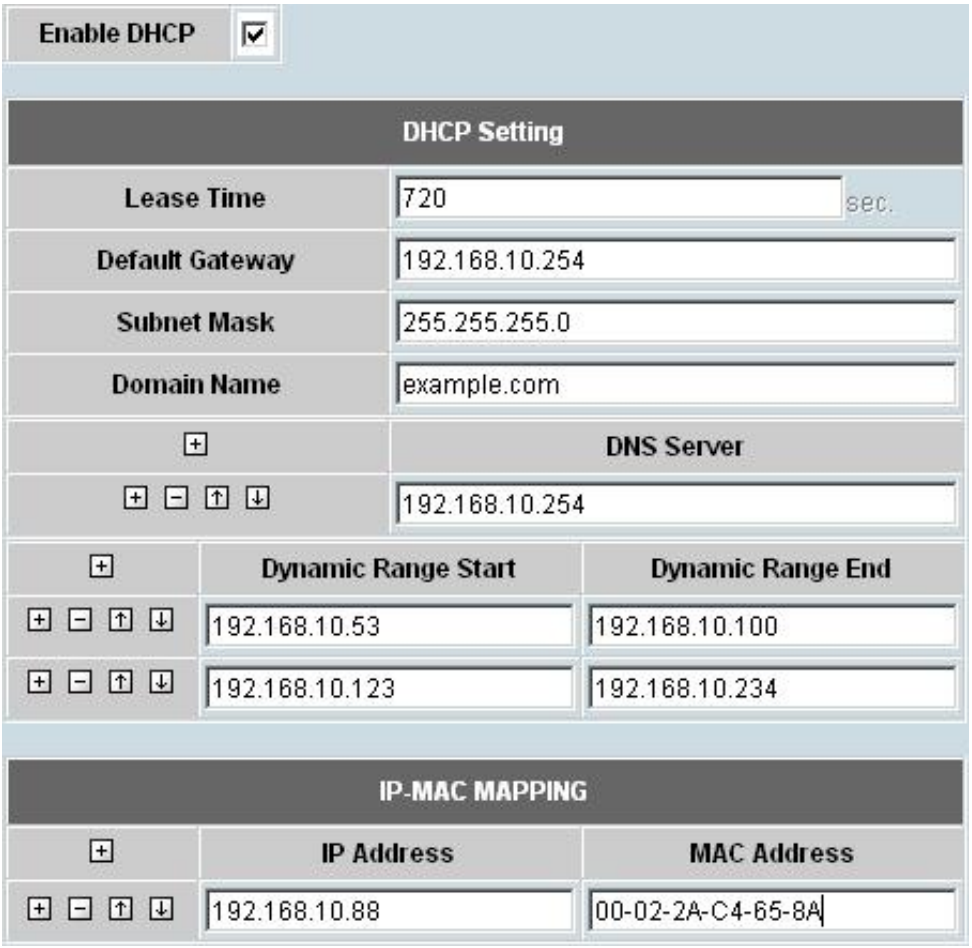
***Caution**: The DMZ is a virtual area, such as in the port of a router within the LAN, assigned as a "neutral zone" between the company's private network and the outside public network. The DLM-3500 supports DMZ public IP addressing for only one IP range, and does not support multi-IP range Routing.*

Example:



4.2.3 DHCP Setting

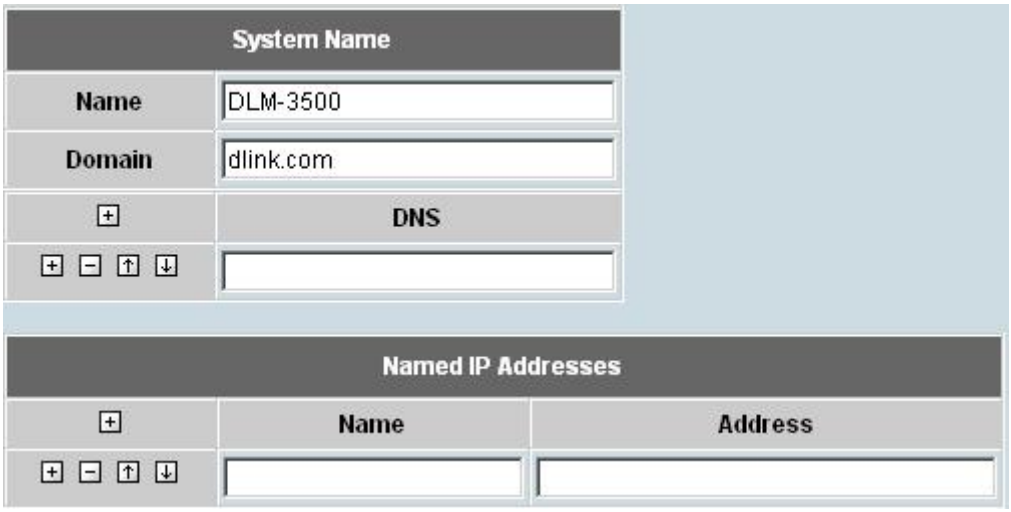
Click on **Enable DHCP** to enable this function. Client can use DHCP to acquire a dynamic IP address from DLM-3500's DHCP server. You will have to fill out two tables: **DHCP Setting** and **IP-MAC MAPPING**.



Field	Description
Lease Time	Input the Lease Time by hour.
Default Gateway	Input the Default Gateway. The Client will take this address as Gateway when DHCP is enabled. Note: This address should be in the subnet of LANs
Subnet Mask	Input the IP Address of DNS. The Client will take this address as DNS Server when DHCP is enabled.
Domain Name	Input the Domain Name of DHCP.
DNS Server	Input the IP Address of DNS.
Range Start -Range End	Input the dynamic Range Start and Range End assigned for LAN host, e.g. 192.168.10.53 -199.168.10.100
IP -MAC Address	If the host in LAN requires a static IP Address, input IP Address and IP-MAC Address. MAC address format: xx-xx-xx-xx-xx-xx

4.2.4 Host Names

This function defines system name, and specify IP address and IP group. The defined names will appear in the sub-menu of source and destination in Firewall, Multihoming, etc. There are two tables to be filled out: **System Name** and **Named IP Address.**



- **System Name:** You need to fill in three items:

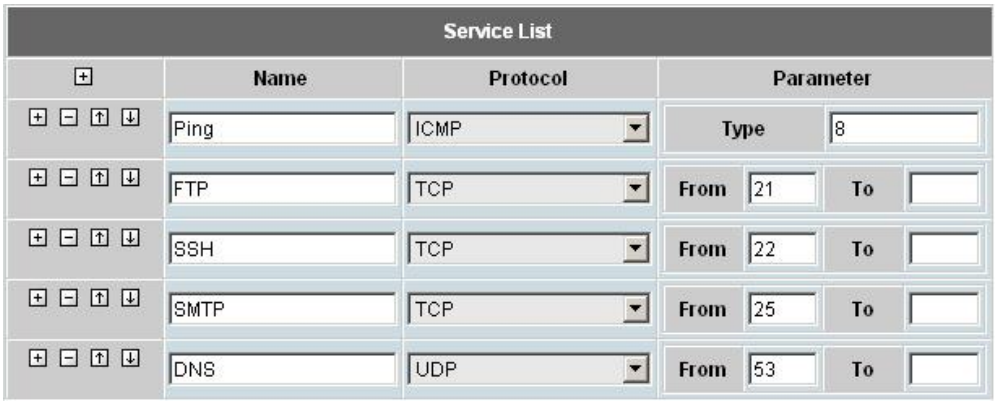
Field	Description
Name	Input the host name of the DLM-3500.
Domain	Input the domain of the DLM-3500.
DNS	Input the IP Address of the DNS, and the DLM-3500 will use it to resolve machine names to obtain IP addresses.

- **Named IP Address:** Specify the Name and Address in the table.

Field	Description
Name	Input the name which is to be substituted for the IP address.
Address	Specify the IP Address. It can be: ▪ IP Address ▪ IP Range

4.2.5 Service Names

This function is for configuring the **Name**, **Protocol**, and other **Parameter**s of service. DLM-3500 comes with a default list of commonly used services. These defined names will appear in the sub-menu of service in Firewall, Multihoming, etc.

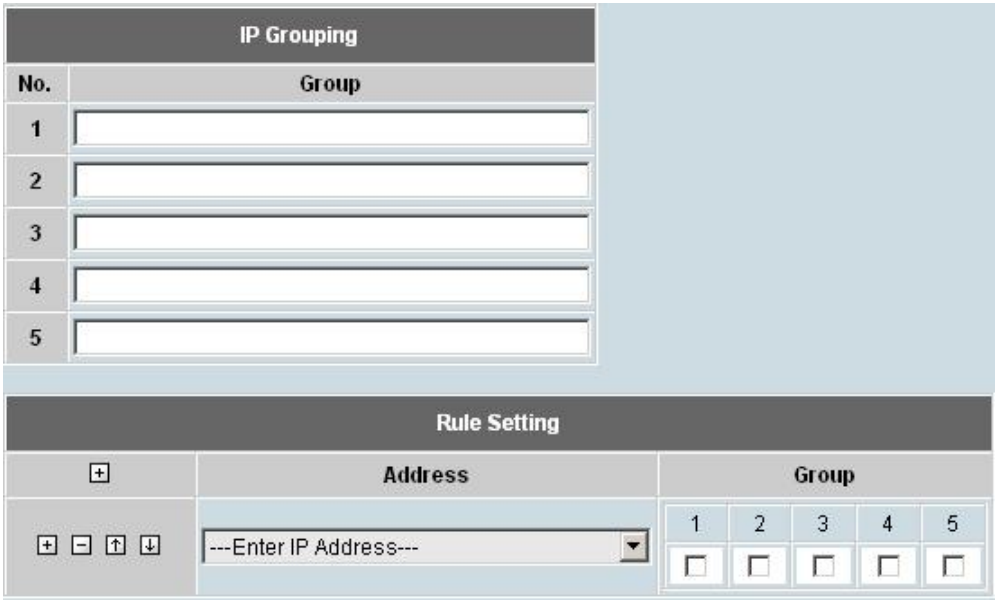


Field	Value	Description
Name	-	Input the name of the service, e.g. PING, FTP…
Protocol	Protocol Number ICMP TCP UDP	Select protocol for service: Protocol Number, e.g. ICMP Protocol Number is “1”, TCP is “6”. For more information, please refer to related document*. ICMP: The service used ICMP, e.g. Ping. TCP: The service used TCP, e.g. FTP. UDP: The service used UDP.
Parameter	Number Type From…To	Specify the parameter for different Protocols. Number: Input Protocol Number. Type: Input the service type of ICMP. From...To: Input the Port Number of TCP/UDP. Single Port Number: A range of Port Number: Input the start port number in [From] and the end port number in [To].

Caution: DLM-3500 provides ICMP, TCP and UDP for selection in the field “Protocol”. If you need other protocols, such as IGMP or GRE, you can select “Protocol Number” and fill in the protocol number, such as 2 and 47 for IGMP and GRE respectively. For other protocol number, please refer to related document such as RFC.*

4.2.6 IP Grouping

In order to help IT managers configure services efficiently, DLM-3500 provides a few management tools. IP Grouping is one of these tools. This function allows you to assign a name to a group of IP addresses. When you need to specify one or more IP addresses later, you can use the name of an IP group instead. The name of this IP group will automatically show up in the IP address selection list if the IP group is enabled. You will need to fill out two tables on the page: **IP Grouping** and **Rule Setting**.



- **IP Grouping:**

Feild	Description
Group	Input the name of the group, and it will appear in the service menu with the relevant options.

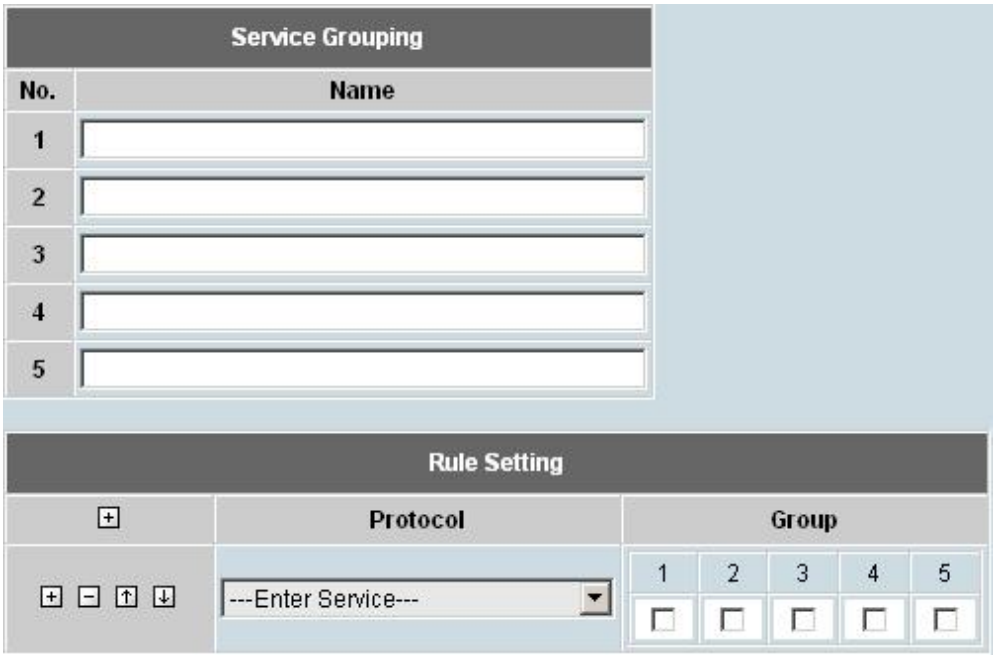
- **Rule Setting:**

Field	Value	Description
Address	<IP address>	Input IP address - One single IP address, or an IP address range in the format of xxx.xxx.xxx.xxx-yyy.yyy.yyy.yyy Or a subnet in the format of xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy
Group	belong to not belong to	Select the in group which the IP Address belongs to.

Caution: *The difference between setting the* ***IP Group*** *and the* ***Named IP Addresses*** *is in their format.* ***Named IP Addresses*** *can only be* ***a range of IP Address****, while* ***IP Group*** *provides* ***several types of format****. The DLM-3500 gives higher priority to the group in Named IP Addresses. It is recommended that groups defined in* ***Host Name*** *be used.*

4.2.7 Service Grouping

This function allows you to assign a name to a group of TCP or UDP services. When you are asked to specify a port later, you can use the name of the service group instead. The name of a service group will automatically show up in the port selection list if the service group is enabled. You will need to fill out two tables on the page: **Service Grouping** and **Rule Setting**.



- **Service Grouping:**

Field	Value	Description
Name	<name>	Input the group name, e.g. MSN File Transfer, and it will appear in the service menu and relevant options. Note: You can set up to 5 groups

Note: *You can set at up to five groups for Service Grouping.*

- **Rule Setting:**

Field	Value	Description
Protocol	Protocol Number ICMP TCP@ UDP@	Define the assigned TCP, UDP, and ICMP as a group for the usage in the service menu. The format is port (xxx) for single Port and port (xxx-yyy) for a range of port, e.g. 6891-6900.
Group	belong to not belong to	Define if these service ports in former field belong to the group.

4.3 Service

DLM-3500 provides the following services: **Firewall**, **Auto Routing**, **Virtual Server**, **QoS**, **Per IP Max Connection**, **Per IP Max Rate Control**, **Multihoming**, **Internal DNS**, **SNMP**, and **UPnP**.

4.3.1 Firewall

Setting up the firewall can be a complex job for the first-time user. Please read the instruction carefully. The rule setting requires you to fill in six fields in order to make the firewall function properly: **When**, **Source**, **Destination**, **Service**, **Action**, and **Log**.

You can enable or disable rules in the list individually. The rules are matched from top down, which mean rules listed at the top of the list are given highest precedence, wherein succeeding rules will not be examined once a match is found.

Field	Value	Description
When	Busy Idle All-Time	There are three options available: Busy hour, idle hour, and All-times. Please refer to item 4.1.5 of this document on [System]→[Date/Time] for setting up busy or idle hours.
Source	Any LAN WAN IP Address IP Range Subnet <Group >	Packets sent from the specified source will be matched: **Any:** Match all packets regardless of its source. **LAN:** Match all packets that come from the LAN. **WAN:** Match all packets that come from the WAN. **IP Address:** Match packets from a single IP address. e.g. 192.168.1.4. **IP Range:** Match packets from a continuous range of IP addresses. e.g. 192.168.1.10-192.168.1.20。 **Subnet:** Match packets that come from a subnet. e.g. 192.168.1.0/255.255.255.0。 **Group:** If you predefined IP groups in [Group]→[IP Grouping], their Group Name will be shown in the list.
Destination	Any LAN WAN IP Address IP Range Subnet <Group>	Packets sent to specified destination will be matched. This field is the same as the “Source” field, except it matches packets with specified destination. Likewise, All IP groups setup in [Network]->[IP Grouping] will be shown here.

Service	FTP(21) SSH (22) TELNET(23) SMTP(25) HTTP(80) POP3(110) H323 (1720) Protocol Number ICMP@ TCP@ UDP@ Any <Group>	The services, which are predefined in [Service Name], will be matched. For example: **FTP(21):** Where packets with predefined TCP port number 21 in [Service Name] are matched. **Protocol Number:** Where Protocol Number is defined, and packets with the said Protocol Numbers are matched. **ICMP @:** Where Type value is defined, and packets whose ICMP take this Type value are matched. **TCP/UDP @:** Where the TCP/UDP service type is matched. You can select the matching criteria from the publicly known service types (e.g. FTP), or you can choose the port number in TCP/UDP packet. To specify a range of port numbers, type starting port number plus hyphen "-"and ending port number. e.g. "TCP@123-234". **Group:** Where packets from the group are predefined in [Service Grouping]. **Any:** Where all packets are matched. Note: The default value for DLM-3500 is set to accept all packets.
Action	Accept Deny	Accept: The firewall will let the matched packets pass through. Deny: The firewall will drop all matched packets.
Log	Enable Disable	Enable: Logging will be enabled. Whenever the rule is matched, the system will write the event to the log file. Disable: No log will be generated.

Note: *The default value for DLM-3500 is set to accept all packets.*

4.3.2 Auto Routing

Auto Routing service allows administrators to specify how traffic is routed to WAN links. If you have only one WAN link, please do not change the default configuration.

If you have multiple WAN links, you may like to setup your routing rules in many situations. For example, an administrator can reserve a WAN link to a group of private IP addresses, or an administrator can force an application to take a particular WAN link depending on the traffic loads in each WAN links. You will need to fill in following fields in **Auto Routing** table:

Field	Value	Description
When	Busy Idle All-Time	Select when the rule will be applied. There are three options available: Busy hour, idle hour, and All-time. All-time mean the rule will be applied for all the 24 hours a day. Please refer to item 4.1.5 of this document on [System]->[Date&Time]->[Busyhour Setting] for setting up the definition of busy or idle hours.
Source	Any LAN Local host IP Address IP Range Subnet < Group >	Packets sent from the specified source will be matched: **Any:** Match all packets regardless of its source. **LAN:** Match all packets that come from the LAN. **Localhost:** Match all packets that come from DLM-3500 Localhost. **IP Address:** Match packets from a single IP address. e.g. 192.168.1.4. **IP Range:** Match packets from a continuous range of IP addresses. e.g. 192.168.1.10-192.168.1.20 **Subnet:** Match packets that come from a subnet. e.g. 192.168.1.0/255.255.255.0 **Group:** If you predefined IP groups in [Network]→[IP Grouping], their Group Name will be shown in the list.
Destination	WAN Local host IP Address IP Range Subnet < Group >	Packets sent from the specified destination will be matched: **WAN:** Match all packets that come from the WAN. Localhost: Match all packets that come from DLM-3500 Localhost. **IP Address:** Match packets from a single IP address. e.g. 192.168.1.4. **IP Range:** Match packets from a continuous range of IP addresses. e.g. 192.168.1.10-192.168.1.20

		Subnet: Match packets that come from a subnet. e.g. 192.168.1.0/255.255.255.0 **Group:** If you predefined IP groups in [System]→[IP Grouping], their Group Name will be shown in the list.
Service	FTP(21) SSH (22) TELNET(23) SMTP(25) POP3(110) H323 (1720) Protocol Number ICMP@ TCP@ UDP@ < Group > Any	The services, which are predefined in [Service Name], will be matched. For example: **FTP(21):** Where packets with predefined TCP port number 21 in [Service Name] are matched. **Protocol Number:** Where Protocol Number is defined, and packets with the said Protocol Numbers are matched. **ICMP @:** Where Type value is defined, and packets with ICMP taking this Type value are matched. **TCP/UDP @:** Where TCP/UDP service type is matched. You can select the matching criteria from the publicly known service types (e.g. FTP), or you can choose the port number in TCP/UDP packet. To specify a range of port numbers, type starting port number plus hyphen "-"and ending port number. e.g. "TCP@123-234". **Group:** Where packets from the group are predefined in [Service Grouping]. **Any:** Where all packets are matched
Algorithm	Fixed By Weight By Traffic	Algorithm for Auto Routing: **Fixed:** Only route the connections on a fixed WAN link. **By Weight:** Input the weight to route the connections to WAN link according to weight. **By Traffic:** Route the connection to the WAN link according to total traffic. Connection will be route to the link which has more remained bandwidth.
Parameter	<select WAN link(s) for the algorithm, or put a weight on each WAN link>	The type of parameter depends on the algorithm you choose. The number of parameter's range is always 1 to 4. That represents the number of WAN link. You can check the check box under the number to instruct DLM-3500 to apply the algorithm to this WAN link. In the case of "By Weight", if users do not want to use a WAN link, fill in "0" to the WAN number.
Log	Enable Disable	Enable: Logging will be enabled. Whenever the rule is matched, the system will write the event to the log file. Disable: No log will be generated.

4.3.3 Virtual Server

Virtual Server in DLM-3500 is a feature to make your intranet (LAN) servers available to the Internet (WAN). Because the private IP addresses assigned to the intranet servers are invisible to the external environment, if you wish to make designated services (provided on the servers) accessible to outsiders, you must tell the DLM-3500 to redirect these external requests to the right servers in the LAN or DMZ. When the DLM-3500 receives an external request, it will look up the Virtual Server table and redirect the packet to the corresponding server in the LAN or DMZ.

You can use this function to respond to the outside request with the server in the LAN or DMZ when you do not want the private IP address to be made public. You will need to fill in following fields in **Virtual Server** table:

Field	Value	Description
When	Busy Idle All-Time	There are three options available: Busy hour, idle hour, and All-times. Please refer to [System]→[Date/Time] for setting up the definition of busy or idle hours.
WAN IP	<WAN IP>	To the users from the Internet, your virtual server is visible as a public IP on the WAN port. This WAN IP is the “visible” IP for your virtual server in the external environment (Internet). You must specify a public IP if your WAN type is “Routing Mode”. If the WAN type is “Bridge Mode One Static IP”, your WAN IP in this field should be the public IP assigned from your ISP. If your WAN type is none of the above, then choose “dynamic IP at WAN”.
Service	FTP(21) SSH (22) TELNET(23) H323 (1720) Protocol Number ICMP@ TCP@ UDP@ < Group > Any	The services, which are predefined in [Service Name], will be matched. For example: **FTP(21):** Where packets with predefined TCP port number 21 in [Service Name] are matched. **Protocol Number:** Where Protocol Number is defined, and packets with the said Protocol Numbers are matched. **ICMP @:** Where Type value is defined, and packets with ICMP taking this Type value are matched. **TCP/UDP @:** Where TCP/UDP service type is

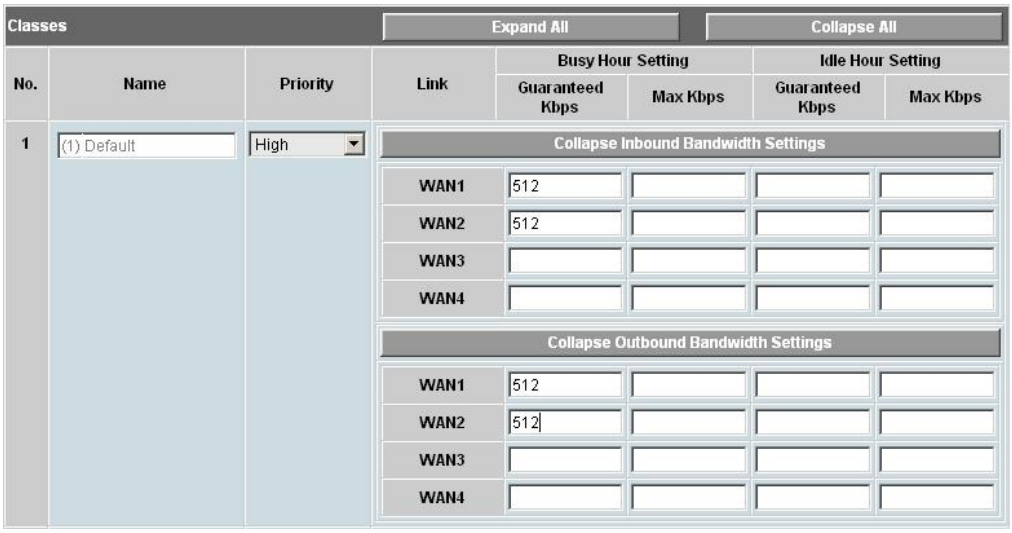
		matched. You can select the matching criteria from the publicly known service types (e.g. FTP), or you can choose the port number in TCP/UDP packet. To specify a range of port numbers, type starting port number plus hyphen “-“and ending port number. e.g. “TCP@123-234”. **Group:** Where packets from the group are predefined in [Service Grouping]. **Any:** Where all packets are matched.
Server IP	<Server IP>	The actual IP address of your virtual server. It can be a private IP in the LAN or a public IP in DMZ.
Server Port	Port Number	Input the Port Number of Server IP.
Log	Enable Disable	Enable: Logging will be enabled. Whenever the rule is matched, the system will write the event to the log file. Disable: No log will be generated.

4.3.4 QoS

DLM-3500 provides built-in QoS that comes with integrated bandwidth management of both inbound and outbound traffic. It ensures certain services are allocated with enough bandwidth to provide satisfactory quality. For example, in the case of bandwidth-hungry applications such as voice/video/data, the burst in data transmission may sometimes result in the amount of traffic exceeding the speed of a link. This function helps manage the bandwidth so as to fine-tune bandwidth utilization. The QoS in DLM-3500 is separated by the direction of traffic flow, either inbound (from WAN to LAN), or outbound (from LAN to WAN).

The setting of QoS includes two parts: **Class** and **Filters. Class** will define the QoS classes that the rules are imposed on, and **Filters** classify the traffic.

- **Class:** Define the QoS classes that the rules are imposed on. The definition of the class can be according to **Priority** and **Idle/Busy Hour Setting**. You can configure your own bandwidth limit for each WAN link in **Inbound Bandwidth Settings** and **Outbound Bandwidth Settings** by collapsing or expanding them.



Field	Description	
Name	<Input name>	The name for this bandwidth class. We recommend you using a self-explanatory name so that you can understand it easily when it is used later in the filter table. For example, you can name your bandwidth class “HTTP” to manage the bandwidth of HTTP service.
Priority	Normal High Low	The priority of the connections on the WAN link. It can be High, Normal, or Low. The connections with higher priority are allocated with available bandwidth first.
Link	-	The WAN link which you want your bandwidth limit to apply.
Busy Hour	Guaranteed	The guaranteed bandwidth for this class:

Settings Note: Set Busy Hour in [System]→[Date Time].	Kbps	This makes sure the connections through the WAN link will at least be allocated with the specified bandwidth. It is particularly useful when you want to ensure the quality of a certain type of service (e.g. VoIP).
	Max Kbps	This defines the maximum bandwidth allowed for the connections on the WAN link. Normally, we will set up maximum bandwidth for services like WWW or SMTP that have a high volume of traffic and may affect the quality of other services.
Idle Hour Settings Note: Set Idle Hour in [System]→[Date Time].	Guaranteed Kbps	The guaranteed bandwidth for this class: This makes sure the connections through the WAN link will be at least allocated with the specified bandwidth. It is particularly useful when you want to ensure the quality of a certain type of service (e.g. VoIP).
	Max Kbps	This defines the maximum bandwidth allowed for the connections on the WAN link. Normally, we will set up maximum bandwidth for services like WWW or SMTP that have high volume of traffic and may affect the quality of other services.

- **Filters:**

Field	Value	Description
Source	Any address LAN WAN Localhost IP Address IP Range Subnet < Group >	Packets sent from the specified source will be matched: **Any Address:** Match all packets regardless of its source. **LAN:** Match all packets that come from the LAN. **WAN:** Match all packets that come from the WAN. **Localhost:** Match all packets that come from DLM-3500 Localhost. **IP Address:** Match packets from a single IP address. e.g. 192.168.1.4 **IP Range:** Match packets from a continuous range of IP addresses. e.g. 192.168.1.10-192.168.1.20 **Subnet:** Match packets that come from a subnet. e.g. 192.168.1.0/255.255.255.0 **Group:** If you predefined IP groups in [Network]→[IP Grouping], their Group Name will be shown in the list.

Destination	Any address LAN WAN Localhost IP Address IP Range Subnet < Group >	Connections to the specified destination will be matched. This field is the same as the “Source” field, except it matches packets with the specified destination. In addition, the predefined IP groups will also be shown in the list. Please See [Network]→[IP Grouping] for setting up your own IP groups.
Service	FTP(21) SSH (22) TELNET(23) SMTP(25) POP3(110) H323 (1720) Protocol Number ICMP@ TCP@ UDP@ < Group > Any	The services, which are predefined in [Service Name], will be matched. For example: **FTP(21):** Where packets with predefined TCP port number 21 in [Service Name] are matched. **Protocol Number:** Where Protocol Number is defined, and packets with the said Protocol Numbers are matched. **ICMP @:** Where Type value is defined, and packets with ICMP taking this Type value are matched. **TCP/UDP @:** Where TCP/UDP service type is matched. You can select the matching criteria from the publicly known service types (e.g. FTP), or you can choose the port number in TCP/UDP packet. To specify a range of port numbers, type starting port number plus hyphen “-“and ending port number. e.g. “TCP@123-234”. **Group:** Where packets from the group are predefined in [Service Grouping]. **Any:** Where all packets are matched.
Classes	<Name>	The QoS class to be imposed. These classes are defined in the QoS class table, as mentioned in earlier part of this document.

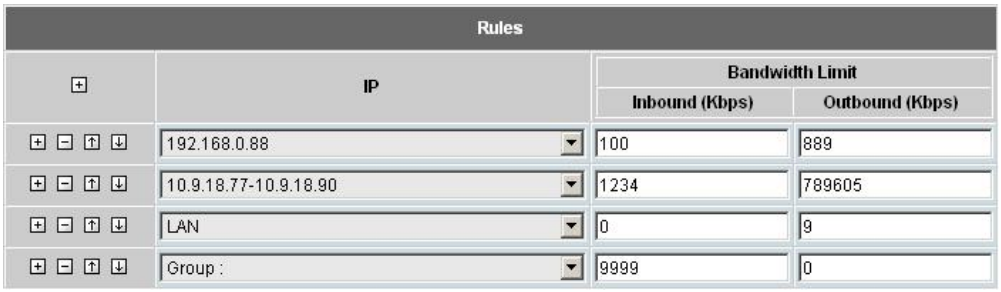
4.3.5 Per IP Max Connection

This function is used to protect network against excessive network sessions generated by virus or hackers. When the number of connections exceeds the preset value, DLM-3500 will block the rest of the connections and write the event to a log file, if the checkbox of **Log** is ticked. The settings include the following information:

Field	Value	Description
Log Interval	<in seconds>	The time interval used for system to write the event to the log file.
Source	<IP Address>	Connections established from the specified source will be matched, including Any Address, LAN, WAN, IP Address, IP Range, Subnet, and IP Group.
Limit	<value>	The maximum number of the connections allowed.
Log	Enable Disable	If this check box is ticked, whenever the rule is matched, the system will write the event to the log file.

4.3.6 Per IP Max Rate Control

This function is used to set the maximum bandwidth assigned to inbound and outbound traffic per IP in order to prevent network congestion from non-business application bandwidth consumption. The settings include the following information:



Field	Value	Description
IP	<IP Address>	The IP address where the packets come from will be matched, including LAN, IP Address, IP Range, IP Subnet, and specified IP Group.
Inbound (Kbps)	<value>	Maximum bandwidth assigned to inbound traffic per IP/IP Group.
Outbound (Kbps)	<value>	Maximum bandwidth assigned to outbound traffic per IP/IP Group.

4.3.7 Multihoming

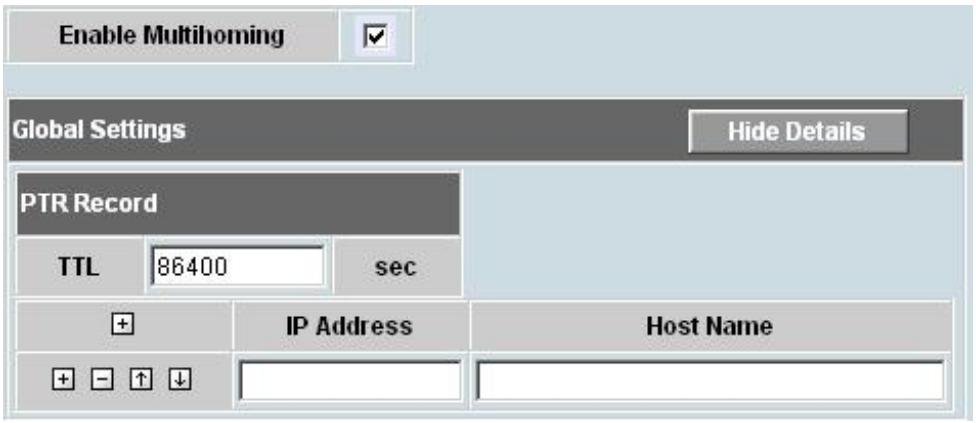
Based on a unique technology called PromptDNS, DLM-3500 offers a Multihoming service for load balancing and fault tolerance for inbound requests. To make use of this service, you must have multiple WAN links and registered domain names for your publicly accessible servers. Whenever the DLM-3500 receives a DNS query; it will answer the DNS query with a public IP address assigned to one of the WAN links according to the settings of your answering policies. Subsequent requests to your server will therefore also be sent the public IP of the WAN link based on the DLM-3500's previous response. You can configure your answering policies with a weight for each WAN link so that the public IPs returned will be distributed evenly by weight. If one of your WAN links fails, DLM-3500 will not return the public IP assigned to that failed link, nevertheless, your publicly accessible servers will still be reachable via other live WAN links.

In order for the Multihoming function to work properly, you must make sure that the prerequisites listed below are met:

- Mulitple WAN links (at least two).
- Registered domain names for the publicly accessible servers.
- The publicly accessible servers must be configured as virtual servers, or have public IP addresses.

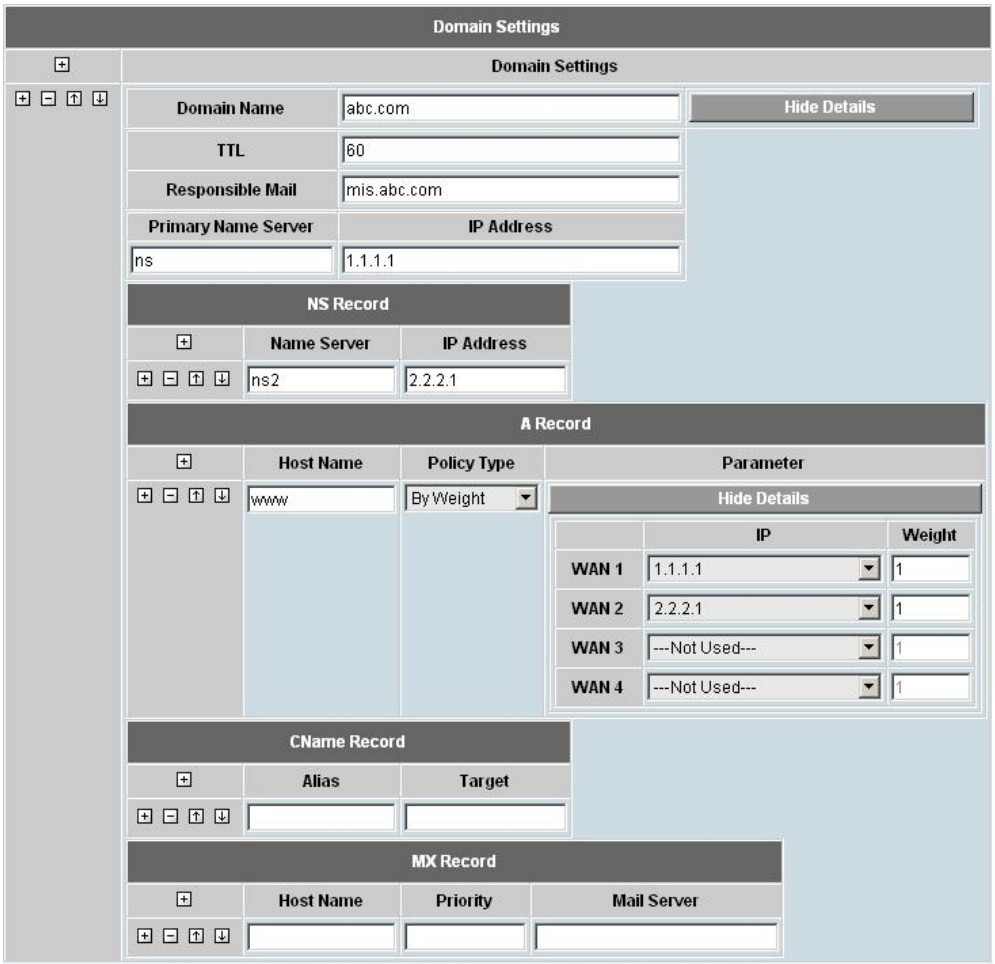
By default, Multihoming is set to off. To use this service, check the checkbox to the right of **Enable Multihoming** on the top of the page. There are two tables for configuring your Multihoming settings: **Global Settings** and **Domain Settings**.

- **Global Settings:** Specify the **PTR Record** in this table:
- **PTR Record**: A PTR record or pointer record, maps an IP address to the canonical name for that host. This record is usually managed by the ISP who provides the domain name.
  For example:
  Name: www.dlink.com.sg
  Address: 1.2.3.4
  Aliases: 4.3.2.1.in-addr.arpa



Field	Value	Description
TTL	<TTL>	TTL (Time To Live) Specifying the amount of time other DNS servers and applications are allowed to cache the record.
IP Address	<IP Address>	Enter the reverse lookup IP address.
Host Name	<Link Number>	Enter the corresponding FQDN to the reverse IP.

- **Domain Settings:** Fill out the information including **Domain Settings**, **NS Record**, **A Record**, **CName Record**, and **MX Record**.



In this table, you are to configure your domain settings, including your multihoming domain names (one or more), the DNS servers for querying your domain names, and the answering policy to apply a given prefix of the domain name.

Domain Settings:

Field	Description
Domain Name	Enter the domain names for Multihoming. To enter additional domain names, press +.
TTL	TTL (Time To Live) Specifying the amount of time other DNS servers and applications are allowed to cache the record.
Responsible Mail	Enter the domain administrator's email.
Primary Name Server	Enter the primary server name.
IP Address	The query IP address can be an IP address, IP range, subnet, or any address.

NS Record:

An **NS record** or **name server record** maps a domain name to a list of DNS servers authoritative for that domain. If you register more than one NS record, you need configure here besides "Primary Name Server"

Field	Description
NS Record	
Name Server	Enter the prefix of the server name. For example, if a server's FQDN is nsl.abc.com, please enter "nsl".
IP Address	Enter the IP address corresponding to the name server.

A Record:

An **A record** gives you the IP address of a domain. For Inbound Load Balancing, you will need to configure here.

Field	Description
A Record	
Host Name	Enter the prefix of the primary workstation's name. For example, if the name is www.abc.com, enter "www".
Policy Type	The algorithm for selecting WAN links, by Weight or Traffic. **By Weight:** Answer DNS queries by the weight given to each link. **By Total Traffic:** Answer DNS queries by selecting the WAN link with the lightest total traffic.
IP	Enter the IP address to answer DNS queries.
Weight	Input the weight for each WAN Link.

CName Record:

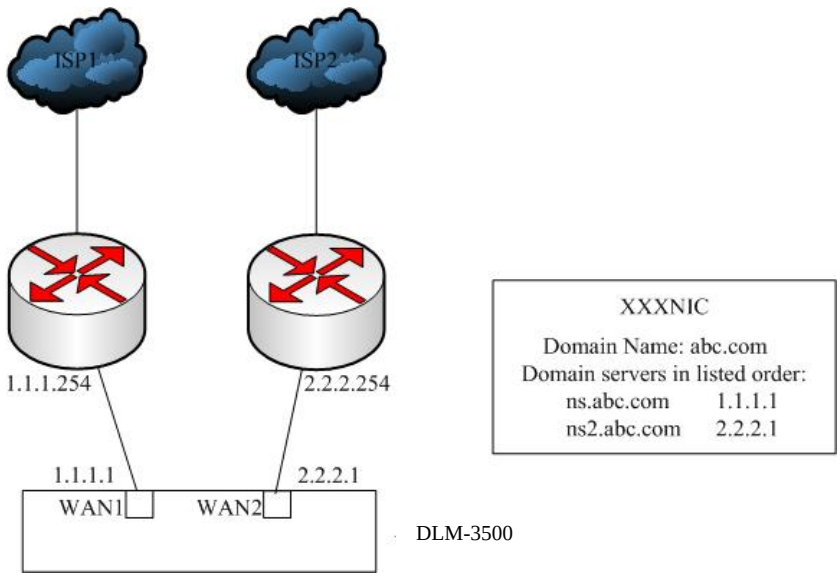
CName records are "canonical name" records which take care of aliases. These should be used with care, only when absolutely necessary, and you must be very familiar with DNS.

Field	Description
CName Record	
Alias	Enter the alias of the domain name. For example, if you wish to use www1.abc.com as the alias of www.abc.com, (domain name), enter “www1” in this field.
Target	Enter the real domain name. For example, if you wish to use www1.abc.com as the alias for www.abc.com, enter “www”.

MX Record:

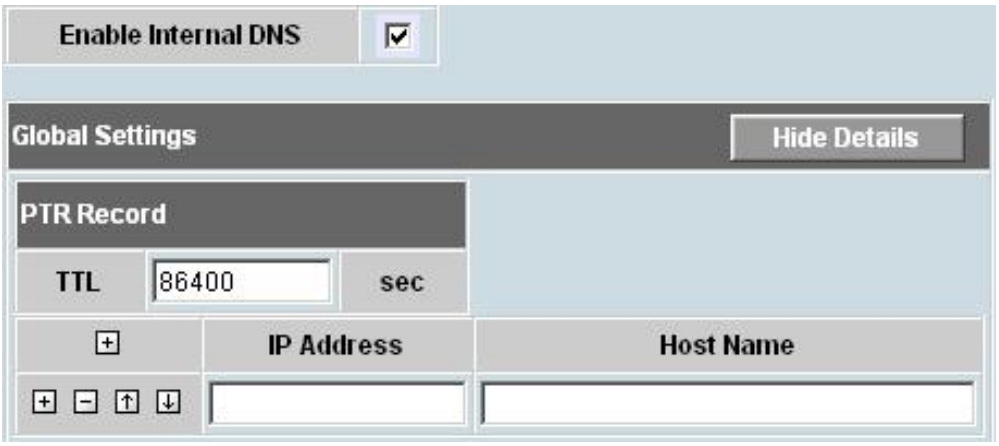
MX record is used for defining the hosts that are willing to accept mail for a given domain. You may want to configure this for your internal mail server.

Field	Description
MX Record	
Host Name	Enter the prefix of the mail server’s domain name. For example, if the domain name is mail.abc.com, enter “mail”.
Priority	Enter the priority of the mail servers. The higher the priority, the lower the number
Mail Server	Enter the IP address of the mail server.



4.3.8 Internal DNS

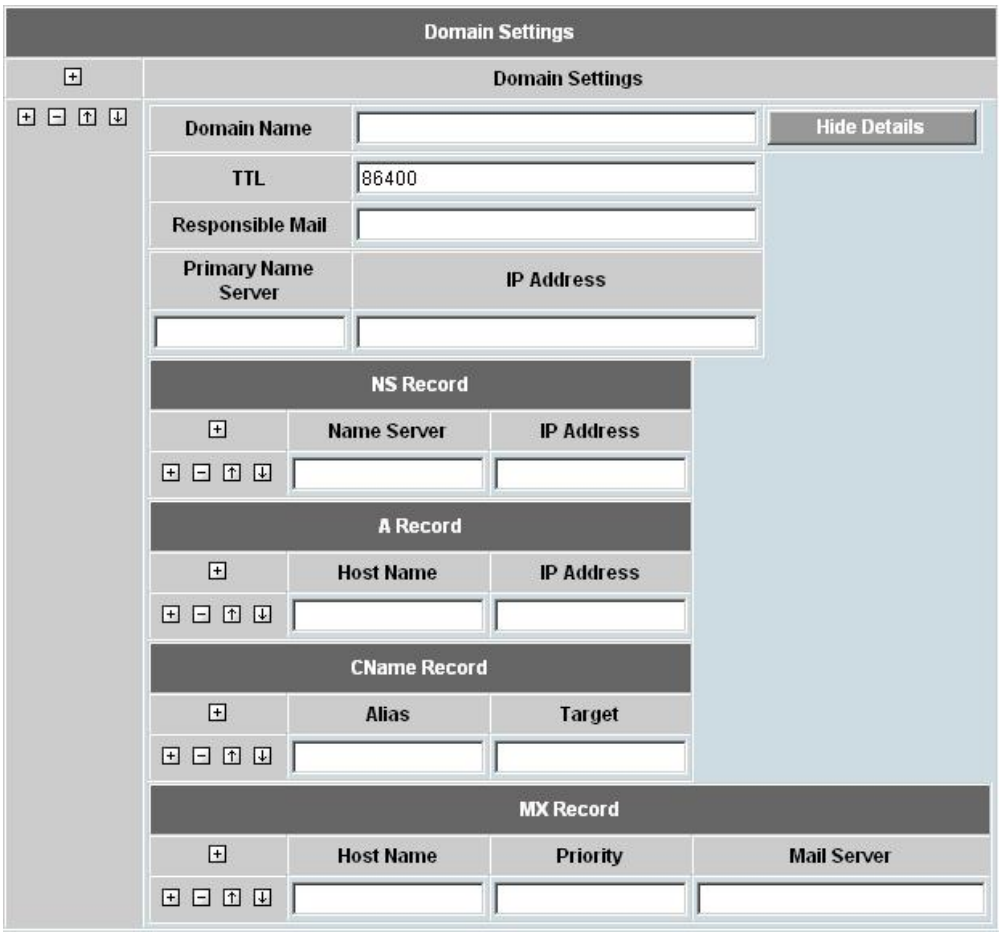
DLM-3500 has a built-in DNS server function which can be activated by completing the fields in this page.
By default, Internal DNS is set to off. To use this service, check the checkbox to the right of **Enable Internal DNS** at the top of the page. There are two tables for configuring your **Internal DNS** settings: **Global Settings** and **Domain Settings**.



- **Global Settings:** Specify the PTR data in this table, which includes following information:

Field	Value
Enable InternalDNS	Turn on/off internal DNS server.
PTR Record	
TTL	TTL (Time To Live) Specifying the amount of time other DNS servers and applications are allowed to cache the record.
IP Address	Enter the reverse lookup IP address.
Host Name	Enter the corresponding FQDN to the reverse IP.

- **Domain Settings:** Fill out the information including **Domain Settings, NS Record, A Record, CName Record, and MX Record.**

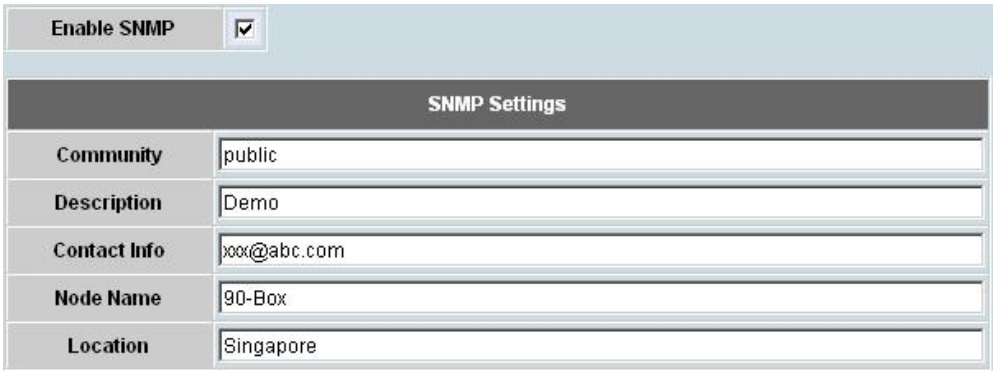


Field	Description
Domain Name	Enter the domain names for internal DNS. To enter additional domain names, press +.
TTL	TTL (Time To Live) Specifying the amount of time other DNS servers and applications are allowed to cache the record.
Responsible Mail	Enter the domain administrator's email address.
Primary Name Server	Enter the primary server name.
IP Address	The query IP address can be an IP address, IP range, subnet, or any address.
NS Record	
Name Server	Enter the prefix of the server name. For example, if a server's FQDN is nsl.abc.com, please enter "nsl".
IP Address	Enter the IP address.

A Record	
Host Name	Enter the prefix of the primary workstation’s name. For example, if the name is www.abc.com, enter “www”.
IP Address	Input the IP Address of Localhost.
Cname Record	
Alias	Enter the alias of the domain name. For example, if you wish to use www1.abc.com as the alias of www.abc.com, (domain name), enter “www1” in this field.
Target	Enter the real domain name. For example, if you wish to use www1.abc.com as the alias for www.abc.com, enter “www”.
MX Record	
Host Name	Enter the prefix of the mail server’s domain name. For example, if the domain name is mail.abc.com, enter “mail”.
Priority	Enter the priority of the mail servers. The higher the priority, the lower the number.
Mail Server	Enter the IP address of the mail server.

4.3.9 SNMP

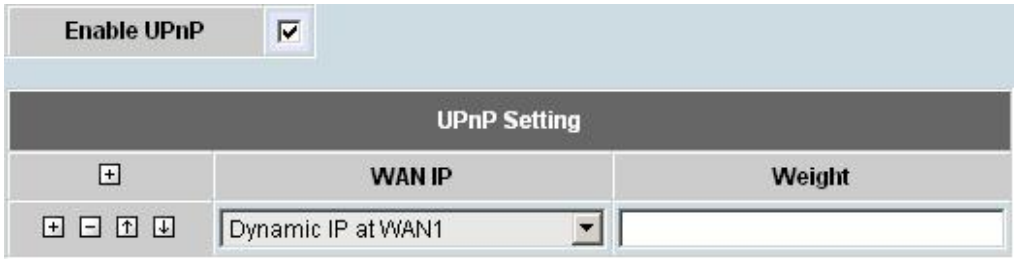
SNMP (Simple Network Management Protocol) can be used to manage networks by providing statistical data regarding network performance and security. It is often used in the management of TCP/IP networks. The settings of SNMP include following information:



Field	Description
Enable SNMP	Enable/Disable SNMP.
Community	Enter the community which the SNMP belongs to. The default value is “public”.
Description	Enter the description of the machine.
Contact Info	Enter the contact information of the machine.
Node Name	Enter the Node Name.
Location	Enter the location of the machine.

4.3.10 UPnP

DLM-3500 will detect the public UPnP (Universal Plug and Play) equipment in the network and automatically respond to its predefined IP Address. The UPnP settings include following information:



Field	Value	Description
Enable UPnP	Enable Disable	Enable or disable the function.
WAN IP	<IP Address>	Input the WAN IP preserved for public UPnP, including dynamic IP address at WAN and setting of IP address.
Weight	E.g.:1,2…	Input the weight, the bigger number will be given the higher priority.

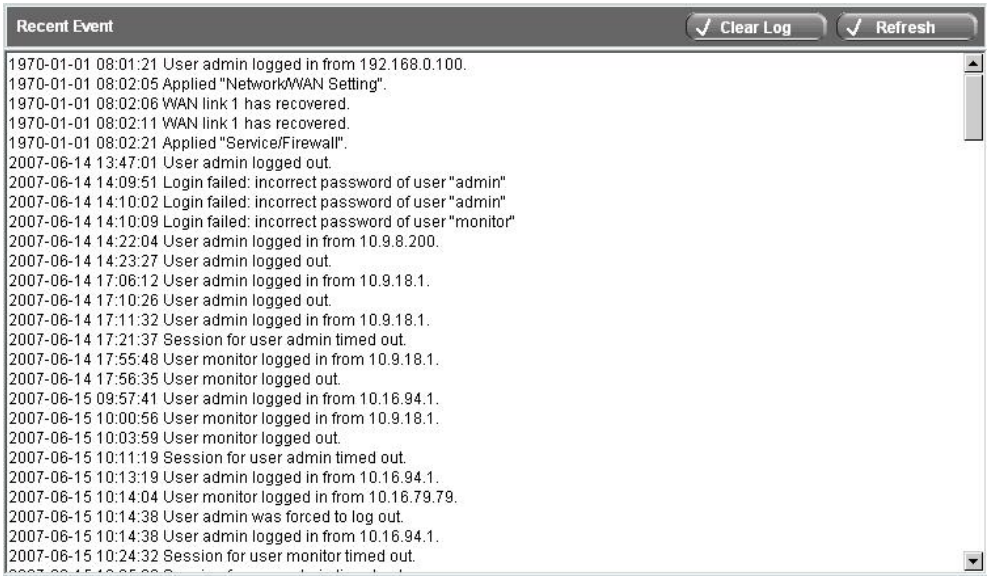
4.4 Log

DLM-3500 offers a complete set of logging activities for various functionalities such as System, Firewall, Routing, and more. Administrators can fully understand the network status, and improve its efficiency, especially in the area of problem identification. There are three parts under the logging system: **View**, **Control**, and **Notification**.

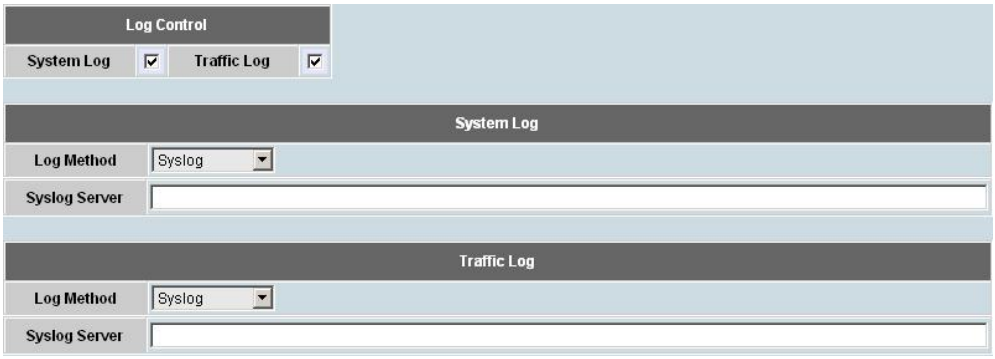
- **View:** DLM-3500 provides two types of log: **System Log** and **Traffic Log.** The associated operations of this are:

  Log Type: Administrators can pick the desired log type either **System Log** or **Traffic Log** from the drop-down menu.

  Recent Event: Event log will be printed out in the time order.
  Clear Log: Clear all logs.
  Refresh: Click the button to get a copy of the latest log.



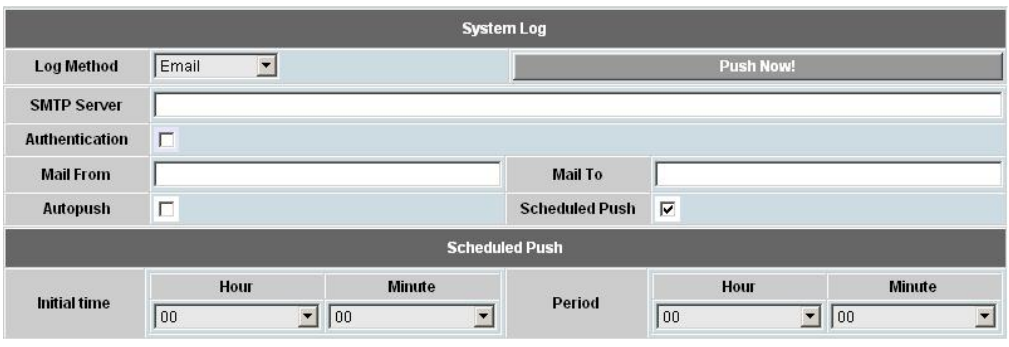
- **Control:** You can setup how log data will be transmitted to other servers for archiving and further analysis. First of all, you have to select the type of log from **System Log** and **Traffic Log** in **the Log Control** table. You will then see a **Traffic Log** table for log control settings, which includes the following information:



Field	Value	Description
Log Control	System Log Traffic Log	Select the type of Log file to be pushed.
System Log		
Log Method	E-Mail FTP Syslog	See below.
Push Now		Use this button to start log pushing immediately.
Traffic Log		
Log Method	E-Mail FTP Syslog	See below.
Push Now		Use this button to start log pushing immediately.

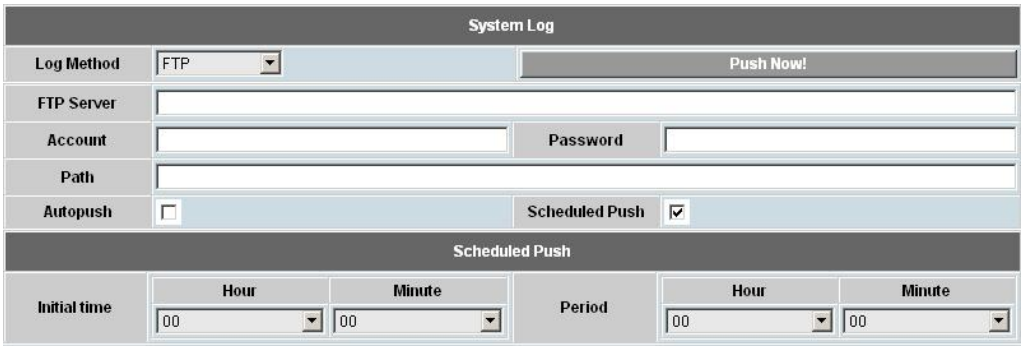
Log Method: DLM-3500 offers three types of log transmissions: FTP to external FTP server, Syslog to a syslog server, or Send e-mail via SMTP to the administrator's mailbox.

- **E-mail**



Field	Value	Description
SMTP Server	<IP> or <Domain Name>	SMTP server for the logs.
Account	<SMTP Account>	Authenticated account for mail server.
Password	<Account's Password>	Authenticated password for mail server.
Mail From	<e-Mail address>	Sender of the Email.
Mail To	<e-Mail address>	Receiver of the Email.
Auto Push		Push this button to start log pushing automatically.
Scheduled Push		Turn on scheduled push.
Initial Time	<Year/Month/Day/Hour/Minute/Second>	Start time for the scheduled push.
Period	<Day/Hour/Minute>	Scheduled push duration.

- **FTP**

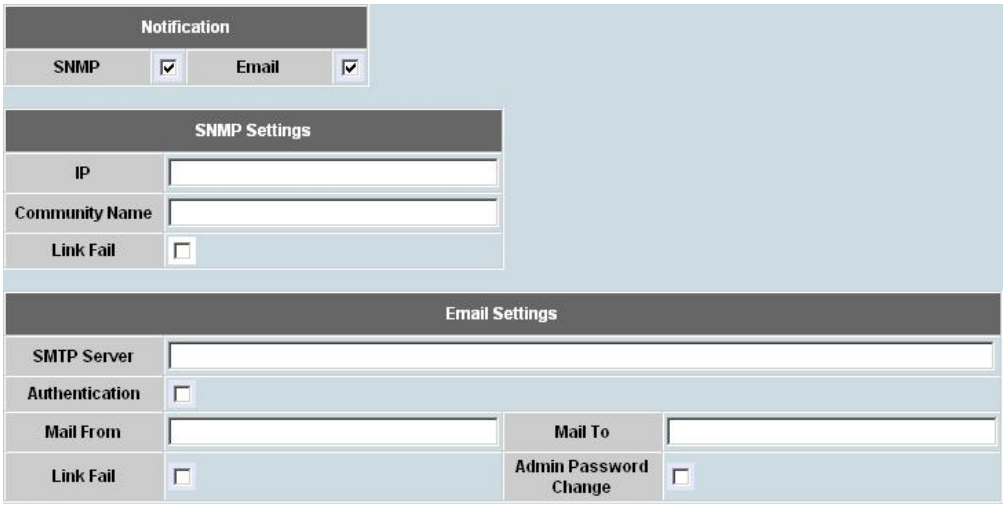


Field	Value	Description
FTP Server	<IP> or <Domain Name>	FTP Server's IP or domain name.
Account	<FTP Account>	FTP user account.
Password	<Account's Password>	FTP user password.
Path	<Path>	The path you want to push log to on FTP server. Note: Relative path and "." Is indicated FTP root directory
Auto Push		Push this button to start log pushing automatically.
Scheduled Push		Turn on scheduled push.
Initial Time	<Year/Month/Day/Hour/Minute/Second>	Start time for the scheduled push.
Period	<Day/Hour/Minute>	Scheduled push duration.

- **Syslog**

Field	Value	Description
Syslog Server	<IP> or <Domain Name>	Syslog Server's IP or domain name.

- **Notification:** You can set up how e-mail notifications are sent out for important system events. DLM-3500 provides two methods of notification: **SNMP** and **Email.**



Field	Value	Description
SNMP Email		Select how e-mail notifications are sent out.
SNMP Settings		
Destination IP	<IP Address>	The SNMP managing device IP.
Community Name	<Community Name>	The community name.
Link Fail		Enable this function, system will notify administrator when a Link Fail happened.
Email Settings		
SMTP Server		SMTP Server.
Account		Authenticated account for mail server.
Password		Authenticated password for mail server.
Mail From		Sender.
Mail To		Receiver.
Link Fail		Enable this function for system to notify administrator when a Link Fail occurs.
Admin Password Change		Enable this function for system to notify administrator when Administrator password is changed.