



# Bandwidth Management Gateway

BM-525

User's Manual

## Copyright

Copyright© 2006 by PLANET Technology Corp. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of PLANET.

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

## Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

## Trademarks

The PLANET logo is a trademark of PLANET Technology.

This documentation may refer to numerous hardware and software products by their trade names. In most, if not all cases, these designations are claimed as trademarks or registered trademarks by their respective companies.

## CE mark Warning

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

## Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

## **FCC Caution:**

To assure continued compliance (example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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

## **R&TTE Compliance Statement**

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

## **WEEE**



To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

## **Safety**

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

## **Revision**

User's Manual for Bandwidth Management Gateway

Model: BM-525

Rev: 1.0 (August, 2006)

Part No: EM-BM525v1

## Table of Contents

<b>CHAPTER 1: INTRODUCTION</b> .....	<b>1</b>
1.1 FEATURES.....	1
1.2 PACKAGE CONTENTS.....	2
1.3 BANDWIDTH MANAGEMENT GATEWAY TOP VIEW.....	2
1.4 BANDWIDTH MANAGEMENT GATEWAY REAR PANEL.....	2
1.5 SPECIFICATION.....	3
<b>CHAPTER 2: SYSTEM</b> .....	<b>4</b>
2.1 ADMINISTRATION.....	4
2.2 ADMIN.....	5
2.3 PERMITTED IPS.....	8
2.4 LOGOUT.....	9
2.5 SOFTWARE UPDATE.....	10
2.6 CONFIGURE.....	11
2.7 SETTINGS.....	12
2.8 DATE/TIME.....	22
2.9 MULTIPLE SUBNET.....	23
2.10 ROUTE TABLE.....	28
2.11 DHCP.....	32
2.12 DDNS.....	34
2.13 HOST TABLE.....	36
2.14 LANGUAGE.....	37
<b>CHAPTER 3 INTERFACE</b> .....	<b>38</b>
3.1 INTERFACE.....	39
3.2 LAN.....	42
3.3 WAN.....	43
3.4 DMZ.....	48
<b>CHAPTER 4 POLICY OBJECT</b> .....	<b>50</b>
4.1 ADDRESS.....	50
4.2 EXAMPLE.....	53
4.3 SERVICE.....	60
4.4 CUSTOM.....	63
4.5 GROUP.....	67
4.6 SCHEDULE.....	70
4.7 QoS.....	73

---

4.8 EXAMPLE .....	77
4.9 AUTHENTICATION .....	79
4.10 EXAMPLE .....	85
4.11 CONTENT BLOCKING .....	89
4.12 URL.....	93
4.13 SCRIPT.....	96
4.14 P2P .....	98
4.15 IM.....	100
4.16 DOWNLOAD.....	102
4.17 VIRTUAL SERVER.....	104
4.18 EXAMPLE .....	108
<b>CHAPTER 5 POLICY .....</b>	<b>122</b>
5.1 POLICY .....	124
5.2 EXAMPLE .....	128
<b>CHAPTER 6 ANOMALY FLOW IP.....</b>	<b>146</b>
6.1 SETTINGS.....	147
<b>CHAPTER 7 MONITOR .....</b>	<b>157</b>
7.1 LOG.....	157
7.2 TRAFFIC LOG.....	159
7.3 EVENT LOG .....	164
7.4 CONNECTION LOG .....	167
7.5 LOG BACKUP.....	170
7.6 ACCOUNTING REPORT .....	172
7.7 OUTBOUND.....	175
7.8 INBOUND .....	181
7.9 STATISTICS.....	187
7.10 WAN.....	189
7.11 POLICY .....	191
7.12 WAKE ON LAN.....	193
7.13 STATUS .....	195
7.14 INTERFACE.....	196
7.15 AUTHENTICATION .....	198
7.16 ARP TABLE .....	199
7.17 DHCP CLIENTS .....	200

## Chapter 1: Introduction

The BM-525 is specifically designed for SOHO networks. It has built-in one 10/100Mbps Ethernet LAN, DMZ, and WAN ports. No broadband router is required for users with only one public IP address. It also supports virtual server, Multi-DMZ, and dynamic DNS functions that are very useful for our customers to share local resources with Internet users.

For bandwidth management, packets can be classified based on IP address, IP subnet, and TCP/UDP port number. The device has more than 40 of the most common protocols such as H.323, Oracle, HTTP, FTP, and so on for easy definition. The administrator can then define policies to ensure committed and maximum bandwidth levels for inbound and outbound traffic in each class. The administrator can also define three priority levels for each policy to ensure high priority packets receive the maximum available bandwidth. In addition, each policy can have a schedule defined for when the policy is activated or inactivated in increments of 30 minutes.

Both the NAT mode and DMZ mode are supported, and therefore can maintain the existing network infrastructure without reconfiguring. The BM-525 provides policy-based firewall protection and several hacker protections to prevent hackers' attack. Besides, the comprehensive alarm and log function allow the network manager to easily enhance the security of local network.

### 1.1 Features

- One 10/100Mbps LAN, DMZ, and WAN port
- NAT mode and DMZ mode
- DMZ mode requires no changing for the original network structure
- Traffic classification based on IP, IP range/subnet, and TCP/UDP port range
- Guaranteed and maximum bandwidth with three levels of priorities
- Policy-based bandwidth management
- Assign daily and weekly access schedule to each individual policy
- Professional Monitor function includes Log, Accounting Report, Statistics, and Status
- MRTG-like Traffic Statistics, easy to trace and analyze
- Multi-Servers Load Balancing
- Dynamic DNS and DHCP server functions
- Content Filter includes URL, Script, P2P, IM, and Download blocking
- Hacker Alert and Anomaly Flow Detection
- Virtual Server and IP mapping (Multi-DMZ Host)
- Multi-language Web UI and easy to manage
- User authentication based on user name and password

## 1.2 Package Contents

The following items should be included:

- ◆ Bandwidth Management Gateway
- ◆ Power Adapter
- ◆ Quick Installation Guide
- ◆ User's Manual CD

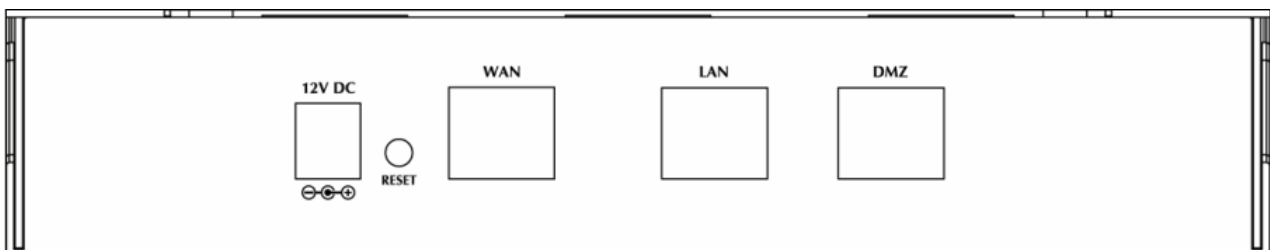
If any of the contents are missing or damaged, please contact your dealer or distributor immediately.

## 1.3 Bandwidth Management Gateway Top View



LED	Description
PWR	Power is supplied to this device.
WAN	Steady on indicates the port is connected to other network device. Blink to indicates there is traffic on the port
LAN	Steady on indicates the port is connected to other network device. Blink to indicates there is traffic on the port
DMZ	Steady on indicates the port is connected to other network device. Blink to indicates there is traffic on the port

## 1.4 Bandwidth Management Gateway Rear Panel



Port or button	Description
Power	12V DC, 1.5A
RESET	Press this button to restore to factory default settings.
WAN	Connect to your xDSL/Cable modem or other Internet connection device

LAN	Connect to your local PC, switch, or other local network device
DMZ	Connect to your local PC, switch, or other local network device

## 1.5 Specification

Product	Bandwidth Management Gateway	
Model	BM-525	
Hardware		
Connections	WAN	1 x 10/100Base-TX
	LAN	1 x 10/100Base-TX, Auto-MDI/MDI-X
	DMZ	1 x 10/100Base-TX, Auto-MDI/MDI-X
Button	Reset button for hardware reset / factory default	
System LED	PWR, WAN, LAN, DMZ	
Software		
Maximum Bandwidth	25Mbps	
Maximum concurrent session	20,000	
Management	Web (English, Traditional Chinese, Simplified Chinese)	
Operation Mode	DMZ_NAT, DMZ_Transparent, NAT	
WAN connection type in NAT mode	PPPoE, DHCP, and Fixed IP	
Traffic Classification	IP, IP subnet, and TCP/UDP port	
Bandwidth Allocation	Policy rules with Inbound/Outbound traffic management Guaranteed and maximum bandwidth Scheduled in unit of 30 minutes 3 Priorities	
Log	Traffic Log, Event Log, Connection Log, Log backup by mail or syslog server	
Statistics	WAN port statistics and policy statistics with graph display	
Firewall Security	Policy-based access control Stateful Packet Inspection (SPI) Scheduled in unit of 30 minutes	
Hacker Alert and Anomaly Flow Detection	Detect SYN Attack, Detect ICMP Flood, Detect UDP Flood, Detect Ping of Death Attack, Detect Tear Drop Attack, Detect IP Spoofing Attack, Filter IP Route Option, Detect Port Scan Attack, Detect Land Attack, Virus-Infected Blocking, E-Mail Alert Notification, NetBIOS Notification	
Alarm	<ul style="list-style-type: none"> <li>◆ Traffic alarm for user-defined traffic level</li> <li>◆ Event alarm for hacker attack</li> <li>◆ The alarm message can sent to administrator by e-mail</li> </ul>	
Other Functions	Firmware Upgradeable through Web NTP support Configuration Backup and Restore through Web Dynamic DNS support Multiple NAT and multiple DMZ (mapped IP) support Multiple server load balancing	



## Chapter 2: System

### 2.1 Administration

“System” is the managing of settings such as the privileges of packets that pass through the BM-525 and monitoring controls. The System Administrators can manage, monitor, and configure BM-525 settings. But all configurations are “read-only” for all users other than the System Administrator; those users are not able to change any setting of the BM-525.

## 2.2 Admin

### Define the required fields of Administrator

#### Administrator Name:

- The user name of Administrators and Sub Administrator for the BM-525. The **admin** user name cannot be removed; and the sub-admin user can be removed or configure.



The default Account: **admin**; Password: **admin**

#### Privilege:

- The privileges of Administrators (Admin or Sub Admin). The user name of the main Administrator is **Administrator** with **reading / writing** privilege. Administrator also can change the system setting, log system status, and to increase or delete sub-administrator. Sub-Admin may be created by the **Admin** by clicking **New Sub Admin**. Sub Admin have **only** read and monitor privilege and cannot change any system setting value.

#### Configure:

- Click **Modify** to change the “Sub-Administrator’s” password or click **Remove** to delete a “Sub Administrator.”

## Adding a new Sub Administrator

**STEP 1** . In the **Admin** Web UI, click the **New Sub Admin** button to create a new **Sub Administrator**.

**STEP 2** . In the **Add New Sub Administrator** Web UI and enter the following setting:

- Sub Admin Name: sub\_admin
- Password: 12345
- Confirm Password: 12345

**STEP 3** . Click **OK** to add the user or click **Cancel** to cancel it.

Add New Sub Admin		
Sub Admin name	<input type="text" value="sub_admin"/>	(Max. 16 characters)
Password	<input type="password" value="*****"/>	(Max. 16 characters)
Confirm Password	<input type="password" value="*****"/>	(Max. 16 characters)
		<input type="button" value="OK"/> <input type="button" value="Cancel"/>

**Add New Sub Admin**

## Modify the Administrator's Password

**STEP 1** . In the **Admin** Web UI, locate the **Administrator** name you want to edit, and click on **Modify** in the **ConFigure** field.

**STEP 2** . The **Modify Administrator Password** Web UI will appear. Enter the following information:

- **Password:** admin
- **New Password:** 52364
- **Confirm Password:** 52364

**STEP 3** . Click **OK** to confirm password change.

Modify Admin Password	
Admin Name	admin
Password	<input type="password" value="*****"/> (Max. 16 characters)
New Password	<input type="password" value="*****"/> (Max. 16 characters)
Confirm Password	<input type="password" value="*****"/> (Max. 16 characters)
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

### Modify Admin Password

## 2.3 Permitted IPs

**STEP 1** . Add the following setting in **Permitted IPs** of **Administration**:

- **Name:** Enter master
- **IP Address:** Enter 163.173.56.11
- **Netmask:** Enter 255.255.255.255
- **Service:** Select Ping and HTTP
- Click **OK**
- Complete add new permitted IPs

Add New Permitted IPs	
Name	<input type="text" value="master"/> (Max. 20 characters)
IP Address	<input type="text" value="163.173.56.11"/>
Netmask	<input type="text" value="255.255.255.255"/>
Service	<input checked="" type="checkbox"/> Ping <input checked="" type="checkbox"/> HTTP
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

**Setting Permitted IPs Web UI**

Name	IP Address / Netmask	Ping	HTTP	Configure
master	163.173.56.11 / 255.255.255.255	✓	✓	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
<input type="button" value="New Entry"/>				

**Complete Add New Permitted IPs**



To make Permitted IPs be effective, it must cancel the **Ping** and **Web UI** selection in the Web UI of BM-525 that Administrator enter. (LAN, WAN, or DMZ Interface)

Before canceling the **Web UI** selection of Interface, must set up the Permitted IPs first, otherwise, it would cause the situation of cannot enter Web UI by appointed Interface.

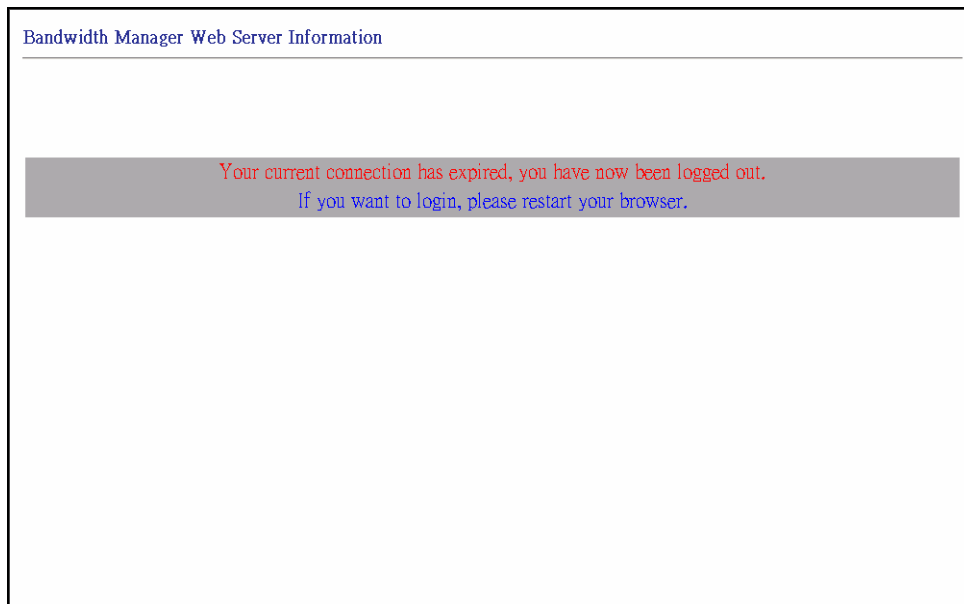
## 2.4 Logout

**STEP 1** . Click **Logout** in **System** to protect the system while Administrator is away.



**Confirm Logout Web UI**

**STEP 2** . Click **OK** and the logout message will appear in Web UI.

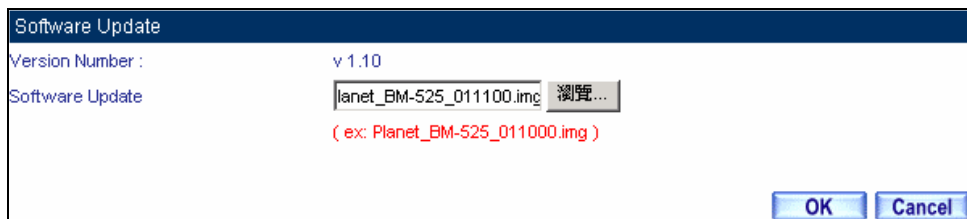


**Logout Web UI Message**

## 2.5 Software Update

**STEP 1** . Select **Software Update** in **System**, and follow the steps below:

- To obtain the version number from **Version Number** and obtain the latest version from Internet. And save the latest version in the hardware of the PC, which manage the BM-525
- Click **Browse** and choose the latest software version file.
- Click **OK** and the system will update automatically.



### Software Update



It takes 3 minutes to update software. The system will reboot after update. During the updating time, please don't turn off the PC or leave the Web UI. It may cause some unexpected mistakes. (Strong suggests updating the software from LAN to avoid unexpected mistakes.)

## 2.6 Configure

The Configure is according to the basic setting of the BM-525. In this section the definition is Setting, Date/Time, Multiple Subnet, Route Table, DHCP, Dynamic DNS, Hosts Table, and Language settings.



## 2.7 Settings

### BM-525 Configuration:

- The Administrator can import or export the system settings. Click **OK** to import the file into the BM-525 or click **Cancel** to cancel importing. You also can revive to default value here.

### Email Settings:

- Select **Enable E-mail Alert Notification** under E-mail Settings. This function will enable the BM-525 to send e-mail alerts to the System Administrator when the network is being attacked by hackers or when emergency conditions occur. (It can be set from Settings-Anomaly Flow IP in System to detect Anomaly Flow Attacks)

### Web Management (WAN Interface):

- The System Manager can change the port number used by HTTP port anytime. (Remote Web UI management)



After HTTP port has changed, if the administrator wants to enter Web UI from WAN, he will have to change the port number of browser (For example: <http://61.62.108.172:8080>).

### MTU Setting:

- It provides the Administrator to modify the networking package length anytime. Its default value is 1500 Bytes.

**Dynamic Routing (RIPv2)**

- By enable LAN, WAN, or DMZ Port to send and receive RIPv2 packets, the BM-525 appliance can communicate with internal or external routers and dynamically update the route table (The MIS engineers can set up routing information update timer and routing information timeout when it stop to receive the RIPv2 packets and the router will automatically cancel the dynamic routing table).

**SIP protocol pass-through:**

- When user use VoIP or Video Conference has abnormally situation, can use this function to resolve this problem.

**Administration Packet Logging:**

- After enable this function; the BM-525 will record packet which source IP or destination address is BM-525. And record in Traffic Log for System Manager to inquire about.

Define the required fields of Time Settings

**Synchronize Time/Date:**

- Synchronizing the BM-525 with the System Clock. The administrator can configure the BM-525's date and time by either syncing to an Internet Network Time Server (NTP) or by syncing to your computer's clock.

**GMT:**

- International Standard Time (Greenwich Mean Time)

**Daylight saving time setting:**

- When user live in the time zone implement daylight saving time, during this time unit will adjust system time as the local time.

## **Define the required fields of Multiple Subnet**

### **Forwarding Mode:**

- To display the mode that Multiple Subnet use. (NAT mode or Routing Mode)

### **WAN Interface Address:**

- The IP address that Multiple Subnet corresponds to WAN.

### **LAN Interface Address/Subnet Netmask:**

- The Multiple Subnet range.

**NAT Mode:**

- It allows Internal Network to set multiple subnet address and connect with the Internet through different WAN IP Addresses. For example, the lease line of a company applies several real IP Addresses 168.85.88.0/24. The company is divided into R&D department, service, sales department, procurement department, and accounting department. The company can distinguish each department by different subnet for the purpose of managing conveniently. The settings are as the following :

1. R&D department subnet : 192.168.1.1/24 (LAN)  $\leftrightarrow$  168.85.88.253 (WAN)
2. Service department subnet : 192.168.2.1/24 (LAN)  $\leftrightarrow$  168.85.88.252 (WAN)
3. Sales department subnet : 192.168.3.1/24 (LAN)  $\leftrightarrow$  168.85.88.251 (WAN)
4. Procurement department subnet  
192.168.4.1/24 (LAN)  $\leftrightarrow$  168.85.88.250(WAN)
5. Accounting department subnet  
192.168.5.1/24 (LAN)  $\leftrightarrow$  168.85.88.249(WAN)

The first department (R&D department) had set while setting interface IP; the other four ones have to be added in Multiple Subnet. After completing the settings, each department uses the different WAN IP Address to connect to the Internet. The settings of each department are as following:

	Service	Sales	Procurement	Accounting
IP Address	192.168.2.2~254	192.168.3.2~254	192.168.4.2~254	192.168.5.2~254
Subnet Netmask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	192.168.2.1	192.168.3.1	192.168.4.1	192.168.5.1

**Routing Mode:**

- It is the same as NAT mode approximately but does not have to correspond to the real WAN IP address, which let internal PC to access to Internet by its own IP (External user also can use the IP to connect with the Internet).

## Define the required fields of DHCP

### Subnet:

- The domain name of LAN

### Netmask:

- The LAN Netmask

### Gateway:

- The default Gateway IP address of LAN

### Broadcast IP:

- The Broadcast IP of LAN

## Define the required fields of DDNS

### Domain Name:

- The domain name that provided by DDNS

### WAN IP Address:

- The WAN IP Address, which the domain name corresponds to.

## Define the required fields of Host Table

### Domain Name:

- It can be set by System Manager. To let the internal user to access to the information that provided by the host by this domain name

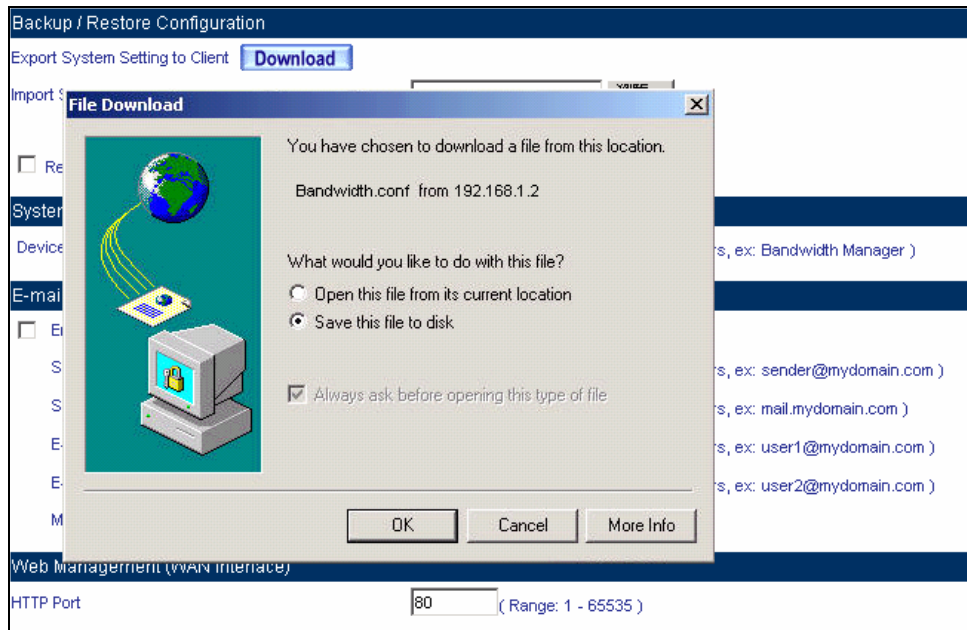
### Virtual IP Address:

- The virtual IP address respective to Host Table. It must be LAN or DMZ IP address.

## System Settings- Exporting

**STEP 1** . In System Setting Web UI, click on button next to Export System Settings to Client.

**STEP 2** . When the **File Download** pop-up window appears, choose the destination place where to save the exported file and click on **Save**. The setting value of BM-525 will copy to the appointed site instantly.

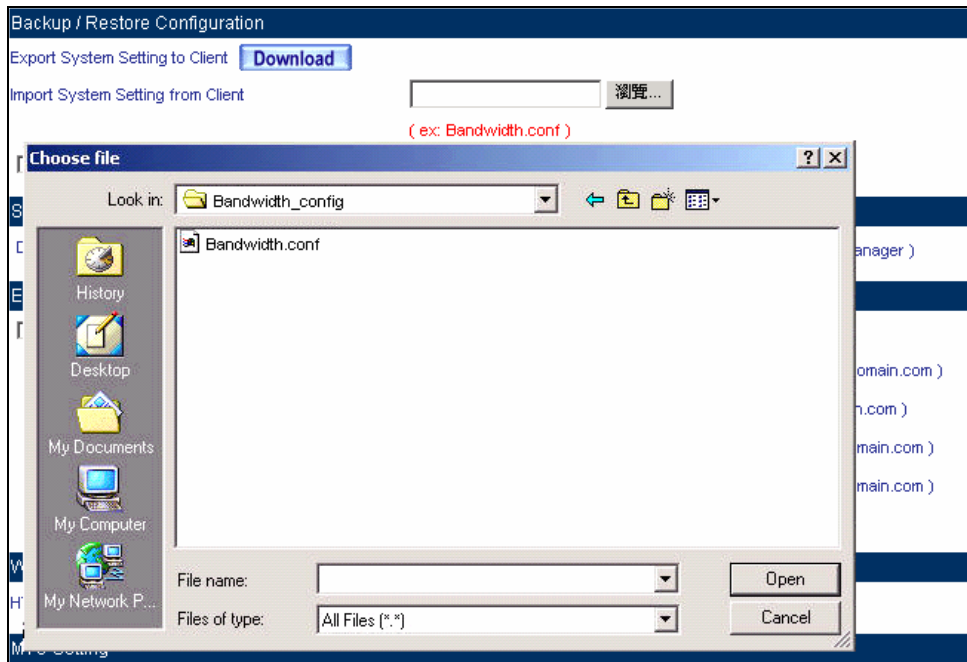


**Select the Destination Place to Save the Exported File**

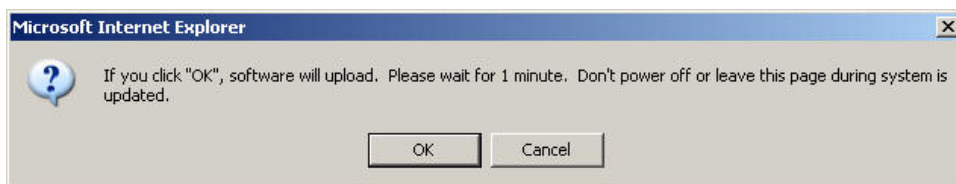
## System Settings- Importing

**STEP 1** . In **System Setting** Web UI, click on the **Browse** button next to **Import System Settings from Client**. When the Choose File pop-up window appears, select the file to which contains the saved BM-525 Settings, then click **OK**.

**STEP 2** . Click **OK** to import the file into the BM-525



**Enter the File Name and Destination of the Imported File**



**Upload the Setting File Web UI**

## Restoring Factory Default Settings

**STEP 1 .** Select **Reset Factory Settings** in **BM-525 Configuration** Web UI

**STEP 2 .** Click **OK** at the bottom-right of the page to restore the factory settings.

Backup / Restore Configuration	
Export System Setting to Client	<input type="button" value="Download"/>
Import System Setting from Client	<input type="text"/> <input type="button" value="瀏覽..."/>
( ex: Bandwidth.conf )	
<input checked="" type="checkbox"/> Reset Factory Setting	
System Name Setting	
Device Name	<input type="text"/> ( Max. 30 characters, ex: Bandwidth Manager )
E-mail Setting	
<input type="checkbox"/> Enable E-mail Alert Notification	
Sender Address ( Required by some ISPs )	<input type="text"/> ( Max. 60 characters, ex: sender@mydomain.com )
SMTP Server	<input type="text"/> ( Max. 80 characters, ex: mail.mydomain.com )
E-mail Address 1	<input type="text"/> ( Max. 60 characters, ex: user1@mydomain.com )
E-mail Address 2	<input type="text"/> ( Max. 60 characters, ex: user2@mydomain.com )
Mail Test	<input type="button" value="Mail Test"/>
Web Management (WAN Interface)	
HTTP Port	<input type="text" value="80"/> ( Range: 1 - 65535 )
MTU Setting	
MTU	<input type="text" value="1500"/> Bytes ( Range: 40 - 1500 )
Dynamic Routing (RIPv2)	
Enable	<input type="checkbox"/> LAN <input type="checkbox"/> WAN <input type="checkbox"/> DMZ
Routing information update timer	<input type="text" value="30"/> Seconds ( Range: 5 - 99999 )
Routing information timeout	<input type="text" value="180"/> Seconds ( Range: 5 - 99999 )
SIP protocol pass-through	
<input type="checkbox"/> Enable SIP protocol pass-through	
To-Appliance Packets Log	
<input type="checkbox"/> Enable To-Appliance Packets Log	
System Reboot	
Reboot Bandwidth Manager Appliance	<input type="button" value="Reboot"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

### Reset Factory Settings

#### Enabling E-mail Alert Notification

**STEP 1 . Device Name:** Enter the Device Name or use the default value.

**STEP 2 .** Select **Enable E-mail Alert Notification** under E-Mail Settings.

**STEP 3 . Sender Address:** Enter the Sender Address. (Required by some ISPs.)



**STEP 4 . SMTP Server IP:** Enter SMTP server's IP address.

**STEP 5 . E-Mail Address 1:** Enter the e-mail address of the first user to be notified.

**STEP 6 . E-Mail Address 2:** Enter the e-mail address of the second user to be notified. (Optional)

**STEP 7 .** Click **OK** on the bottom-right of the screen to enable E-mail Alert Notification.

System Name Setting	
Device Name	<input type="text" value="Bandwidth Manager"/> ( Max. 30 characters, ex: Bandwidth Manager )
E-mail Setting	
<input checked="" type="checkbox"/> Enable E-mail Alert Notification	
Sender Address (Required by some ISPs)	<input type="text" value="sender@mydomain.c"/> ( Max. 60 characters, ex: sender@mydomain.com )
SMTP Server	<input type="text" value="mail.mydomain.com"/> ( Max. 80 characters, ex: mail.mydomain.com )
E-mail Address 1	<input type="text" value="user1@mydomain.cc"/> ( Max. 60 characters, ex: user1@mydomain.com )
E-mail Address 2	<input type="text" value="user2@mydomain.cc"/> ( Max. 60 characters, ex: user2@mydomain.com )
Mail Test	<input type="button" value="Mail Test"/>

### Enable E-mail Alert Notification



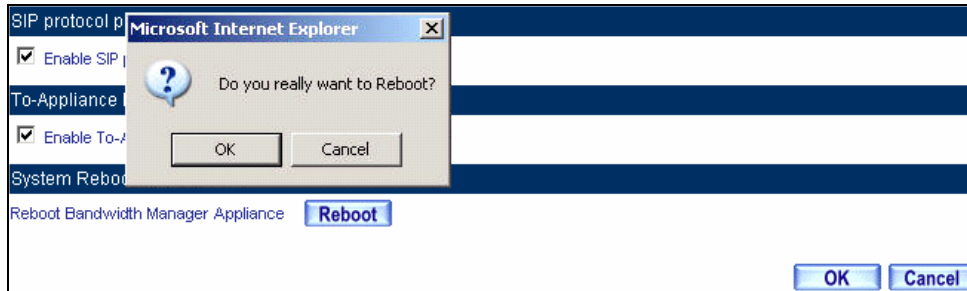
Click on **Mail Test** to test if E-mail Address 1 and E-mail Address 2 can receive the Alert Notification correctly.

## Reboot BM-525

**STEP 1** . Reboot BM-525 : Click **Reboot** button next to **Reboot BM-525 Appliance**.

**STEP 2** . A confirmation pop-up page will appear.

**STEP 3** . Follow the confirmation pop-up page; click **OK** to restart BM-525.



### Reboot BM-525

## 2.8 Date/Time

**STEP 1** . Select **Enable synchronize with an Internet time Server**.

**STEP 2** . Click the down arrow to select the **offset time from GMT**.

**STEP 3** . Enter the **Server IP / Name** with which you want to synchronize.

**STEP 4** . Set the interval time to synchronize with outside servers.

System time : Mon Aug 14 04:10:36 2006

Synchronize system clock

Enable synchronize with an Internet time Server

Set offset +8 hours from GMT Assist

Enable daylight saving time setting

From 1 / 1 To 1 / 1

Server IP / Name 220.130.158.52 Assist

Update system clock every 360 minutes ( Range: 1 - 99999, 0: means update at booting time )

Synchronize system clock with this client Sync

OK Cancel

### System Time Setting



Click on the **Sync** button and then the BM-525's date and time will be synchronized to the Administrator's PC



The value of **Set Offset From GMT** and **Server IP / Name** can be looking for from **Assist**.



If the local area executes the daylight saving time, then **enable the daylight saving time setting**.

## 2.9 Multiple Subnet

Connect to the Internet through Multiple Subnet NAT or Routing Mode by the IP address that set by the LAN user's network card.

### **Preparation**

To connect the Internet, WAN IP (211.22.22.22) connects with ATUR.

## Adding Multiple Subnet

Add the following settings in **Multiple Subnet** of **System** function:

- Click on **New Entry**
- **Alias IP of LAN Interface** : Enter 172.16.30.1
- **Netmask** : Enter 255.255.255.0
- **WAN** : Enter Interface IP 211.22.22.22, and choose **NAT** in **Forwarding Mode**
- Click **OK**
- Complete Adding Multiple Subnet

Add New Multiple Subnet IP			
Interface	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ		
Alias IP of Interface	<input type="text" value="172.16.30.1"/>		
Netmask	<input type="text" value="255.255.255.0"/>		
WAN Interface IP		Forwarding Mode	
WAN	<input type="text" value="211.22.22.22"/> <a href="#">Assist</a>	<input checked="" type="radio"/> NAT	<input type="radio"/> Routing
<input type="button" value="OK"/> <input type="button" value="Cancel"/>			

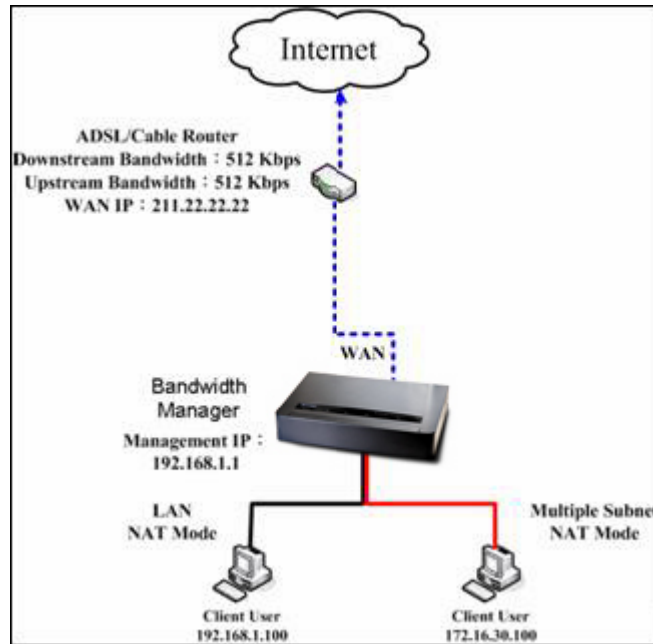
### Add Multiple Subnet Web UI



WAN Interface can use **Assist** to enter the data.



After setting, there will be two subnets in LAN: 192.168.1.0/24 (default LAN subnet) and 172.16.30.0/24. So if LAN IP is: 192.168.1.xx, it must use NAT Mode to connect to the Internet. 162.172.50.xx, it's also use NAT mode through WAN (The Internet Server can see your WAN IP directly).



**Multiple Subnet Network**

- The BM-525's Interface Status:  
 WAN IP : 211.22.22.22  
 LAN Port IP : 192.168.1.1  
 LAN Port Multiple Subnet : 172.16.30.1

WAN IP (10.10.10.1) connects to the Router of ISP (10.10.10.2) directly. The IP address provided by ISP is 162.172.50.0/24

Add the following settings in **Multiple Subnet** of **System** function:

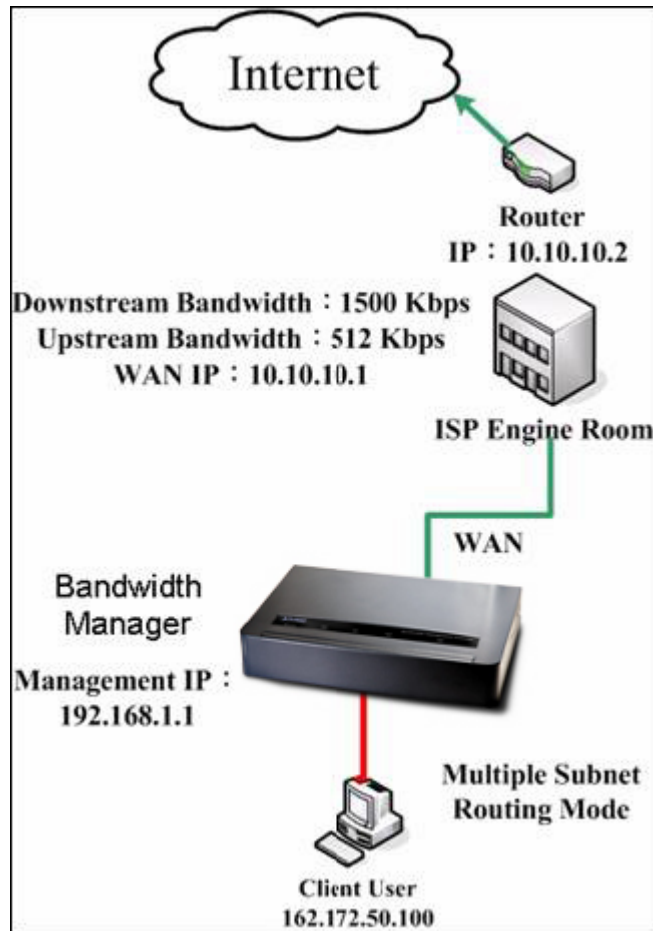
- Click on **New Entry**
- **Alias IP of LAN Interface** : Enter 162.172.50.1
- **Netmask** : Enter 255.255.255.0
- **WAN** : Enter Interface IP: 10.10.10.1, and choose **Routing** in **Forwarding Mode**
- Click **OK**
- Complete Adding Multiple Subnet

Add New Multiple Subnet IP			
Interface	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ		
Alias IP of Interface	<input type="text" value="172.16.30.1"/>		
Netmask	<input type="text" value="255.255.255.0"/>		
WAN Interface IP		Forwarding Mode	
WAN	<input type="text" value="211.22.22.22"/> <a href="#">Assist</a>	<input checked="" type="radio"/> NAT	<input type="radio"/> Routing
<input type="button" value="OK"/> <input type="button" value="Cancel"/>			

### Multiple Subnet Web UI Setting



After setting, if LAN IP of BM-525 is 162.172.50.xx, it uses Routing Mode (Internet Server can see your IP 162.172.50.xx directly)



### Multiple Subnet Network

- The BM-525's Interface Status:  
WAN IP : 10.10.10.1  
LAN Port IP : 192.168.1.1  
LAN Port Multiple Subnet : 162.172.50.1



## 2.10 Route Table

**To connect two different subnet router with the BM-525 and makes them to connect to Internet through BM-525.**

### **Preparation**

Company A: WAN (61.11.11.11) connects with ATUR to Internet

LAN subnet: 192.168.1.1/24

The Router1 which connect with LAN (10.10.10.1, support RIPv2) its LAN subnet is 192.168.10.1/24

Company B: Router2 (10.10.10.2, support RIPv2), its LAN subnet is 192.168.20.1/24

Company A's Router1 (10.10.10.1) connect directly with Company B's Router2 (10.10.10.2).

**STEP 1 .** Enter the following settings in **Route Table** in **System** function:

- **Destination IP:** Enter 192.168.10.1
- **Netmask:** Enter 255.255.255.0 °
- **Gateway:** Enter 192.168.1.252
- **Interface:** Select LAN
- Click **OK**

Add New Static Route	
Destination IP	<input type="text" value="192.168.10.1"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.1.252"/>
Interface	<input type="text" value="LAN"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

**Add New Static Route1**

**STEP 2 .** Enter the following settings in **Route Table** in **System** function:

- **Destination IP:** Enter 192.168.20.1
- **Netmask:** Enter 255.255.255.0
- **Gateway:** Enter 192.168.1.252
- **Interface:** Select LAN
- Click **OK**

Add New Static Route	
Destination IP	<input type="text" value="192.168.20.1"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.1.252"/>
Interface	<input type="text" value="LAN"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

**Add New Static Route2**

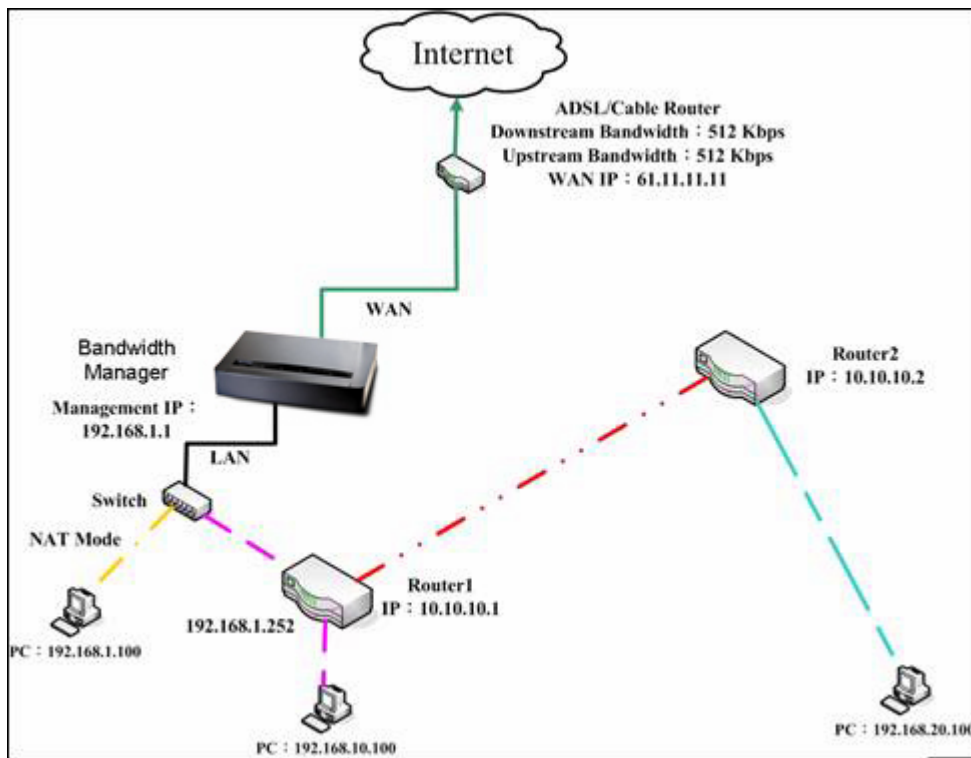
**STEP 3** . Enter the following setting in **Route Table** in **System** function:

- **Destination IP:** Enter 10.10.10.0
- **Netmask:** Enter 255.255.255.0
- **Gateway:** Enter 192.168.1.252
- **Interface:** Select LAN
- Click **OK**

Add New Static Route	
Destination IP	<input type="text" value="10.10.10.0"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.1.252"/>
Interface	<input type="text" value="LAN"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

**Add New Static Route3**

**STEP 4** . Adding successful. At this time the computer of 192.168.10.1/24, 192.168.20.1/24 and 192.168.1.1/24 can connect with each other and connect to Internet by NAT.



### Route Table Setting

## 2.11 DHCP

**STEP 1** . Select **DHCP** in **System** and enter the following settings:

- **Domain Name** : Enter the Domain Name
- **DNS Server 1**: Enter the distributed IP address of DNS Server1.
- **DNS Server 2**: Enter the distributed IP address of DNS Server2.
- **WINS Server 1**: Enter the distributed IP address of WINS Server1.
- **WINS Server 2**: Enter the distributed IP address of WINS Server2.
- **LAN Interface**:
  - ◆ **Client IP Address Range 1**: Enter the starting and the ending IP address dynamically assigning to DHCP clients. The default value is 192.168.1.2 to 192.168.1.254 (it must be in the same subnet)
  - ◆ **Client IP Address Range 2**: Enter the starting and the ending IP address dynamically assigning to DHCP clients. But it must in the same subnet as **Client IP Address Range 1** and the range cannot be repeated.
- **DMZ Interface**: the same as LAN Interface. (DMZ works only if to enable DMZ Interface)
- **Leased Time**: Enter the leased time for Dynamic IP. The default time is 24 hours.
- Click **OK** and DHCP setting is completed.

Dynamic IP Address			
Subnet	192.168.1.0	Netmask	255.255.255.0
Gateway	192.168.1.1	Broadcast	192.168.1.255
-----			
<input checked="" type="checkbox"/>	Enable DHCP Support		
	Domain Name	<input type="text"/>	( Max. 40 characters, ex: dhcp.domain_name )
<input type="checkbox"/>	Automatically Get DNS		
	DNS Server 1	<input type="text" value="192.168.1.1"/>	
	DNS Server 2	<input type="text"/>	
	WINS Server 1	<input type="text"/>	
	WINS Server 2	<input type="text"/>	
	LAN Interface :		
	Client IP Range 1	<input type="text" value="192.168.1.2"/>	To <input type="text" value="192.168.1.254"/>
	Client IP Range 2	<input type="text"/>	To <input type="text"/>
	DMZ Interface :		
	Client IP Range 1	<input type="text" value="192.168.3.2"/>	To <input type="text" value="192.168.3.254"/>
	Client IP Range 2	<input type="text"/>	To <input type="text"/>
	Leased Time	<input type="text" value="24"/>	hours ( Range: 0 - 99999 )
			<input type="button" value="OK"/> <input type="button" value="Cancel"/>

### DHCP Web UI



When selecting **Automatically Get DNS**, the DNS Server will lock it as LAN Interface IP. (Using Occasion: When the system Administrator starts Authentication, the users' first DNS Server must be the same as LAN Interface IP in order to enter Authentication Web UI)

## 2.12 DDNS

**STEP 1** . Select **Dynamic DNS** in **System** function. Click **New Entry** button





- **Service providers** : Select service providers.
- **Automatically fill in the WAN IP** : Check to automatically fill in the WAN IP. °
- **User Name** : Enter the registered user name.
- **Password** : Enter the password
- **Domain name** : Enter Your host domain name
- Click **OK** to add Dynamic DNS.

Add New Dynamic DNS	
Service Provider :	DynDNS (www.dyndns.com) [ U.S.A. ] <span style="color: red;">Sign up</span>
WAN IP:	61.11.11.11 <input checked="" type="checkbox"/> Automatically WAN
User Name :	rayearth (Max. 59 characters)
Password :	***** (Max. 44 characters)
Domain Name:	rayearth . dnsalias.org (Max. 34 characters)
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

**DDNS Web UI**

i	Domain Name	WAN IP	Configure
	rayearth.dnsalias.org	61.11.11.11	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
<input type="button" value="New Entry"/>			

**Complete DDNS Setting**

Chart				
Meaning	Update successfully	Incorrect username or password	Connecting to server	Unknown error



If System Administrator had not registered a DDNS account, click on **Sign up** then can enter the website of the provider.



If you do not select **Automatically fill in the WAN IP** and then you can enter a specific IP in **WAN IP**. Let DDNS to correspond to that specific IP address.



## 2.13 Host Table

**STEP 1.** Select **Host Table** in **Settings** function and click on **New Entry**

- **Domain Name:** The domain name of the server
- **Virtual IP Address:** The virtual IP address respective to Host Table
- Click **OK** to add Host Table.

Add New Host Table	
Host Name	<input type="text" value="www.rayearth.com"/> ( Max. 80 characters, ex: www.my_domain.com )
Virtual IP Address	<input type="text" value="192.168.1.2"/> ( ex: 192.168.100.102 )
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

### Add New Host Table



To use Host Table, the user PC's first DNS Server must be the same as the LAN Port or DMZ Port IP of BM-525. That is the default gateway.

## 2.14 Language

Select the Language version (**English Version**, **Traditional Chinese Version**, or **Simplified Chinese Version**) and click **OK**.



**Language Setting Web UI**

## Chapter 3 Interface

In this section, the **Administrator** can set up the IP addresses for the office network. The Administrator may configure the IP addresses of the LAN network, the WAN network, and the DMZ network. The Netmask and gateway IP addresses are also configured in this section.

## 3.1 Interface

### Define the required fields of Interface

#### LAN:

- Using the LAN **Interface**, the Administrator can set up the LAN network of BM-525.

#### Ping:

- Select this function to allow the LAN users to ping the Interface IP Address.

#### HTTP:

- Select to enable the user to enter the Web UI of BM-525 from Interface IP.

#### WAN:

- The System Administrator can set up the WAN network of BM-525.

#### Connect Mode:

- Display the current connection mode:
  - ◆ PPPoE (ADSL user)
  - ◆ Dynamic IP Address (Cable Modem User)
  - ◆ Static IP Address
  - ◆ PPTP (European User Only)

#### Upstream/Downstream Bandwidth:

- The System Administrator can set up the correct Bandwidth of WAN network Interface here.

#### Auto Disconnect:

- The PPPoE connection will automatically disconnect after a length of idle time (no activities). Enter the amount of idle time before disconnection in the field. Enter "0" if you do not want the PPPoE connection to disconnect at all.

**DMZ:**

- The Administrator uses the DMZ Interface to set up the DMZ network.
- The DMZ includes:
  - ◆ **NAT Mode** : In this mode, the DMZ is an independent virtual subnet. This virtual subnet can be set by the Administrator but cannot be the same as LAN Interface.
  - ◆ **Transparent Mode:** In this mode, the DMZ and WAN Interface are in the same subnet.

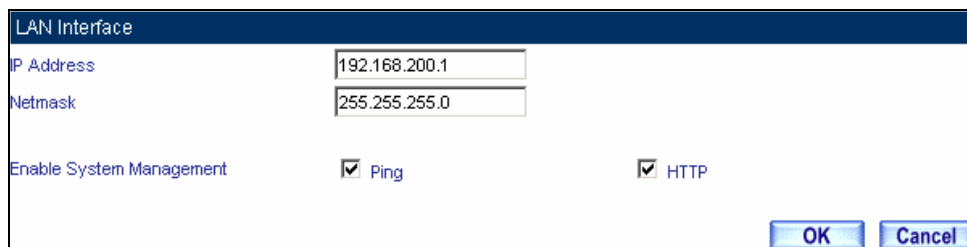
We set up four Interface Address examples in this section:

No.	Suitable Situation	Example
Ex1	<b>LAN</b>	Modify LAN Interface Settings
Ex2	<b>WAN</b>	Setting WAN Interface Address
Ex3	<b>DMZ</b>	Setting DMZ Interface Address (NAT Mode)
Ex4	<b>DMZ</b>	Setting DMZ Interface Address (Transparent Mode)

## 3.2 LAN

**STEP 1** . Select **LAN** in **Interface** and enter the following setting:

- Enter the new **IP Address** and **Netmask**
- Select **Ping** and **HTTP**
- Click **OK**



LAN Interface	
IP Address	192.168.200.1
Netmask	255.255.255.0
Enable System Management	<input checked="" type="checkbox"/> Ping <input checked="" type="checkbox"/> HTTP
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

### Setting LAN Interface Web UI



The default LAN IP Address is 192.168.1.1. After the Administrator setting the new LAN IP Address on the computer , he/she has to restart the System to make the new IP address effective (when the computer obtain IP by DHCP).



Do not cancel Web UI selection before not setting Permitted IPs yet. It will cause the Administrator cannot be allowed to enter the BM-525's Web UI from LAN.

### 3.3 WAN

**STEP 1** . Select **WAN** in **Interface** and click **Modify**

**STEP 2** . Select the Connecting way:

■ **PPPoE (ADSL User):**

1. Select **PPPoE**
2. Enter **User Name** as an account
3. Enter **Password** as the password
4. Select **Dynamic** or **Fixed** in **IP Address provided by ISP**. If you select Fixed, please enter IP Address, Netmask, and Default Gateway.
5. Enter **Max. Downstream Bandwidth** and **Max. Upstream Bandwidth**.  
(According to the flow that user apply)
6. Select **Ping** and **Web UI**
7. Click **OK**

The screenshot shows the 'WAN Interface' configuration window. The 'PPPoE (ADSL User)' option is selected. The 'Current Status' is 'Disconnected', with 'Connecting' and 'Disconnect' buttons. The 'IP Address' is '0.0.0.0'. The 'User Name' is 'rayearth' and the 'Password' is masked with asterisks. Under 'IP Address provided by ISP', the 'Dynamic' option is selected. The 'Max. Downstream Bandwidth' is set to 12000 Kbps and the 'Max. Upstream Bandwidth' is set to 1024 Kbps. The 'Service-On-Demand' checkbox is checked, and the 'Auto Disconnect if idle' is set to 0 minutes. The 'Enable System Management' section has 'Ping' and 'HTTP' checkboxes checked. 'OK' and 'Cancel' buttons are at the bottom right.

#### PPPoE Connection



If the connection is PPPoE, you can choose **Service-On-Demand** for WAN Interface to connect automatically when disconnect (suggested); or to set up **Auto Disconnect if idle** (not recommend)



**■ Dynamic IP Address (Cable Modem User):**

1. Select **Dynamic IP Address (Cable Modem User)**
2. Click **Renew** in the right side of IP Address and then can obtain IP automatically.
3. If the MAC Address is required for ISP then click on **Clone MAC Address** to obtain MAC IP automatically.
4. **Hostname:** Enter the hostname provided by ISP.
5. **Domain Name:** Enter the domain name provided by ISP.
6. **User Name** and **Password** are the IP distribution method according to Authentication way of DHCP+ protocol (like ISP in China)
7. Enter **Max. Downstream Bandwidth** and **Max. Upstream Bandwidth** (According to the flow that user apply)
8. Select **Ping** and **Web UI**
9. Click **OK**

The screenshot shows the 'WAN Interface' configuration window. The 'Dynamic IP Address (Cable Modem User)' option is selected. The IP Address field is set to 0.0.0.0, with 'Renew' and 'Release' buttons to its right. The MAC Address field is set to 00:88:56:78:22:9D, with a 'Clone MAC Address' button to its right. Below these are input fields for Hostname, Domain Name, User Name, and Password, each with a character limit. The Max. Downstream Bandwidth is set to 12000 Kbps and the Max. Upstream Bandwidth is set to 1024 Kbps. At the bottom, 'Enable System Management' is checked for both 'Ping' and 'HTTP'. 'OK' and 'Cancel' buttons are at the bottom right.

**Dynamic IP Address Connection**

## ■ Static IP Address

1. Select **Static IP Address**
2. Enter **IP Address**, **Netmask**, and **Default Gateway** that provided by ISP
3. Enter **DNS Server1** or **DNS Server2**
4. Enter **Max. Downstream Bandwidth** and **Max. Upstream Bandwidth**  
(According to the flow that user apply)
5. Select **Ping** and **Web UI**
6. Click **OK**

The screenshot shows the 'WAN Interface' configuration window. The 'Static IP Address' radio button is selected. The fields are filled with the following values:

IP Address	211.22.22.18
Netmask	255.255.255.0
Default Gateway	211.22.22.17
DNS Server 1	168.95.1.1
DNS Server 2	
Max. Downstream Bandwidth	12000 Kbps ( Range: 1 - 25600 )
Max. Upstream Bandwidth	1024 Kbps ( Range: 1 - 25600 )
Enable System Management	<input checked="" type="checkbox"/> Ping <input checked="" type="checkbox"/> HTTP

Buttons for 'OK' and 'Cancel' are visible at the bottom right.

### Static IP Address Connection



When selecting **Ping** and **Web UI** on WAN network Interface, users will be able to ping the BM-525 and enter the Web UI WAN network. It may influence network security. The suggestion is to **Cancel Ping** and **Web UI** after all the settings have finished. And if the System Administrator needs to enter UI from WAN, he/she can use **Permitted IPs** to enter.

## ■ PPTP (European User Only):

1. Select **PPTP (European User Only)**
2. Enter the name of applied account in **User Name**.
3. Enter the password of applied account in **Password**.
4. Select **Obtain an IP address automatically** or **Use the following IP address** (use the assigned IP address) in **IP Address provided by ISP**.
  - ◆ Select **Obtain as IP address automatically**, please enter the value of **MAC Address**, **Host Name** and **Domain Name**.
  - ◆ Select **Use the following IP address**. Please enter the value of **IP address**,

**Netmask, and Default Gateway.**

5. Enter value of **PPTP Gateway**. (**Connect ID** is required by some ISP provider).
6. Enter the value of **MAX. Downstream Bandwidth** and **MAX. Upstream Bandwidth** (According to the applied bandwidth).
7. Select **Ping** and **HTTP** in **Enable System Management**.
8. Click **OK**.

WAN Interface	
<input type="radio"/> PPPoE (ADSL User) <input type="radio"/> Dynamic IP Address (Cable Modem User) <input type="radio"/> Static IP Address <input checked="" type="radio"/> PPTP (European User Only)	
Current Status	Disconnected <span style="float: right;"><input type="button" value="Connecting"/></span>
IP Address	0.0.0.0 <span style="float: right;"><input type="button" value="Disconnect"/></span>
User Name	<input type="text" value="Rayearth"/>
Password	<input type="text" value="*****"/>
IP Address provided by ISP	<input checked="" type="radio"/> Obtain an IP address automatically <input type="radio"/> Use the following IP address
MAC Address	<input type="text" value="00:88:56:78:22:9D"/> <span style="float: right;"><input type="button" value="Clone MAC Address"/></span>
Hostname	<input type="text"/>
Domain Name	<input type="text"/>
IP Address	<input type="text"/>
Netmask	<input type="text"/>
Default Gateway	<input type="text"/>
PPTP Gateway	<input type="text" value="172.19.1.254"/>
Connect ID	<input type="text"/>
Max. Downstream Bandwidth	<input type="text" value="12000"/> Kbps ( Range: 1 - 25600 )
Max. Upstream Bandwidth	<input type="text" value="1024"/> Kbps ( Range: 1 - 25600 )
<input type="checkbox"/> BEZEG-ISRAEL <input checked="" type="checkbox"/> Service-On-Demand	
Auto Disconnect if idle	<input type="text" value="0"/> minutes( Range: 1 - 99999, 0: means always connected )
Enable System Management	<input checked="" type="checkbox"/> Ping <input checked="" type="checkbox"/> HTTP
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

### Dynamic IP Address Connection



If the connection is PPPoE, you can choose **Service-On-Demand** for WAN Interface to connect automatically when disconnect (suggested); or to set up **Auto Disconnect if idle** (not recommend)

## 3.4 DMZ

### Setting DMZ Interface Address (NAT Mode)

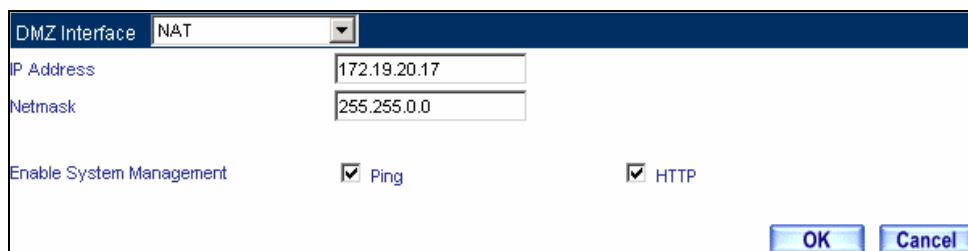
**STEP 1** . Click **DMZ Interface**

**STEP 2** . Select NAT Mode in DMZ Interface

- Select **NAT** in **DMZ Interface**
- Enter **IP Address** and **Netmask**

**STEP 3** . Select **Ping** and **HTTP**

**STEP 4** . Click **OK**



The screenshot shows a web interface for configuring the DMZ Interface. At the top, there is a dropdown menu labeled "DMZ Interface" with "NAT" selected. Below this, there are two input fields: "IP Address" with the value "172.19.20.17" and "Netmask" with the value "255.255.0.0". Underneath these fields, there are two checkboxes: "Enable System Management" (unchecked), "Ping" (checked), and "HTTP" (checked). At the bottom right, there are two buttons: "OK" and "Cancel".

Setting DMZ Interface Address (NAT Mode) Web UI

## Setting DMZ Interface Address (Transparent Mode)

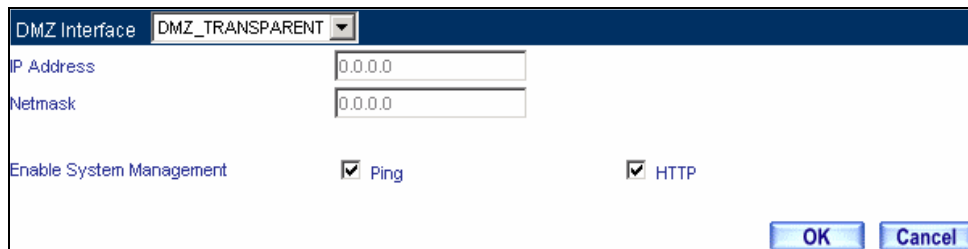
**STEP 1** . Select **DMZ** Interface

**STEP 2** . Select Transparent Mode in DMZ Interface

- Select **DMZ\_Transparent** in **DMZ Interface**

**STEP 1** . Select **Ping** and **HTTP**

**STEP 2** . Click **OK**



DMZ Interface	DMZ_TRANSPARENT	
IP Address	0.0.0.0	
Netmask	0.0.0.0	
Enable System Management	<input checked="" type="checkbox"/> Ping	<input checked="" type="checkbox"/> HTTP
		<input type="button" value="OK"/> <input type="button" value="Cancel"/>

Setting DMZ Interface Address (Transparent Mode) Web UI



In WAN, the connecting way must be **Static IP Address** and can choose **Transparent Mode** in **DMZ**.

## Chapter 4 Policy Object

### 4.1 Address

The BM-525 allows the Administrator to set Interface addresses of the LAN network, LAN network group, WAN network, WAN network group, DMZ and DMZ group.

An IP address in the Address Table can be an address of a computer or a sub network. The Administrator can assign an easily recognized name to an IP address. Based on the network it belongs to, an IP address can be an LAN IP address, WAN IP address or DMZ IP address. If the Administrator needs to create a control policy for packets of different IP addresses, he can first add a new group in the LAN Group or the WAN Group and assign those IP addresses into the newly created group. Using group addresses can greatly simplify the process of building control policies.



With easily recognized names of IP addresses and names of address groups shown in the address table, the Administrator can use these names as the source address or destination address of control policies. The address table should be setup before creating control policies, so that the Administrator can pick the names of correct IP addresses from the address table when setting up control policies.

## **Define the required fields of Address**

### **Name:**

- The System Administrator set up a name as IP Address that is easily recognized.

### **IP Address:**

- It can be a PC's IP Address or several IP Address of Subnet. Different network area can be: Internal IP Address, External IP Address, and DMZ IP Address.

### **Netmask:**

- When correspond to a specific IP, it should be set as: 255.255.255.255.
- When correspond to several IP of a specific Domain. Take 192.168.100.1 (C Class subnet) as an example, it should be set as: 255.255.255.0.

### **MAC Address:**

- Correspond a specific PC's MAC Address to its IP; it can prevent users changing IP and accessing to the net service through policy without authorizing.

### **Get Static IP address from DHCP Server:**

- When enable this function and then the IP obtain from DHCP Server automatically under LAN or DMZ will be distributed to the IP that correspond to the MAC Address.



We set up two Address examples in this section:

No	Suitable Situation	Example
Ex1	<b>LAN</b>	Under DHCP circumstances, assign the specific IP to static users and restrict them to access FTP net service only through policy.
Ex2	<b>LAN Group WAN</b>	Set up a policy that only allows partial users to connect with specific IP (External Specific IP)

## 4.2 Example

**Under DHCP situation, assign the specific IP to static users and restrict them to access FTP net service only through policy**

**STEP 1** . Select **LAN** in **Address** and enter the following settings:

- Click **New Entry** button
- **Name:** Enter Rayearth
- **IP Address:** Enter 192.168.3.2
- **Netmask:** Enter 255.255.255.255
- **MAC Address :** Enter the user's MAC Address ( 00:B0:18:25:F5:89 )
- Select **Get static IP address from DHCP Server**
- Click **OK**

### Setting LAN Address Book Web UI

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		In Use
Rayearth	192.168.3.2/255.255.255.255	00:B0:18:25:F5:89	Modify Remove

New Entry

### Complete the Setting of LAN

**STEP 2 . Adding the following setting in **Outgoing Policy**:**

Comment :	<input type="text" value=""/>	(Max. 32 characters)
<b>Add New Policy</b>		
Source Address	Rayearth	
Destination Address	Outside_Any	
Service	FTP	
Schedule	None	
Authentication User	None	
Action	PERMIT	
Traffic Log	<input type="checkbox"/> Enable	
Statistics	<input type="checkbox"/> Enable	
Content Blocking	<input type="checkbox"/> Enable	
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )	
QoS	None	
		<input type="button" value="OK"/> <input type="button" value="Cancel"/>

**Add a Policy of Restricting the Specific IP to Access to Internet**

**STEP 3 . Complete assigning the specific IP to static users in **Outgoing Policy** and restrict them to access FTP net service only through policy:**

Source	Destination	Service	Action	Option	Configure	Move
Rayearth	Outside_Any	FTP	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1
<input type="button" value="New Entry"/>						

**Complete the Policy of Restricting the Specific IP to Access to Internet**



When the System Administrator setting the **Address Book**, he/she can choose the way of clicking on **Clone MAC Address** to make the BM-525 to fill out the user's MAC Address automatically.



In **LAN** of **Address** function, the BM-525 will default an **Inside Any** address represents the whole LAN network automatically. Others like **WAN**, **DMZ** also have the **Outside Any** and **DMZ Any** default address setting to represent the whole subnet.



The setting mode of **WAN** and **DMZ** of **Address** are the same as **LAN**; the only difference is **WAN** cannot set up MAC Address.

## Setup a policy that only allows partial users to connect with specific IP (External Specific IP)

**STEP 1** . Setting several LAN network Address.

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		<a href="#">In Use</a>
Rayearth	192.168.1.2/255.255.255.255	00:01:80:41:D0:FB	<a href="#">Modify</a> <a href="#">Remove</a>
Josh	192.168.1.4/255.255.255.255		<a href="#">Modify</a> <a href="#">Remove</a>
SinSan	192.168.1.5/255.255.255.255	00:01:80:B1:C2:FB	<a href="#">Modify</a> <a href="#">Remove</a>
Daniel	192.168.1.7/255.255.255.255		<a href="#">Modify</a> <a href="#">Remove</a>
Luke	192.168.1.8/255.255.255.255	00:01:76:41:1D:C3	<a href="#">Modify</a> <a href="#">Remove</a>
<a href="#">New Entry</a>			

Setting Several LAN Network Address

**STEP 2.** Enter the following settings in **LAN Group of Address**:

- Click **New Entry**
- Enter the **Name** of the group
- Select the users in the **Available Address** column and click **Add**
- Click **OK**

**Add New LAN Address Group**

Name	Member	Configure
TestTeam	Rayearth, Josh, SinSan	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>
<input type="button" value="New Entry"/>		

**Complete Adding LAN Address Group**



The setting mode of **WAN Group** and **DMZ Group of Address** are the same as **LAN Group**.

**STEP 3 .** Enter the following settings in **WAN** of **Address** function:

- Click **New Entry**
- Enter the following data (**Name, IP Address, Netmask**)
- Click **OK**

Add New Address	
Name	<input type="text" value="Yahoo"/> (Max. 16 characters)
IP Address	<input type="text" value="202.1.237.21"/>
Netmask	<input type="text" value="255.255.255.255"/> ( 255.255.255.255 means the specified PC ) ( 255.255.255.0 means class C subnet )
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

**Add New WAN Address**

Name	IP / Netmask	Configure
Outside_Any	0.0.0.0/0.0.0.0	<input type="button" value="In Use"/>
Yahoo	202.1.237.21/255.255.255.255	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
<input type="button" value="New Entry"/>		

**Complete the Setting of WAN Address**

**STEP 4 . To exercise STEP1~3 in Policy**

Comment :  (Max. 32 characters)

Modify Policy	
Source Address	TestTeam
Destination Address	Yahoo
Service	ANY
Schedule	None
Authentication User	None
Action	PERMIT
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
QoS	None

**To Exercise Address Setting in Policy**

Source	Destination	Service	Action	Option	Configure	Move
TestTeam	Yahoo	ANY	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1

**Complete the Policy Setting**



The **Address** function really take effect only if use with **Policy**.



## 4.3 Service

TCP and UDP protocols support varieties of services, and each service consists of a TCP Port or UDP port number, such as TELNET (23), SMTP (21), SMTP (25), POP3 (110), etc. The BM-525 includes two services: **Pre-defined Service** and **Custom Service**.

The common-use services like TCP and UDP are defined in the Pre-defined Service and cannot be modified or removed. In the custom menu, users can define other TCP port and UDP port numbers that are not in the pre-defined menu according to their needs. When defining custom services, the client port ranges from 0 to 65535 and the server port ranges from 0 to 65535.

In this chapter, network services are defined and new network services can be added. There are three sub menus under Service which are: **Pre-defined**, **Custom**, and **Group**. The Administrator can simply follow the instructions below to define the protocols and port numbers for network communication applications. Users then can connect to servers and other computers through these available network services.







### How to use Service?

The Administrator can add new service group names in the **Group** option under **Service** menu, and assign desired services into that new group. Using service group the Administrator can simplify the processes of setting up control policies. For example, there are 10 different computers that want to access 5 different services on a server, such as HTTP, FTP, SMTP, POP3, and TELNET. Without the help of service groups, the Administrator needs to set up 50 (10x5) control policies, but by applying all 5 services to a single group name in the **Service** field, it takes only one control policy to achieve the same effect as the 50 control policies.

## Define the required fields of Service

Pre-defined Web UI's Chart and Illustration:

Chart	Illustration
	Any Service
	TCP Service, For example : FTP, FINGER, HTTP, HTTPS , IMAP, SMTP, POP3, ANY, AOL, BGP, GOPHER, Inter Locator, IRC, L2TP, LDAP, NetMeeting, NNTP, PPTP, Real Media, RLOGIN, SSH, TCP ANY, TELNET, VDO Live, WAIS, WINFRAME, X-WINDOWS, ...etc.
	UDP Service, For example : IKE, DNS, NTP, IRC, RIP, SNMP, SYSLOG, TALK, TFTP, UDP-ANY, UUCP,...etc.
	ICMP Service, Foe example : PING, TRACEROUTE...etc.

### New Service Name:

- The System Manager can name the custom service.

### Protocol:

- The protocol type to be used in connection for device, such as TCP and UDP mode

### Client Port:

- The port number of network card of clients. (The range is 0~65535, suggest to use the default range)

■

### Server Port:

- The port number of custom service

We set up two Service examples in this section:

No	Suitable Situation	Example
Ex1	<b>Custom</b>	Allow external user to communicate with internal user by VoIP through policy. (VoIP Port: TCP 1720, TCP 15325-15333, UDP 15325-15333)
Ex2	<b>Group</b>	Setting service group and restrict the specific users only can access to service resource that provided by this group through policy. (Group: HTTP, POP3, SMTP, DNS)

## 4.4 Custom

**Allow external user to communicate with internal user by VoIP through policy.  
(VoIP Port: TCP 1720, TCP 15328-15333, UDP 15328-15333)**

**STEP 1 . Set LAN and LAN Group in Address function as follows:**

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		In Use
VoIP_01	192.168.1.2/255.255.255.255		Modify Remove
VoIP_02	192.168.1.3/255.255.255.255		Modify Remove
VoIP_03	192.168.1.4/255.255.255.255		Modify Remove
VoIP_04	192.168.1.5/255.255.255.255		Modify Remove

[New Entry](#)

**Setting LAN Address Book Web UI**

Name	Member	Configure
VoIP_Group	VoIP_01, VoIP_02, VoIP_03...	Modify Remove Pause

[New Entry](#)

**Setting LAN Group Address Book Web UI**

**STEP 2 .** Enter the following setting in **Custom** of **Service** function:

- Click **New Entry**
- **Service Name:** Enter the preset name **VoIP**
- Protocol#1 select **TCP**, need not to change the **Client Port**, and set the **Server Port** as: 1720:1720
- Protocol#2 select **TCP**, need not to change the **Client Port**, and set the **Server Port** as: 15328:15333
- Protocol#3 select **UDP**, need not to change the **Client Port**, and set the **Server Port** as: 15328:15333
- Click **OK**

Add User Defined Service				
Service NAME :		VoIP (Max. 16 characters)		
#	Protocol ( Range: 1 - 255 )	Client Port ( Range: 0 - 65535 )	Server Port ( Range: 0 - 65535 )	
1	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other 6	0 : 65535	1720	1720
2	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other 6	0 : 65535	15328	15333
3	<input type="radio"/> TCP <input checked="" type="radio"/> UDP <input type="radio"/> Other 17	0 : 65535	15328	15333
4	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	0 : 0	0	0
5	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	0 : 0	0	0
6	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	0 : 0	0	0
7	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	0 : 0	0	0
8	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	0 : 0	0	0

**Add User Define Service**

Service name	Protocol	Client Port	Server Port	Configure
VoIP	TCP	0:65535	1720:1720	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

**Complete the Setting of User Define Service of VoIP**



Under general circumstances, the range of port number of client is 0-65535. Change the client range in **Custom** of is not suggested.



If the port numbers that enter in the two spaces are different port number, then enable the port number under the range between the two different port numbers (for example: 15328:15333). And if the port number that enter in the two space are the same port number, then enable the port number as one (for example: 1720:1720).

**STEP 3 . Compare Service to Virtual Server.**

Virtual Server Real IP 61.62.236.53			
Service	WAN Port	Server Virtual IP	Configure
VoIP	From-Service(Custom)	192.168.1.2 192.168.1.3 192.168.1.4 192.168.1.5	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>
<input type="button" value="New Entry"/>			

Compare Service to Virtual Server

**STEP 4 . Compare Virtual Server to Incoming Policy.**

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1(61.62.236.53)	VoIP	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1
<input type="button" value="New Entry"/>						

Complete the Policy for External VoIP to Connect with Internal VoIP

**STEP 5 . In Outgoing Policy, complete the setting of internal users using VoIP to connect with external network VoIP:**

Source	Destination	Service	Action	Option	Configure	Move
VoIP_Group	Outside_Any	VoIP	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1
<input type="button" value="New Entry"/>						

Complete the Policy for Internal VoIP to Connect with External VoIP



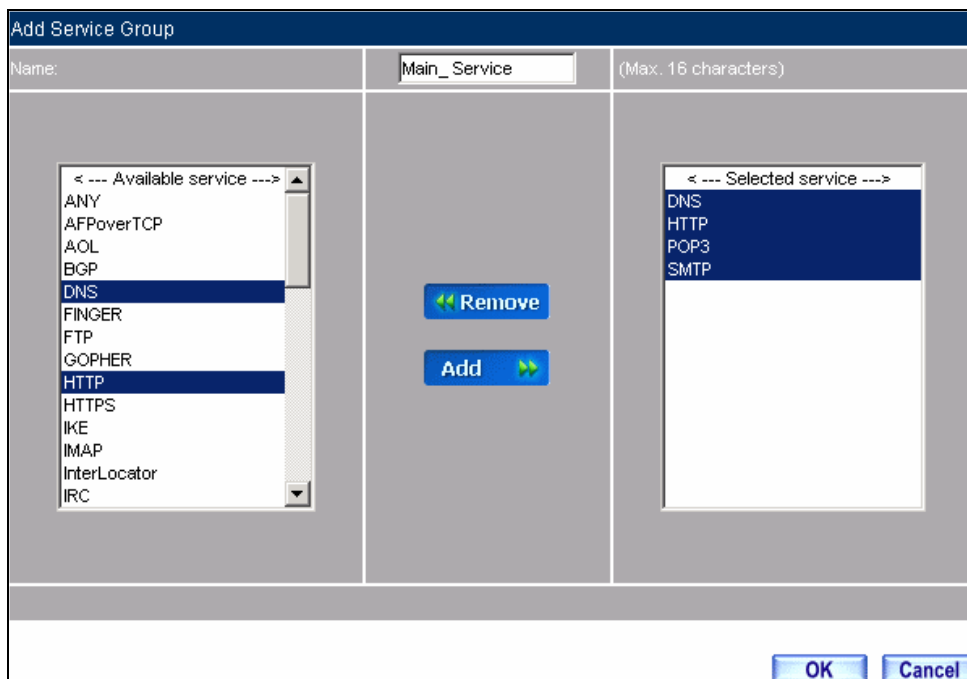
**Service must cooperate with Policy and Virtual Server that the function can take effect**

## 4.5 Group

**Setting service group and restrict the specific users only can access to service resource that provided by this group through policy (Group: HTTP, POP3, SMTP, DNS)**

**STEP 1** . Enter the following setting in **Group of Service**:

- Click **New Entry**
- **Name:** Enter Main\_Service
- Select HTTP, POP3, SMTP, DNS in **Available Service** and click **Add**
- Click **OK**



**Add Service Group**



Group name	Service	Configure
Main_Service	DNS,HTTP,POP3...	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
<input type="button" value="New Entry"/>		

### Complete the setting of Adding Service Group



If you want to remove the service you choose from **Selected Service**, choose the service you want to delete and click **Remove**.

**STEP 2 .** In **LAN Group** of **Address** function, setting an **Address Group** that can include the service of access to Internet.

Name	Member	Configure
Laboratory	Rayearth, Josh, SinSan	<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>
<a href="#">New Entry</a>		

**Setting Address Book Group**

**STEP 3 .** Compare **Service Group** to **Outgoing Policy**.

Source	Destination	Service	Action	Option	Configure	Move
Laboratory	Outside_Any	Main_Service	✔		<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>	To 1 ▾
<a href="#">New Entry</a>						

**Setting Policy**

## 4.6 Schedule

In this chapter, the BM-525 provides the Administrator to configure a schedule for policy to take effect and allow the policies to be used at those designated times. And then the Administrator can set the start time and stop time or VPN connection in **Policy** or **VPN**. By using the **Schedule** function, the Administrator can save a lot of management time and make the network system most effective.



### How to use the Schedule?

The system Administrator can use schedule to set up the device to carry out the connection of Policy or VPN during several different time division automatically.

**To configure the valid time periods for LAN users to access to Internet in a day**

**STEP 1** . Enter the following in **Schedule**:

- Click **New Entry**
- Enter **Schedule Name**
- Set up the working time of Schedule for each day
- Click **OK**

Week Day	Period	
	Start Time	Stop Time
Monday	08:30	18:30
Tuesday	08:30	18:30
Wednesday	08:30	18:30
Thursday	08:30	18:30
Friday	All day	All day
Saturday	Disable	Disable
Sunday	Disable	Disable

**Setting Schedule Web UI**

Name	Configure
WorkingTime	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

**Complete the Setting of Schedule**

**STEP 2 . Compare Schedule with Outgoing Policy**

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 ▾
<input type="button" value="New Entry"/>						

**Complete the Setting of Comparing Schedule with Policy**



The Schedule must compare with **Policy**.

## 4.7 QoS

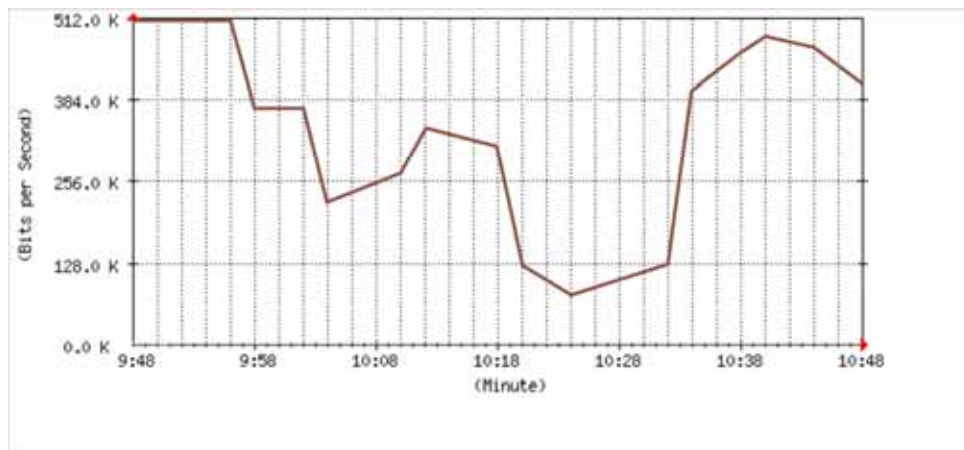
By configuring the QoS, you can control the OutBound and InBound Upstream/Downstream Bandwidth. The administrator can configure the bandwidth according to the WAN bandwidth.

**Downstream Bandwidth** : Configure the Guaranteed Bandwidth and Maximum Bandwidth.

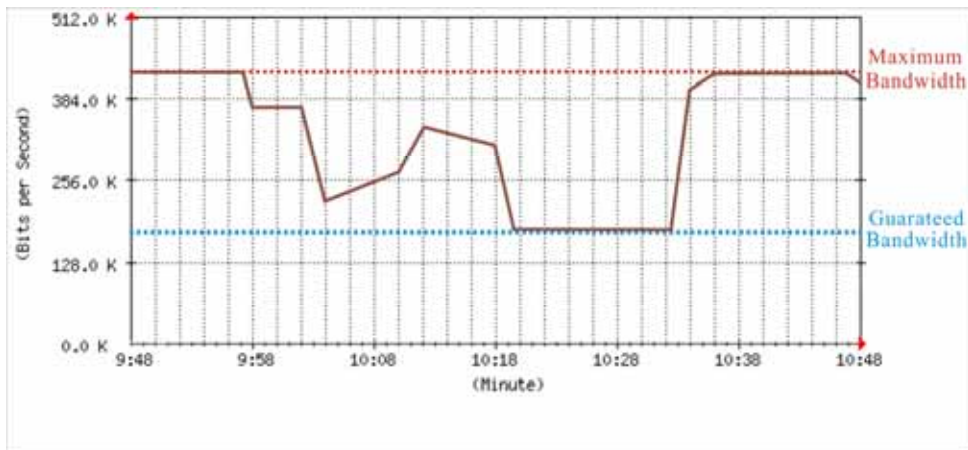
**Upstream Bandwidth** : Configure the Guaranteed Bandwidth and Maximum Bandwidth.

**QoS Priority** : Configure the priority of distributing Upstream/Downstream and unused bandwidth.

The BM-525 configures the bandwidth by different QoS, and selects the suitable QoS through Policy to control and efficiently distribute bandwidth. The BM-525 also makes it convenient for the administrator to make the Bandwidth to reach the best utility.



**The Flow Before Using QoS Function**



**The Flow After Using QoS (Max. Bandwidth: 400Kbps, Guaranteed Bandwidth: 200Kbps)**

## Define the required fields of QoS

### Downstream Bandwidth:

- To configure the Guaranteed Bandwidth and Maximum Bandwidth according to the bandwidth range you apply from ISP

### Upstream Bandwidth:

- To configure the Guaranteed Bandwidth and Maximum Bandwidth according to the bandwidth range you apply from ISP

### Priority:

- To configure the priority of distributing Upstream/Downstream and unused bandwidth.

### G. Bandwidth (Guaranteed Bandwidth):

- The basic bandwidth of QoS. The connection that uses the IPsec Auto key of VPN or Policy will preserve the basic bandwidth.

### M. Bandwidth (Maximum Bandwidth):

- The maximum bandwidth of QoS. The connection that uses the IPsec Auto key of VPN or Policy, which bandwidth will not exceed the amount you set.



We set up two QoS examples in this section:

No	Suitable Situation	Example
Ex1	<b>QoS</b>	Setting a policy that can restrict the user's downstream and upstream bandwidth.

## 4.8 Example

### Setting a policy that can restrict the user's downstream and upstream bandwidth

**STEP 1** . Enter the following settings in **QoS**:

- Click **New Entry**
- **Name:** The name of the QoS you want to configure.
- Enter the bandwidth in **G. Bandwidth, M. Bandwidth**
- Select **QoS Priority**
- Click **OK**

Downstream Bandwidth			Upstream Bandwidth			QoS Priority
G.Bandwidth =	<input type="text" value="200"/>	Kbps ( Range: 1 - 10000 )	G.Bandwidth =	<input type="text" value="200"/>	Kbps ( Range: 1 - 10000 )	Middle
M.Bandwidth =	<input type="text" value="400"/>	Kbps ( Range: 200 - 10000 )	M.Bandwidth =	<input type="text" value="400"/>	Kbps ( Range: 200 - 10000 )	

#### QoS Web UI Setting

Name	Downstream Bandwidth	Upstream Bandwidth	Priority	Configure
Policy_QoS	G.Bandwidth = 200 Kbps M.Bandwidth = 400 Kbps	G.Bandwidth = 200 Kbps M.Bandwidth = 400 Kbps	Middle	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

#### Complete the QoS Setting

**STEP 2 . Use the QoS that set by STEP1 in **Outgoing Policy**.**

Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
QoS	Policy_QoS ▾

**Setting the QoS in Policy**

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 ▾
<input type="button" value="New Entry"/>						

**Complete Policy Setting**



When the administrator are setting QoS, the bandwidth range can be set the value that system administrator sets in the **WAN** of **Interface**. So when the System Administrator sets the downstream and upstream bandwidth in **WAN** of **Interface**, he/she must set up precisely.

## 4.9 Authentication

By configuring the Authentication, you can control the user's connection authority. The user has to pass the authentication to access to Internet.

The BM-525 configures the authentication of LAN's user by setting account and password to identify the privilege.

## Define the required fields of Authentication

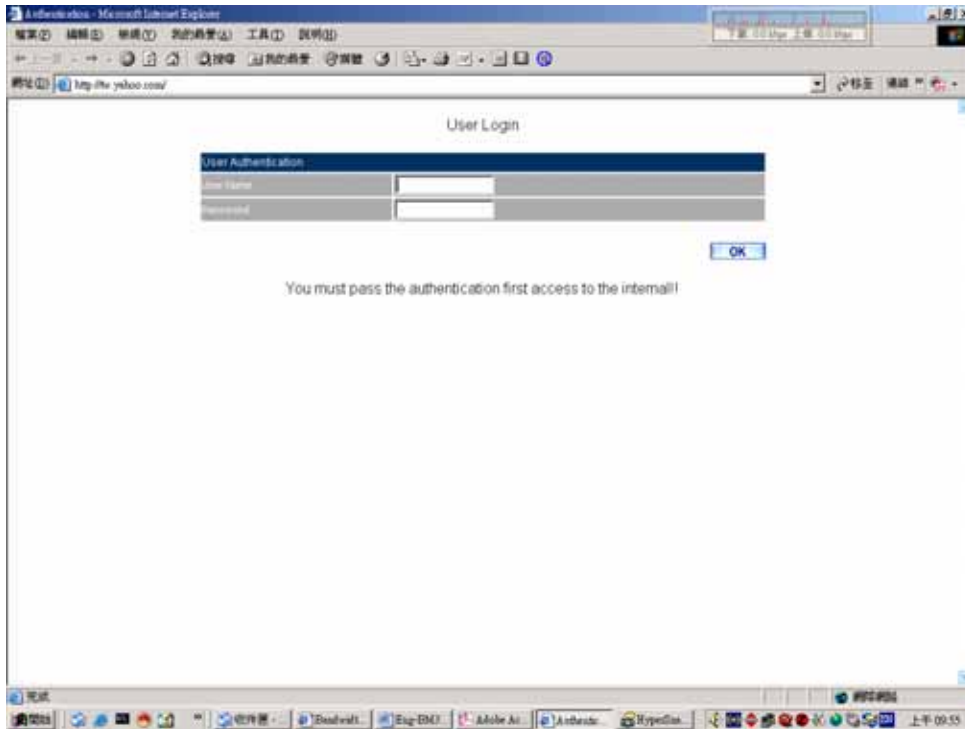
### Authentication Management

- Provide the Administrator the port number and valid time to setup BM-525 authentication. (Have to setup the Authentication first)
  - ◆ **Authentication Port:** The internal user has to pass the authentication to access to the Internet when enable BM-525.
  - ◆ **Re-Login if Idle:** When the internal user access to Internet, can setup the idle time after passing authentication. If idle time exceeds the time you setup, the authentication will be invalid. The default value is 30 minutes.
  - ◆ **URL to redirect when authentication succeeds:** The user who had passes Authentication has to connect to the specific web site. (It will connect to the web site directly which the user want to login) The default value is blank.
  - ◆ **Messages to display when user login:** It will display the login message in the authentication Web UI. (Support HTML) The default value is blank (display no message in authentication Web UI)
    - Add the following setting in this function:

The screenshot shows the 'Authentication Management' configuration page. It features several input fields and a text area. The 'Authentication Port' is set to 82. 'Re-Login if Idle' is set to 30 minutes. 'Re-Login after user login successfully' is set to 0 hours. There is an unchecked checkbox for 'Disallow Re-Login if the auth user has login'. The 'URL to redirect when authentication succeed' is set to 'tw.yahoo.com'. The 'Messages to display when user login' text area contains the message: 'You must pass the authentication first access to the internal!!'. At the bottom right, there are 'OK' and 'Cancel' buttons.

### Authentication Setting Web UI

- When the user connects to external network by Authentication, the following page will be displayed.



**Authentication Login Web UI**

- It will connect to the appointed website after passing Authentication.



### Connecting to the Appointed Website After Authentication



If the users ask for authentication positively, they can enter the LAN IP by the Authentication port number. And then the Authentication Web UI will be displayed.

**Auth-User Name:**

- The user account for Authentication you want to set.

**Password:**

- The password when setting up Authentication.

**Confirm Password:**

- Enter the password that correspond to Password



We set up four Authentication examples in this section:

No	Suitable Situation	Example
Ex1	<b>Auth User</b> <b>Auth Group</b>	Setting specific users to connect with external network, only those pass the authentication of policy. ( Adopt the built-in Auth User and Auth Group Function )

## 4.10 Example

**Setting specific users to connect with external network, only those pass the authentication of policy.**

**( Adopt the built-in Auth User and Auth Group Function )**

**STEP 1 . Setup several Auth User in Authentication.**

Authentication-User Name	Configure
Rayearth	<a href="#">Modify</a> <a href="#">Remove</a>
josh	<a href="#">Modify</a> <a href="#">Remove</a>
SlhSam	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

**Setting Several Auth Users Web UI**



To use Authentication, the DNS Server of the user's network card must be the same as the LAN Interface Address of BM-525.

**STEP 2 . Add Auth User Group Setting in Authentication function and enter the following settings:**

- Click **New Entry**
- **Name:** Enter laboratory
- Select the Auth User you want and **Add** to Selected Auth User
- Click **OK**
- Complete the setting of Auth User Group

The screenshot shows a web interface titled "New Authentication Group". At the top, there is a "Name:" label followed by a text input field containing "laboratory" and a note "(Max. 16 characters)". Below this, there are two columns of user selection. The left column is titled "< --- Available Authentication User --->" and contains a list of users: "Rayearth", "josh", and "SinSam". The right column is titled "< --- Selected Authentication User --->" and also contains a list of users: "Rayearth", "josh", and "SinSam". Between these two columns are two buttons: "Remove" (with a left-pointing arrow) and "Add" (with a right-pointing arrow). At the bottom right of the interface are "OK" and "Cancel" buttons.

**Setting Auth Group Web UI**

**STEP 3 .** Add a policy in **Outgoing Policy** and input the Address and Authentication of STEP 2.

Comment :	<input type="text" value=""/>	(Max. 32 characters)
<b>Modify Policy</b>		
Source Address	Inside_Any ▾	
Destination Address	Outside_Any ▾	
Service	ANY ▾	
Schedule	None ▾	
Authentication User	laboratory ▾	
Action	PERMIT ▾	
Traffic Log	<input type="checkbox"/> Enable	
Statistics	<input type="checkbox"/> Enable	
Content Blocking	<input type="checkbox"/> Enable	
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )	
QoS	None ▾	
		<input type="button" value="OK"/> <input type="button" value="Cancel"/>

**Auth-User Policy Setting**

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	✓	⚠	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 ▾
<input type="button" value="New Entry"/>						

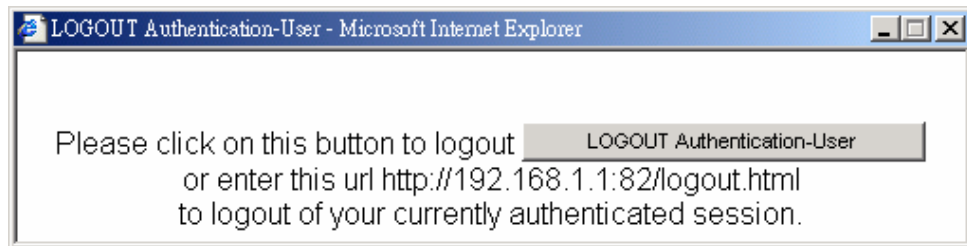
**Complete the Policy Setting of Auth-User**

**STEP 4 .** When user is going to access to Internet through browser, the authentication UI will appear in Browser. After entering the correct user name and password, click **OK** to access to Internet.

**STEP 5.** If the user does not need to access to Internet anymore and is going to logout, he/she can click **LOGOUT Auth-User** to logout the system. Or enter the Logout Authentication Web UI ([http:// LAN Interface: Authentication port number/ logout.html](http://LAN Interface: Authentication port number/logout.html)) to logout.

The image shows a web form titled "User Login". It has a dark blue header bar with the text "User Authentication". Below the header, there are two input fields: "User Name" and "Password". To the right of the "Password" field is a blue button labeled "OK".

**Access to Internet through Authentication Web UI**



**Logout Auth-User Web UI**

## 4.11 Content Blocking

Content Filtering includes 「URL」, 「Script」, 「P2P」, 「IM」, 「Download」, 「Upload」.

**【URL Blocking】**: The administrator can set up to “Allow” or “Restrict” entering the specific website by complete domain name, key words, and met character (~ and \*).

**【Script Blocking】**: The access authority of Popup, ActiveX, Java, and Cookies

**【P2P Blocking】**: The authority of sending files by eDonkey, eMule, Bit Torrent, WinMX, and Foxy.

**【IM Blocking】**: To restrict the authority of receiving video, file and message from MSN Messenger, Yahoo Messenger, ICQ, QQ, and Skype.

**【Download Blocking】**: To restrict the authority of download specific sub-name file, audio, and some common video by http protocol directly.

**【Upload Blocking】**: To restrict the authority of upload specific sub-name file.

## Define the required fields of Content Blocking

### URL String:

- The domain name that restricts to enter or only allow entering.

### Popup Blocking:

- Prevent the pop-up Web UI appearing

### ActiveX Blocking:

- Prevent ActiveX packets

### Java Blocking:

- Prevent Java packets

### Cookies Blocking:

- Prevent Cookies packets

### eDonkey Blocking:

- Prevent users to deliver files by eDonkey and eMule

### BitTorrent Blocking:

- Prevent users to deliver files by BitTorrent

### WinMX Blocking:

- Prevent users to deliver files by WinMX

### Foxy Blocking:

- Prevent users to deliver files by Foxy

**IM Blocking:**

- Prevent users to login MSN Messenger, Yahoo Messenger, ICQ, QQ, and Skype

**Audio and Video Types:**

- Prevent users to transfer sounds and video file by http

**Sub-name file Blocking:**

- Prevent users to deliver specific sub-name file by http

**All Type:**

- Prevent users to send the Audio, Video types, and sub-name file...etc. by http protocol.



We set up five Content Blocking examples in this section:

No	Suitable Situation	Example
Ex1	<b>URL Blocking</b>	Restrict the Internal Users only can access to some specific Website
Ex2	<b>Script Blocking</b>	Restrict the Internal Users to access to Script file of Website.
Ex3	<b>P2P Blocking</b>	Restrict the Internal Users to access to the file on Internet by P2P.
Ex4	<b>IM Blocking</b>	Restrict the Internal Users to send message, files, video and audio by Instant Messaging.
Ex5	<b>Download Blocking</b>	Restrict the Internal Users to access to video, audio, and some specific sub-name file from http or ftp protocol directly.

## 4.12 URL

### Restrict the Internal Users only can access to some specific Web site

#### URL Blocking:

Symbol: ~ means open up; \* means meta character

Restrict not to enter specific website: Enter the 「complete domain name」 or 「key word」 of the website you want to restrict in **URL String**. For example: www.kcg.gov.tw or gov.

Only open specific website to enter:

1. Add the web site you want to open up in URL String. While adding, you must enter the symbol “~” in front of the 「complete domain name」 or 「key word」 that represents to open these website to enter”. For example: ~www.kcg.gov.tw or ~gov.
2. After setting up the web site you want to open up, enter an order to “forbid all” in the last URL String; means only enter \* in URL String.



**Warning!** The order to forbid all must be placed at last forever. If you want to open a new web site, you must delete the order of forbidding all and then enter the new domain name. At last, re-enter the “forbid all” order again.

**STEP 1** . Enter the following in **URL** of **Content Filtering** function:

- Click **New Entry**
- **URL String:** Enter ~yahoo, and click **OK**
- Click **New Entry**
- **URL String:** Enter ~google, and click **OK**
- Click **New Entry**
- **URL String:** Enter \*, and click **OK**
- Complete setting a URL Blocking policy

URL String	Configure
~yahoo	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
~google	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
*	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
<input type="button" value="New Entry"/>	

**Content Filtering Table**

**STEP 2 . Add an **Outgoing Policy** and use in **Content Blocking** function.**

Comment :	<input type="text" value=""/> (Max. 32 characters)
<b>Modify Policy</b>	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Action	PERMIT
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input checked="" type="checkbox"/> Enable
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
QoS	None
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

### URL Blocking Policy Setting

**STEP 3 . Complete the policy of permitting the internal users only can access to some specific web site in **Outgoing Policy** function.**

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	✓	⊘	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1
<input type="button" value="New Entry"/>						

### Complete Policy Settings



Afterwards the users only can browse the web sites that include “yahoo” and “google” in domain name by the above policy.

## 4.13 Script

### Restrict the Internal Users to access to Script file of Website

**STEP 1** . Select the following data in **Script** of **Content Blocking** function:

- Select **Popup** Blocking
- Select **ActiveX** Blocking
- Select **Java** Blocking
- Select **Cookies** Blocking
- Click **OK**
- Complete the setting of Script Blocking



**Script Blocking Web UI**

**STEP 2 .** Add a new **Outgoing Policy** and use in **Content Blocking** function.

Comment :	<input type="text" value=""/> (Max. 32 characters)
<b>Modify Policy</b>	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Action	PERMIT
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input checked="" type="checkbox"/> Enable
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
QoS	None
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

### New Policy of Script Blocking Setting

**STEP 3 .** Complete the policy of restricting the internal users to access to Script file of Website in **Outgoing Policy**.

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	✔	⊘	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1
<input type="button" value="New Entry"/>						

### Complete Script Blocking Policy Setting



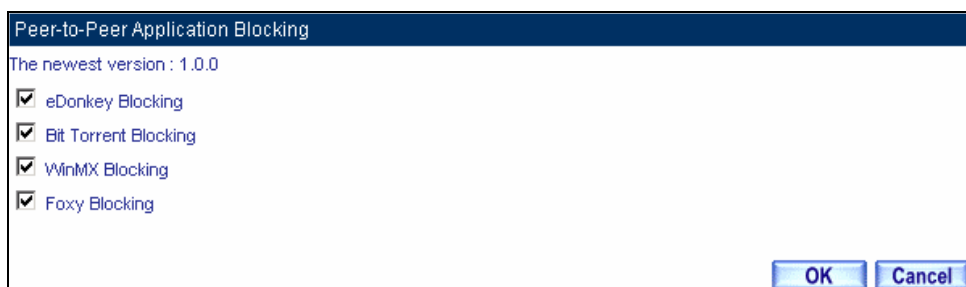
The users may not use the specific function (like JAVA, cookie...etc.) to browse the website through this policy. It can forbid the user browsing stock exchange website...etc.

## 4.14 P2P

### Restrict the Internal Users to access to the file on Internet by P2P

**STEP 1** . Select the following data in **P2P** of **Content Blocking** function:

- Select **eDonkey Blocking**
- Select **BitTorrent Blocking**
- Select **WinMX Blocking**
- Click **OK**
- Complete the setting of P2P Blocking



**P2P Blocking Web UI**

**STEP 2 .** Add a new **Outgoing Policy** and use in **Content Blocking** function.

Comment :	<input type="text" value=""/> (Max. 32 characters)
<b>Modify Policy</b>	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Action	PERMIT
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input checked="" type="checkbox"/> Enable
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
QoS	None
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

**Add New Policy of P2P Blocking**

**STEP 3 .** Complete the policy of restricting the internal users to access to the file on Internet by P2P in **Outgoing Policy**.

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	✓	⊘	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1
<input type="button" value="New Entry"/>						

**Complete P2P Blocking Policy Setting**



P2P Transfer will occupy large bandwidth so that it may influence other users. And P2P Transfer can change the service port free so it is invalid to restrict P2P Transfer by **Service**. Therefore, the system manager must use **P2P Blocking** in **Content Blocking** to restrict users to use P2P Transfer efficiently.



## 4.15 IM

### Restrict the Internal Users to send message, files, video and audio by Instant Messaging

**STEP 1** . Enter as following in **IM Blocking** of **Content Blocking** function:

- Select **MSN Messenger, Yahoo Messenger, ICQ Messenger, QQ Messenger, and Skype.**
- Click **OK**
- Complete the setting of IM Blocking.



**IM Blocking Web UI**

**STEP 2 .** Add a new **Outgoing Policy** and use in **Content Blocking** function.

Comment :	<input type="text" value=""/> (Max. 32 characters)
<b>Modify Policy</b>	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Action	PERMIT
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input checked="" type="checkbox"/> Enable
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
QoS	None
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

**Add New Policy of IM Blocking**

**STEP 3 .** Complete the policy of restricting the internal users to send message, files, audio, and video by instant messaging in **Outgoing Policy**.

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	✔	⊘	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1
<input type="button" value="New Entry"/>						

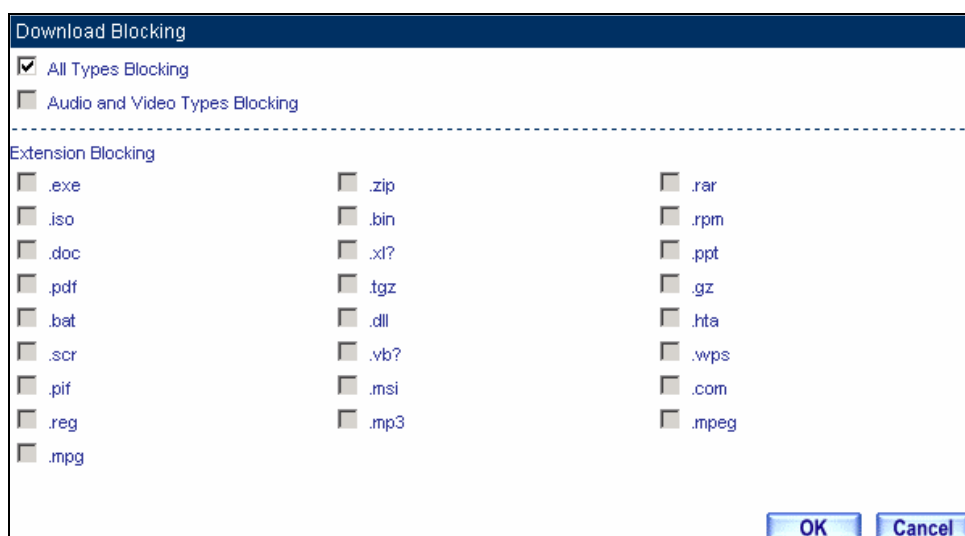
**Complete IM Blocking Policy Setting**

## 4.16 Download

**Restrict the Internal Users to access to video, audio, and some specific sub-name file from http or ftp protocol directly**

**STEP 1** . Enter the following settings in **Download** of **Content Blocking** function:

- Select **All Types Blocking**
- Click **OK**
- Complete the setting of Download Blocking.



**Download Blocking Web UI**

**STEP 2 .** Add a new **Outgoing Policy** and use in **Content Blocking** function.

Comment :	<input type="text" value=""/> (Max. 32 characters)
<b>Modify Policy</b>	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Action	PERMIT
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input checked="" type="checkbox"/> Enable
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
QoS	None
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

**Add New Download Blocking Policy Setting**

**STEP 3 .** Complete the **Outgoing Policy** of restricting the internal users to access to video, audio, and some specific sub-name file by http protocol directly.

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	✓	⊘	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1
<input type="button" value="New Entry"/>						

**Complete Download Blocking Policy Setting**

## 4.17 Virtual Server

The real IP address provided from ISP is always not enough for all the users when the system manager applies the network connection from ISP. Generally speaking, in order to allocate enough IP addresses for all computers, an enterprise assigns each computer a private IP address, and converts it into a real IP address through BM-525's NAT (Network Address Translation) function. If a server that provides service to WAN network is located in LAN networks, external users cannot directly connect to the server by using the server's private IP address.

The BM-525's Virtual Server function can solve this problem. A Virtual Server has set the real IP address of the BM-525's WAN network interface to be the Virtual Server IP. Through the Virtual Server function, the BM-525 translates the Virtual Server's IP address into the private IP address in the LAN network.

Virtual Server owns another feature know as one-to-many mapping. This is when one real server IP address on the WAN interface can be mapped into four LAN network servers provide the same service private IP addresses. This option is useful for Load Balancing, which causes the Virtual Server to distribute data packets to each private IP addresses (which are the real servers) by session. Therefore, it can reduce the loading of a single server and lower the crash risk. And can improve the work efficiency.

In this section, we will have detailed introduction and instruction of **Mapped IP** and **Server 1/2/3/4**:

**Mapped IP:** Because the Intranet is transferring the private IP by NAT Mode (Network Address Translation). And if the server is in LAN, its IP Address is belonging to Private IP Address. Then the external users cannot connect to its private IP Address directly. The user must connect to the BM-525's WAN subnet's Real IP and then map Real IP to Private IP of LAN by the BM-525. It is a one-to-one mapping. That is, to map all the service of one WAN Real IP Address to one LAN Private IP Address.

**Server 1/2/3/4:** Its function resembles Mapped IP's. But the Virtual Server maps one to many. That is, to map a Real IP Address to 1~4 LAN Private IP Address and provide the service item in Service.

## **Define the required fields of Virtual Server**

### **WAN IP :**

- WAN IP Address (Real IP Address)

### **Map to Virtual IP :**

- Map the WAN Real IP Address into the LAN Private IP Address

### **Virtual Server Real IP :**

- The WAN IP address which mapped by the Virtual Server.

### **Service name (Port Number) :**

- The service name that provided by the Virtual Server.

### **External Service Port :**

- The WAN Service Port that provided by the virtual server. If the service you choose only have one port and then you can change the port number here. (If change the port number to 8080 and then when the external users going to browse the Website; he/she must change the port number first to enter the Website.)

### **Server Virtual IP :**

- The virtual IP which mapped by the Virtual Server.

We set up four Virtual Server examples in this section:

No.	Suitable Situation	Example
Ex1	<b>Mapped IP</b>	Make a single server that provides several services such as FTP, Web, and Mail, to provide service by policy.
Ex2	<b>Virtual Server</b>	Make several servers that provide a single service, to provide service through policy by Virtual Server. (Take Web service for example)
Ex3	<b>Virtual Server</b>	The external user use VoIP to connect with VoIP of LAN. (VoIP Port: TCP 1720, TCP 153210-15333, UDP 153210-15333)
Ex4	<b>Virtual Server</b>	Make several servers that provide several same services, to provide service through policy by Virtual Server. (Take HTTP, POP3, SMTP, and DNS Group for example)

### **Preparation**

Apply for two ADSL that have static IP  
(WAN static IP is 61.11.11.10~ 61.11.11.14)



## 4.18 Example

**Make a single server that provides several services such as FTP, Web, and Mail, to provide service by policy**

**STEP 1** . Setting a server that provide several services in LAN, and set up the network card's IP as 192.168.1.100. DNS is External DNS Server.

**STEP 2** . Enter the following setting in **LAN** of **Address** function.

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		In Use
Main_Server	192.168.1.100/255.255.255.255	00:01:7A:41:55:FB	Modify Remove

[New Entry](#)

### Mapped IP Settings of Server in Address

**STEP 3** . Enter the following data in **Mapped IP** of **Virtual Server** function:

- Click **New Entry**
- **WAN IP:** Enter 61.11.11.12 (click **Assist** for assistance)
- **Map to Virtual IP:** Enter 192.168.1.100
- Click **OK**
- Complete the setting of adding new mapped IP

Add New Mapped IP	
WAN IP	61.11.11.12 <a href="#">Assist</a>
Map To Virtual IP	192.168.1.100

[OK](#) [Cancel](#)

### Mapped IP Setting Web UI

**STEP 4 .** Group the services (DNS, FTP, HTTP, POP3, SMTP...) that provided and used by server in **Service** function. And add a new service group for server to send mails at the same time.

Group name	Service	Configure
Main_Service	DNS,HTTP,POP3...	<a href="#">Modify</a> <a href="#">Remove</a>
<a href="#">New Entry</a>		

### Service Setting

**STEP 5 .** Add a policy that includes settings of STEP3, 4 in **Incoming Policy**.

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Mapped IP(61.11.11.12)	ANY	✓		<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>	To 1 ▾
<a href="#">New Entry</a>						

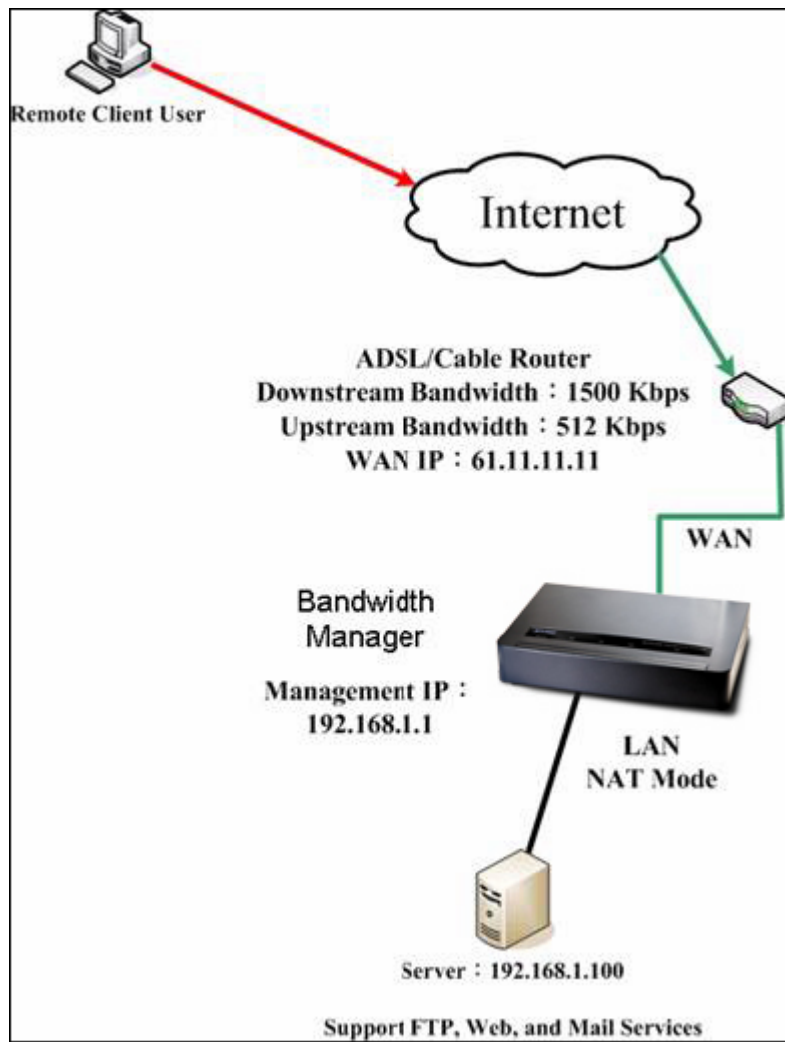
### Complete the Incoming Policy

**STEP 6 .** Add a policy that includes STEP2, 4 in **Outgoing Policy**. It makes the server to send e-mail to external mail server by mail service.

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	Main_Service	✓		<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>	To 1 ▾
<a href="#">New Entry</a>						

### Complete the Outgoing Policy

**STEP 7** . Complete the setting of providing several services by mapped IP.



### A Single Server that Provides Several Services by Mapped IP



Strong suggests **not** to choose **ANY** when setting Mapped IP and choosing service. Otherwise the Mapped IP will be exposed to Internet easily and may be attacked by Hacker.

**Make several servers that provide a single service, to provide service through policy by Virtual Server (Take Web service for example)**

**STEP 1** . Setting several servers that provide Web service in LAN network, which IP Address is 192.168.1.101, 192.168.1.102, 192.168.1.103, and 192.168.1.104

**STEP 2 .** Enter the following data in **Server 1** of **Virtual Server** function:

- Click the button next to **Virtual Server Real IP** (“**click here to configure**”) in **Server 1**
- **Virtual Server Real IP:** Enter 61.11.11.12 (click **Assist** for assistance)
- Click **OK**

### Virtual Server Real IP Setting

- Click **New Entry**
- **Service:** Select HTTP (80)
- **External Service Port:** Change to 8080
- **Load Balance Server1:** Enter 192.168.1.101
- **Load Balance Server2:** Enter 192.168.1.102
- **Load Balance Server3:** Enter 192.168.1.103
- **Load Balance Server4:** Enter 192.168.1.104
- Click **OK**
- Complete the setting of Virtual Server

Load Balance Server	Server Virtual IP
1	192.168.1.101
2	192.168.1.102
3	192.168.1.103
4	192.168.1.104

### Virtual Server Configuration Web UI

**STEP 3.** Add a new policy in **Incoming Policy**, which includes the virtual server, set by STEP2.

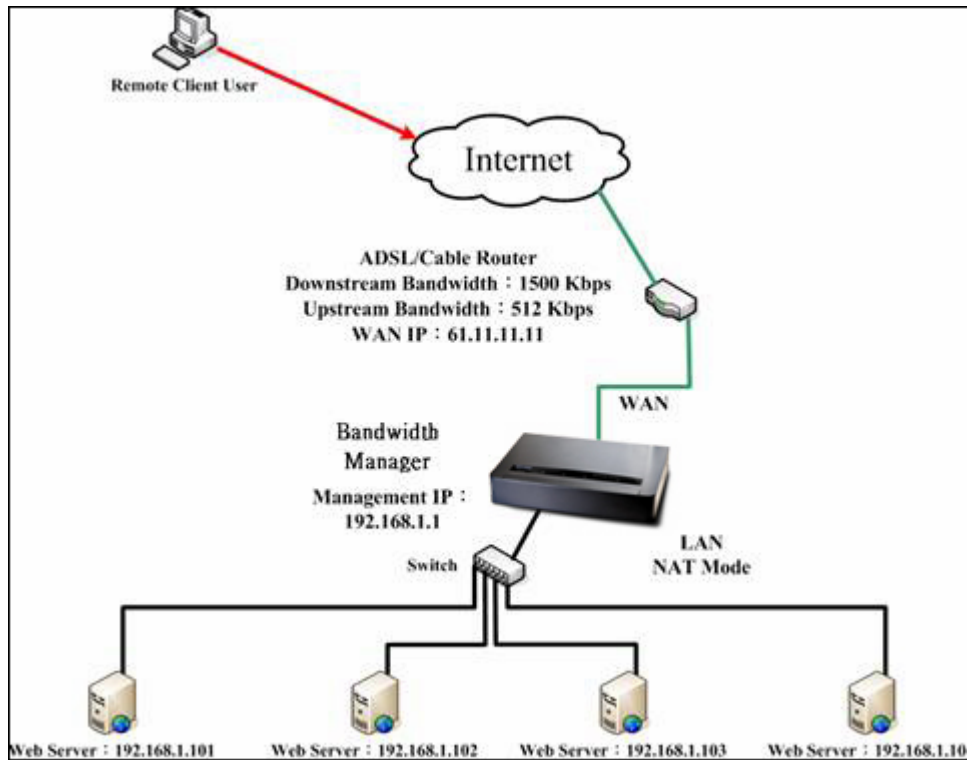
Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1(61.11.11.12)	HTTP(8080)	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 ▾
<input type="button" value="New Entry"/>						

### Complete Virtual Server Policy Setting



In this example, the external users must change its port number to 8080 before entering the Website that set by the Web server.

**STEP 4 .** Complete the setting of providing a single service by virtual server.



### Several Servers Provide a Single Service by Virtual Server

**The external user use VoIP to connect with VoIP of LAN (VoIP Port: TCP 1720, TCP 153210-15333, UDP 153210-15333)**

**STEP 1** . Set up VoIP in LAN network, and its IP is 192.168.1.100

**STEP 2** . Enter the following setting in **LAN** of **Address** function.

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		In Use
VoIP	192.168.1.100/255.255.255.255		Modify Remove

[New Entry](#)

**Setting LAN Address Web UI**

**STEP 3** . Add new VoIP service group in **Custom** of **Service** function.

Service name	Protocol	Client Port	Server Port	Configure
VoIP_Service	TCP	0:65535	1720:1720	Modify Remove

[New Entry](#)

**Add Custom Service**

**STEP 4 .** Enter the following setting in **Server1** of **Virtual Server** function:

- Click the button next to **Virtual Server Real IP** (“**click here to configure**”) in **Server1**
- **Virtual Server Real IP:** Enter 61.11.11.12 (click **Assist** for assistance) (Use WAN)
- Click **OK**

**Virtual Server Real IP Setting Web UI**

- Click **New Entry**
- **Service:** Select (Custom Service) VoIP\_Service
- **External Service Port:** From-Service (Custom)
- **Load Balance Server1:** Enter 192.168.1.100
- Click **OK**
- Complete the setting of Virtual Server

Load Balance Server	Server Virtual IP
1	192.168.1.100
2	
3	
4	

**Virtual Server Configuration Web UI**



When the custom service only has one port number, then the external network port of **Virtual Server** is changeable. On the contrary, if the custom service has more than one port network number, then the external network port of **Virtual Server** cannot be changed.



**STEP 5 .** Add a new **Incoming Policy**, which includes the virtual server that set by STEP4.

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1(61.11.11.12)	VoIP_Service	✓		<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>	To 1 ▾
<a href="#">New Entry</a>						

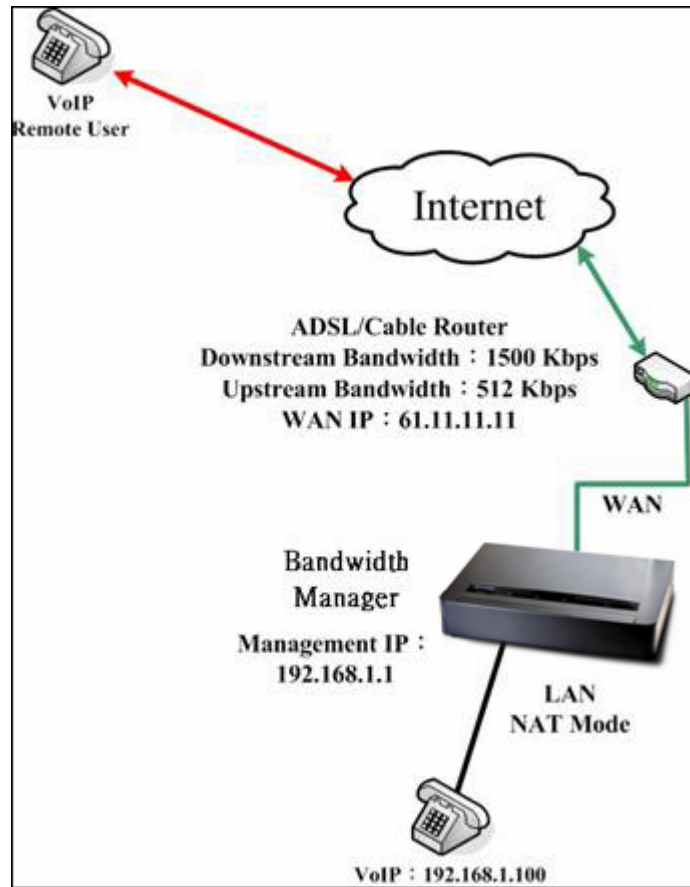
**Complete the Policy includes Virtual Server Setting**

**STEP 6 .** Enter the following setting of the internal users using VoIP to connect with external network VoIP in **Outgoing Policy**.

Source	Destination	Service	Action	Option	Configure	Move
VoIP	Outside_Any	VoIP_Service	✓		<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>	To 1 ▾
<a href="#">New Entry</a>						

**Complete the Policy Setting of VoIP Connection**

**STEP 7 .** Complete the setting of the external/internal user using specific service to communicate with each other by Virtual Server.



**Complete the Setting of the External/Internal User using specific service to communicate with each other by Virtual Server**

**Make several servers that provide several same services, to provide service through policy by Virtual Server. (Take HTTP, POP3, SMTP, and DNS Group for example)**

**STEP 1 .** Setting several servers that provide several services in LAN network. Its network card's IP is 192.168.1.101, 192.168.1.102, 192.168.1.103, 192.168.1.104 and the DNS setting is External DNS server.

**STEP 2 .** Enter the following in **LAN** and **LAN Group** of **Address** function.

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		In Use
Server_01	192.168.1.101/255.255.255.255		Modify Remove
Server_02	192.168.1.102/255.255.255.255		Modify Remove
Server_03	192.168.1.103/255.255.255.255		Modify Remove
Server_04	192.168.1.104/255.255.255.255		Modify Remove

[New Entry](#)

**Mapped IP Setting of Virtual Server in Address**

Name	Member	Configure
Sever_Group	Server_01, Server_02, Server_03...	Modify Remove Pause

[New Entry](#)

**Group Setting of Virtual Server in Address**

**STEP 3 .** Group the service of server in **Custom** of **Service**. Add a Service Group for server to send e-mail at the same time.

Group name	Service	Configure
Main_Service	DNS,HTTP,POP3...	Modify Remove

[New Entry](#)

**Add New Service Group**

**STEP 4 .** Enter the following data in **Server1** of **Virtual Server**:

- Click the button next to **Virtual Server Real IP** (“**click here to configure**”) in **Server1**
- **Virtual Server Real IP:** Enter 61.11.11.12 (click **Assist** for assistance)
- Click **OK**

**Virtual Server Real IP Setting**

- Click **New Entry**
- **Service:** Select (Group Service) Main\_Service
- **External Service Port:** From-Service (Group)
- Enter the server IP in Load Balance Server
- Click **OK**
- Complete the setting of Virtual Server

Load Balance Server	Server Virtual IP
1	192.168.1.101
2	192.168.1.102
3	192.168.1.103
4	192.168.1.104

**Virtual Server Configuration Web UI**

**STEP 5 .** Add a new **Incoming Policy**, which includes the virtual server that set by STEP 3.

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1(61.11.11.12)	Main_Service	✓		<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>	To 1 ▾
<a href="#">New Entry</a>						

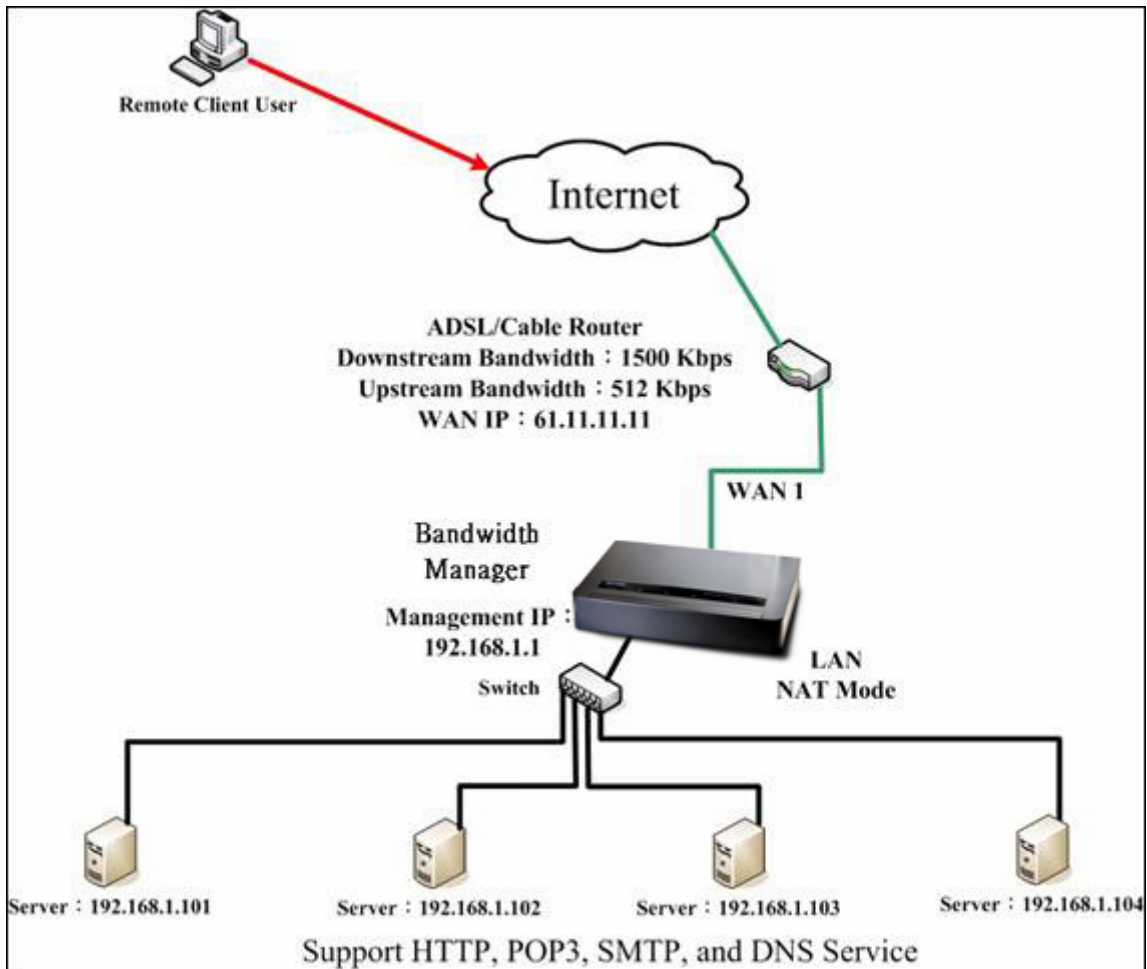
### Complete Incoming Policy Setting

**STEP 6 .** Add a new policy that includes the settings of STEP2, 3 in **Outgoing Policy**. It makes server can send e-mail to external mail server by mail service.

Source	Destination	Service	Action	Option	Configure	Move
Sever_Group	Outside_Any	Main_Service	✓		<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>	To 1 ▾
<a href="#">New Entry</a>						

### Complete Outgoing Policy Setting

**STEP 7 .** Complete the setting of providing several services by Virtual Server.



**Complete the Setting of Providing Several Services by Several Virtual Servers**

## Chapter 5 Policy

Every packet has to be detected if it corresponds with Policy or not when it passes the BM-525. When the conditions correspond with certain policy, it will pass the BM-525 by the setting of Policy without being detected by other policy. But if the packet cannot correspond with any Policy, the packet will be intercepted.

The parameter of the policy includes Source Address, Destination Address, Service, Action, WAN Port, Traffic Log, Statistics, Content Blocking, Anti-Virus, Authentication User, Schedule, Alarm Threshold, Trunk, Max. Concurrent Sessions, and QoS. Control policies decide whether packets from different network objects, network services, and applications are able to pass through the BM-525.



### How to use Policy?

The device uses policies to filter packets. The policy settings are: source address, destination address, services, permission, packet log, packet statistics, and flow alarm. Based on its source addresses, a packet can be categorized into:

- (1) **Outgoing:** The source IP is in LAN network; the destination is in WAN network. The system manager can set all the policy rules of Outgoing packets in this function
- (2) **Incoming:** The source IP is in WAN network; the destination is in LAN network. (For example: Mapped IP, Virtual Server) The system manager can set all the policy rules of Incoming packets in this function
- (3) **WAN to DMZ:** The source IP is in WAN network; the destination is in DMZ network. (For example: Mapped IP, Virtual Server) The system manager can set all the policy rules of WAN to DMZ packets in this function

- (4) **LAN to DMZ:** The source IP is in LAN network; the destination is in DMZ network. The system manager can set all the policy rules of LAN to DMZ packets in this function
- (5) **DMZ to LAN:** The source IP is in DMZ network; the destination is in LAN network. The system manager can set all the policy rules of DMZ to LAN packets in this function
- (6) **DMZ to WAN:** The source IP is in DMZ network; the destination is in WAN network. The system manager can set all the policy rules of DMZ to WAN packets in this function



All the packets that go through BM-525 must pass the policy permission (except VPN). Therefore, the LAN, WAN, and DMZ network have to set the applicable policy when establish network connection.



## 5.1 Policy

### Define the required fields of Policy

#### Source and Destination:



- Source IP and Destination IP is according to the BM-525's point of view. The active side is the source; passive side is destination.

#### Service:

- It is the service item that controlled by Policy. The user can choose default value or the custom services that the system manager set in **Service** function.







#### Action, WAN Port:

- Control actions to permit or reject packets that delivered between LAN network and WAN network when pass through BM-525 (See the chart and illustration below)

Chart	Name	Illustration
	Permit all WAN network Interface	Allow the packets that correspond with policy to be transferred by WAN Port
	DENY	Reject the packets that correspond with policy to be transferred by WAN Port

**Option:**

- To display if every function of Policy is enabled or not. If the function is enabled and then the chart of the function will appear (See the chart and illustration below)

Chart	Name	Illustration
	Traffic Log	Enable traffic log
	Statistics	Enable traffic statistics
	Authentication User	Enable Authentication User
	Schedule	Enable the policy to automatically execute the function in a certain time
	Content Blocking	Enable Content Blocking
	QoS	Enable QoS

**Traffic Log:**

- Record all the packets that go through policy.

**Statistics:**

- Chart of the traffic that go through policy

**Content Blocking:**

- To restrict the packets that passes through the policy

**Authentication-User:**

- The user have to pass the authentication to connect by Policy

**Schedule:**

- Setting the policy to automatically execute the function in a certain time

**MAX. Concurrent Sessions:**

- Set the concurrent sessions that permitted by policy. And if the sessions exceed the setting value, the surplus connection cannot be set successfully.

**QoS:**

- Setting the Guarantee Bandwidth and Maximum Bandwidth of the Policy (the bandwidth is shared by the users who correspond to the Policy)

**Move:**

- Every packet that passes the BM-525 is detected from the front policy to the last one. So it can modify the priority of the policy from the selection.

We set up six Policy examples in this section:

No.	Suitable Situation	Example
Ex1	<b>Outgoing</b>	Set up the policy that can monitor the internal users. (Take Logging, Statistics, Alarm Threshold for example)
Ex2	<b>Outgoing</b>	Forbid the users to access to specific network. (Take specific WAN IP and Content Blocking for example)
Ex3	<b>Outgoing</b>	Only allow the users who pass Authentication to access to Internet in particular time.
Ex4	<b>Incoming</b>	The external user control the internal PC through remote control software (Take PC-Anywhere for example)
Ex5	<b>WAN to DMZ</b>	Under DMZ NAT Mode, set a FTP Server and restrict the download bandwidth from external and MAX. Concurrent Sessions.
Ex6	<b>WAN to DMZ</b> <b>DMZ to WAN</b> <b>LAN to DMZ</b>	Set a Mail Server to allow the internal and external users to receive and send e-mail under DMZ Transparent Mode

## 5.2 Example

**Set up the policy that can monitor the internal users. (Take Logging, Statistics, and Alarm Threshold for example)**


**STEP 1** . Enter the following setting in **Outgoing Policy**:

- Click **New Entry**
- Select **Logging**
- Select **Statistics**
- Click **OK**

Comment :	<input type="text"/>	(Max. 32 characters)
<b>Modify Policy</b>		
Source Address	Inside_Any ▾	
Destination Address	Outside_Any ▾	
Service	ANY ▾	
Schedule	None ▾	
Authentication User	None ▾	
Action	PERMIT ▾	
Traffic Log	<input checked="" type="checkbox"/> Enable	
Statistics	<input checked="" type="checkbox"/> Enable	
Content Blocking	<input type="checkbox"/> Enable	
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )	
QoS	None ▾	
		<input type="button" value="OK"/> <input type="button" value="Cancel"/>

**Setting the different Policies**

**STEP 2 .** Complete the setting of Logging, Statistics, and Alarm Threshold in **Outgoing Policy**.

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	✓	 	Modify Remove Pause	To 1
<a href="#">New Entry</a>						

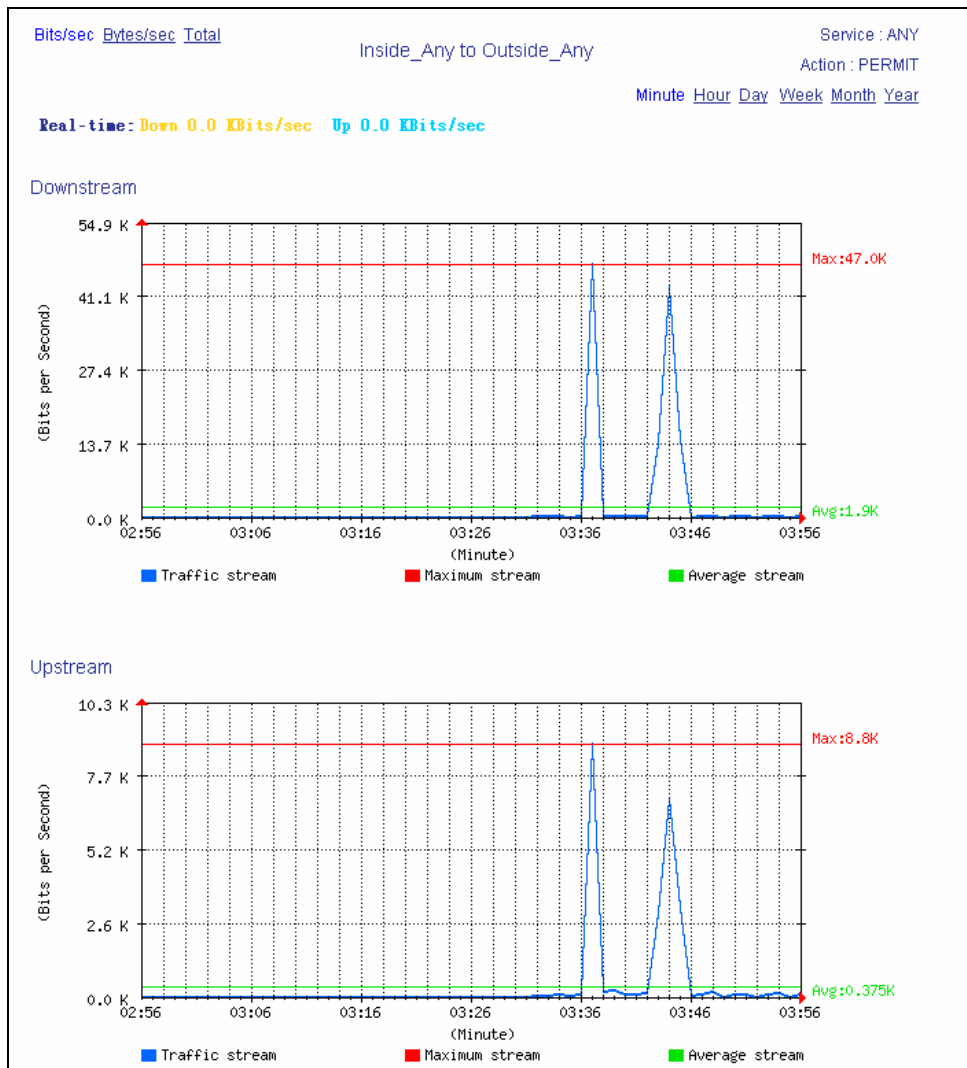
### Complete Policy Setting

**STEP 3 .** Obtain the information in **Traffic** of **Log** function if you want to monitor all the packets of the BM-525.

Aug 17 03:40:23 <span style="float: right;"><a href="#">Next</a></span>					
Time	Source	Destination	Protocol	Port	Disposition
Aug 17 03:40:23	192.168.1.2	192.168.1.1	TCP	1238 => 80	✓
Aug 17 03:40:23	192.168.1.2	192.168.1.1	TCP	1237 => 80	✓
Aug 17 03:40:23	192.168.1.2	192.168.1.1	TCP	1236 => 80	✓
Aug 17 03:40:23	192.168.1.2	192.168.1.1	TCP	1235 => 80	✓
Aug 17 03:40:22	192.168.1.2	192.168.1.1	TCP	1234 => 80	✓
Aug 17 03:40:20	192.168.1.2	172.19.1.106	TCP	1118 => 445	✓
Aug 17 03:40:20	172.19.1.106	192.168.1.2	TCP	445 => 1118	✓
Aug 17 03:40:03	70.30.212.120	192.168.1.2	UDP	41331 => 43145	✓
Aug 17 03:40:03	69.203.11.148	192.168.1.2	UDP	13009 => 43145	✓
Aug 17 03:40:02	192.168.1.2	69.203.11.148	UDP	43145 => 13009	✓
Aug 17 03:40:02	192.168.1.2	70.30.212.120	UDP	43145 => 41331	✓
Aug 17 03:40:02	70.225.176.190	192.168.1.2	UDP	45470 => 43145	✓
Aug 17 03:40:02	216.7.81.252	192.168.1.2	UDP	52595 => 43145	✓
Aug 17 03:40:02	192.168.1.2	216.7.81.252	UDP	43145 => 52595	✓
Aug 17 03:40:02	192.168.1.2	70.225.176.190	UDP	43145 => 45470	✓
Aug 17 03:40:00	192.168.1.2	12.207.211.87	TCP	4997 => 63536	✓
Aug 17 03:40:00	12.207.211.87	192.168.1.2	TCP	63536 => 4997	✓
Aug 17 03:39:59	192.168.1.2	12.207.211.87	TCP	4997 => 63536	✓
<a href="#">Clear Logs</a> <span style="margin-left: 100px;"><a href="#">Download Logs</a></span>					

### Traffic Log Monitor Web UI

**STEP 4 .** To display the traffic record that through Policy to access to Internet in **Policy Statistics** of **Statistics** function.



Statistics Web UI

**Forbid the users to access to specific network. (Take specific WAN IP and Content Blocking for example)**

**STEP 1 .** Enter the following setting in **URL Blocking**, **Script Blocking**, **P2P Blocking**, **IM Blocking**, and **Download Blocking** in **Content Blocking** function.

URL String	Configure
~yahoo	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
~google	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
*	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

**URL Blocking Setting**

**Script Blocking**

Popup Blocking                       ActiveX Blocking

Java Blocking                               Cookie Blocking

**Script Blocking Setting**

**Peer-to-Peer Application Blocking**

The newest version : 1.0.0

eDonkey Blocking

Bit Torrent Blocking

WinMX Blocking

Foxy Blocking

**P2P Blocking Setting**

**Instant Messaging Blocking**

The newest version : 1.0.0

MSN Messenger Blocking

Yahoo Messenger Blocking

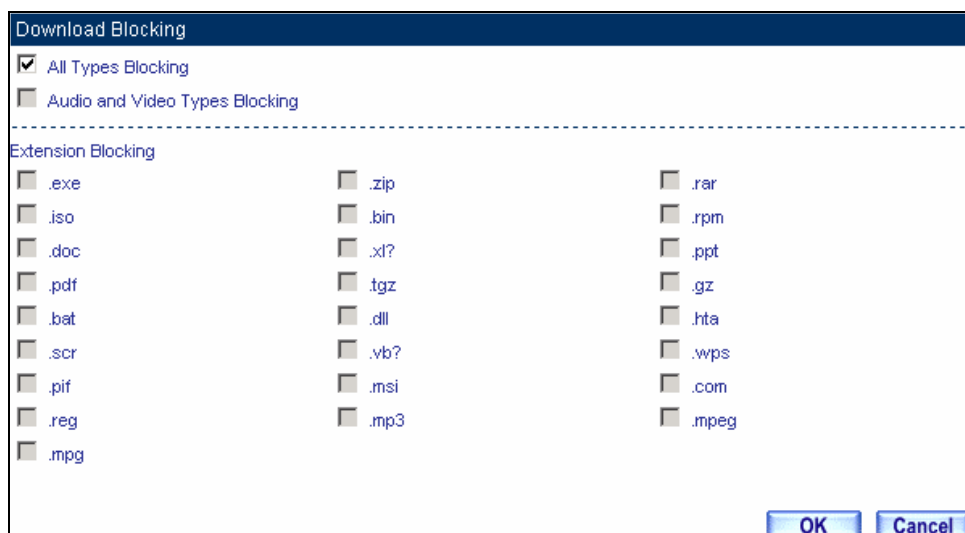
ICQ Messenger Blocking

QQ Messenger Blocking

Skype Messenger Blocking

**IM Blocking Setting**





### Download Blocking Setting



1. URL Blocking can restrict the Internal Users only can access to some specific Website.
2. Script Blocking can restrict the Internal Users to access to Script file of Website. (Java, Cookies...etc.)
3. P2P Blocking can restrict the Internal Users to access to the file on Internet by P2P. (eDonkey, BT)
4. IM Blocking can restrict the Internal Users to send message, files, audio, and video by instant messaging. (Ex: MSN Messenger, Yahoo Messenger, QQ, ICQ, and Skype)
5. Download Blocking can restrict the Internal Users to access to video, audio, and some specific sub-name file by http protocol directly.

**STEP 2 .** Enter as following in **WAN** and **WAN Group** of **Address** function.

Name	IP / Netmask	Configure
Outside_Any	0.0.0.0/0.0.0.0	<input type="button" value="In Use"/>
Remote_Server1	61.219.38.39/255.255.255.255	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
Remote_Server2	202.1.237.21/255.255.255.255	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
<input type="button" value="New Entry"/>		

**Setting the WAN IP that going to block**

Name	Member	Configure
WAN_Group	Remote_Server1, Remote_Server2	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>
<input type="button" value="New Entry"/>		

**WAN Address Group**



The Administrator can group the custom address in **Address**. It is more convenient when setting policy rule.

**STEP 3 .** Enter the following setting in **Outgoing Policy**:

- Click **New Entry**
- **Destination Address:** Select WAN\_Group that set by **STEP 2.** (Blocking by IP)
- **Action, WAN Port:** Select **DENY ALL**
- Click **OK**

Comment :	<input type="text" value=""/>	(Max. 32 characters)
<b>Modify Policy</b>		
Source Address	Inside_Any ▾	
Destination Address	WAN_Group ▾	
Service	ANY ▾	
Schedule	None ▾	
Authentication User	None ▾	
Action	DENY ALL ▾	
Traffic Log	<input type="checkbox"/> Enable	
Statistics	<input type="checkbox"/> Enable	
Content Blocking	<input type="checkbox"/> Enable	
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )	
QoS	None ▾	
		<input type="button" value="OK"/> <input type="button" value="Cancel"/>

**Setting Blocking Policy**

**STEP 4 .** Enter the following setting in **Outgoing Policy**:

- Click **New Entry**
- Select **Content Blocking**
- Click **OK**

Comment :	<input type="text" value=""/>	(Max. 32 characters)
<b>Add New Policy</b>		
Source Address	Inside_Any ▾	
Destination Address	Outside_Any ▾	
Service	ANY ▾	
Schedule	None ▾	
Authentication User	None ▾	
Action	PERMIT ▾	
Traffic Log	<input type="checkbox"/> Enable	
Statistics	<input type="checkbox"/> Enable	
Content Blocking	<input checked="" type="checkbox"/> Enable	
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )	
QoS	None ▾	
		<input type="button" value="OK"/> <input type="button" value="Cancel"/>

**Setting Content Blocking Policy**

**STEP 5 .** Complete the setting of forbidding the users to access to specific network.

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	WAN_Group	ANY	✘		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 ▾
Inside_Any	Outside_Any	ANY	✔	-	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 2 ▾
<input type="button" value="New Entry"/>						

**Complete Policy Setting**



**Deny** in Policy can block the packets that correspond to the policy rule. The System Administrator can put the policy rule in the front to prevent the user connecting with specific IP.

**Only allow the users who pass Authentication to access to Internet in particular time**

**STEP 1** . Enter the following in **Schedule** function.

Name	Configure
WorkingTime	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
<input type="button" value="New Entry"/>	

**Add New Schedule**

**STEP 2** . Enter the following in **Auth User** and **Auth User Group** in **Authentication** function.

Name	Member	Configure
laboratory	Rayearth, josh, SinSam	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>
<input type="button" value="New Entry"/>		

**Setting Auth User Group**



The Administrator can use group function the **Authentication** and **Service**. It is more convenient when setting policy.

**STEP 3 .** Enter the following setting in **Outgoing Policy**:

- Click **New Entry**
- **Authentication User:** Select laboratory
- **Schedule:** Select Working Time
- Click **OK**

Comment :	<input type="text" value=""/>	(Max. 32 characters)
<b>Add New Policy</b>		
Source Address	Inside_Any ▾	
Destination Address	Outside_Any ▾	
Service	ANY ▾	
Schedule	WorkingTime ▾	
Authentication User	laboratory ▾	
Action	PERMIT ▾	
Traffic Log	<input type="checkbox"/> Enable	
Statistics	<input type="checkbox"/> Enable	
Content Blocking	<input type="checkbox"/> Enable	
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )	
QoS	None ▾	
		<input type="button" value="OK"/> <input type="button" value="Cancel"/>

**Setting a Policy of Authentication and Schedule**

**STEP 4 .** Complete the policy rule of only allows the users who pass authentication to access to Internet in particular time.

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	✔	🔄 🗑️	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 ▾
<input type="button" value="New Entry"/>						

**Complete Policy Setting**

**The external user control the internal PC through remote control software (Take PC-Anywhere for example)**

**STEP 1** . Set up a Internal PC controlled by external user, and Internal PC's IP Address is 192.168.1.2

**STEP 2** . Enter the following setting in **Virtual Server1** of **Virtual Server** function.

Virtual Server Real IP		61.11.11.12	
Service	WAN Port	Server Virtual IP	Configure
PC-Anywhere (5631-5632)	5631-5632	192.168.1.2 192.168.1.104	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>
<input type="button" value="New Entry"/>			

**Setting Virtual Server**

**STEP 3 .** Enter the following in **Incoming Policy**:

- Click **New Entry**
- **Destination Address:** Select Virtual Server1 (61.11.11.12)
- **Service:** Select PC-Anywhere (5631-5632)
- Click **OK**

Comment :	<input type="text" value=""/>	(Max. 32 characters)
<b>Add New Policy</b>		
Source Address	Outside_Any	
Destination Address	Virtual Server 1(61.11.11.12)	
Service	PC-Anywhere(5631-5632)	
Schedule	None	
Action	PERMIT	
Traffic Log	<input type="checkbox"/> Enable	
Statistics	<input type="checkbox"/> Enable	
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )	
QoS	None	
NAT	<input type="checkbox"/> Enable	
		<input type="button" value="OK"/> <input type="button" value="Cancel"/>

**Setting the External User Control the Internal PC Policy**

**STEP 4 .** Complete the policy for the external user to control the internal PC through remote control software.

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1(61.11.11.12)	PC-Anywhere(5631-5632)	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To: 1
<input type="button" value="New Entry"/>						

**Complete Policy Setting**



**Set a FTP Server under DMZ NAT Mode and restrict the download bandwidth from external and MAX. Concurrent Sessions.**

**STEP 1** . Set a FTP Server under **DMZ**, which IP is 192.168.3.2 (The DMZ Interface Address is 192.168.3.1/24)

**STEP 2** . Enter the following setting in **Virtual Server1** of **Virtual Server** function.

Virtual Server Real IP 61.11.11.12			
Service	WAN Port	Server Virtual IP	Configure
FTP (21)	21	192.168.3.2	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>
<input type="button" value="New Entry"/>			

**Setting up Virtual Server Corresponds to FTP Server**



When using the function of **Incoming** or **WAN to DMZ** in **Policy**, strong suggests that cannot select **ANY** in **Service**. It may be attacked by Hacker easily.

**STEP 3** . Enter the following in **QoS**.

Name	Downstream Bandwidth	Upstream Bandwidth	Priority	Configure
FTP_QoS	G.Bandwidth = 100 Kbps M.Bandwidth = 500 Kbps	G.Bandwidth = 50 Kbps M.Bandwidth = 200 Kbps	Middle	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
<input type="button" value="New Entry"/>				

**QoS Setting**

**STEP 4 .** Enter the following in **WAN to DMZ Policy**:

- Click **New Entry**
- **Destination Address:** Select Virtual Server1 (61.11.11.12)
- **Service:** Select FTP (21)
- **QoS:** Select FTP\_QoS
- **MAX. Concurrent Sessions:** Enter 100
- Click **OK**

Comment :	<input type="text" value=""/> (Max. 32 characters)
<b>Add New Policy</b>	
Source Address	Outside_Any
Destination Address	Virtual Server 1(61.11.11.12)
Service	FTP(21)
Schedule	None
Action	PERMIT
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
MAX. Concurrent Sessions	100 ( Range: 1 - 99999, 0: means unlimited )
QoS	FTP_QoS
NAT	<input type="checkbox"/> Enable
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

**Add New Policy**

**STEP 5 .** Complete the policy of restricting the external users to access to internal network server (which may occupy the resource of network)

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1(61.11.11.12)	FTP(21)	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1
<input type="button" value="New Entry"/>						

**Complete the Policy Setting**

## Set a Mail Server to allow the internal and external users to receive and send e-mail under DMZ Transparent Mode

**STEP 1** . Set a Mail Server in **DMZ** and set its network card's IP Address as 61.11.11.12. The DNS setting is external DNS Server.

**STEP 2** . Add the following setting in **DMZ** of **Address** function.

Name	IP / Netmask	MAC Address	Configure
DMZ_Any	0.0.0.0/0.0.0.0		<input type="button" value="In Use"/>
Maj_Server	61.11.11.12/255.255.255.255	00:0E:18:25:87:1A	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

**The Mail Server's IP Address Corresponds to Name Setting in Address Book of Mail Server**

**STEP 3** . Add the following setting in **Group** of **Service** function.

Group name	Service	Configure
E-Mail	DNS,POP3,SMTP	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

**Setting up a Service Group that has POP3, SMTP, and DNS**

**STEP 4 .** Enter the following setting in **WAN to DMZ Policy**:

- Click **New Entry**
- **Destination Address:** Select Mail\_Server
- **Service:** Select E-mail
- Click **OK**

Comment :	<input type="text" value=""/>	(Max. 32 characters)
<b>Modify Policy</b>		
Source Address	Outside_Any	
Destination Address	Mail_Server	
Service	E-Mail	
Schedule	None	
Action	PERMIT	
Traffic Log	<input type="checkbox"/> Enable	
Statistics	<input type="checkbox"/> Enable	
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )	
QoS	None	
NAT	<input type="checkbox"/> Enable	
		<input type="button" value="OK"/> <input type="button" value="Cancel"/>

**Setting a Policy to access Mail Service by WAN to DMZ**

**STEP 5 .** Complete the policy to access mail service by **WAN to DMZ**.

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Mail_Server	E-Mail	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1
<input type="button" value="New Entry"/>						

**Complete the Policy to access Mail Service by WAN to DMZ**

**STEP 6 . Add the following setting in LAN to DMZ Policy:**

- Click **New Entry**
- **Destination Address:** Select Mail\_Server
- **Service:** Select E-mail
- Click **OK**

Comment :  (Max. 32 characters)

Add New Policy	
Source Address	Inside_Any
Destination Address	Mail_Server
Service	E-Mail
Schedule	None
Action	PERMIT
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
NAT	<input type="checkbox"/> Enable

**Setting a Policy to access Mail Service by LAN to DMZ**

**STEP 7 . Complete the policy to access mail service by LAN to DMZ.**

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Mail_Server	E-Mail	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1

**Complete the Policy to access Mail Service by LAN to DMZ**

**STEP 8 . Add the following setting in DMZ to WAN Policy:**

- Click **New Entry**
- **Source Address:** Select Mail\_Server
- **Service:** Select E-mail
- Click **OK**

Comment :  (Max. 32 characters)

**Add New Policy**

Source Address	Mail_Server
Destination Address	Outside_Any
Service	E-Mail
Schedule	None
Authentication User	None
Action	PERMIT
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
QoS	None

**Setting the Policy of Mail Service by DMZ to WAN**

**STEP 9 . Complete the policy access to mail service by DMZ to WAN.**

Source	Destination	Service	Action	Option	Configure	Move
Mail_Server	Outside_Any	E-Mail	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1

**Complete the Policy access to Mail Service by DMZ to WAN**

## Chapter 6 Anomaly Flow IP

When the BM-525 received the intrusion packets from hackers, the internal PC will block this abnormal packets in it, to prevent the Company's network be paralyzed. In this chapter, we will make the introduction and settings of Anomaly Flow IP.

## 6.1 Settings

### Sasser Block

- Can block the external Sasser virus attack.

### MSBlaster Block

- Can block the external MSBlaster virus attack.

### Code Red Block

- Can block the external Code Red virus attack.

### Nimda Block

- Can block the external Nimda virus attack.

### Detect SYN Attack

- Can detect the disconnection situation as the hacker keeps sending the TCP SYN data packets to paralyze the server connection.
  - ◆ **SYN Flood Threshold (Total)** : Define all the IP and the total SYN packets (Pkts/Sec) pass through the BM-525. If over the setting value, then BM-525 will define it to be attacked. ◦
  - ◆ **SYN Flood Threshold ( Per Source IP )** : Define every source IP and the total SYN packets (Pkts/Sec) pass through the BM-525. If over the setting value, then BM-525 will define it to be attacked. ◦
  - ◆ **SYN Flood Threshold Blocking Time (Per Source IP)** : The BM-525 will block the packets from the attack source IP according to the time setting. After the blocking time, the BM-525 will re calculate the total SYN flow from every source IP, if over the setting value, then BM-525 will keep blocking.



### Detect ICMP Flood

- Can detect the data packets sent from hacker and use the Broadcast to send to every internal PC.
  - ◆ **ICMP Flood Threshold** : Define all the IP and the total ICMP packets ( Pkts/Sec ) pass through the BM-525. If over the setting value, then BM-525 will define it to be attacked. °
  - ◆ **ICMP Flood Threshold (Per Source IP)** : Define every source IP and the total ICMP packets ( Pkts/Sec ) pass through the BM-525. If over the setting value, then BM-525 will define it to be attacked.
  - ◆ **ICMP Flood Threshold Blocking Time ( Per Source IP )** : The BM-525 will block the packets from the attack source IP according to the time setting. After the blocking time, the BM-525 will re calculate the total ICMP flow from every source IP, if over the setting value, then BM-525 will keep blocking.

### Detect UDP Flood

- Can detect the UDP data packets sent from hacker and use the Broadcast to send to every internal PC.
  - ◆ **UDP Flood Threshold (Total)** : Define all the IP and the total UDP packets ( Pkts/Sec ) pass through the BM-525. If over the setting value, then BM-525 will define it to be attacked. °
  - ◆ **UDP Flood Threshold (Per Source IP)** : Define every source IP and the total UDP packets ( Pkts/Sec ) pass through the BM-525. If over the setting value, then BM-525 will define it to be attacked.
  - ◆ **UDP Flood Threshold Blocking Time ( Per Source IP )** : The BM-525 will block the packets from the attack source IP according to the time setting. After the blocking time, the BM-525 will re calculate the total UDP flow from every source IP, if over the setting value, then BM-525 will keep blocking.

### **Detect Ping of Death Attack**

- Can detect the status of PING data packets sent from the hackers, in order to paralyze the network.

### **Detect IP Spoofing Attack**

- Can detect the hacker which pretends the legal user to pass through the BM-525.

### **Detect Port Scan Attack**

- Can detect the Port ID which the hacker use it to detect the port and attack them.

### **Detect Tear Drop Attack**

- Can detect the IP data packets which pretend the normal data packets, but actually this kind of packets contain the mount of data packets, which can let the system crash, hold on or reboot.

### **Detect Tear Drop Attack**

- Select the function can prevent some IP packets which the hacker use it to enter the domain.

### **Detect Land Attack**

- Select this function can prevent the data packets which includes the source port as the same as destination port. Or this kind of packets has the SYN characters in TCP packets header.



When the MIS engineer enable the **Anomaly Flow** function, the BM-525 will instantly show the message in **Virus-infected IP** and **Attack Events**. If the MIS engineers enable the function in **System → E-mail alert notification**, then the BM-525 will automatically send the notification to the MIS engineer.

## To alert and block the external or internal anomalous data packets

Step1. In **Anomaly IP → Setting** :

- **The threshold sessions of virus-infected is ( default is 30 sessions/sec)**
- **Select Enable Virus-infected IP Blocking ( Blocking Time 600 seconds)**
- **Select Enable E-Mail alert notification.**
- **Select Enable NetBIOS Alert Notification.**
- Enter 192.168.189.30 in IP Address of Administrator.
- Enable all the function in DoS / Anti-Attack Setting.
- Click OK.

**Virus-infected IP Setting**

The threshold sessions of virus-infected (per source IP) is  Sessions / Sec ( Range: 1 - 9999 )

Enable Virus-infected IP Blocking      Blocking Time  seconds ( Range: 1 - 999 )

Enable E-Mail Alert Notification

Enable NetBIOS Alert Notification      IP Address of Administrator

---

**DoS / Anti-Attack Setting**

Sasser Block       MSBlaster Block

Code Red Block       Nimda Block

Detect SYN Attack      SYN Flood Threshold (Total)  Pkts/Sec ( Range: 0 - 9999 )

   SYN Flood Threshold (Per Source IP)  Pkts/Sec ( Range: 0 - 9999 )

   SYN Flood Threshold Blocking Time (Per Source IP)  Seconds ( Range: 0 - 9999 )

Detect ICMP Flood      ICMP Flood Threshold (Total)  Pkts/Sec ( Range: 0 - 9999 )

   ICMP Flood Threshold (Per Source IP)  Pkts/Sec ( Range: 0 - 9999 )

   ICMP Flood Threshold Blocking Time (Per Source IP)  Seconds ( Range: 0 - 9999 )

Detect UDP Flood      UDP Flood Threshold (Total)  Pkts/Sec ( Range: 0 - 9999 )

   UDP Flood Threshold (Per Source IP)  Pkts/Sec ( Range: 0 - 9999 )

   UDP Flood Threshold Blocking Time (Per Source IP)  Seconds ( Range: 0 - 9999 )

Detect Ping of Death Attack       Detect Tear Drop Attack

Detect IP Spoofing Attack       Filter IP Route Option

Detect Port Scan Attack       Detect Land Attack

---

**Non-detected IP**

Interface	IP Address / Netmask	Configure
LAN	192.168.1.2 / 255.255.255.255	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

**The setting of anomaly flow IP and Dos / Anti-Attack**

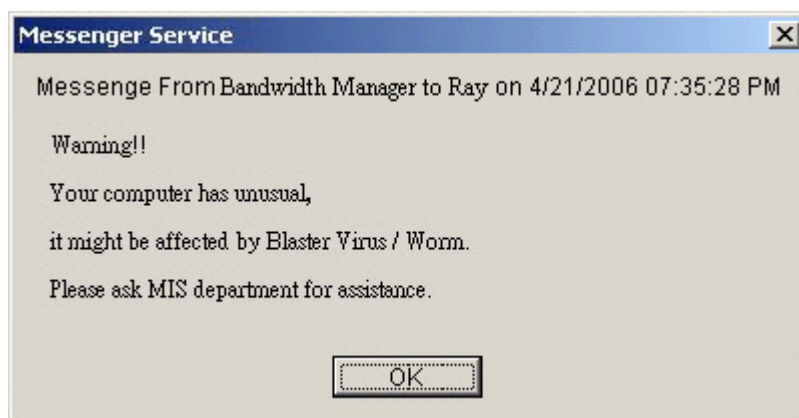


Can add **Non-detected IP**, and these IP will not controlled by this function.

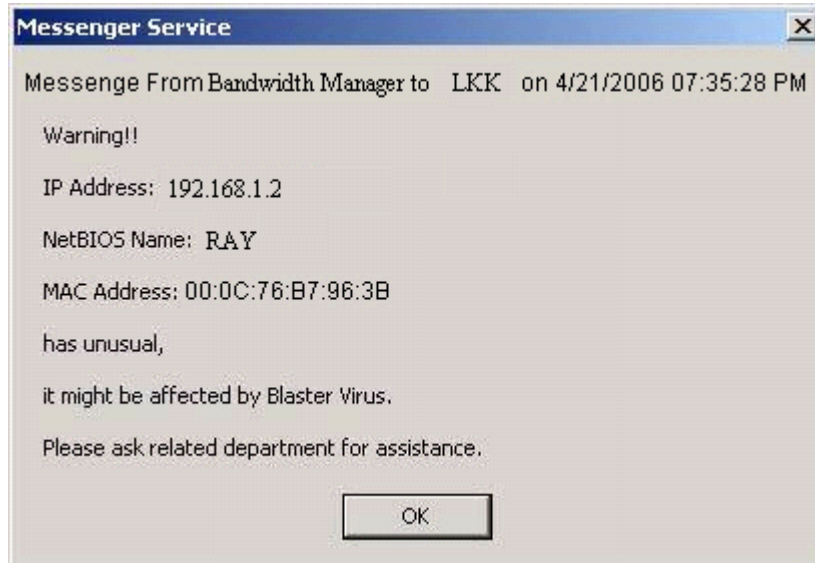
Step2. When the system detects the DDoS attack packets, it will show the message in **Anomaly Flow IP → Virus-infected IP**. Or send the Net BIOS Notification to the MIS and virus-infected PC.

Threshold Sessions / Sec : 30		
Interface	Virus-infected IP	Alarm Time
LAN	192.168.1.2	08/17 23:37:08

**Anomaly flow IP and Virus-infected IP**

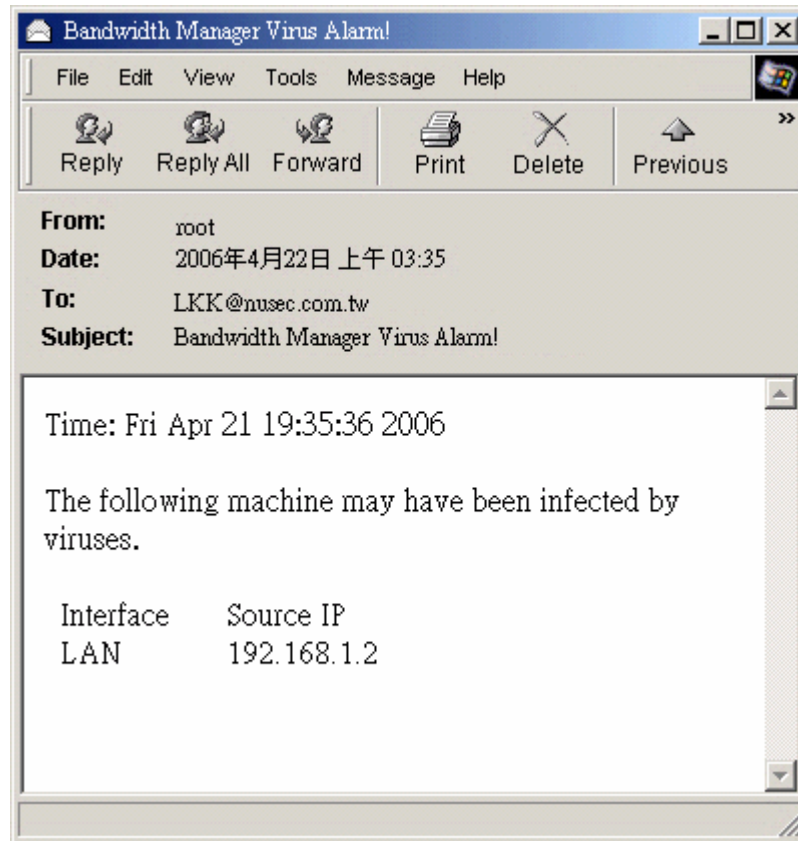


**Send the NetBIOS Alert notification to the virus-infected PC**



**Send the NetBIOS Alert Notification to the MIS engineer**

Step3. Enable the **System → E-Mail alert notification**, and then the BM-525 will send the mail notice to the MIS engineer.



**Send the e-mail alert notification**



Step4. Enable the Anomaly Flow → Attack Event , then the BM-525 shows the attack information in detail.

Aug 18 12:43:46 ▾	
Time	Event
Aug 18 12:43:46	The system has detected the attack of TCP port scan , suspected to be 203.84.196.97
Aug 18 10:39:20	The system has detected the attack of TCP port scan , suspected to be 172.19.1.106
Aug 18 10:39:07	The system has detected the attack of TCP port scan , suspected to be 172.19.1.106
Aug 18 10:39:05	The system has detected the attack of TCP port scan , suspected to be 172.19.1.106

[Clear Alarm](#)
[Download Alarm](#)

**Anomaly Flow IP attack event**

## Chapter 7 Monitor

### 7.1 LOG

**Log** records all connections that pass through the BM-525's control policies. The information is classified as Traffic Log, Event Log, and Connection Log.

**Traffic Log's** parameters are setup when setting up policies. Traffic logs record the details of packets such as the start and stop time of connection, the duration of connection, the source address, the destination address and services requested, for each control policy.

**Event Log** record the contents of System Configurations changes made by the Administrator such as the time of change, settings that change, the IP address used to log in...etc.

**Connection Log** records all of the connections of BM-525. When the connection occurs some problem, the Administrator can trace back the problem from the information.



#### **How to use the Log**

The Administrator can use the log data to monitor and manage the device and the networks. The Administrator can view the logged data to evaluate and troubleshoot the network, such as pinpointing the source of traffic congestions.

We set up four LOG examples in the section:

No.	Suitable Situation	Example
Ex 1	<b>Traffic Log</b>	To detect the information and Protocol port that users use to access to Internet or Intranet by BM-525.
Ex 2	<b>Event Log</b>	To record the detailed management events (such as Interface and event description of BM-525) of the Administrator
Ex 3	<b>Connection Log</b>	To detect event description of WAN Connection
Ex 4	<b>Log Backup</b>	To save or receive the records that sent by the BM-525

## 7.2 Traffic Log

To detect the information and Protocol port that users use to access to Internet or Intranet by BM-525

**STEP 1 .** Add new policy in **DMZ to WAN** of **Policy** and select **Enable Logging**.

Comment :	<input type="text" value=""/>	(Max. 32 characters)
<b>Modify Policy</b>		
Source Address	DMZ_Any	
Destination Address	Outside_Any	
Service	ANY	
Schedule	None	
Authentication User	None	
Action	PERMIT	
Traffic Log	<input checked="" type="checkbox"/> Enable	
Statistics	<input type="checkbox"/> Enable	
Content Blocking	<input type="checkbox"/> Enable	
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )	
QoS	None	
		OK Cancel

**Logging Policy Setting**

**STEP 2 .** Complete the Logging Setting in **DMZ to WAN** Policy.

Source	Destination	Service	Action	Option	Configure	Move
DMZ_Any	Outside_Any	ANY	✓	👁	Modify Remove Pause	To 1
New Entry						

**Complete the Logging Setting of DMZ to WAN**

**STEP 3 .** Click **Traffic Log**. It will show up the packets records that pass this policy.

Aug 18 14:15:22 <span style="float: right;"><a href="#">Next</a></span>					
Time	Source	Destination	Protocol	Port	Disposition
Aug 18 14:15:22	192.168.1.2	203.84.197.167	TCP	3575 => 80	✓
Aug 18 14:15:22	192.168.1.2	203.84.197.167	TCP	3567 => 80	✓
Aug 18 14:15:22	192.168.1.2	203.84.197.167	TCP	3575 => 80	✓
Aug 18 14:15:22	192.168.1.2	203.84.197.167	TCP	3567 => 80	✓
Aug 18 14:15:22	202.43.195.52	192.168.1.2	TCP	80 => 3610	✓
Aug 18 14:15:22	192.168.1.2	202.43.195.52	TCP	3610 => 80	✓
Aug 18 14:15:22	192.168.1.2	202.43.195.52	TCP	3610 => 80	✓
Aug 18 14:15:22	192.168.1.2	202.43.195.52	TCP	3610 => 80	✓
Aug 18 14:15:22	202.43.195.52	192.168.1.2	TCP	80 => 3610	✓
Aug 18 14:15:22	202.43.195.52	192.168.1.2	TCP	80 => 3610	✓
Aug 18 14:15:22	202.43.195.52	192.168.1.2	TCP	80 => 3610	✓
Aug 18 14:15:22	202.43.195.52	192.168.1.2	TCP	80 => 3609	✓
Aug 18 14:15:22	192.168.1.2	202.43.195.52	TCP	3609 => 80	✓
Aug 18 14:15:22	192.168.1.2	202.43.195.52	TCP	3609 => 80	✓
Aug 18 14:15:22	202.43.195.52	192.168.1.2	TCP	80 => 3609	✓
Aug 18 14:15:22	202.43.195.52	192.168.1.2	TCP	80 => 3609	✓
Aug 18 14:15:22	192.168.1.2	202.43.195.52	TCP	3610 => 80	✓
Aug 18 14:15:22	192.168.1.2	202.43.195.52	TCP	3610 => 80	✓

Clear Logs
Download Logs

**Traffic Log Web UI**

**STEP 4 .** Click on a specific IP of **Source IP** or **Destination IP**, it will prompt out a Web UI about Protocol and Port of the IP.

Time	Source	Destination	Protocol	Port	Disposition
Aug 18 14:16:42	192.168.1.2	207.46.4.117	TCP	2205 => 1863	✓
Aug 18 14:16:40	192.168.1.2	172.19.1.106	TCP	2792 => 445	✓
Aug 18 14:16:40	192.168.1.2	172.19.1.106	TCP	2792 => 445	✓
Aug 18 14:16:34	192.168.1.2	203.84.197.167	TCP	3572 => 80	✓
Aug 18 14:16:34	192.168.1.2	203.84.197.167	TCP	3572 => 80	✓
Aug 18 14:16:29	192.168.1.2	203.84.197.167	TCP	3625 => 80	✓
Aug 18 14:16:29	192.168.1.2	203.84.197.167	TCP	3623 => 80	✓
Aug 18 14:16:29	192.168.1.2	203.84.197.167	TCP	3568 => 80	✓
Aug 18 14:16:29	192.168.1.2	203.84.197.167	TCP	3622 => 80	✓
Aug 18 14:16:29	192.168.1.2	203.84.197.167	TCP	3621 => 80	✓
Aug 18 14:16:29	192.168.1.2	203.84.197.167	TCP	3619 => 80	✓
Aug 18 14:16:28	192.168.1.2	203.84.197.167	TCP	3623 => 80	✓
Aug 18 14:16:28	192.168.1.2	203.84.197.167	TCP	3568 => 80	✓
Aug 18 14:16:28	192.168.1.2	203.84.197.167	TCP	3621 => 80	✓
Aug 18 14:16:28	192.168.1.2	203.84.197.167	TCP	3619 => 80	✓
Aug 18 14:16:28	192.168.1.2	203.84.197.167	TCP	3622 => 80	✓
Aug 18 14:16:28	192.168.1.2	203.84.197.167	TCP	3625 => 80	✓
Aug 18 14:16:19	192.168.1.2	220.130.117.63	TCP	3598 => 80	✓

The Web UI of detecting the Traffic Log by IP Address



**STEP 6.** Click **Clear Logs** and click **OK** on the confirm Web UI. The records will be deleted from the BM-525 instantly.

The screenshot displays a web interface for clearing traffic logs. At the top, there is a dropdown menu showing 'Aug 18 14:15:22' and a 'Next' link. Below this is a table with the following columns: Time, Source, Destination, Protocol, Port, and Disposition. The table contains 20 rows of log entries, all with a 'Disposition' of a green checkmark. A 'Microsoft Internet Explorer' dialog box is overlaid on the table, asking 'Do you really want to clean?' with 'OK' and 'Cancel' buttons. At the bottom of the interface, there are two buttons: 'Clear Logs' and 'Download Logs'.

Time	Source	Destination	Protocol	Port	Disposition
Aug 18 14:15:22	192.168.1.2	203.84.197.167	TCP	3575 => 80	✓
Aug 18 14:15:22	192.168.1.2	203.84.197.167	TCP	3567 => 80	✓
Aug 18 14:15:22	192.168.1.2	203.84.197.167	TCP	3575 => 80	✓
Aug 18 14:15:22	192.168.1.2	203.84.197.167	TCP	3567 => 80	✓
Aug 18 14:15:22	202.43.195.52	192.168.1.2	TCP	80 => 3610	✓
Aug 18 14:15:22	192.168.1.2	202.43.195.52	TCP	3610 => 80	✓
Aug 18 14:15:22	192.168.1.2	202.43.195.52	TCP	3610 => 80	✓
Aug 18 14:15:22	192.168.1.2	202.43.195.52	TCP	3610 => 80	✓
Aug 18 14:15:22	202.43.195.52	192.168.1.2	TCP	80 => 3610	✓
Aug 18 14:15:22	202.43.195.52	192.168.1.2	TCP	80 => 3610	✓
Aug 18 14:15:22	202.43.195.52	192.168.1.2	TCP	80 => 3610	✓
Aug 18 14:15:22	202.43.195.52	192.168.1.2	TCP	80 => 3609	✓
Aug 18 14:15:22	192.168.1.2	202.43.195.52	TCP	3609 => 80	✓
Aug 18 14:15:22	192.168.1.2	202.43.195.52	TCP	3609 => 80	✓
Aug 18 14:15:22	202.43.195.52	192.168.1.2	TCP	80 => 3609	✓
Aug 18 14:15:22	202.43.195.52	192.168.1.2	TCP	80 => 3609	✓
Aug 18 14:15:22	192.168.1.2	202.43.195.52	TCP	3610 => 80	✓
Aug 18 14:15:22	192.168.1.2	202.43.195.52	TCP	3610 => 80	✓

Clearing Traffic Log Records Web UI



### 7.3 Event Log

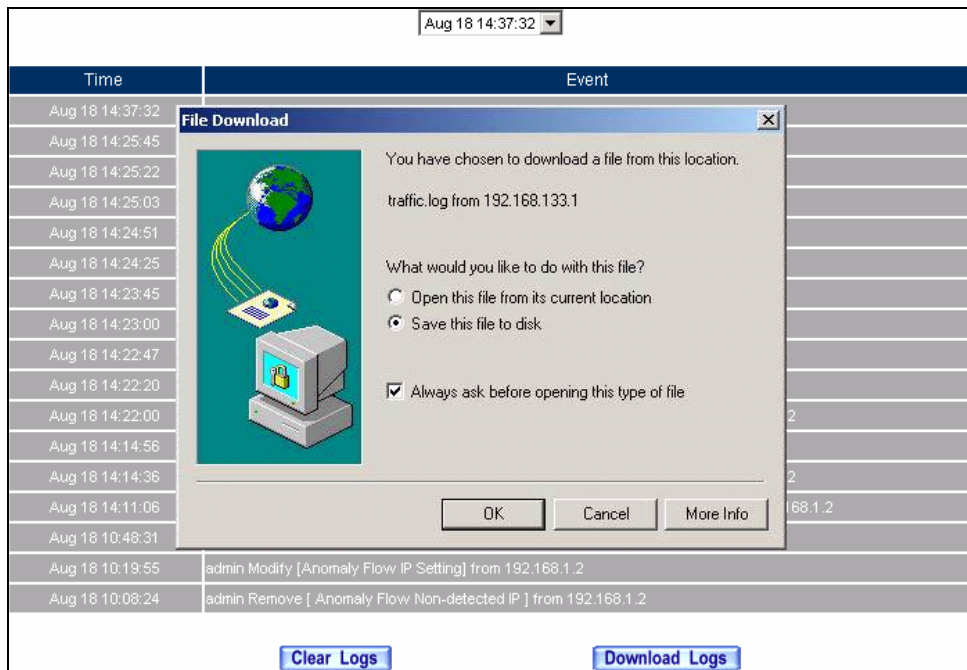
To record the detailed management events (such as Interface and event description of BM-525) of the Administrator

**STEP 1** . Click **Event** log of **LOG**. The management event records of the administrator will show up

Aug 18 14:37:32 ▾	
Time	Event
Aug 18 14:37:32	admin Modify [IM Blocking] from 192.168.1.2
Aug 18 14:25:45	admin Modify [P2P Blocking] from 192.168.1.2
Aug 18 14:25:22	admin Modify [Component Blocking] from 192.168.1.2
Aug 18 14:25:03	admin Add [Auth User] 02 from 192.168.1.2
Aug 18 14:24:51	admin Add [Auth User] 03 from 192.168.1.2
Aug 18 14:24:25	admin Add [QoS] (Name : FTP_QoS) from 192.168.1.2
Aug 18 14:23:45	admin Remove [ Anomaly Flow Non-detected IP ] from 192.168.1.2
Aug 18 14:23:00	admin Add [Address] 11 from 192.168.1.2
Aug 18 14:22:47	admin Add [Address] 03 from 192.168.1.2
Aug 18 14:22:20	admin Add [Policy](Outgoing,Inside_Any=>Outside_Any,DNS,permit) from 192.168.1.2
Aug 18 14:22:00	admin Modify [Policy](Outgoing,Inside_Any=>Outside_Any,ANY,permit) from 192.168.1.2
Aug 18 14:14:56	admin Modify [Setting] from 192.168.1.2
Aug 18 14:14:36	admin Modify [Policy](Outgoing,Inside_Any=>Outside_Any,ANY,permit) from 192.168.1.2
Aug 18 14:11:06	admin Modify [Policy](DMZ to External,DMZ_Any=>Outside_Any,ANY,permit) from 192.168.1.2
Aug 18 10:48:31	admin Add [ Anomaly Flow Non-detected IP ] 192.168.1.2 from 192.168.1.2
Aug 18 10:19:55	admin Modify [Anomaly Flow IP Setting] from 192.168.1.2
Aug 18 10:08:24	admin Remove [ Anomaly Flow Non-detected IP ] from 192.168.1.2

Event Log Web UI

**STEP 2 .** Click on **Download Logs** and select **Save** in **File Download** Web UI. Then choose the place to save in PC and click **OK**. The records will be saved instantly.



**Download Event Log Records Web UI**

**STEP 3.** Click **Clear Logs** and click **OK** on the confirm Web UI; the records will be deleted from the BM-525.

Aug 18 14:37:32 ▾

Time	Event
Aug 18 14:37:32	admin Modify [IM Blocking] from 192.168.1.2
Aug 18 14:25:45	admin Modify [P2P Blocking] from 192.168.1.2
Aug 18 14:25:22	admin Modify [Component Blocking] from 192.168.1.2
Aug 18 14:25:03	admin Add [Auth User] 02 from 192.168.1.2
Aug 18 14:24:51	admin Add [Auth User] 03 from 192.168.1.2
Aug 18 14:24:25	admin Add [QoS] (Name)
Aug 18 14:23:45	admin Remove [ Anomaly Flow Non-detected IP ] 192.168.1.2 from 192.168.1.2
Aug 18 14:23:00	admin Add [Address]
Aug 18 14:22:47	admin Add [Address]
Aug 18 14:22:20	admin Add [Policy](Outgoing,Inside_Any=>Outside_Any,ANY,permit) from 192.168.1.2
Aug 18 14:22:00	admin Modify [Policy](Outgoing,Inside_Any=>Outside_Any,ANY,permit) from 192.168.1.2
Aug 18 14:14:56	admin Modify [Setting] from 192.168.1.2
Aug 18 14:14:36	admin Modify [Policy](Outgoing,Inside_Any=>Outside_Any,ANY,permit) from 192.168.1.2
Aug 18 14:11:06	admin Modify [Policy](DMZ to External,DMZ_Any=>Outside_Any,ANY,permit) from 192.168.1.2
Aug 18 10:48:31	admin Add [ Anomaly Flow Non-detected IP ] 192.168.1.2 from 192.168.1.2
Aug 18 10:19:55	admin Modify [Anomaly Flow IP Setting] from 192.168.1.2
Aug 18 10:08:24	admin Remove [ Anomaly Flow Non-detected IP ] from 192.168.1.2

Clear Logs
Download Logs

### Clearing Event Log Records Web UI

## 7.4 Connection Log

### To Detect Event Description of WAN Connection

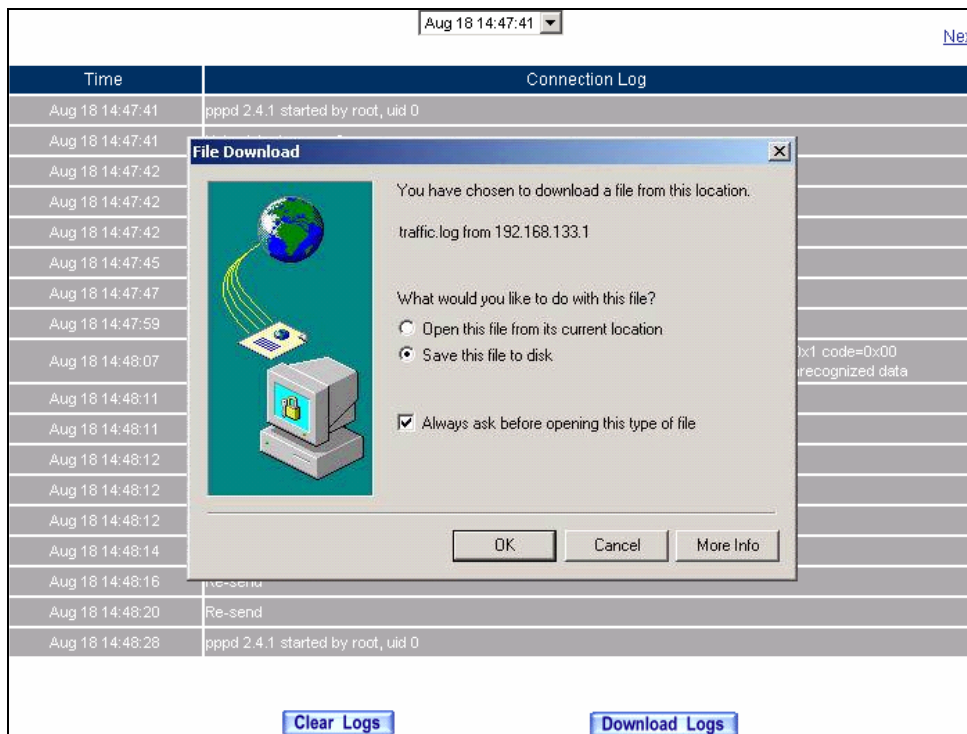
**STEP 1** . Click **Connection** in **LOG**. It can show up WAN Connection records of the BM-525.

Aug 18 14:47:41 <span style="float: right;"><a href="#">Next</a></span>	
Time	Connection Log
Aug 18 14:47:41	pppd 2.4.1 started by root, uid 0
Aug 18 14:47:41	Using interface ppp0
Aug 18 14:47:42	local IP address 10.64.64.64
Aug 18 14:47:42	remote IP address 10.98.42.216
Aug 18 14:47:42	linkname : wan1 interface : ppp0
Aug 18 14:47:45	Sending PADI 1
Aug 18 14:47:47	Re-send
Aug 18 14:47:59	message repeated 2 times
Aug 18 14:48:07	invalid packet Ether addr: 00:90:1a:40:09:87 (PPPOE Session) PPPoE hdr: ver=0x1 type=0x1 code=0x00 sid=0x0cdb length=0x000a (Unknown) PPPoE tag: type=c021 length=0965 (Unknown) unrecognized data
Aug 18 14:48:11	pppd 2.4.1 started by root, uid 0
Aug 18 14:48:11	Using interface ppp0
Aug 18 14:48:12	local IP address 10.64.64.64
Aug 18 14:48:12	remote IP address 10.245.13.24
Aug 18 14:48:12	linkname : wan1 interface : ppp0
Aug 18 14:48:14	Sending PADI 1
Aug 18 14:48:16	Re-send
Aug 18 14:48:20	Re-send
Aug 18 14:48:28	pppd 2.4.1 started by root, uid 0

[Clear Logs](#)
[Download Logs](#)

**Connection records Web UI**

**STEP 2 .** Click on **Download Logs** and select **Save** in **File Download** Web UI. And then choose the place to save in PC and click **OK**; the records will be saved instantly.



**Download Connection Log Records Web UI**

**STEP 3.** Click **Clear Logs** and click **OK** on the confirm Web UI, the records will be deleted from the BM-525 instantly.

The screenshot shows a web interface for viewing connection logs. At the top, there is a dropdown menu set to 'Aug 18 14:47:41' and a 'Next' link. Below this is a table with two columns: 'Time' and 'Connection Log'. The table contains several rows of log entries, including 'pppd 2.4.1 started by root, uid 0', 'Using interface ppp0', 'local IP address 10.64.64.64', 'remote IP address 10.98.42.216', 'linkname : wan1 interface : ppp0', 'Sending PADI 1', 'Re-send', and 'message repeated 2'. A 'Microsoft Internet Explorer' dialog box is overlaid on the table, asking 'Do you really want to clean?' with 'OK' and 'Cancel' buttons. At the bottom of the interface, there are two buttons: 'Clear Logs' and 'Download Logs'.

Time	Connection Log
Aug 18 14:47:41	pppd 2.4.1 started by root, uid 0
Aug 18 14:47:41	Using interface ppp0
Aug 18 14:47:42	local IP address 10.64.64.64
Aug 18 14:47:42	remote IP address 10.98.42.216
Aug 18 14:47:42	linkname : wan1 interface : ppp0
Aug 18 14:47:45	Sending PADI 1
Aug 18 14:47:47	Re-send
Aug 18 14:47:59	message repeated 2
Aug 18 14:48:07	invalid packet Ether e sid=0x0cdb length=0
Aug 18 14:48:11	pppd 2.4.1 started by
Aug 18 14:48:11	Using interface ppp0
Aug 18 14:48:12	local IP address 10.64.64.64
Aug 18 14:48:12	remote IP address 10.245.13.24
Aug 18 14:48:12	linkname : wan1 interface : ppp0
Aug 18 14:48:14	Sending PADI 1
Aug 18 14:48:16	Re-send
Aug 18 14:48:20	Re-send
Aug 18 14:48:28	pppd 2.4.1 started by root, uid 0

### Clearing Connection Log Records Web UI

## 7.5 Log Backup

To save or receive the records that sent by the BM-525

**STEP 1** . Enter **Setting** in **System**, select **Enable E-mail Alert Notification** function and set up the settings.

E-mail Setting	
<input checked="" type="checkbox"/> Enable E-mail Alert Notification	
Sender Address (Required by some ISPs)	sender@mydomain.c ( Max. 60 characters, ex: sender@mydomain.com )
SMTP Server	mail.mydomain.com ( Max. 80 characters, ex: mail.mydomain.com )
E-mail Address 1	user1@mydomain.cc ( Max. 60 characters, ex: user1@mydomain.com )
E-mail Address 2	user2@mydomain.cc ( Max. 60 characters, ex: user2@mydomain.com )
Mail Test	<input type="button" value="Mail Test"/>

**E-mail Setting Web UI**

**STEP 2**. Enter **Log Backup** in **Log**, select **Enable Log Mail Support** and click **OK**

Log Mail Configuration	
<input checked="" type="checkbox"/> Enable Log Mail Support	
When Log Full (300Kbytes), Bandwidth Manager Appliance sends Log	
From SMTP Server	mail.mydomain.com
To E-mail Address 1	user1@mydomain.com
E-mail Address 2	user2@mydomain.com

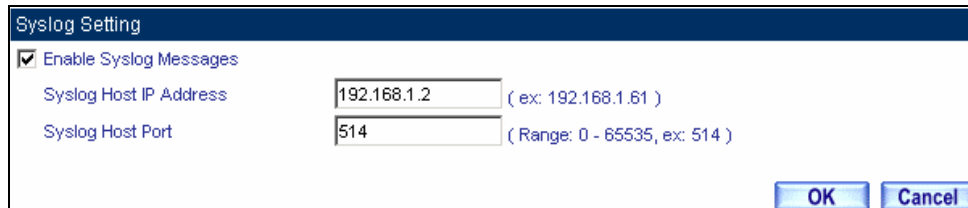
**Log Mail Configuration Web UI**



After **Enable Log Mail Support**, every time when **LOG** is up to 300Kbytes and it will accumulate the log records instantly. And the device will e-mail to the Administrator and clear logs automatically.

**STEP 3** . Enter **Log Backup** in **Log**, enter the following settings in **Syslog Settings**:

- Select **Enable Syslog Messages**
- Enter the IP in **Syslog Host IP Address** that can receive Syslog
- Enter the receive port in **Syslog Host Port**
- Click **OK**
- Complete the setting



Screenshot of the Syslog Setting dialog box. The dialog has a title bar "Syslog Setting". It contains a checked checkbox "Enable Syslog Messages". Below it are two input fields: "Syslog Host IP Address" with the value "192.168.1.2" and a hint "( ex: 192.168.1.61 )", and "Syslog Host Port" with the value "514" and a hint "( Range: 0 - 65535, ex: 514 )". At the bottom right are "OK" and "Cancel" buttons.

**Syslog Messages Setting Web UI**



## 7.6 Accounting Report

Administrator can use this Accounting Report to inquire the LAN IP users and WAN IP users, and to gather the statistics of **Downstream/Upstream, First packet/Last packet/Duration** and the **Service** of the entire user's IP that passes the BM-525.

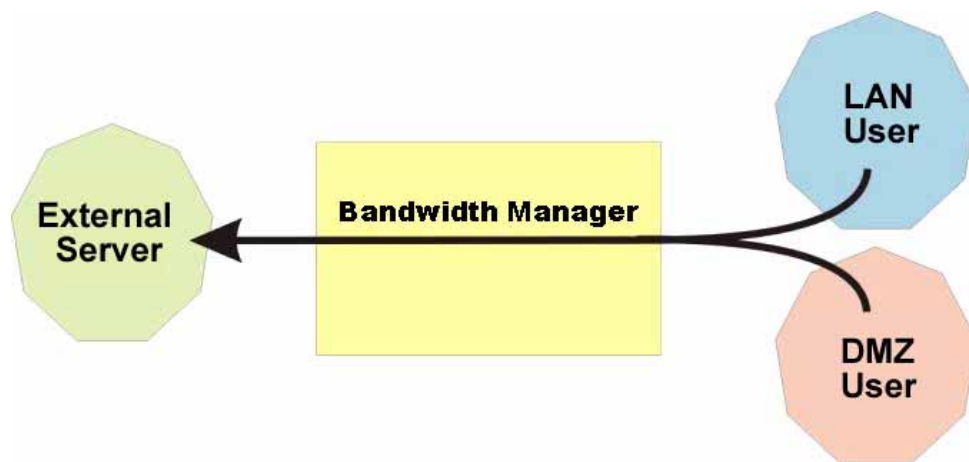
## Define the required fields of Accounting Report

### Accounting Report Setting:

- By accounting report function can record the sending information about Intranet and the external PC via BM-525.

Accounting Report can be divided into two parts: **Outbound Accounting Report** and **Inbound Accounting Report**

### Outbound Accounting Report



It is the statistics of the downstream and upstream of the LAN, WAN and all kinds of communication network services

### Source IP :

- The IP address used by LAN users who use BM-525

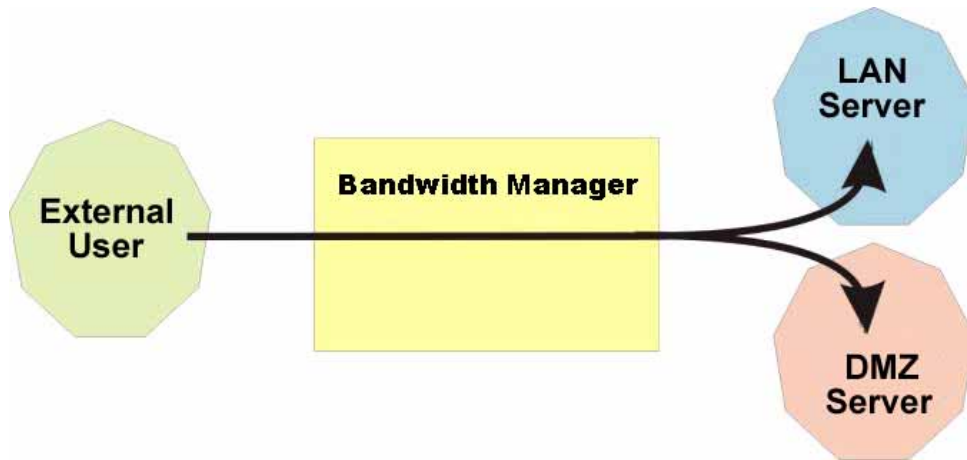
### Destination IP :

- The IP address used by WAN service server which uses BM-525.

### Service :

- The communication service which listed in the menu when LAN users use BM-525 to connect to WAN service server.

## Inbound Accounting Report



It is the statistics of downstream / upstream for all kinds of communication services. The Inbound Accounting report will be shown when WAN users use BM-525 to connect with LAN Server.

### Source IP :

- The IP address used by WAN users who use BM-525

### Destination IP :

- The IP address used by LAN service server who use BM-525

### Service :

- The communication service which listed in the menu when WAN users use BM-525 to connect to LAN Service server.

## 7.7 Outbound

**STEP 1** . Enter **Outbound** in **Accounting Report** and select **Top Users** to inquire the statistics of Send / Receive packets, **Downstream / Upstream, First packet/Last packet/Duration** and the service from the LAN or DMZ user's IP that pass the BM-525.

- **TOP:** Select the data you want to view; it presents 10 results in one page.

### **Pull-down menu selection**

- **Source IP :** The IP address used by LAN users who use BM-525 to connect to WAN service server.
- **Downstream :** The percentage of downstream and the value of each WAN service server which uses BM-525 to LAN user.
- **Upstream :** The percentage of upstream and the value of each LAN user who uses BM-525 to WAN service server.
- **First Packet :** When the first packet is sent to WAN service server from LAN user, the sent time will be recorded by the BM-525.
- **Last Packet :** When the last packet sent from WAN service server is received by the LAN user, the sent time will be recorded by the BM-525.
- **Duration :** The period of time which starts from the first packet to the last packet to be recorded.
- **Total Traffic :** The BM-525 will record the sum of packet sent/receive time and show the percentage of each LAN user's upstream/downstream to WAN service server.
- **Reset Counter :** Click Reset Counter button to refresh Accounting Report.

Top:

Starting Time : Fri Aug 18 15:02:07 2006

No.	Source IP	Downstream		Upstream		First Packet	Last Packet	Duration	Action
1	192.168.1.2	88.1 KB	100.0%	24.1 KB	100.0%	08/18 15:02:31	08/18 15:03:44	00:01:13	<input type="button" value="Remove"/>
Total Traffic		88.1 KB		24.1 KB		Reporting time: Fri Aug 18 15:03:51 2006			

### Outbound Source IP Statistics Report

**STEP 2.** Enter **Outbound** in **Accounting Report** and select **Top Sites** to inquire the statistics website of Send/Receive packets, **Downstream/Upstream, First packet/Last packet/Duration** and the service from the WAN Server to pass the BM-525.

- **TOP** : Select the data you want to view; it presents 10 results in one page.

**Pull-down menu selection**

- **Destination IP** : The IP address used by WAN service server which uses BM-525.
- **Downstream** : The percentage of downstream and the value of each WAN service server which uses BM-525 to LAN user.
- **Upstream** : The percentage of upstream and the value of each LAN user who uses BM-525 to WAN service server.
- **First Packet** : When the first packet is sent from WAN service server to LAN users, the sent time will be recorded by the BM-525.
- **Last Packet** : When the last packet from LAN user is sent to WAN service server, the sent time will be recorded by the BM-525.
- **Duration** : The period of time which starts from the first packet to the last packet to be recorded.
- **Total Traffic** : The BM-525 will record the sum of time and show the percentage of each WAN service server's upstream/downstream to LAN user.
- **Reset Counter** : Click Reset Counter button to refresh Accounting Report.

Top: 1 - 10

Starting Time : Fri Aug 18 15:02:07 2006


No.	Destination IP	Downstream		Upstream		First Packet	Last Packet	Duration	Action
1	203.66.88.89	370.2 KB	76.2%	52.2 KB	55.5%	08/18 15:03:24	08/18 15:05:32	00:02:08	<a href="#">Remove</a>
2	61.219.38.88	69.5 KB	14.3%	6.4 KB	6.8%	08/18 15:03:26	08/18 15:03:29	00:00:03	<a href="#">Remove</a>
3	207.46.4.83	13.3 KB	2.7%	2.7 KB	2.9%	08/18 15:04:25	08/18 15:05:22	00:00:57	<a href="#">Remove</a>
4	168.95.192.1	4.5 KB	0.9%	1.4 KB	1.5%	08/18 15:02:33	08/18 15:05:46	00:03:12	<a href="#">Remove</a>
5	207.46.78.247	4.0 KB	0.8%	1.4 KB	1.4%	08/18 15:04:31	08/18 15:05:10	00:00:39	<a href="#">Remove</a>
6	207.46.219.35	3.7 KB	0.8%	6.0 KB	6.4%	08/18 15:04:30	08/18 15:05:23	00:00:53	<a href="#">Remove</a>
7	211.78.161.178	3.5 KB	0.7%	629.0 B	0.7%	08/18 15:04:30	08/18 15:04:54	00:00:24	<a href="#">Remove</a>
8	65.54.179.192	2.7 KB	0.6%	1.3 KB	1.3%	08/18 15:04:25	08/18 15:04:27	00:00:02	<a href="#">Remove</a>
9	207.46.213.123	2.5 KB	0.5%	624.0 B	0.6%	08/18 15:04:29	08/18 15:05:39	00:01:10	<a href="#">Remove</a>
10	211.72.252.21	1.6 KB	0.3%	447.0 B	0.5%	08/18 15:04:31	08/18 15:04:48	00:00:17	<a href="#">Remove</a>
<b>Total Traffic</b>		<b>485.6 KB</b>		<b>94.1 KB</b>		Reporting time Fri Aug 18 15:05:48 2006			

[Reset Counters](#)

### Outbound Destination IP Statistics Report

**STEP 3 .** Enter **Outbound** in **Accounting Report** and select **Top Services** to inquire the statistics website of **Send / Receive packets, Downstream/Upstream, First packet/Last packet/Duration** and the service from the WAN Server to pass the BM-525.

- **TOP** : Select the data you want to view. It presents 10 results in one page.

-  : According to the downstream / upstream report of the selected TOP numbering to draw the Protocol Distribution chart.

#### **Pull-down menu selection**

- **Service** : The report of Communication Service when LAN users use the BM-525 to connect to WAN service server.
- **Downstream** : The percentage of downstream and the value of each WAN service server who uses BM-525 to connect to LAN user.
- **Upstream** : The percentage of upstream and the value of each LAN user who uses BM-525 to WAN service server.
- **First Packet** : When the first packet is sent to the WAN Service Server, the sent time will be recorded by the BM-525.
- **Last Packet** : When the last packet is sent from the WAN Service Server, the sent time will be recorded by the BM-525.
- **Duration** : The period of time starts from the first packet to the last packet to be recorded.
- **Total Traffic** : The BM-525 will record the sum of time and show the percentage of each Communication Service's upstream/downstream to WAN service server.
- **Reset Counter** : Click the Reset Counter button to refresh the Accounting Report.



Top: 1 - 10

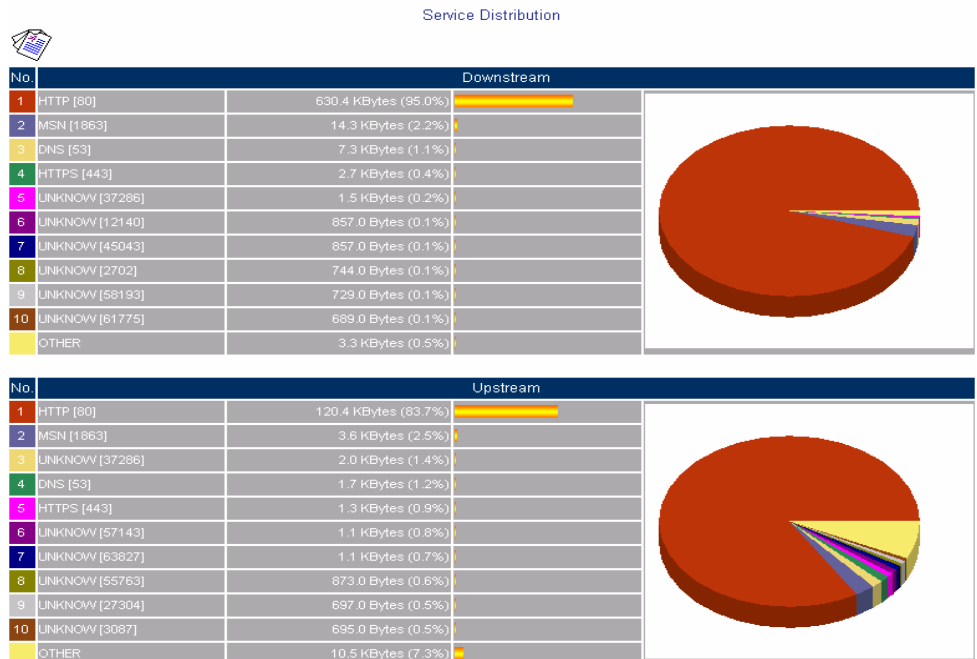
Starting Time : Fri Aug 18 15:02:07 2006

No.	Service	Downstream	Upstream	First Packet	Last Packet	Duration	Action
1	HTTP [80]	538.9 KB 94.3%	102.0 KB 81.5%	08/18 15:03:24	08/18 15:04:28	00:01:04	Remove
2	MSN [1863]	14.3 KB 2.5%	3.5 KB 2.8%	08/18 15:04:24	08/18 15:06:26	00:02:02	Remove
3	DNS [53]	7.3 KB 1.3%	1.7 KB 1.3%	08/18 15:02:33	08/18 15:05:51	00:03:18	Remove
4	HTTPS [443]	2.7 KB 0.5%	1.3 KB 1.0%	08/18 15:04:25	08/18 15:04:27	00:00:02	Remove
5	UNKNOWN [37286]	1.4 KB 0.2%	1.8 KB 1.5%	08/18 15:02:41	08/18 15:05:43	00:03:02	Remove
6	UNKNOWN [12140]	857.0 B 0.1%	65.0 B 0.1%	08/18 15:02:43	08/18 15:02:44	00:00:01	Remove
7	UNKNOWN [46043]	857.0 B 0.1%	62.0 B 0.0%	08/18 15:02:44	08/18 15:02:44	00:00:00	Remove
8	UNKNOWN [2702]	744.0 B 0.1%	50.0 B 0.0%	08/18 15:02:43	08/18 15:02:43	00:00:00	Remove
9	UNKNOWN [58193]	729.0 B 0.1%	61.0 B 0.0%	08/18 15:02:43	08/18 15:02:43	00:00:00	Remove
10	UNKNOWN [61775]	689.0 B 0.1%	117.0 B 0.1%	08/18 15:02:43	08/18 15:02:44	00:00:01	Remove
<b>Total Traffic</b>		<b>571.7 KB</b>	<b>125.2 KB</b>				

Reporting time Fri Aug 18 15:06:32 2006

[Reset Counters](#)

### Outbound Services Statistics Report



According to the downstream / upstream report of the selected TOP numbering to draw the Protocol Distribution chart



Press



to return to Accounting Report window.

## 7.8 Inbound

**STEP 1** . Enter **Inbound** in **Accounting Report** and select **Top Users** to inquire the statistics website of **Send / Receive packets, Downstream / Upstream, First packet/Last packet / Duration** and the service from the WAN user to pass the BM-525.

- **TOP** : Select the data you want to view. It presents 10 pages in one page.

### Select from the Pull-down menu

- **Source IP** : The IP address used by WAN users who use BM-525.
- **Downstream** : The percentage of Downstream and the value of each WAN user who uses BM-525 to LAN service server.
- **Upstream** : The percentage of Upstream and the value of each LAN service server who uses BM-525 to WAN users.
- **First Packet** : When the first packet is sent from WAN users to LAN service server, the sent time will be recorded by the BM-525.
- **Last Packet** : When the last packet is sent from LAN service server to WAN users, the sent time will be recorded by the BM-525.
- **Duration** : The period of time starts from the first packet to the last packet to be recorded.
- **Total Traffic** : The BM-525 will record the sum of time and show the percentage of each WAN user's upstream / downstream to LAN service server.
- **Reset Counter** : Click the Reset Counter button to refresh the Accounting Report.

Top: 1 - 4

Starting Time : Fri Aug 18 15:02:11 2006

No.	Source IP	Upstream		Downstream		First Packet	Last Packet	Duration	Action
1	172.19.1.106	382.9 kB	34.7%	22.8 kB	25.5%	08/18 15:12:46	08/18 15:12:49	00:00:03	<a href="#">Remove</a>
2	172.19.50.26	361.2 kB	32.7%	48.1 kB	53.8%	08/18 15:13:34	08/18 15:14:53	00:01:19	<a href="#">Remove</a>
3	172.19.20.1	360.1 kB	32.6%	18.3 kB	20.5%	08/18 15:14:56	08/18 15:15:00	00:00:04	<a href="#">Remove</a>
4	172.19.50.11	0.0 B	0.0%	180.0 B	0.2%	08/18 15:13:54	08/18 15:13:56	00:00:02	<a href="#">Remove</a>
Total Traffic		1.1 MB		89.3 KB		Reporting time Fri Aug 18 15:15:06 2006			

[Reset Counters](#)

### Inbound Top Users Statistics Report

Enter **Inbound** in **Accounting Report** and select **Top Sites** to inquire the statistics website of **Send / Receive packets, Downstream / Upstream, First packet/Last packet / Duration** and the service from the WAN user to pass the BM-525.

- **TOP** : Select the data you want to view. It presents 10 pages in one page.

Pull-down menu selection


- **Destination IP** : The IP address used by WAN users who uses BM-525.
- **Downstream** : The percentage of Downstream and the value of each WAN user who uses BM-525 to LAN service server.
- **Upstream** : The percentage of Upstream and the value of each LAN service server who uses BM-525 to WAN users.
- **First Packet** : When the first packet is sent from WAN users to LAN service server, the sent time will be recorded by the BM-525.
- **Last Packet** : When the last packet is sent from LAN service server to WAN users, the sent time will be recorded by the BM-525.
- **Duration** : The period of time starts from the first packet to the last packet to be recorded.
- **Total Traffic** : The BM-525 will record the sum of time and show the percentage of each WAN user's upstream / downstream to LAN service server.
- **Reset Counter** : Click the Reset Counter button to refresh the Accounting Report.

Top: 1 - 1								Starting Time : Fri Aug 18 15:02:11 2006	
No.	Destination IP	Upstream		Downstream		First Packet	Last Packet	Duration	Action
1	192.168.1.2	1.4 MB	100.0%	108.8 KB	100.0%	08/18 15:12:46	08/18 15:13:57	00:01:11	<a href="#">Remove</a>
Total Traffic		1.4 MB		108.8 KB		Reporting time Fri Aug 18 15:16:15 2006			

[Reset Counters](#)

### Inbound Destination IP Statistics Report

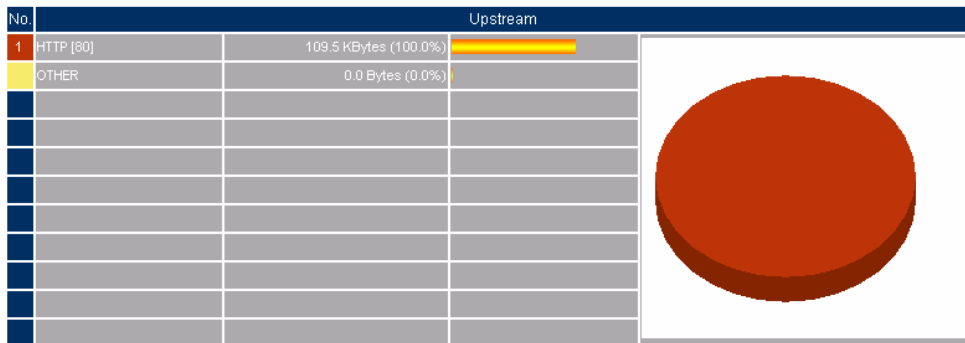
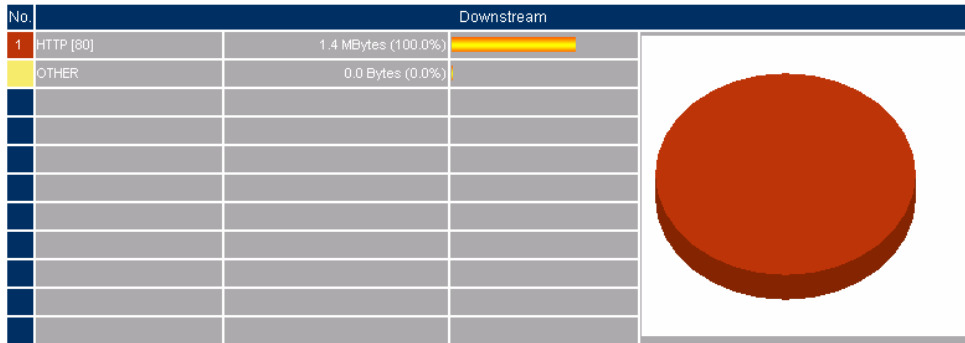
**STEP 2 .** Enter **Inbound** in **Accounting Report** and select **Top Services** to inquire the statistics website of Send/Receive packets, **Downstream/Upstream**, **First packet/Last packet/Duration** and the service from the WAN Server to pass the BM-525.

- **TOP** : Select the data you want to view. It presents 10 results in one page.
  -  : According to the downstream / upstream report of the selected TOP numbering to draw the Protocol Distribution chart.
- Pull-down menu selection
- **Service** : The report of Communication Service when WAN users use the BM-525 to connect to LAN service server.
  - **Downstream** : The percentage of downstream and the value of each WAN user who uses BM-525 to LAN service server.
  - **Upstream** : The percentage of upstream and the value of each LAN service server who uses BM-525 to WAN user.
  - **First Packet** : When the first packet is sent to the LAN Service Server, the sent time will be recorded by the BM-525.
  - **Last Packet** : When the last packet is sent from the LAN Service Server, the sent time will be recorded by the BM-525.
  - **Duration** : The period of time starts from the first packet to the last packet to be recorded.
  - **Total Traffic** : The BM-525 will record the sum of time and show the percentage of each Communication Service's upstream / downstream to LAN service server.
  - **Reset Counter** : Click the Reset Counter button to refresh the Accounting Report.

		Top: 1-1		Starting Time: Fri Aug 18 15:02:11 2006					
No.	Service	Upstream		Downstream		First Packet	Last Packet	Duration	Action
1	HTTP [80]	1.4 MB	100.0%	109.5 KB	100.0%	08/18 15:12:46	08/18 15:14:56	00:02:10	<a href="#">Remove</a>
Total Traffic		1.4 MB		109.5 KB		Reporting time: Fri Aug 18 15:17:09 2006			
<a href="#">Reset Counters</a>									

### Inbound Services Statistics Report

Service Distribution



**According to the downstream / upstream report of the selected TOP numbering to draw the Protocol Distribution chart**

## 7.9 Statistics

**WAN Statistics:** The statistics of Downstream / Upstream packets and Downstream/Upstream traffic record that pass WAN Interface

**Policy Statistics:** The statistics of Downstream / Upstream packets and Downstream/Upstream traffic record that pass Policy

In this chapter, the Administrator can inquire the BM-525 for statistics of packets and data that passes across the BM-525. The statistics provides the Administrator with information about network traffics and network loads.



## Define the required fields of Statistics:

### Statistics Chart:

- **Y-Coordinate** : Network Traffic ( Kbytes/Sec )
- **X-Coordinate** : Time ( Hour/Minute )

### Source IP, Destination IP, Service, and Action:

- These fields record the original data of Policy. From the information above, the Administrator can know which Policy is the Policy Statistics belonged to.

### Time:

- To detect the statistics by minutes, hours, days, months, or years.

### Bits/sec, Bytes/sec, Utilization, Total:

- The unit that used by Y-Coordinate, which the Administrator can change the unit of the Statistics Chart here.
  - ◆ **Utilization** : The percentage of the traffic of the Max. Bandwidth that System Manager set in Interface function.
  - ◆ **Total**: To consider the accumulative total traffic during a unit time as Y-Coordinate

## 7.10 WAN

**STEP 1** . Enter **WAN** in **Statistics** function, it will display all the statistics of Downstream/Upstream packets and Downstream/Upstream record that pass **WAN** Interface.

- **Time:** To detect the statistics by minutes, hours, days, months, or years.

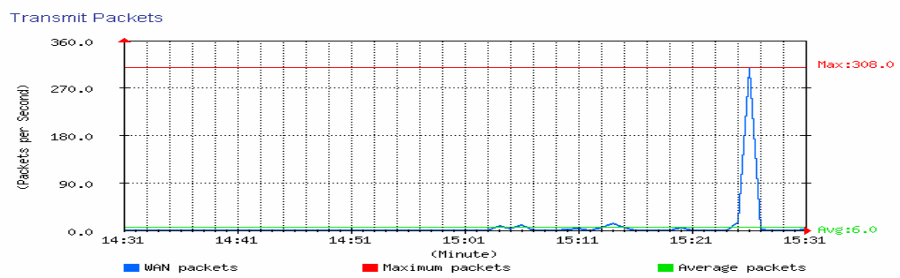
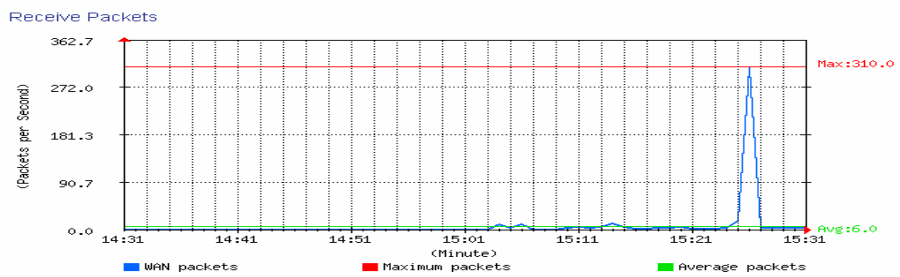
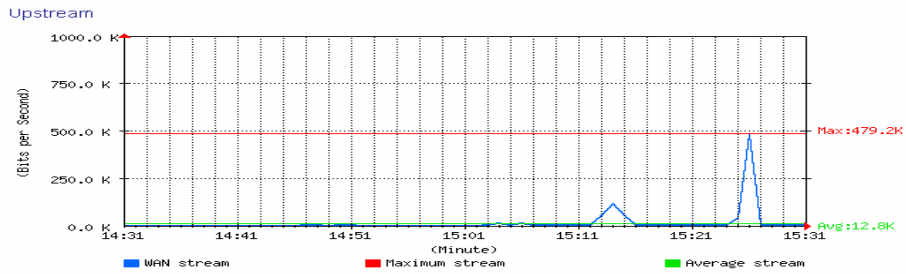
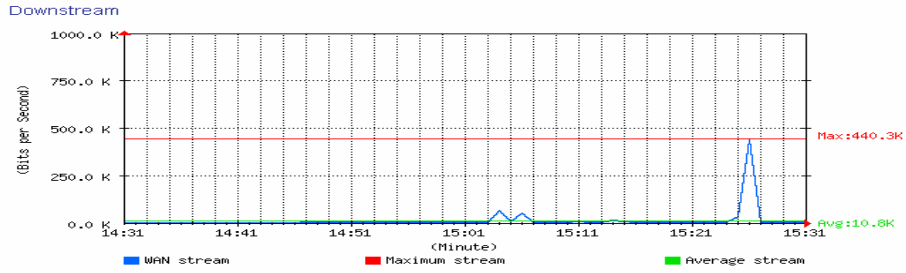


**WAN Statistics** is the additional function of **WAN** Interface. When enable **WAN** Interface, it will enable **WAN Statistics** too.

**STEP 2 . Statistics Chart**

- **Y-Coordinate** : Network Traffic ( Kbytes/Sec )
- **X-Coordinate** : Time ( Hour/Minute )

Bits/sec Bytes/sec Utilization Total Minute Hour Day Week Month Year  
**Real-time: Down 0.0 KBits/sec Up 0.0 KBits/sec**



**WAN Statistics**

## 7.11 Policy

**STEP 1** . If you had select **Statistics** in **Policy**, it will start to record the chart of that policy in **Policy Statistics**.

Source	Destination	Service	Action	Time					
Inside_Any	Outside_Any	ANY	✓	Minute	Hour	Day	Week	Month	Year

### Policy Statistics Function



If you are going to use **Policy Statistics** function, the System Manager has to enable the **Statistics** in **Policy** first.

**STEP 2** . In the **Statistics** Web UI, find the network you want to check and click **Minute** on the right side, and then you will be able to check the Statistics chart every minute; click **Hour** to check the Statistics chart every hour; click **Day** to check the Statistics chart every day; click **Week** to check the Statistics Figure every week; click **Month** to check the Statistics Figure every month; click **Year** to check the Statistics Figure every year.

**STEP 3 . Statistics Chart**

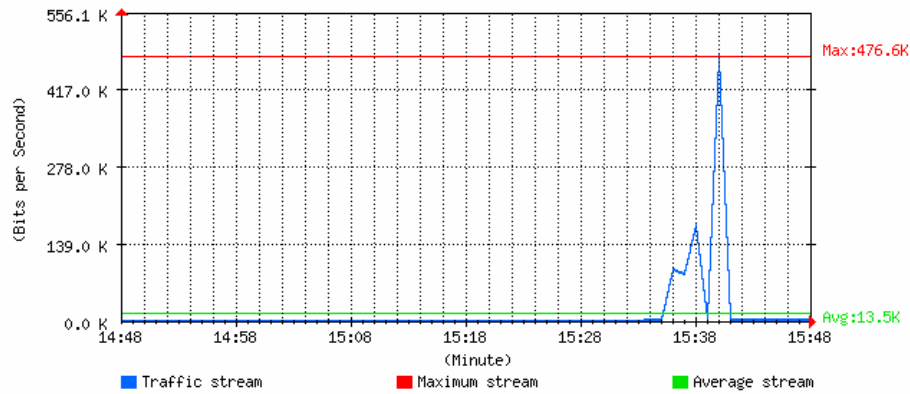
- **Y-Coordinate** : Network Traffic ( Kbytes/Sec )
- **X-Coordinate** : Time ( Hour/Minute/Day )

[Bits/sec](#) [Bytes/sec](#) [Total](#)
Inside\_Any to Outside\_Any
Service : ANY  
Action : PERMIT

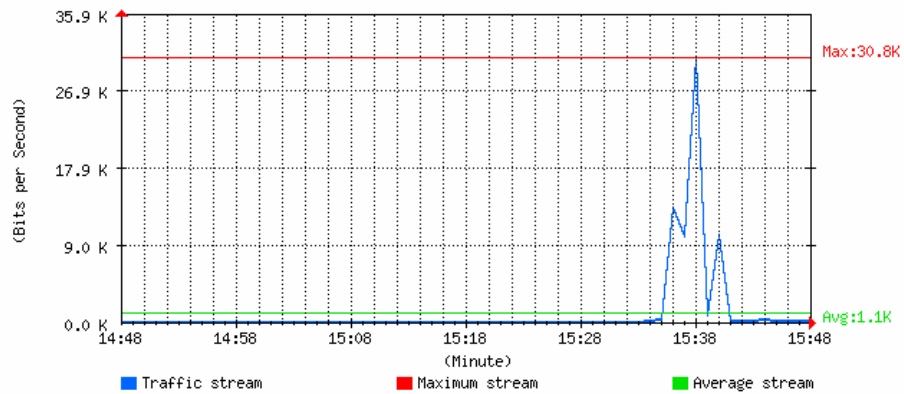
[Minute](#) [Hour](#) [Day](#) [Week](#) [Month](#) [Year](#)

**Real-time: Down 0.0 KBits/sec Up 0.0 KBits/sec**

**Downstream**



**Upstream**



**Policy Statistics**

## 7.12 Wake on LAN

The MIS engineers can use the BM-525 appliance to start up the internal PCs (by sending packets) which included the network bootable network adapter and can additionally use the remote monitor software such as VNC, Terminal Service and PC Anywhere.

In this section, we will make the introduction of Wake on LAN.

## Remote monitor the internal PC

Step1. The internal PC to be remote monitored, and its MAC is 00:0C:76:B7:96:3B.

Step2. In **Wake on LAN → Setting**, add the following settings :

- Click **New Entry**.
- **Name**, enter Rayearth.
- **MAC Address**, enter 00:01:80:41:D0:FB.
- Click **OK**.

**Set the internal PC to be monitored**

Step3. Click **Wake Up**, to start up the internal PC.

Name	MAC Address	Configure
Rayearth	00:01:80:41:D0:FB	<input type="button" value="Wake Up"/> <input type="button" value="Modify"/> <input type="button" value="Remove"/>
<input type="button" value="New Entry"/>		

**Start up the PC**

## 7.13 Status

The users can know the connection status in Status. For example: LAN IP, WAN IP, Subnet Netmask, Default Gateway, DNS Server Connection, and its IP...etc.

- **Interface:** Display all of the current Interface status of the BM-525
- **Authentication:** The Authentication information of BM-525
- **ARP Table:** Record all the ARP that connect to the BM-525
- **DHCP Clients:** Display the table of DHCP clients that are connected to the BM-525.



## 7.14 Interface

**STEP 1** . Enter **Interface** in **Status** function; it will list the setting for each Interface.

- **PPPoE Con. Time:** The last time of the BM-525 to be enabled
- **MAC Address:** The MAC Address of the Interface
- **IP Address/ Netmask:** The IP Address and its Netmask of the Interface
- **Rx Pkts, Err. Pkts:** To display the received packets and error packets of the Interface
- **Tx Pkts, Err. Pkts:** To display the sending packets and error packets of the Interface
- **Ping, Web UI:** To display whether the users can Ping to the BM-525 from the Interface or not; or enter its Web UI
- **Forwarding Mode:** The connection mode of the Interface
- **Connection Status:** To display the connection status of WAN
- **DnS/ UpS Kbps:** To display the Maximum DownStream/UpStream Bandwidth of that WAN (set from **Interface**)
- **DnStream Alloca.:** The distribution percentage of DownStream according to WAN traffic
- **UpStream Alloca.:** The distribution percentage of UpStream according to WAN traffic
- **Default Gateway:** To display the Gateway of WAN
- **DNS1:** The DNS1 Server Address provided by ISP
- **DNS2:** The DNS2 Server Address provided by ISP

Active Sessions Number : 13		System Uptime : 0 Day 1 Hour 16 Min 17 Sec		
	LAN	WAN	DMZ	
Forwarding Mode	NAT	Static IP	---	
Max. Downstream / Upstream	---	1000 / 1000 Kbps	---	
PPPoE Con. Time	---	---	---	
MAC Address	00:88:56:78:22:9c	00:88:56:78:22:9d	00:88:56:78:22:9e	
IP Address	192.168.1.1	172.19.100.113	0.0.0.0	
Netmask	255.255.255.0	255.255.0.0	0.0.0.0	
Default Gateway	---	172.19.1.254	---	
DNS1	---	168.95.1.1	---	
DNS2	---	0.0.0.0	---	
Rx Pkts, Error Pkts	37883, 0	37981, 0	0, 0	
Tx Pkts, Error Pkts	36322, 0	28294, 0	0, 0	
Ping	✓	✓	---	
HTTP	✓	✓	---	

**Interface Status**

## 7.15 Authentication

**STEP 1.** Enter **Authentication** in **Status** function. It will display the record of login status.

- **IP Address:** The authentication user IP
- **Auth-User Name:** The account of the auth-user to login
- **Login Time:** The login time of the user (Year/Month/Day Hour/Minute/Second)

IP Address	Authentication-User Name	Login Time	Configure
192.168.1.2	Rayearth	2006/8/18 16:0:51	<a href="#">Remove</a>

### Authentication Status Web UI

## 7.16 ARP Table

**STEP 1** . Enter **ARP Table** in **Status** function; it will display a table about IP Address, MAC Address, and the Interface information which is connecting to the BM-525.

- **NetBIOS Name:** The identified name of the network
- **IP Address:** The IP Address of the network
- **MAC Address:** The identified number of the network card
- **Interface:** The Interface of the computer

IP Address	MAC Address	Interface
172.19.1.254	00:0E:F5:00:49:C6	WAN
192.168.1.2	00:01:80:41:D0:FB	LAN

**ARP Table Web UI**

## 7.17 DHCP Clients

**STEP 1.** In **DHCP Clients** of **Status** function, it will display the table of DHCP Clients that are connected to the BM-525.

- **IP Address:** The dynamic IP that provided by DHCP Server
- **MAC Address:** The IP that corresponds to the dynamic IP
- **Leased Time:** The valid time of the dynamic IP (Start/End)  
(Year/Month/Day/Hour/Minute/Second)

IP Address	MAC Address	Leased Time	
		Start	End
192.168.1.2	00:01:80:41:d0:fb	2006/8/18 16:3:45	2006/8/19 16:3:45

**DHCP Clients Web UI**