



# Bandwidth Management Gateway

BM-2101

User's Manual

## Copyright

Copyright (C) 2007 PLANET Technology Corp. All rights reserved.

The products and programs described in this User's Manual are licensed products of PLANET Technology, This User's Manual contains proprietary information protected by copyright, and this User's Manual and all accompanying hardware, software, and documentation are copyrighted.

No part of this User's Manual may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form by any means by electronic or mechanical. Including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of PLANET Technology.

## 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.

## CE mark Warning

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

## 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.



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.

## **Customer Service**

For information on customer service and support for the Internet Monitor, please refer to the following Website URL:

<http://www.planet.com.tw>

Before contacting customer service, please take a moment to gather the following information:

- ◆ Internet Monitor serial number and MAC address
- ◆ Any error messages that displayed when the problem occurred
- ◆ Any software running when the problem occurred
- ◆ Steps you took to resolve the problem on your own

## **Revision**

User's Manual for PLANET Bandwidth Management Gateway

Model: BM-2101

Rev: 1.0 (March, 2007)

PartNo.EM-BM2101v1

# Table of Contents

Chapter 1	Introduction .....	6
1.1	Package Contents.....	6
1.2	Front View .....	6
1.3	Specification .....	7
<b>System</b>		
Chapter 2	Administration.....	9
2.1	Admin.....	11
2.2	Permitted IPs.....	13
2.3	System Log Out.....	14
2.4	Software Update.....	15
Chapter 3	Configure.....	16
3.1	Setting .....	21
3.2	Date/Time .....	27
3.3	Multiple Subnet .....	28
3.4	Route Table .....	32
3.5	DHCP .....	36
3.6	DDNS .....	38
3.7	Host Table .....	40
3.8	SNMP .....	41
3.9	Language .....	43
<b>Interface</b>		
Chapter 4	Interface .....	44
4.1	LAN.....	49
4.2	WAN.....	50
4.3	DMZ.....	58
<b>Policy Object</b>		
Chapter 5	Address.....	60
5.1	Example.....	63

Chapter 6	Service.....	70
6.1	Custom.....	73
6.2	Group.....	77
Chapter 7	Schedule.....	80
Chapter 8	QoS.....	83
8.1	Example.....	86
Chapter 9	Authentication.....	88
9.1	User / User Group.....	94
9.2	RADIUS .....	98
9.3	POP3 .....	119
9.4	LDAP .....	122
Chapter 10	Content Blocking.....	147
10.1	URL .....	150
10.2	Script .....	153
10.3	Download.....	155
10.4	Upload.....	157
Chapter 11	IM / P2P Blocking.....	159
11.1	Example.....	162
Chapter 12	Virtual Server.....	167
12.2	Example .....	171
<b>Policy</b>		
Chapter 13	Policy.....	185
13.1	Example.....	191
<b>Anomaly Flow IP</b>		
Chapter 14	Anomaly Flow IP.....	212
14.1	Example.....	217
<b>Monitor</b>		
Chapter 15	Monitor.....	224
15.1	Traffic.....	226
15.2	Event.....	231
15.3	Connection.....	232

15.4	Backup.....	235
Chapter 16	Accounting Report.....	237
16.1	Outbound.....	241
16.2	Inbound.....	247
Chapter 17	Statistics.....	253
17.1	WAN.....	255
17.2	Policy.....	257
Chapter 18	Diagnostic.....	259
18.1	Ping .....	260
18.2	Traceroute .....	263
Chapter 19	Wake On Lan.....	265
19.1	Example.....	266
Chapter 20	Status.....	267
20.1	Interface.....	270
20.1	System Info.....	272
20.3	Authentication.....	274
20.4	ARP Table.....	275
20.5	Sessions Info.....	276
20.6	DHCP Client.....	277

## Chapter 1

# Introduction

The BM-2101 is specifically designed for SMB networks. It has built-in four 10/100Mbps Ethernet ports include two WAN and one LAN and DMZ 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 and DMZ mode are supported, and therefore can maintain the existing network infrastructure without reconfiguring. The BM-2101 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 Package Contents

- BM-2101 x 1
- Power Cord x 1
- Quick Installation Guide x 1
- User's Manual CD x 1
- Console cable x 1
- Cat5 cross cable x 1
- Cat5 cable x 1
- Rack-mount ear x 2
- Mat x 4

## 1.2 Front View



## LED definition

LED	Description	
PWR	Power is supplied to this device.	
WAN1, WAN2, LAN, DMZ	Green	Steady on indicates the port is connected to other network device. Blink to indicates there is traffic on the port
	Orange	Steady on indicates the port is connected at 100Mbps speed

## 1.3 SPECIFICATION

Product	Bandwidth Management Gateway	
Model	BM-2101	
Hardware		
Connections	WAN	2 x 10/100Base-TX
	LAN	1 x 10/100Base-TX, Auto-MDI/MDI-X
	DMZ	1 x 10/100Base-TX, Auto-MDI/MDI-X
Console	1 x RS-232 (DB-9)	
H/W Watch-Dog	Auto reboot when detecting system fail	
Software		
Maximum Controlled Bandwidth	100Mbps	
Maximum Controlled concurrent session	241,000	
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 Quota per Session and Quota per Day
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	Event alarm for hacker attack The alarm message can sent to administrator by e-mail
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

# Administration

Generally speaking, the system administration refers to the privileges of log in/out, monitor and control the BM-2101 appliance with some relevant settings. In this Chapter, the system administration will be defined as the management of the **MIS engineer** , **Permitted IPs** , **System Log-Out**, and **Software Update**.

Chief administrator configures and manages the BM-2101 appliance. The administrator can add, delete or modify system settings and monitor system status while sub-administrator (title named by first MIS engineer) is read-only.

# Administrator

## Administrator

- The title of chief administrator and sub administrator. Administrator is the default name and cannot be removed. But other sub administrator can be modified or removed.



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



The default chief administrator can add or modify the other admin to be the sub admin or chief admin , otherwise the other chief admin can modify its privilege to be the sub admin but can not be deleted . The BM-2101 appliance still force to reserve a chief admin .

## Privilege

- Chief administrator has the **Write/Read** privilege. Administrator is allowed to modify the configurations, monitor the system status, and add or remove the other administrator .
- Sub administrator only has **Read** privilege. He is allowed to view and monitor data, but cannot modify the configurations.

## Password/New Password/Confirm Password :

- Can add or modify the password of chief / sub administrator .

## 2.1 Admin

Step1. Click **Admin** → **New Sub-Admin** .

Step2. In **Add New Sub Admin** , add the settings :

- **Sub Admin name:** sub\_admin.
- **Password:** 12345.
- **Confirm Password:** 12345.



If select **Write Access** and **View Log & Privilege**, the new sub-admin becomes chief admin.

Step3. Click **OK** for the user to log in, or click **Cancel** to cancel adding new sub admin.

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="checkbox"/> Write Access	
<input type="checkbox"/> View Log & Report Privilege	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

**Add new sub admin**

Step1. In **Admin**, select the admin to change , correspond to the **Configure**→**Modify**.

Step2. In **Modify Admin Password** , enter the following information:

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

Step3. Click **OK** to change the password, or click **Cancel** to cancel the modification

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 checked="" type="checkbox"/> Write Access	
<input checked="" type="checkbox"/> View Log & Report Privilege	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

**Modify admin password**

## 2.2 Permitted IPs

Step1. In **Administration** → **Permitted IPs** → **New Entry** , add the settings :

- **Name** : Enter master
- **IP Address** : Enter 163.173.56.11
- **Netmask** : Enter 255.255.255.255
- **Service** : Check Ping, HTTP and HTTPS
- Click **OK**
- Complete adding **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 checked="" type="checkbox"/> HTTPS

### Add new Permitted IPs

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

### Complete add new Permitted IPs



To activate Permitted IPs, click **Interface** → **LAN, WAN, and DMZ** to uncheck **Ping, HTTP, and HTTPS**. However, **Permitted IPs** must be set before the cancellation of HTTP and HTTPS, or MIS engineer can not enter BM-2101's Web UI via the appointed interface.

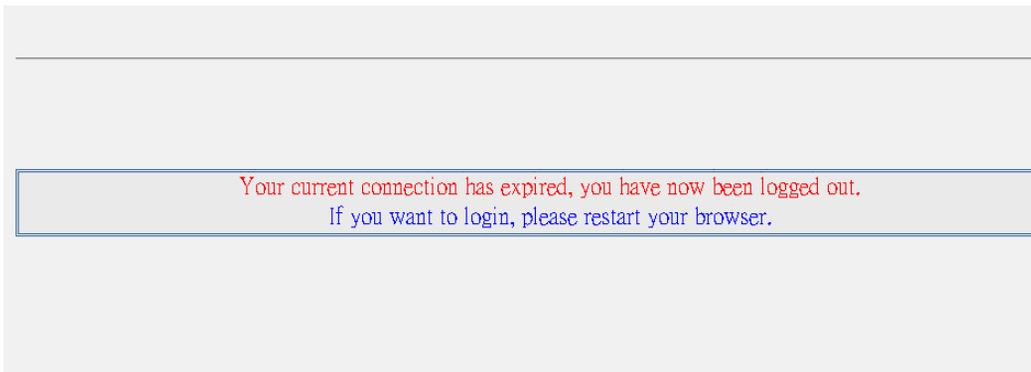
## 2.3 System Log Out

Step1. Click the Logged icon at the upper right of the WebUI. The MIS engineer can log out the system anytime, to prevent the other person change the setting through other PC.



**Confirm to log out**

Step2. Click **OK** . It shows the logout message.

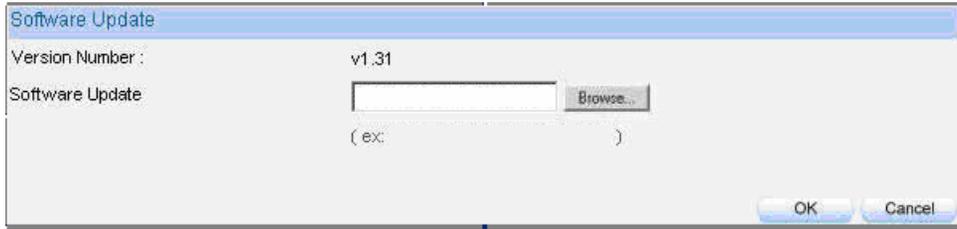


**Log out message**

## 2.4 Software Update

Step1. In **System**→**Administration**→**Software Update** :

- In **Version Number**, to know the version number, then connect to network and download the latest version in the BM-2101 appliance.
- Click **Browse** → **Choose File** , select the latest update file and open it.
- Click **OK** to run automatic software update.



**Firmware update**



It takes 3 minutes to run software update then the system will restart. Please do not turn off the system or quit the web page during the update process, or it will cause an unpredictable error (It is recommended to update through LAN).

## Chapter 3

# Configure

The configuration here is about the basic operating settings of the BM-2101 appliance. In this Chapter, it will be defined as **Setting, Date/Time, Multiple Subnet, Route Table, DHCP, Dynamic DNS, Host Table, SNMP, and Language.**

## Setting

### Bandwidth Management Gateway Configuration

- The MIS engineer can export or import system setting files and reset factory setting

### System Name Setting

- The administrator can set the device name.

### E-mail Setting

- Enabling this function and the BM-2101 appliance will automatically send instant e-mail alert notification to the MIS engineer when the system be attacked or some urgent events occurred .

### Web Management

- The MIS engineer can remote the BM-2101 appliance anywhere via Web UI. In addition, the MIS engineer can change the used port number in BM-2101's remote management .
- Set up the idle timeout as the MIS engineer log into the BM-2101 appliance. The BM-2101 appliance will forced to logout the Web UI as the MIS engineer did not process any system monitoring or management.



After changing HTTP or HTTPS port number, if the MIS engineer want to log in to Web UI from the WAN , he must change the web browser's port when log in to Web UI ( For example , <http://61.62.108.172:8080> and <https://61.62.108.172:1025> )

### MTU Setting

- The MIS engineer can modify the length of the sent and received packets anytime. The default value is 1500 Bytes.

## Dynamic Routing (RIPv2)

- By enable LAN, WAN or DMZ Port to send and receive RIPv2 packets, the BM-2101 appliance can communicate with internal or external routers and dynamically update the route table. ( The MIS engineer can set up routing information update timer and routing information timeout when it stopp to receive the RIPv2 packets and the router will automatically cancel the dynamic routing table according to the setting.)

## Administration Packet Logging

- After enabled this function, the system will record the source or destination packet information of BM-2101 in **Monitor** → **Log** → **Traffic** for the MIS engineer to query.

## Date / Time

### Synchronize System Clock

- Synchronize the BM-2101 appliance time to the MIS engineer's PC or the external time server.

### GMT

- International Standard Time (Greenwich Mean Time)

## Multiple Subnet

### WAN Interface IP

- The WAN interface IP which a multiple subnet corresponds to.

### Forwarding Mode

- To indicate the multiple subnet use NAT or Routing mode.

### Interface

- To indicate the multiple subnet interface is LAN or DMZ interface.

## Alias IP of Interface/Netmask

- The multiple subnet segment range.

## NAT Mode

- Allow the internal network to set up multiple subnet addresses and connect to network via different WAN IP addresses. For example , the company applies several real IP addresses 168.85.88.0/24 for its lease line, and the company is divided into R&D, Customer Service, Sales, Procurement, Accounting Department. For easy management, assignate different IP segment for each department. The settings are as the following :

R&D Dep.	192.168.1.1/24(Internal) ↔ 168.85.88.253(External)
Customer Service Dep.	192.168.2.1/24(Internal) ↔ 168.85.88.252(External)
Sales Dep.	192.168.3.1/24(Internal) ↔ 168.85.88.251(External)
Procurement Dep.	192.168.4.1/24(Internal) ↔ 168.85.88.250(External)
Accounting Dep.	192.168.5.1/24(Internal) ↔ 168.85.88.249(External)

R&D Dep. has already been set up in **Interface** configurations, so set up the reserving four departments by adding 4 new Multiple Subnets . After completing the settings, every department can connect to network via its own WAN IP address. The settings of each department are as the following :

	Customer 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
Netmask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Default Gateway	192.168.2.1	192.168.3.1	192.168.4.1	192.168.5.1

## Routing Mode

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

## **DHCP**

### **Subnet**

- The domain belongs to internet network.

### **Netmask**

- The domain name netmask belongs to the internet network.

### **Gateway**

- Internal network default gateway.

### **Broadcast**

- LAN broadcast address.

## **Dynamic DNS**

### **Domain Name**

- The domain name that the MIS engineer applied from the DDNS provider.

### **WAN IP**

- The real IP which the domain name correspond to.

## **Host Table**

### **Host Name**

- Customized by the MIS engineer. The internal user can access the resources provided by a corresponded host.

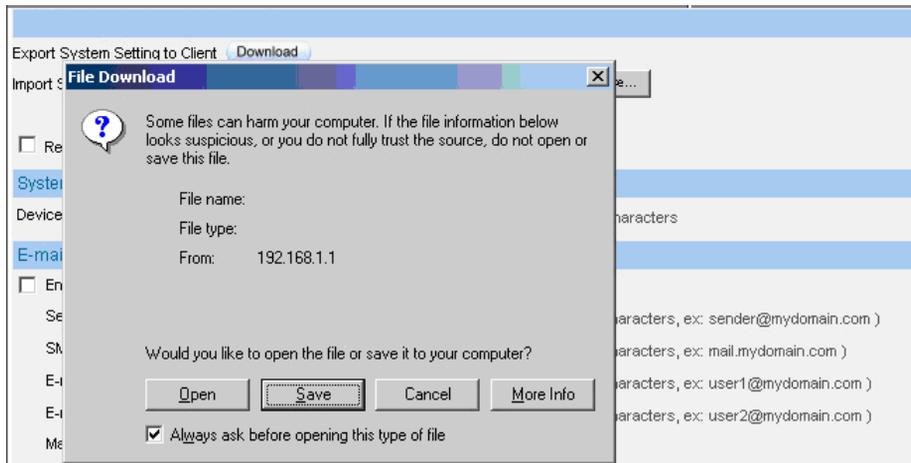
### **Virtual IP Address**

- The mapped virtual IP Address correspond to the host name. It must be the LAN or DMZ IP address.

## 3.1 Setting

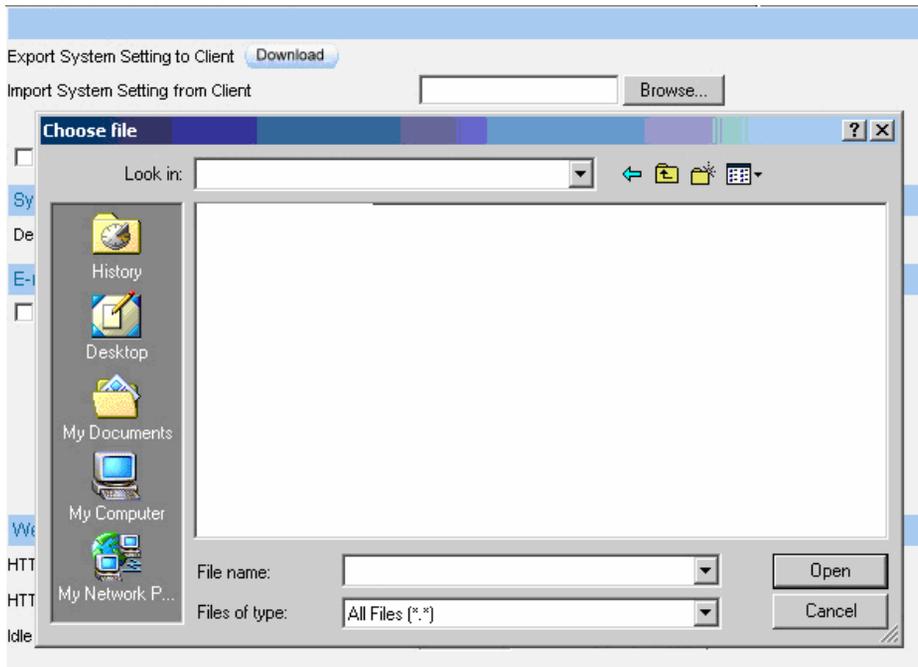
Step1. In **System**→**Configure**→**Setting** →**Bandwidth Management Gateway Configuration** , click **Download** near **Export System Setting to Client**.

Step2. In **File Download** window , click **Save** . Then, choose the destination location to save the exported file. Finally, click **Save** for BM-2101 to copy the configuration file to the oppointed storage location.

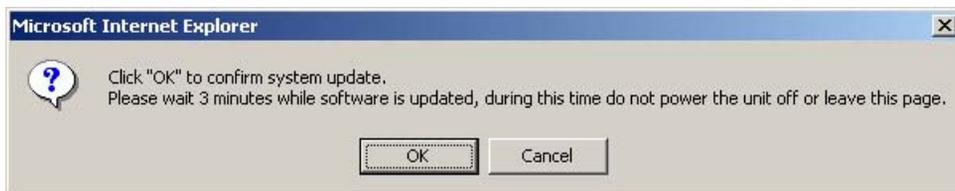


**Choose the location to save files**

- Step1. In **Setting** window, click **Browse** near **Import System Setting from Client**.
- Step2. In **Choose File** window, select the previously saved settings and click **Open**.
- Step3. Click **Open**, and a confirmation dialogue box pop out.
- Step4. Click the **OK** to import the configuration file.



**Import the file**



**To confirm to import the file**

Step1. In **Setting** → **Bandwidth Management Gateway Configuration** , select **Restore Factory Setting**.

Step2. Click **OK** to restore the default settings

The screenshot shows a configuration page with several sections. At the top, there are options for 'Export System Setting to Client' (with a 'Download' button) and 'Import System Setting from Client' (with a text input field and a 'Browse...' button). Below this, the 'Reset Factory Setting' checkbox is checked. The 'System Name Setting' section contains a 'Device Name' input field with a '( Max. 30 characters )' label. The 'E-mail Setting' section includes an unchecked 'Enable E-mail Alert Notification' checkbox, followed by four input fields for 'Sender Address', 'SMTP Server', 'E-mail Address 1', and 'E-mail Address 2', each with a '( Max. 60 characters, ex: sender@mydomain.com )' label. Below these are two more input fields for 'Username' and 'Password' under the 'Enable SMTP Server Authentication' checkbox, and a 'Mail Test' button.

**Restore to factory setting**

Step1. **Device Name** : Enter the BM-2101 name.

Step2. In **E-Mail Setting**→**Enable Email Alert Notification** .

Step3. **Sender Address** : Enter the sender's email address. (Required by some ISP).

Step4. **SMTP Server** : Enter the IP address of the SMTP server.

Step5. **E-mail Address 1** : Enter the first e-mail address to receive the notification.

Step6. **E-mail Address 2** : Enter the second e-mail address to receive the notification.

Step7. Click **OK** to enable this function.

The screenshot shows a configuration window with two sections. The top section, titled "System Name Setting", contains a "Device Name" field with a placeholder and a "( Max. 30 characters )" label. The bottom section, titled "E-mail Setting", contains several options and fields. A checkbox labeled "Enable E-mail Alert Notification" is checked. Below it are four rows, each with a label and a text input field: "Sender Address" (placeholder: sender@mydomain.com, label: ( Max. 60 characters, ex: sender@mydomain.com )), "SMTP Server" (placeholder: mail.mydomain.com, label: ( Max. 80 characters, ex: mail.mydomain.com )), "E-mail Address 1" (placeholder: user1@mydomain.com, label: ( Max. 60 characters, ex: user1@mydomain.com )), and "E-mail Address 2" (placeholder: user2@mydomain.com, label: ( Max. 60 characters, ex: user2@mydomain.com )). Below these is an unchecked checkbox labeled "Enable SMTP Server Authentication". Underneath are "Username" and "Password" fields. At the bottom right is a "Mail Test" button.

**Enable e-mail alert notification**



Click **Mail Test** to test if e-mail address 1 and e-mail address 2 can receive the notification or not.



If the MIS engineer want to send the mails via the authentication, then he must **Enable SMTP Server Authentication.**

Step1. To restart the BM-2101 appliance, Click **Reboot** near **Reboot Bandwidth Management Gateway Appliance**.

Step2. It shows the confirm dialogue of **Are you sure to reboot ?**

Step3. Click **OK** to restart, or click **Cancel** to terminate the action.



**Start to reboot**

## 3.2 Date / Time

Step1. Select **Enable synchronize with an Internet time Server.**

Step2. **Set offset hours from GMT** , select the correct option.

Step3. Enter the time server's IP address in **Server IP / Name.**

Step4. Enter the update time.

System time : Tue Jul 18 16:32:56 2006

Synchronize system clock

Enable synchronize with an Internet time Server:

Set offset  hours from GMT [Assist](#)

Enable daylight saving time setting

From  /  To  /

Server IP / Name  [Assist](#)

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

---

Synchronize system clock with this client

Set system clock



Click **Sync** near **Synchronize system clock with this client**, to synchronize the BM-2101 time to the MIS engineer's PC.



Click **Assist** near **Set Offset From GMT** or **Server IP / Name** to consult the setting value.

### **3.3 Multiple Subnet**

Internal user use the IP address to link the internet via the multiple subnet NAT or Routing mode.

#### **Preparations**

Connect the BM-2101 appliance WAN 1(10.10.10.1 ) to the ISP's Router (10.10.10.2).

The segment is 162.172.50.0/24 (Distributed by the ISP).

Connect the BM-2101's WAN 2 ( 211.22.22.22 ) to ATUR to link to the network.

Step1. Click **Configure** → **Multiple Subnet** :

- Click **New Entry** .
- **Interface** : select **LAN**
- **Alias IP of Interface** : enter 162.172.50.1
- **Netmask** : enter 255.255.255.0
- **WAN 1**: 10.10.10.1 , **Forwarding Mode** : select routing
- **WAN 2**: 211.22.22.22 , **Forwarding Mode** : select NAT
- Click **OK** .
- Complete to add new multiple subnet IP.

Add New Multiple Subnet IP			
Interface	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ		
Alias IP of Interface	<input type="text" value="162.172.50.1"/>		
Netmask	<input type="text" value="255.255.0.0"/>		
WAN Interface IP		Forwarding Mode	
WAN1	<input type="text" value="0.0.0.0"/> <a href="#">Assist</a>	<input type="radio"/> NAT	<input checked="" type="radio"/> Routing
WAN2	<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 new multiple subnet IP**

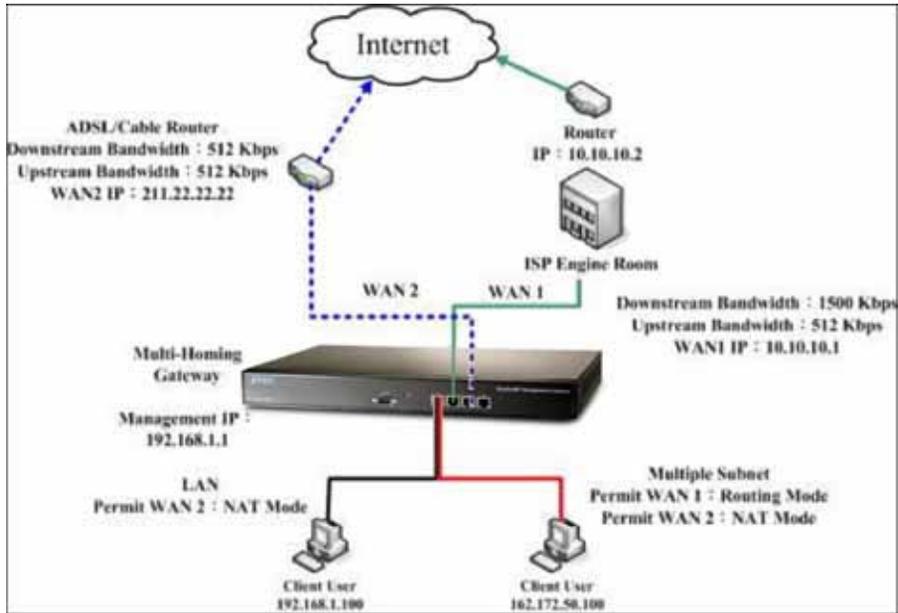


Can enter the interface IP of **WAN 1 & WAN 2** by **Assist**.



After completed the settings, there are two LAN segment 192.168.1.0/24 (the default LAN segment) and 162.172.50.0/24. Therefore, if the LAN IP is :

- 192.168.1.xx –Use the NAT Mode to connect to the network (As regulated in **Policy**, one can only connect to network via WAN2. If use Routing mode via WAN 1, an virtual IP can't be used to connect to network).
- 162.172.50.xx—WAN 1: Routing mode (MIS engineer IP 162.172.50.xx can be seen by the internet server ) ; WAN2: NAT mode (The IP seen by the internet server is WAN2's IP)



Multiple Subnet deployment

- **BM-2101 Interface :**  
 WAN1 IP : 10.10.10.1  
 WAN2 IP : 211.22.22.22  
 LAN Port IP : 192.168.1.1  
 LAN Port Multiple Subnet : 162.172.50.1

### 3.4 Route Table

Internet Make the Router which deploy in two different segment can link to the internet via the BM-2101 appliance.

## Preparations

### Company A

Connect WAN 1 ( 61.11.11.11 ) to ATUR and link to network.

Connect WAN 2 ( 211.22.22.22 ) to ATUR and link to network.

LAN segment is 192.168.1.1/24.

LAN Router1 ( 10.10.10.1, supporting RIPv2 ) , the LAN segment is 192.168.10.1/24.

### Company B

Router2 ( 10.10.10.2, supporting RIPv2 ) , the LAN segment is 192.168.20.1/24.

Company A's Router1 ( 10.10.10.1 ) is connected to B company's Router2 ( 10.10.10.2 ) by lease line directly.

Step1. In **Configure** → **Route Table** :

- **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"/>

**Add new static route-1**

Step2. In **Configure** → **Route Table**

- **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"/>

**Add new static route-2**

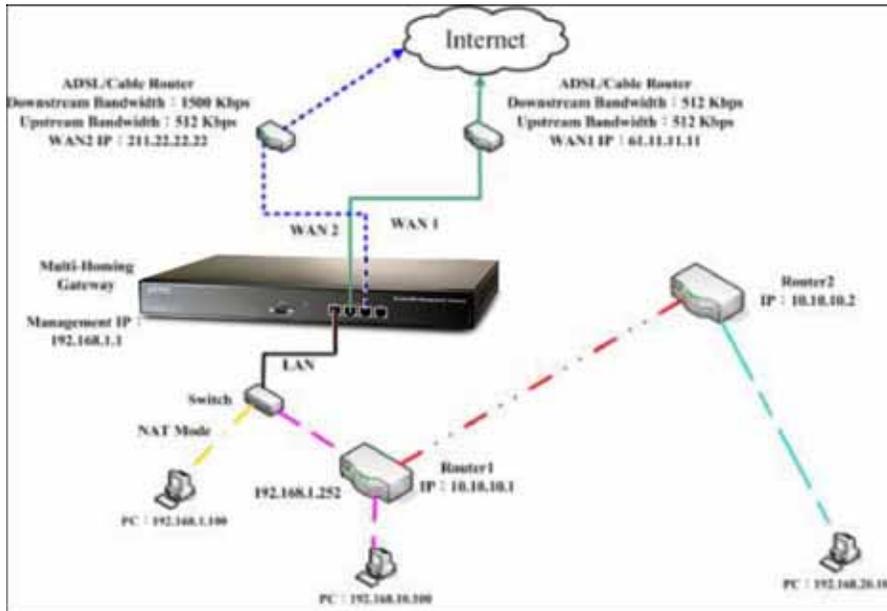
Step3. In **Configure** → **Route Table** :

- **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"/> ▼

**Add new static route -3**

Step4. As completed all. The BM-2101 appliance can translate the virtual IP to real IP. Therefore, the LAN subnet PC 192.168.10.1/24, 192.168.20.1/24 and 192.168.1.1/24 can communicate to each other via the BM-2101 appliance.



Route table environment

## 3.5 DHCP

Step1. In **Configure → DHCP** , to select and set the following setting :

- **Domain Name:** Enter the domain name in private LAN .
- **DNS Server 1:** Enter the IP address distributed to DNS server 1.
- **DNS Server 2:** Enter the IP address distributed to DNS server 2.
- **WINS Server 1:** Enter the IP address distributed to WIN server 1.
- **WINS Server 2:** Enter the IP Address distributed to WIN server 2.
- **LAN Interface:**
  - ◆ Client IP range 1: Enter the first starting and ending IP address, the default value is 192.168.1.2 to 192.168.1.254. (it must be at the same domain).
  - ◆ Client IP range 2: Enter the second starting and ending IP addresss (it must be at the same domain as Client Range 1).
- **DMZ Interface** : Set as the LAN interface address. (Except to enable **DMZ Interface** , click **Interface→DMZ** .)
- **Leased Time** : The lease time of the dynamic IP, and the default value is 24 hours.
- Click **OK** .
- Complete **DHCP** settings.

Dynamic IP Address			
Subnet	192.168.1.0	Netmask	255.255.255.0
Gateway	192.168.1.1	Broadcast	192.168.1.255

---

Enable DHCP Support

Domain Name  ( Max. 40 characters, ex: dhcp.domain\_name )

Automatically Get DNS

DNS Server 1

DNS Server 2

WINS Server 1

WINS Server 2

LAN Interface :

Client IP Range 1  To

Client IP Range 2  To

DMZ Interface :

Client IP Range 1  To

Client IP Range 2  To

Leased Time  hours ( Range: 0 - 99999 )

### DHCP setting



When the LAN network adaptor set to **Automatically Get DNS**. The DNS Server will auto lock the LAN interface IP . ( Note : When enabled the **Authentication** , the first DNS server must correspond to the LAN interface IP).

## 3.6 DDNS

Step1. In **Configure** → **DDNS** .

- Click **New Entry** .
- **Service Provider** : Select from the drop-down menu.
- Select **Automatically** and select a WAN interface to correspond from the menu.
- **User Name** and **Password** : Enter the applied name and password.
- **Domain Name** : Enter the applied domain name.
- Click **OK** .
- Complete **DDNS** setting.

Add New Dynamic DNS	
Service Provider :	NO-IP (www.no-ip.com) [ U.S.A. ] <a href="#">Sign up</a>
WAN IP:	61.11.11.11 <input checked="" type="checkbox"/> Automatically vWAN1
User Name :	<input type="text"/> (Max. 59 characters)
Password :	<input type="password"/> (Max. 44 characters)
Domain Name:	<input type="text"/> . no-ip.org (Max. 34 characters)
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

### DDNS setting

i	Domain Name	WAN IP	Configure
<input checked="" type="checkbox"/>		61.11.11.11	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
<input type="button" value="New Entry"/>			

### Complete the DDNS setting

Icon				
Connotation	Connection Succeed	Wrong Password	Connecting	Errors



If the MIS engineer have not apply the DDNS account, then he can choose the proper DDNS supplier, click **Sign up**, and then it will display the registration web page.



If the MIS engineer do not select **Automatically correspond to the WAN interface Address**, then they can enter the specific IP at **WAN IP**. It can let DDNS correspond to the static IP.

## 3.7 Host Table

Step1. In **Connfigure** → **Host Table** :

- **Host Name** enter the customerized domain name
- **Virtual IP Address** enter the host name that correspond to the virtual IP address.
- Click **OK** .
- Complete **Host Table** setting

Add New Host Table	
Host Name	<input type="text" value="www.fileserver.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 )

**Host table setting**



Use the Host Table of the BM-2101 appliance, the first DNS Server in Client PC must correspond to the LAN or DMZ Port IP; that is the default gateway of the computer.

## 3.8 SNMP

Step1. In **Configure** → **SNMP** → **Enable SNMP Agent** and enter the following setting :

- **Appliance Name** : Can customize the name. Default setting is Bandwidth Management Gateway.
- **Appliance Location** : Can customize the settings. Default setting is Taipei, Taiwan.
- **Community** : Can customize the settings. Default setting is public.
- **Contact Person** : Can customize the settings. Default setting is root@public.
- **Description** : Can customize the settings. Default setting is Multi Home Appliance.
- Click **OK** .
- Complete the **SNMP Agent** settings. The MIS engineer can monitor BM-2101'S operating status by the SNMP Agent message recipient installed in administrator's PC.



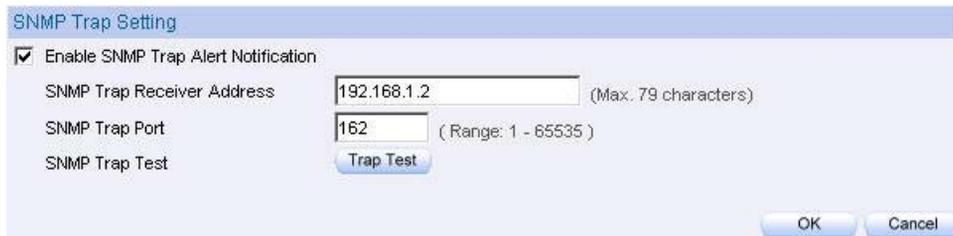
The screenshot shows a configuration window titled "SNMP Agent Setting". It contains a checked checkbox for "Enable SNMP Agent". Below this are five input fields, each with a label and a "(Max. 255 characters)" note:

Appliance Name		(Max. 255 characters)
Appliance Location	Taipei, Taiwan.	(Max. 255 characters)
Community	public	(Max. 255 characters)
Contact Person	root@public	(Max. 255 characters)
Description		(Max. 255 characters)

**SNMP Agent setting**

Step1. In **Configure** → **SNMP** , select **Enable SNMP Trap Alert Notification** and enter the following setting :

- **SNMP Trap Recipient Address**, enter SNMP trap recipient IP.
- **SNMP Trap Port** : Enter the port number. (Default value: 162).
- Click **OK** .
- Complete the **SNMP Trap** setting. The MIS engineer can use the SNMP Trap software and receive the alarm notification from the BM-2101 appliance. ( it will send the notification about connection / disconnection and the attacks information to the SNMP Trap recipient address.



SNMP Trap Setting

Enable SNMP Trap Alert Notification

SNMP Trap Receiver Address: 192.168.1.2 (Max. 79 characters)

SNMP Trap Port: 162 ( Range: 1 - 65535 )

SNMP Trap Test: Trap Test

OK Cancel

**SNMP Trap setting**



The MIS engineer can click **Trap Test** to test if SNMP Trap can work normally.

### 3.9 Language

Step1. In **Configure** → **Language** to select the language, Click **OK**.



Select language

## Chapter 4

# Interface

The so called interface included the LAN and WAN of the BM-2101 appliance.

In **Interface**, the MIS engineer can set the IP address, netmask, gateway address, and define the WAN and LAN IP address, all depends on the chosen ISP connection.

## Interface

### LAN

- Can set up the LAN network .

### Ping

- Can test the IP via Ethernet interface.

### HTTP

- From the Ethernet interface to the BM-2101 WebUI through HTTP.

### HTTPS

- From the Ethernet interface to the BM-2101 Web UI through HTTPS.

### WAN

- Can set the external connection.

### Balance Mode

- **Auto** : Can auto adjust the usage of WAN depends on the downstream and upstream status . (Suitable for the user who use different downstream bandwidth)
- **Round-Robin** : Forced to use the 1:1 cycling distribution of network download connection (it is appropriate to the users who use the same download bandwidth.)
- **By Traffic** : Allocate the download bandwidth by accumulated network flow.
- **By Session** : Adjust the WAN connection depends on the saturated connections.
- **By Packet** : Allocate the download bandwidth by accumulated packets .

## Connect Mode

- The WAN network connection mode can be divided into :
  - ◆ PPPoE ( ADSL user )
  - ◆ Dynamic IP Address (cable modem user)
  - ◆ Static IP address (static connection or ADSL static line users )

## Saturated Connections

- Can set the WAN connections depend on the traffic , connections and packets.

## Priority

- Set the WAN interface priority by balance mode choice.

## Service

- To test if the WAN can work or not. The testing includes two parts :
  - ◆ ICMP : Ping the IP to see if the connection can work.
  - ◆ DNS : Use the domain name to see if the connection can work.

## Downstream Bandwidth and Upstream Bandwidth

- Can set the proper bandwidth of the WAN interface.

## The Idle Time

- As the WAN interface set to be the PPPoE (ADSL users ) settings, the MIS engineer can set the idle time when the WAN port is not in use. (Its unit is minute)

## DMZ

- Can set the DMZ in the BM-2101 appliance.
- The DMZ includes two modes :
  - ◆ NAT : The DMZ is an isolated virtual domain. (but it can not be at the same segment as LAN).
  - ◆ TRANSPARENT : The DMZ and WAN interface are both in the same domain .

We set 4 environments.

No.	Range	The Application Environment
Example 1	<b>LAN</b>	Modify the LAN interface address.
Example 2	<b>WAN</b>	Set the WAN interface address.
Example 3	<b>DMZ</b>	Set the DMZ interface address ( NAT mode ) .
Example 4	<b>DMZ</b>	Set the DMZ interface address ( DMZ_Transparent mode ) .

## 4.1 LAN

Modify the LAN Interface Address

Step1. In **Interface** → **LAN** to enter the following settings :

- Enter the new LAN **IP Address** and **Netmask** .
- Select **Ping**, **HTTP** and **HTTPS**.
- Click **OK**



LAN Interface

IP Address: 192.168.200.1

Netmask: 255.255.255.0

Enable:  Ping  HTTP  HTTPS

OK Cancel

**LAN Interface IP setting**



The default LAN interface address is 192.168.1.1. After the MIS engineer has modified the LAN IP address, he has to set the PC to obtain the latest IP, then use the modified LAN interface IP address to log in Web UI. ( When the PC set to obtain the IP by DHCP )



Before set the **Permitted IP** , never uncheck HTTP and HTTPS or the MIS engineer will not able to log in the BM-2101 Web UI via LAN.

## 4.2 WAN

Set the WAN Interface Address

Step1. **Interface** → **WAN**, click **Modify** of **WAN 1** .



WAN 2 Interface's settings are almost the same as WAN 1 setting. The difference is that WAN 2 has the additional **Disable** function. The MIS engineer can use this function to disable WAN Interface 2.

WAN2 Interface		Disable			
Service :	DNS	Disable	DNS Server IP Address :	168.95.1.1	<a href="#">Assist</a>
		Enable			

**Disable the WAN Interface**

Step2. The way to test the connection (ICMP and DNS) :

- ICMP: enter the persistent ping IP.( Or click **Assist** ).
- DNS : enter the DNS server IP address and domain name (Or click **Assist**).
- Sets the interval seconds during the packets transferring ( per seconds).

WAN1 Interface

Service :  Alive Indicator Site IP :  [Assist](#)

Wait  seconds between sending alive packet.

ICMP test

WAN1 Interface

Service :  DNS Server IP Address :  [Assist](#)

Domain name :  [Assist](#)

Wait  seconds between sending alive packet. (0 - 99 , 0 : means not checking)

DNS test



Both of the two connection test is the standard to see if the WAN can work properly. The testing such as the IP address, IP address for DNS server and the domain name all must be working forever long , or it will make the BM-2101 appliance error.

Step3. Choose the network connection .

■ PPPoE (ADSL User)

1. Select **PPPoE (ADSL User)**
2. Enter **User Name** as an account.
3. **Password** as the applied password.
4. Select **Dynamic** or **Fixed** in **IP Address provided by ISP**. It depends on the user's network status , click **Fixed** option, please enter the **IP address, Netmask and Default Gateway**.
5. Enter **Max. Downstream Bandwidth** and **Max. Upstream Bandwidth** ( It depends on the network bandwidth which the user applied .)
6. Select **Ping** , **HTTP** , and **HTTPS**
7. Click **OK** .

PPPoE (ADSL User)  
 Dynamic IP Address (Cable Modem User)  
 Static IP Address

Current Status: Disconnected

IP Address: 0.0.0.0

User Name:  (Max. 60 characters)

Password:  (Max. 60 characters)

IP Address provided by ISP:
   
 Dynamic
   
 Fixed

IP Address:   
 Netmask:   
 Default Gateway:

Max. Downstream Bandwidth:  Kbps (Range: 1 - 102400)

Max. Upstream Bandwidth:  Kbps (Range: 1 - 102400)

Auto Disconnect if idle  minutes (Range: 1 - 99999, 0: means always connected)

Enable System Management:
   
 Ping     HTTP     HTTPS

**Select PPPoE**

Balance Mode:  (Auto recommended)

WAN No.	Connect Mode	IP Address	Saturated Connections	Ping	HTTP	HTTPS	Configure	Priority
1	PPPoE	61.228.170.252	<input type="text" value="1"/>	✓	✓	✓	<input type="button" value="Modify"/>	<input type="text" value="1"/>
2	(Disable)	---	<input type="text" value="0"/>	---	---	---	<input type="button" value="Modify"/>	<input type="text" value="0"/>

**Complete PPPoE setting**



If use the PPPoE , the MIS engineer can set the WAN interface auto connect when it disconnect (it is recommended enable this function ) or set the WAN interface disconnect as idle. ( Not Recommended ) .

■ **Dynamic IP Address** ( cable modem user )

1. Click **Dynamic IP Address** .
2. Click **IP Address**→**Renew** , then get the Dynamic IP .
3. If the ISP require to enter the MAC address , Click **MAC Address**→**Clone MAC**, then get the MAC address .
4. **User Name** : Require by the ISP to enter the provided user name .
5. **Domain Name** : Require by the ISP to enter the provided domain name .
6. **Username** and **Password** : The IP machenism of DHCP+authentication. ( According to the ISP in Mainland Cnina )
7. Enter **DownstreamBandwidth** and **Upstream Bandwitdth**( According to the bandwidth which applied by the user)
8. Select **Ping** , **HTTP** and **HTTPS** .
9. Click **OK** .

The screenshot shows a network configuration window with the following fields and options:

- PPPoE (ADSL User)
- Dynamic IP Address** (Cable Modem User)
- Static IP Address

Fields and buttons:

- IP Address: 0.0.0.0 (Buttons: Renew, Release)
- MAC Address: [ ] (Button: Clone MAC)
- Hostname: [ ] (Max. 50 characters)
- Domain Name: [ ] (Max. 80 characters)
- User Name (Required by DHCP+ protocol): [ ] (Max. 127 characters)
- Password (Required by DHCP+ protocol): [ ] (Max. 127 characters)
- Max. Downstream Bandwidth: [512] Kbps (Range: 1 - 102400)
- Max. Upstream Bandwidth: [512] Kbps (Range: 1 - 102400)
- Enable System Management:  Ping,  HTTP,  HTTPS

Buttons: OK, Cancel

Select Dynamic IP address

Balance Mode:  (Auto recommended)

WAN No	Connect Mode	IP Address	Saturated Connections	Ping	HTTP	HTTPS	Configure	Priority
1	Dynamic IP	210.33.241.25	1	✓	✓	✓	Modify...	1
2	(Disable)	---	0	---	---	---	Modify...	0

**Complete to set the Dynamic IP address**

■ Static IP address ( For Static or ADSL user )

1. Select **Static IP Address** .
2. Enter **IP Address , Netmask and Default Gateway** .
3. Enter **DNS Server 1** or **DNS Server 2** .
4. Enter **Max. Downstream Bandwidth** and **Max. Upstream** ( According to the bandwidth applied by the user)
5. Select **Ping , HTTP** and **HTTPS** .
6. Click **OK**

The screenshot shows a network configuration window with the following settings:

- Radio buttons for connection type:  PPPoE (ADSL User),  Dynamic IP Address (Cable Modem User), and  Static IP Address.
- Text input fields for: IP Address (221.22.22.18), Netmask (255.255.255.0), Default Gateway (221.22.22.17), DNS Server 1 (168.95.1.1), and DNS Server 2 (empty).
- Text input fields for bandwidth: Max. Downstream Bandwidth (512 Kbps) and Max. Upstream Bandwidth (512 Kbps), both with a range of 1 - 102400.
- Checkboxes for system management:  Ping,  HTTP, and  HTTPS.
- Buttons for OK and Cancel at the bottom right.

**Set the Static IP address**

Balance Mode : <input type="text" value="Auto"/> ( Auto recommended )								
WAN No.	Connect Mode	IP Address	Saturated Connections	Ping	HTTP	HTTPS	Configure	Priority
1	Static IP	221.22.22.18	<input type="text" value="1"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="Modify"/>	<input type="text" value="1"/>
2	(Disable)	---	<input type="text" value="0"/>	---	---	---	<input type="button" value="Modify"/>	<input type="text" value="0"/>

### Complete to set the Static IP address



In WAN 2 Interface, the MIS engineer has no need to set the DNS server as setting the Static IP address.



When selecting Ping , HTTP and HTTPS in WAN interface , the user can ping the BM-2101 appliance and its WebUI . This action may cause the network security problem. It's recommended do not select the Ping, HTTP, and HTTPS after confirming all the setting is completed . If the MIS engineer want to log in to the WebUI through WAN, he can use **System → Administration → Permitted IPs** .

## 4.3 DMZ

Set up DMZ Interface (NAT Mode)

Step1. In **Interface** → **DMZ** .

Step2. In **DMZ Interface**, select **NAT** mode.

■ In **DMZ Interface** , select **NAT** from the drop-down menu.

■ Enter the value in **IP Address** and **Netmask** .

Step3. Select **Ping** , **HTTP** and **HTTPS** .

Step4. Click **OK**



The screenshot shows a configuration window titled "DMZ Interface" with a dropdown menu set to "NAT". Below this, there are two input fields: "IP Address" containing "192.168.33.1" and "Netmask" containing "255.255.255.0". Under the "Enable" section, three checkboxes are checked: "Ping", "HTTP", and "HTTPS". At the bottom right, there are "OK" and "Cancel" buttons.

Select the NAT mode

## Set up DMZ Interface (Transparent Mode)

Step1. In **Interface** → **DMZ** .

Step2. In **DMZ Interface**, select **Transparent Mode**.

- In **DMZ Interface**, select **DMZ\_ Transparent Mode** from the drop-down menu .

Step3. Select **Ping** , **HTTP** , and **HTTPS** .

Step4. Click **OK**



DMZ Interface: DMZ\_TRANSPARENT

IP Address: 0.0.0.0

Netmask: 0.0.0.0

Enable:  Ping  HTTP  HTTPS

OK Cancel

Select DMZ transparent mode



The MIS engineer has to set the static IP address in WAN interface and select the DMZ\_TRANSPARENT mode in DMZ interface.

## Chapter 5

# Address

In this chapter , it includes the definition of the chief MIS engineer , LAN , LAN group , WAN , WAN group , DMZ and DMZ group.

The IP address recorded in **Address** is probably a host IP address , or represents many IP address in the Domain .The MIS engineer can set an easy to identify name to represent the IP address . Basically , the IP address can be divided into three types : internal IP address , WAN IP address and DMZ IP address. The MIS can apply the different IP address packets filtering rules to the same policy , he can set these IP address in LAN group , WAN group or DMZ group.



After finished the Address setting, the MIS engineer can apply the address setting to the policy( source address or destination address) . In other words , the Address setting must be set before the policy setting , so that it can show the correct IP Address in Address setting.

## **Address**

### **Name**

- The MIS engineer can set the easy to identify name of IP address .

### **IP**

- It can be a host IP address or one of the domain IP address. It included three different types : internal IP address , external IP address and DMZ IP address .

### **Netmask**

- Correspond to the single static IP address , the setting must be : 255.255.255.255.
- Correspond to many IP address in a specific domain . For example, IP Address 192.168.100.1 in C Class segment , the setting must be 255.255.255.0 .

### **MAC Address**

- Mapped the MAC address to its IP address . It can prevent the user to modify the IP address and access the unauthorized network service through the policy .

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

- When enable this function , LAN or DMZ will get the PC 's IP address via the DHCP server in the BM-2101 appliance, and the PC's IP address will correspond to the MAC address.

We set two environments.

No.	Range	The Application Environment
Example 1	<b>LAN</b>	When use the DHCP, to distribute the static IPaddress to the specific user and limit the user can only access the FTP resources through policy .
Example 2	<b>LAN Group and WAN</b>	To set the policy which allow part of users connect to the remote static IPaddress.

## 5.1 Example

When use the DHCP, to distribute the static IP address to the specific user and limit the user can only access the FTP resources through policy.

Step1. In **Address**→**LAN** , make the setting as following :

- Click **New Entry**.
- **Name** , enter the user's identified name , Rayearth .
- **IP Address**, enter the user's IP 192.168.3.2 .
- **Netmask** , enter 255.255.255.255 .
- **MAC Address** , enter MAC address 00:B0:18:25:F5:89 .
- Select **Get static IP address from DHCP Server** .
- Click **OK**

Add New Address	
Name	Rayearth (Max. 16 characters)
IP Address	192.168.3.2
Netmask	255.255.255.255 ( 255.255.255.255 means the specified PC ) ( 255.255.255.0 means class C subnet )
MAC Address	00:B0:18:25:F5:89 <a href="#">Clone MAC</a>
<input checked="" type="checkbox"/> Get static IP address from DHCP Server.	
<a href="#">OK</a> <a href="#">Cancel</a>	

### LAN address setting

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		<a href="#">In Use</a>
Rayearth	192.168.3.2/255.255.255.255	00:B0:18:25:F5:89	<a href="#">Modify</a> <a href="#">Remove</a>
<a href="#">New Entry</a>			

### Complete the LAN address setting

Step2. In **Policy** → **Outgoing** , add the new settings :

Comment :  (Max. 64 characters)

Add New Policy	
Source Address	Rayearth
Destination Address	Outside_Any
Service	FTP
Schedule	None
Authentication User	None
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download <input type="checkbox"/> Upload
QoS	None
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	0 MBytes ( Range: 0 - 999999 )

OK   Cancel

**Limit the single user accessing the network resources through specific service**

Step3. In **Policy** → **Outgoing** , to complete the settings to appointed the static IP to the specific user and limit the user can only accessing FTP resources 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

New Entry

**Complete the settings to limit the single user accessing the network resources through policy**



When the MIS engineer set the Address settings , he can click **Clone MAC** , in order to let the BM-2101 can automatically copy the user's network adapter MAC address .



In **Address → LAN** , the BM-2101 appliance will automatically set an **Inside\_Any Address** , it represents the whole LAN . The WAN or DMZ also has **its Outside\_Any and DMZ\_Any** default address setting to represents its whole domain .



In **Address→WAN and DMZ** , the setting is the same as **LAN** . The only difference is that the WAN can not set the MAC address .

To set the policy which allow part of users connect to the remote static IP address.

Step1. Set many LAN address.

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		<b>In Use</b>
Rayearth	192.168.1.2/255.255.255.255		<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		<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		<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

**Set many LAN address**

Step2. In Address → LAN Group , to set the setting as following :

- Click **New Entry**.
- To set the group **Name** .
- In available address , select the user in the group and click **Add** .
- Click **OK** .

Add New Address Group

Name:  (Max. 16 characters)

< --- Available address --->

- Rayearth
- Josh
- SinSan
- Daniel
- Luke

< --- Selected address --->

- Rayearth
- Josh
- SinSan

Remove

Add

OK Cancel

### Group the LAN address

Name	Member	Configure
TestTeam	Rayearth, Josh, SinSan	Modify Remove Pause

New Entry

### Complete to group the LAN address



In Address → WAN Group and DMZ Group , the setting is the same as LAN Group .

Step3. In **Address** → **WAN** , add the setting as following :

- Click **New Entry**
- Enter the remote static IP information . ( **Name , IP , 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"/>	

#### Set the 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 to set the WAN address

Step4. To apply **Step 1~3** to Policy.

Comment :  (Max. 64 characters)

**Add New Policy**

Source Address	TestTeam
Destination Address	Yahoo
Service	ANY
Schedule	None
Authentication User	None
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download <input type="checkbox"/> Upload
QoS	None
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	0 MBytes ( Range: 0 - 999999 )

**Apply the 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 <input type="text" value="1"/>

**Complete the policy setting**



The Address function works by apply it to policy.

## Chapter 6

# Service

The TCP Protocol and UDP Protocol can provide different services and every service has its TCP port or UDP port number . For example , TELNET(23) , FTP(21), SMTP(25) , POP3(110) , and so on . The Service function includes two parts : Pre-defined and Custom .

The Pre-defined included the common used and pre-identified TCP service or UDP service .This kind of service can not be modified and canceled . On the other hand , the user can set the proper TCP and UDP port number in Custom Service function.. When sets the Custom Service function , the Client port number range is 1024 to 65535, the server port is 0 to 65535 .

In this chapter , we will introduce the three common use services , for example , Pre-defined , Custom and Group. The MIS engineer can define the Protocol and port number in every network applied communication by the following steps . The client port can transfer the data by using different server.



How to use the Service ?

In **Service → Group** , the MIS engineer can add the new group name. In the Group function , the MIS engineer can simply many process when setting the policy . For example, there are 10 different IP address to access 5 different services via the server, for example, such as the HTTP , FTP , SMTP , POP3 and TELNET . If the MIS engineer do not use the Group function , he has to set 50 policy ( $10 \times 5 = 50$ ) . Actually the MIS engineer only need to apply these services to the service group with one policy.

## Service

### Pre-defined

Icon	The Definition
	Any service .
	TCP service , for example , FTP , FINGER , HTTP , HTTPS , IMAP , SMTP , POP3 , ANY , AOL , BGP , GOPHER , InterLocator , IRC , L2TP , LDAP , NetMeeting , NNTP , PPTPReal , Media , RLOGIN , SSH , TCP ANY , TELNET , VDO Live , WAIS , WINFRAME , X-WINDOWS .
	UDP service , for example , IKE , DNS , NTP , IRC , RIP , SNMP , SYSLOG , TALK , TFTP , UDP-ANY , UUCP .
	ICMP service , for example, PING , TRACEROUTE .

### Service name

- The MIS engineer can define the service name.

### Protocol

- The Protocol that is made of the communication between the devices. It included the TCP and UDP mode .

### Client Port

- The Port number of the network adapter of the Client PC , the range is 1024 to 65535 , it is recommended to use the default range .

### Server Port

- The MIS engineer can enter the port number in Custom Service function.

We set two environments.

No .	Range	The application environment
Example . 1	<b>Custom</b>	To permit the WAN user communicate to LAN user via the network phone through policy . ( VoIP port number : TCP 1720 , TCP 15328-15333 , UDP 15328-15333 )
Example . 2	<b>Group</b>	To group the services , and limit the specific user accessing the network resources which provided by the group service through Policy. ( Gruop : HTTP , POP3 , SMTP , DNS )

## 6.1 Custom

To permit the WAN user communicate to LAN user via the network phone through policy . ( VoIP port number : TCP 1720 , TCP 15328-15333 , UDP 15328-15333 )

Step1. In **Address** → **LAN** and **LAN Group** , add the following setting :

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		<b>In Use</b>
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](#)

### LAN address setting

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

[New Entry](#)

### Group the LAN address

Step2. In **Service** → **Custom** add the setting as following :

- Click **New Entry** .
- **Service NAME**, enter the default name , VoIP .
- **Protocol # 1** , select TCP , **Client Port** 's setting reserve the default value , **Server Port** , enter the value of 1720 : 1720 .
- **Protocol #2** , select TCP , **Client Port** 's setting reserve the default value , **Server Port** , enter the value of 15328 : 15333 .
- **Protocol #3** , select UDP , **Client Port** 's setting reserve the default value , **Server Port** , enter the value of 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

OK Cancel

**Custom setting**

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

New Entry

**Complete the VoIP custom setting**



Normally , the default client port number is 0 to 65535. It is recommended not to modify the port number range in **Custom Service** function .



To enter the the port number in the client port , if the MIS engineer have to enter two different port number in server port, then enter the range of 15328 :15333 . To enter the same port number in the server port , the MIS engineer have to enter two same port number , for example, enter the range of 1720 : 1720.

Step3. Apply the **Service** setting to **Virtual Server** .

Virtual Server Real IP

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"/>

Apply the service setting to virtual server

Step4. Apply **Virtual Service** to **Policy** → **Incoming**

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server1(61.62.236.53)	VoIP	✔		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 ▾

Complete to set the incoming VoIP policy

Step5. In **Policy** → **Outgoing** , to complete the Outgoing VoIP setting .

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 ▾

Complete to set the outgoing VoIP policy



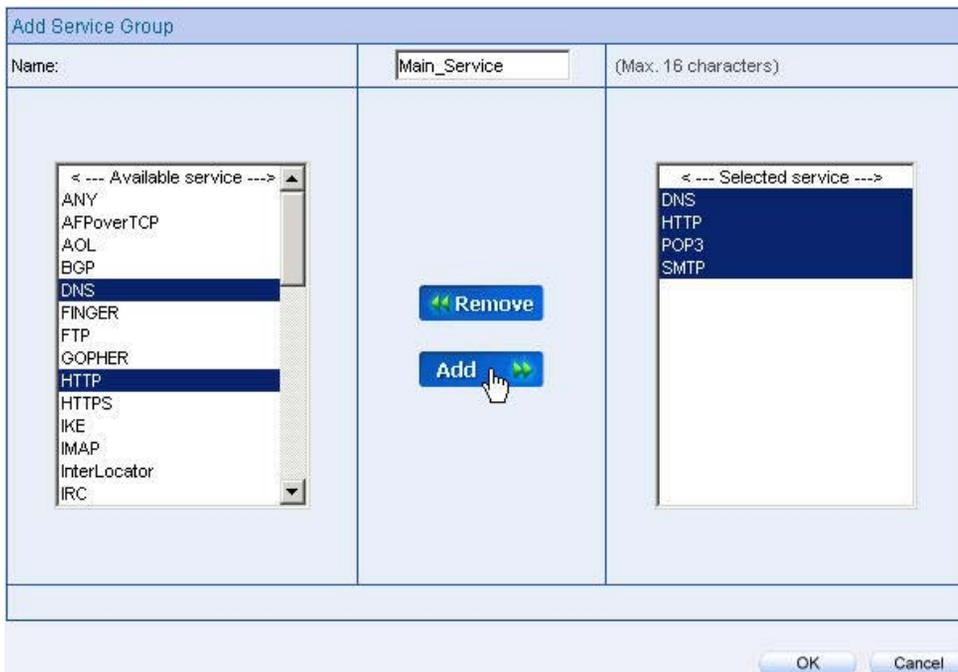
The service setting must apply to **Policy** and **Virtual Server** , to make it real working .

## 6.2 Group

To Group the Service , and limit the user can only access the Network resources provided by the Group through Policy Object . ( Group : HTTP , POP3 , SMTP , DNS )

Step1. In **Service → Group** , add the new setting as following :

- Click **New Entry** .
- Set the **Name** to be the default name of **Main\_Service** .
- In **Available service** , select HTTP , POP3 , SMTP , DNS , Click **Add**.
- Click **OK** .



Service group setting

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

### Complete the service group setting



If the MIS engineer want to remove the group service , then he can choose the **Selected service** , and click **Remove** .

Step2. In **Address** → **LAN Group**, to set the LAN group ,which can only access the specific service.

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

[New Entry](#)

**LAN group setting**

Step3. Apply **Service Group** to **Policy** → **Outgoing** .

Source	Destination	Service	Action	Option	Configure	Move
laboratory	Outside_Any	Man_Service	✓		<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>	To 1 ▾

[New Entry](#)

**Policy setting**

## Chapter 7

# Schedule

In this chapter , the MIS engineer can difine the network connection and the process time period in Schedule. In other words , the MIS engineer can select the specific time period to transfer the data packets by policy management.



How to use Schedule ?

The MIS engineer can use the Schedule function to auto set the packets flow in different time period by **Policy** management.

To set the valid time of LAN user can access the network data everyday through the policy management.

Step1. In **Schedule** , add the new setting as following :

- Click **New Entry**
- Set the **Schedule Name** .
- Use the drop down menu to select the time period everyday .
- Click **OK**

Add New Schedule

Schedule Name:  (Max. 16 characters)

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

OK Cancel

Schedule setting

Name	Configure
WorkingTime	Modify Remove

New Entry

Complete the schedule setting

Step2. Apply schedule setting to **Policy** → **Outgoing**

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 <input type="text" value="1"/>

Complete to apply the schedule setting to policy



The **Schedule** setting must apply into **Policy**.

## Chapter 8

# QoS

The BM-2101 appliance can manage the downstream and upstream bandwidth through the bandwidth parameter setting .

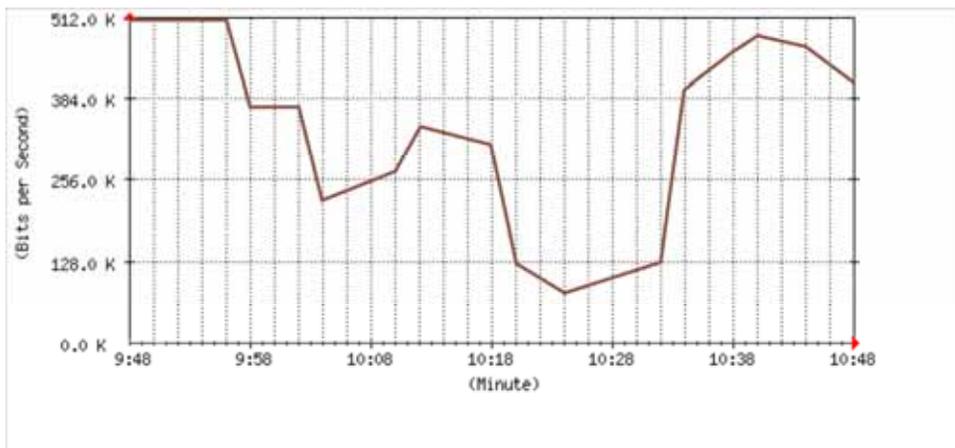
The MIS engineer can set the bandwidth depends on the provided WAN bandwidth.

**Downstream Bandwidth** : Can set the G.Bandwidth and M.Bandwidth .

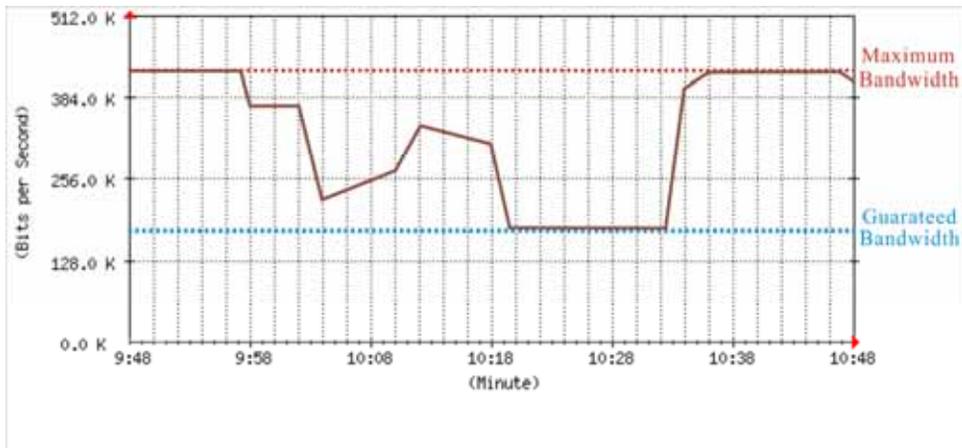
**Upstream Bandwidth** : Can set the G.Bandwidth and M.Bandwidth .

**QoS Priority** : Can set the QoS priority of upstream and downstream bandwidth .

The BM-2101 appliance can set the outgoing bandwidth depends on different QoS , and can select the proper QoS setting by policy . It can let the MIS engineer efficiently to distribute the bandwidth.



Unused QoS Flow



The used QoS Flow (M.Bandwidth : 400 Kbps , G.Bandwidth : 200Kbps)

## QoS

### WAN

- Includes WAN 1 and WAN 2.

### Downstream Bandwidth

- The maximum bandwidth and guarantee bandwidth of downstream bandwidth.

### Upstream Bandwidth

- The maximum bandwidth and guarantee bandwidth of upstream bandwidth.

### QoS Priority

- To set the unused upstream and downstream bandwidth in QoS priority .

### G.Bandwidth

- The basic bandwidth in QoS. The **policy** which applied to the QoS , will at least reserve the QoS settings .

### M.Bandwidth

- The maximum bandwidth in QoS. The **Policy** which applied to the QoS, its bandwidth will not over the QoS Setting .

## 8.1 Example

To set the Policy of the Upstream Bandwidth and Downstream Bandwidth .

Step1. In **QoS** , add the new setting as following :

- Click **New Entry**
- In **Name**, to set the QoS name.
- In WAN 1 , 2 , enter the parameter of limited bandwidth .
- To select the **QoS Priority**.
- Click **OK** .

Add New QoS				
Name <input type="text" value="Policy_QoS"/> (Max. 16 characters)				
WAN	Downstream Bandwidth	Upstream Bandwidth	QoS Priority	
1	G.Bandwidth = <input type="text" value="200"/> Kbps( Range: 1 - 102300 ) M.Bandwidth = <input type="text" value="400"/> Kbps( Range: 1 - 102400 )	G.Bandwidth = <input type="text" value="200"/> Kbps( Range: 1 - 462 ) M.Bandwidth = <input type="text" value="400"/> Kbps( Range: 1 - 512 )	Middle ▾	
2	G.Bandwidth = <input type="text" value="300"/> Kbps( Range: 1 - 101900 ) M.Bandwidth = <input type="text" value="400"/> Kbps( Range: 1 - 102400 )	G.Bandwidth = <input type="text" value="50"/> Kbps( Range: 1 - 102350 ) M.Bandwidth = <input type="text" value="64"/> Kbps( Range: 1 - 102400 )		
<input type="button" value="OK"/> <input type="button" value="Cancel"/>				

### QoS setting

Total entry : 1

Name ▾	WAN	Downstream Bandwidth	Upstream Bandwidth	Priority	Configure
Policy_QoS	1	G.Bandwidth = 200 Kbps M.Bandwidth = 400 Kbps	G.Bandwidth = 200 Kbps M.Bandwidth = 400 Kbps	Middle	<input type="button" value="Modify"/>
	2	G.Bandwidth = 300 Kbps M.Bandwidth = 400 Kbps	G.Bandwidth = 50 Kbps M.Bandwidth = 64 Kbps		<input type="button" value="Remove"/>
<input type="button" value="New Entry"/>					

### Complete the QoS setting

Step2. In **Policy** → **Outgoing** , to apply the QoS Setting in **Step 1**

Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download <input type="checkbox"/> Upload
QoS	Policy_QoS ▾
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )

**Set the QoS 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 ▾

**Complete to set the QoS policy**



When the MIS engineer setting the QoS , he must use the correct upstream and downstream bandwidth range set in **interface** → **WAN**.

## Chapter 9

# Authentication

The BM-2101 appliance can manage the user's connection by authentication. The user has to pass the authentication to connect the network .

The BM-2101 appliance provided 4 authentication modes . The **User** and **User Group** built in ; others are **RADIUS** , **POP3** and **LDAP** self-built Authentication Server. The MIS engineer can use the 5 modes , to manage the authentication.

# Authentication

## Authentication Management

- It can provide the authentication port to the MIS engineer and the valid authentication time . (The MIS engineer has to set the Authentication function first .)
- ◆ **Authentication Port** : When enable the Authentication, the LAN user must pass the authentication to login to the WAN. And the authentication port number is the default value of 82 .
- ◆ **Re-Login if Idle** : When the LAN user connect to the WAN , the MIS engineer can set the Idle time after the Authentication. When the login Idle time has over the default Idle time settings of 30 minutes . The authentication will automatically invalid .
- ◆ **Re-Login after user login successfully** : When the LAN user connect to the WAN through the authentication . The available authentication time depends on the time limit , if over the default time setting , the authentication will be invalid .
- ◆ **Disallow Re-Login if the auth user has login** : When enable this function through **User ,User Group , RADIUS , POP3** or **LDAP** to access the authentication , the authorized account can not be used by other people .
- ◆ **URL to redirect when authentication succeed** : To direct the authorized LAN user to the assigned web site . The default value is blank . ( It will directly link the user to the login web site .
- ◆ **Messages to display when user login** : It shows the login messages in the authentication window ( it supports the HTML ) , the default setting is blank ( it will not show any message in the authentication window. )

- To add the settings in the authentication management :

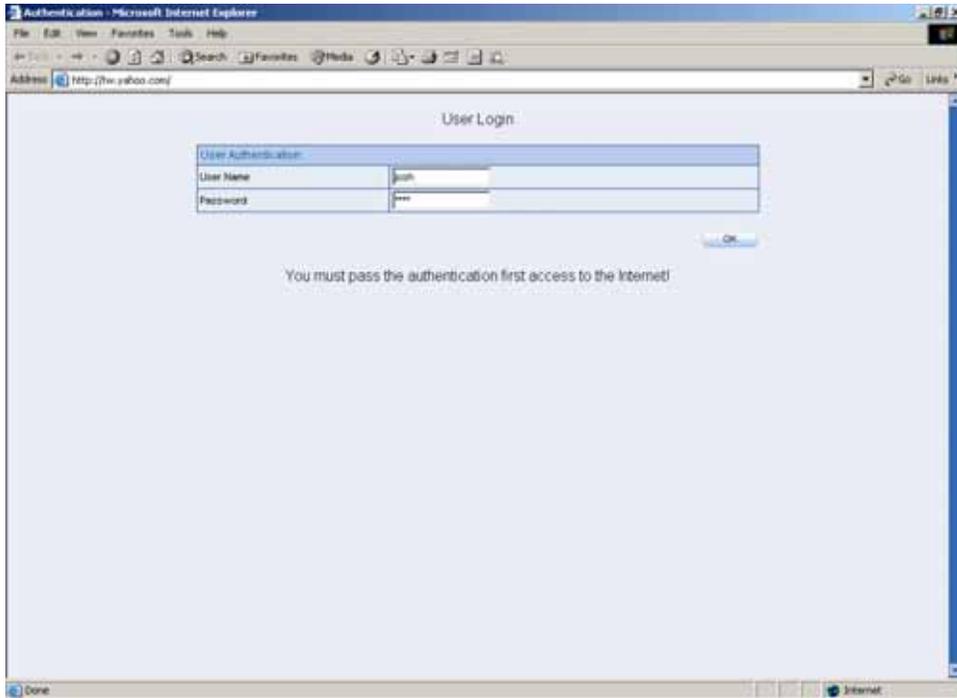
The screenshot shows a configuration window titled "Authentication Management". It contains several input fields and a text area:

- Authentication Port:** A text box containing "82" with a range of "1 - 65535".
- Re-Login if Idle:** A text box containing "30" with a range of "1 - 1000" and the unit "Minutes".
- Re-Login after user login successfully:** A text box containing "0" with a range of "0 - 24, 0: means unlimited" and the unit "Hours".
- Disallow Re-Login if the auth user has login**
- URL to redirect when authentication succeed:** An empty text box with a range of "( Max. 60 characters )".
- Messages to display when user login:** A text area containing the message "You must pass the Authentication first access to the Internet!".

At the bottom right, there are "OK" and "Cancel" buttons.

### Authentication management

When the user connect to the WAN through the authentication , it shows the following window :



**Login Authentication**

After the authentication , it will redirect to the assigned web site.



If the user want to require the authentication , then he can enter the BM-2101's LAN interface IP and the authenticaion port number in the URL address , then shows the authentication window.

### **Authenticatoin- User Name**

- The user's authentication account.

### **Password**

- Create the authentication password.

### **Confirm Password**

- To enter the same password as in the password column .

### Shared Secret

- The required password when accessing the authentication between the BM-2101 appliance and RADIUS server .

### 802.1x RADIUS

- The authentication between the BM-2101 appliance and RADIUS server which included the wireless network.

### Search Distinguished Name

- The identify name of LDAP server .

### LDAP Filter

- To assign the specific account in LDAP server.

### User Distinguished Name

- The required account in the authentication between the BM-2101 appliance and LDAP server .

We set 4 environments.

No.	Range	The Application Environments
Example 1	<b>User User Group</b>	To plan the LAN user connect to the WAN through the authenticaton by policy . ( <b>To use the built-in user and user group authentication.</b> )
Example 2	<b>RADIUS</b>	To plan the user connect to the WAN through the authenticaton in policy . <b>To use the WAN RADIUS server ( Windows 2003 Server built-in authentication . )</b>
Example 3	<b>POP3</b>	To plan the user connect to the WAN through the authenticaton by policy.( <b>To use the WAN POP3 server authentication )</b>
Example 4	<b>LDAP</b>	To plan the user connect to the WAN through the authenticaton by policy .( <b>To use the WAN LDAP server ( Windows 2003 Server built-in authentication )</b>

## 9.1 User / User Group

To plan the LAN user connect to the WAN through the authentication by policy . ( To use the built-in user and user group authentication. )

Step1. In **Authentication** → **User** , to add the Authentication –User Name.

Authentication-User Name	Configure
joy	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
john	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
jack	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

**Set the authentication user**



The user's DNS server must correspond to the LAN interface through the BM-2101 appliance , in order to enable the authentication .

Step2. In **Authentication** → **User Group** , add the new setting as following :

- Click **New Entry** .
- **Name**, enter laboratory.
- Click **Add**, to add the available authentication user to the selected authentication user in the same user group .
- Click **OK** .
- Complete the user group settings in authentication.

The screenshot shows a dialog box 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 list boxes. The left list box is titled "< --- Available Authentication User --->" and contains the items "joy", "john", and "jack", with "joy" highlighted. Below these items are the labels "(Radius User)", "(POP3 User)", and "(LDAP User)". The right list box is titled "< --- Selected Authentication User --->" and is currently empty. Between the two list boxes are two buttons: "Remove" (with a left-pointing arrow) and "Add" (with a right-pointing arrow). A mouse cursor is pointing at the "Add" button. At the bottom right of the dialog box are "OK" and "Cancel" buttons.

**Authenticatoin setting**

Step3. In **Policy** → **Outgoing**, add a new policy , and apply the Step 1, 2 into the new policy setting .

Comment :  (Max. 64 characters)

**Add New Policy**

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	laboratory
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download <input type="checkbox"/> Upload
QoS	None
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	0 MBytes ( Range: 0 - 999999 )

OK Cancel

**Authentication user policy setting**

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY			Modify Remove Pause	To 1

New Entry

**Complete the policy setting**

Step4. When the LAN user want to connect to the network via browser , it will shows the authentication window. After enter the correct user name and password, Click **OK** , to connect to the network via the BM-2101 appliance.



The image shows a 'User Login' window with a light blue background. At the top, it says 'User Login'. Below that is a section titled 'User Authentication'. There are two input fields: 'User Name' and 'Password'. The 'User Name' field has a placeholder text '( ex: auth\_user1 )'. At the bottom right of the window is an 'OK' button.

**To create the IPSec VPN connection via the authentication**

Step5. If the remote user want to logout , click **Logout Auth-User** in **Auth-User Logout window** ( The logout window will appear when pass the authentication ) , the MIS engineer can also log in **Auth-User Logout window** ( **http:// LAN Interface : Authentication Port / logout.html** ) , click **Logout Auth-User** .



**Logout confirmation**

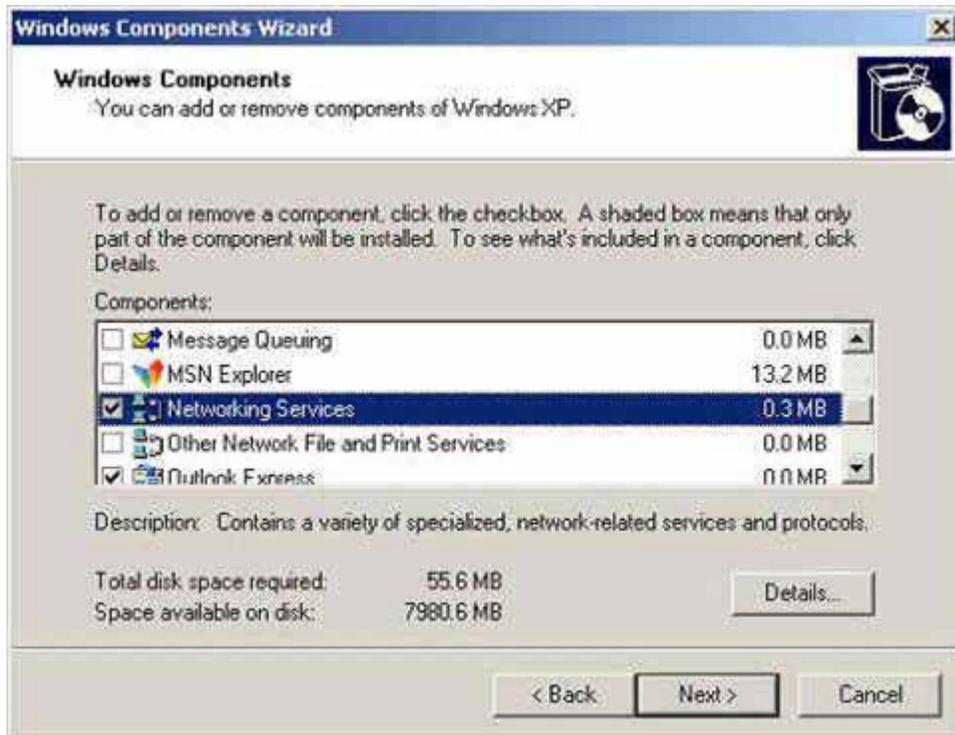
## 9.2 RADIUS

To plan the user connect to the WAN through the authentication in policy .To use the WAN RADIUS server ( Windows 2003 Server built-in authentication . )

### ※ Windows 2003 RADIUS Server Deployment

Step1. Click **Start** → **Control Panel** → **Add / Remove Programs** , select **Add / Remove Windows Components** , then it shows the **Windows Components Wizard** .

Step2. Select **Networking Services** , then click **Details** .



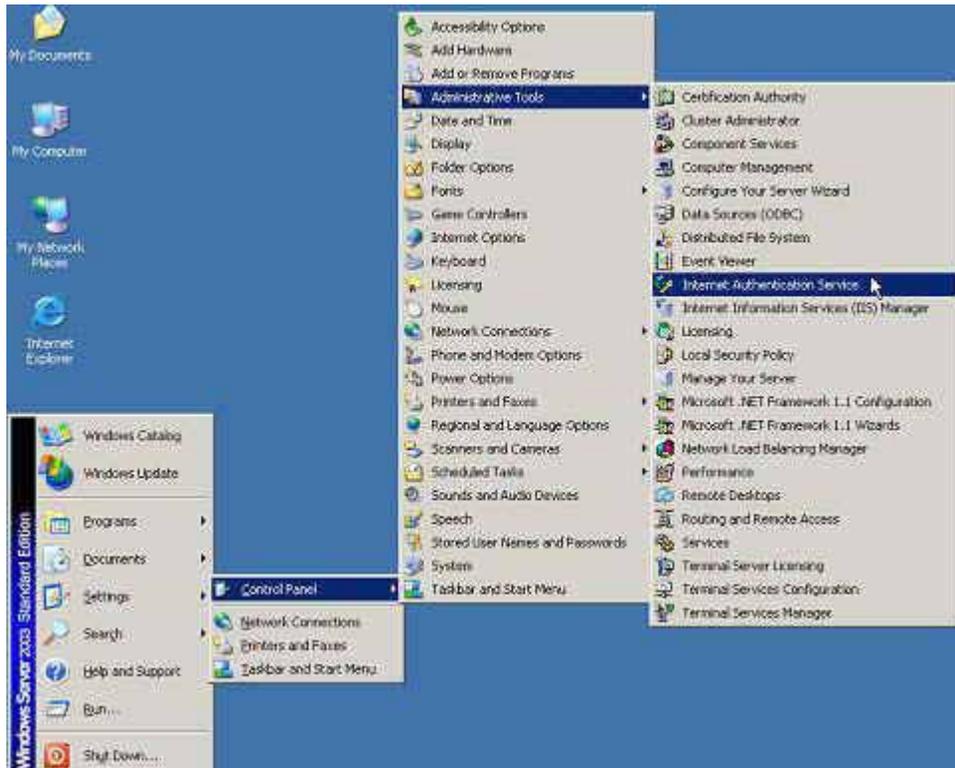
Windows Components Wizard

Step3. Select **Internet Authentication Service**



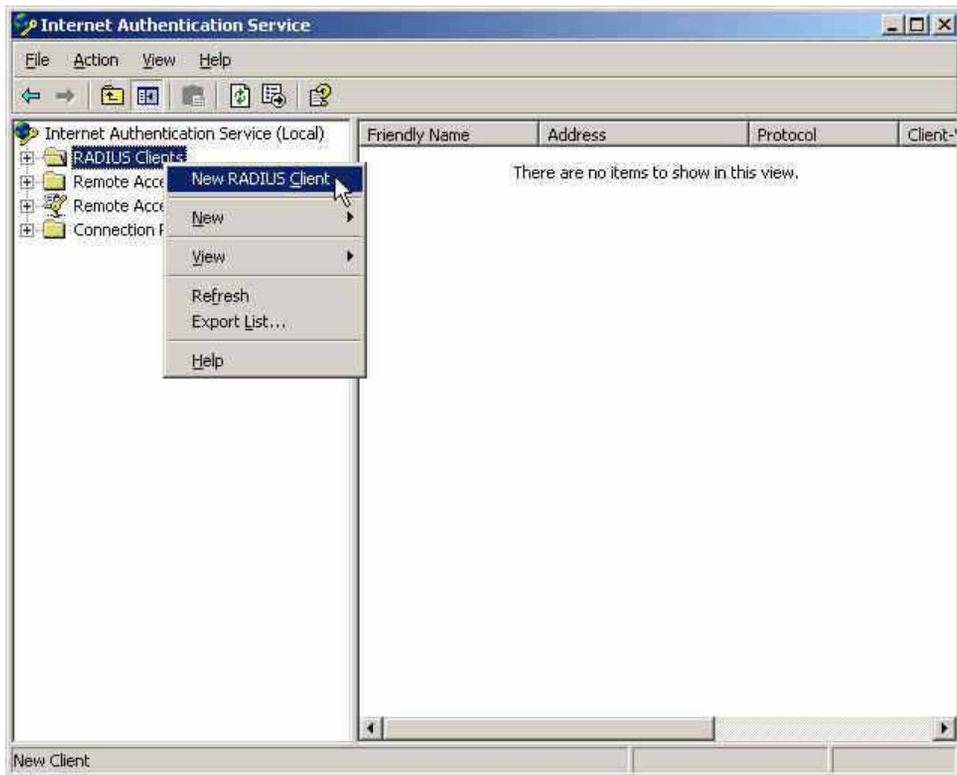
**Add new network authentication service components**

Step4. Click **Start** → **Control Panel** → **Administrative Tools** , select **Network Authentication Service** .



Select network authentication service

Step5. Right click **RADIUS Clients** → **New RADIUS Client**



**Add new RADIUS client**

Step6. Enter the **Name and Client Address** ( It is the same as BM-2101 IP address ) .

New RADIUS Client

Name and Address:

Type a friendly name and either an IP Address or DNS name for the client.

Friendly name: 254

Client address (IP or DNS): 172.19.1.254

Verify...

< Back Next > Cancel

**Add New RADIUS client name and IP address setting**

Step7. Select **RADIUS Standard** , enter the Shared secret and Confirm Shared secret . ( It must be the same setting as RADIUS in BM-2101).

New RADIUS Client

Additional Information

If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.

Client-Vendor:

RADIUS Standard

Shared secret: \*\*\*\*\*

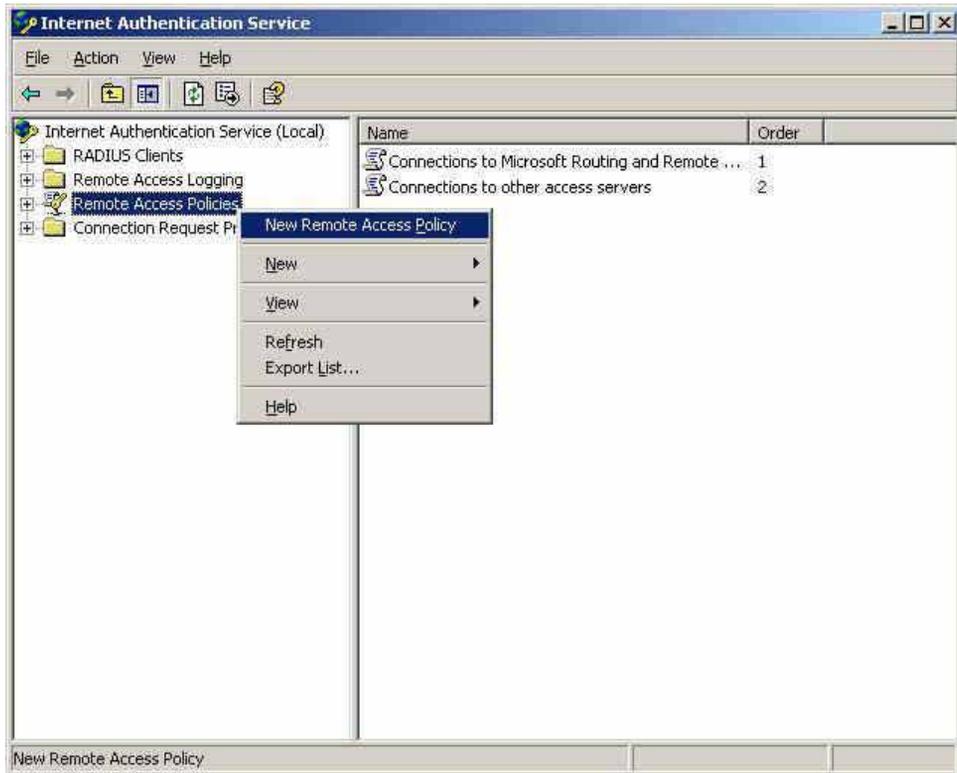
Confirm shared secret: \*\*\*\*\*

Request must contain the Message Authenticator attribute

< Back Finish Cancel

**Add new RADIUS client-vendor and shared secret**

Step8. Right click on **Remote Access Policies**→ **New Remote Access Policy**



**Add new remote access policies**

Step9. Select **Use the wizard to set up a typical policy for a common scenario** , and enter the **Policy name**

**New Remote Access Policy Wizard**

**Policy Configuration Method**  
The wizard can create a typical policy, or you can create a custom policy.

How do you want to set up this policy?

Use the wizard to set up a typical policy for a common scenario

Set up a custom policy

Type a name that describes this policy:

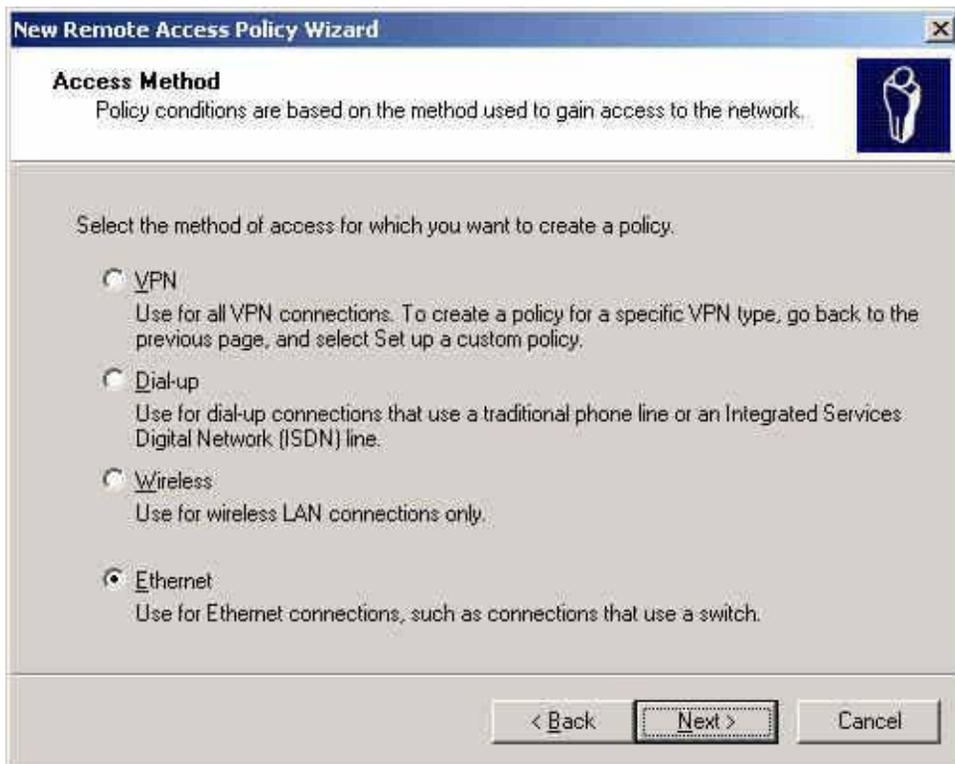
Policy name:

Example: Authenticate all VPN connections.

< Back   Next >   Cancel

**Add new remote access policies and policy name**

Step10. Select **Ethernet** .



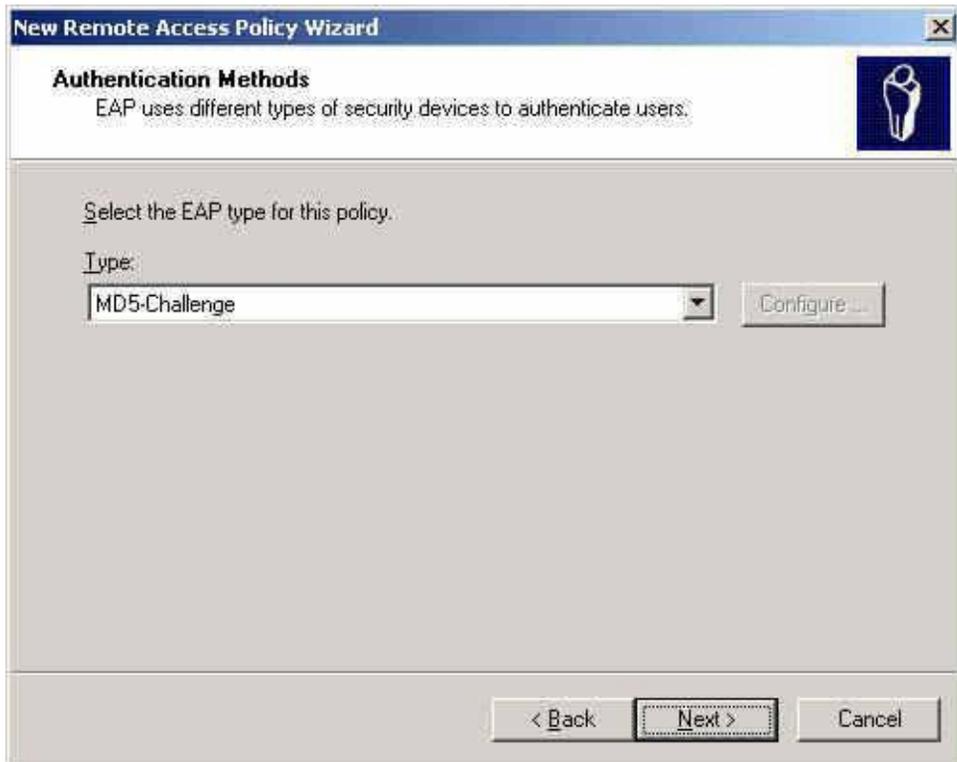
**The way to add new remote access policy**

## Step11. Select User



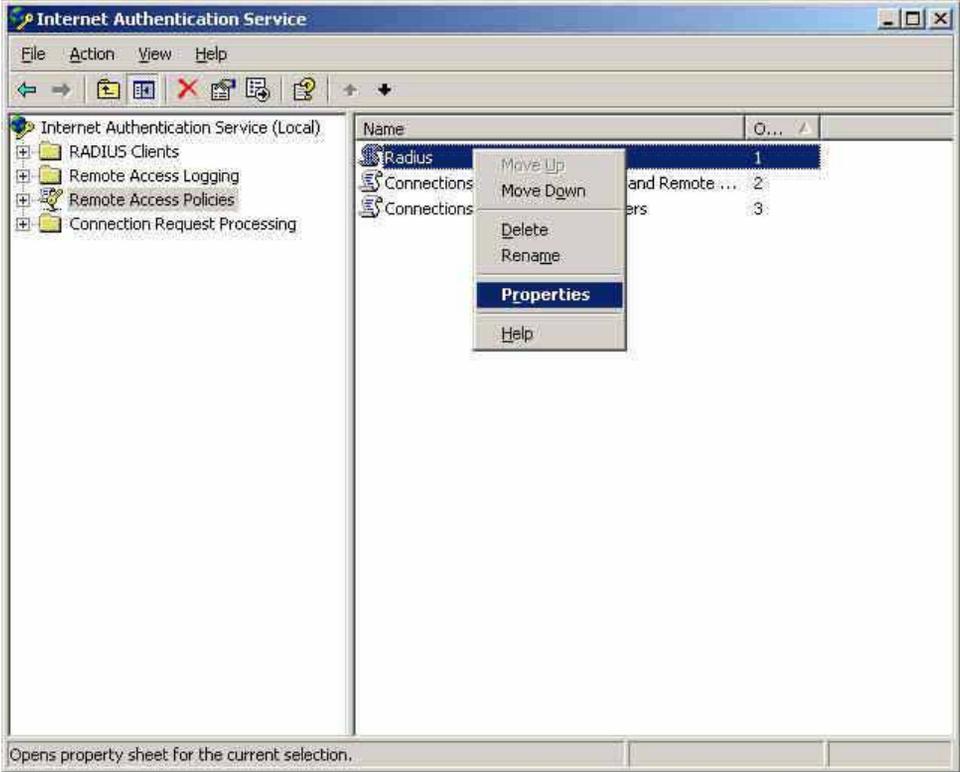
**Add new remote access policy user and group**

Step12. Select MD5-Challenge.



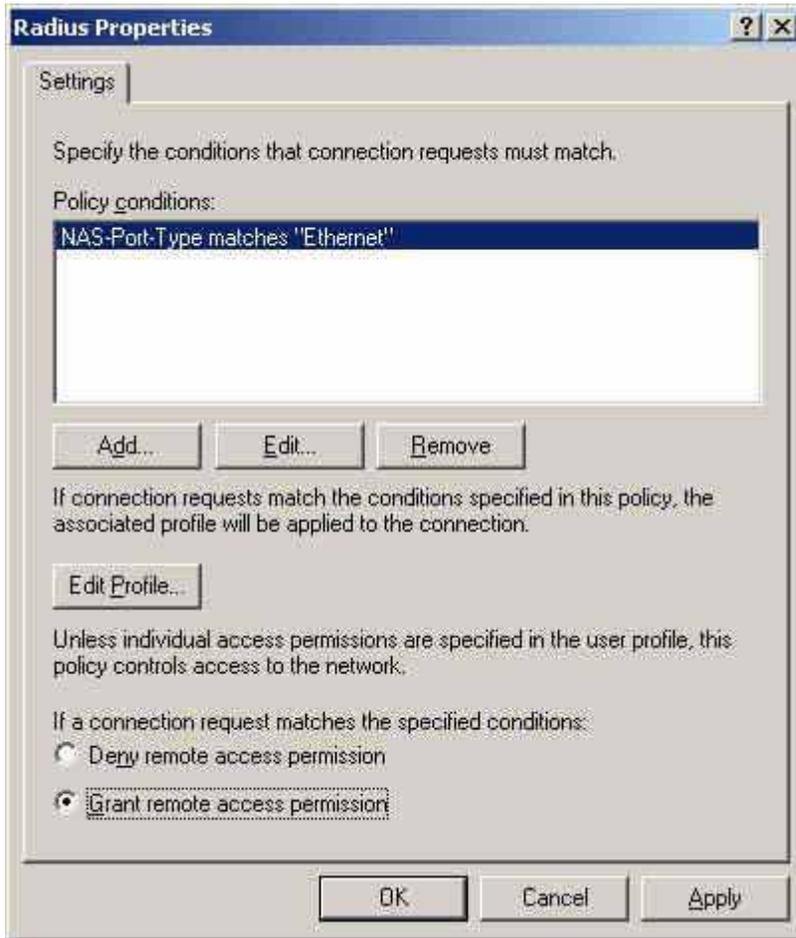
The authentication of add new remote access policy

Step13. Right click on the **Radius** → **Properties**



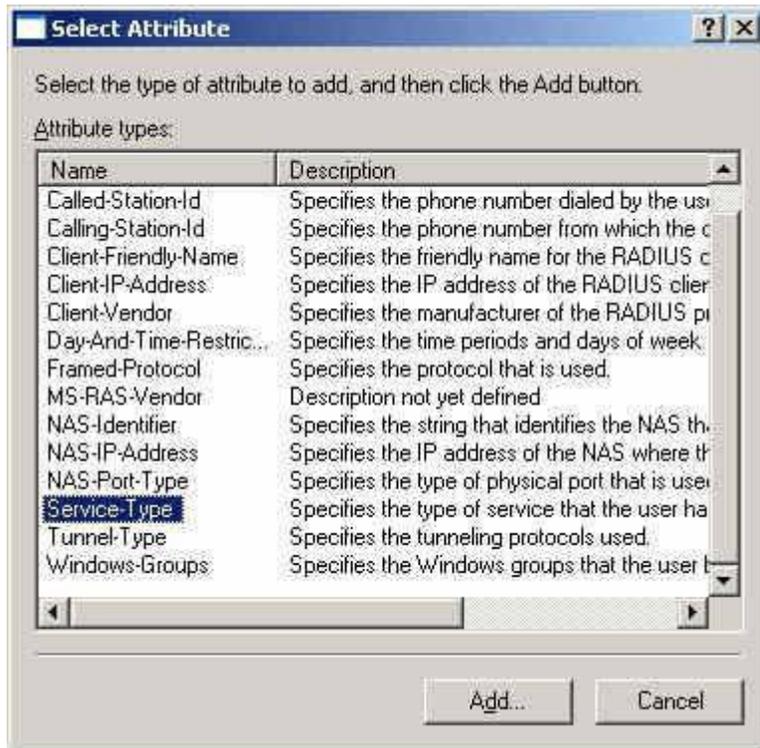
The network authentication service setting

Step14. Select **Grant remote access permission** , and **Remove** the original setting , then click **Add** .



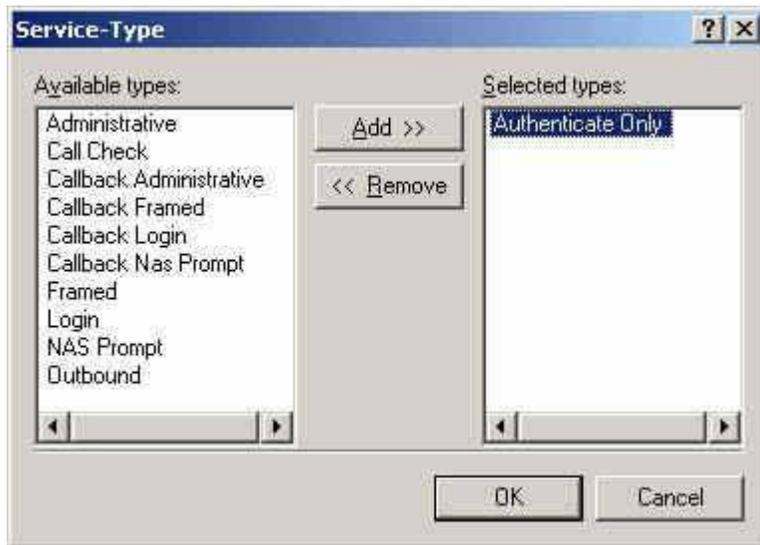
**The RADIUS properties settings**

Step15. **Add Service-Type.**



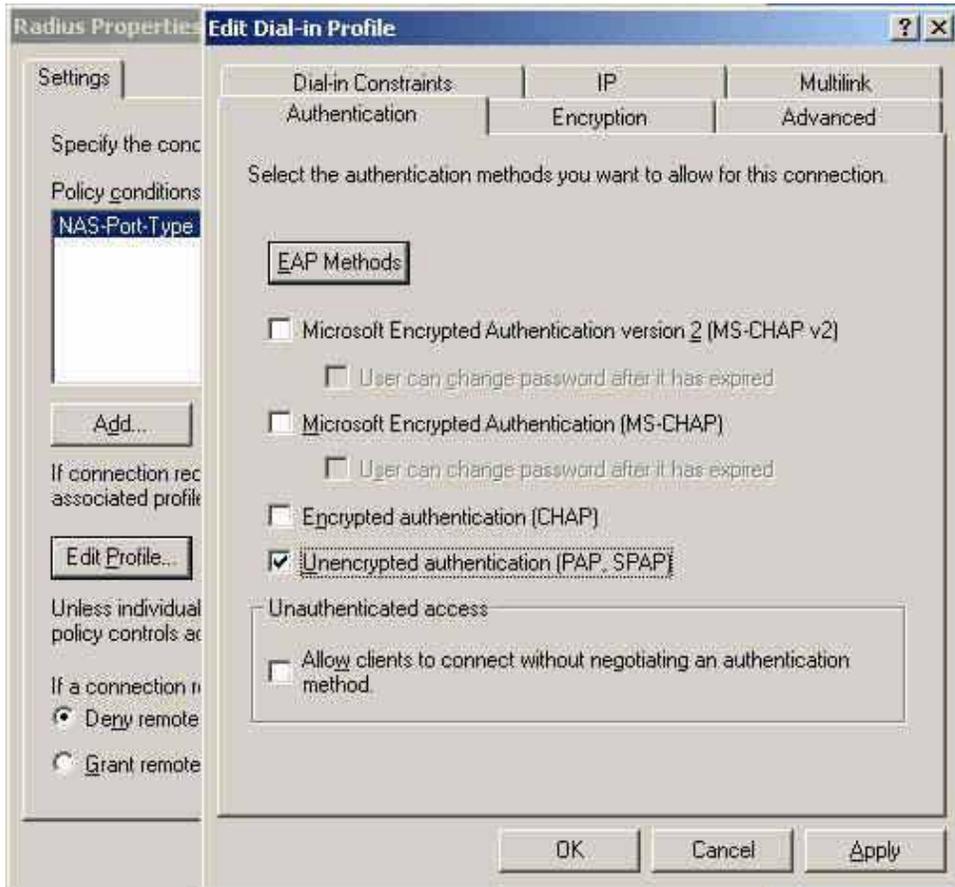
**Add new RADIUS properties attribute**

Step16. **Add Authenticate Only** from the left side .



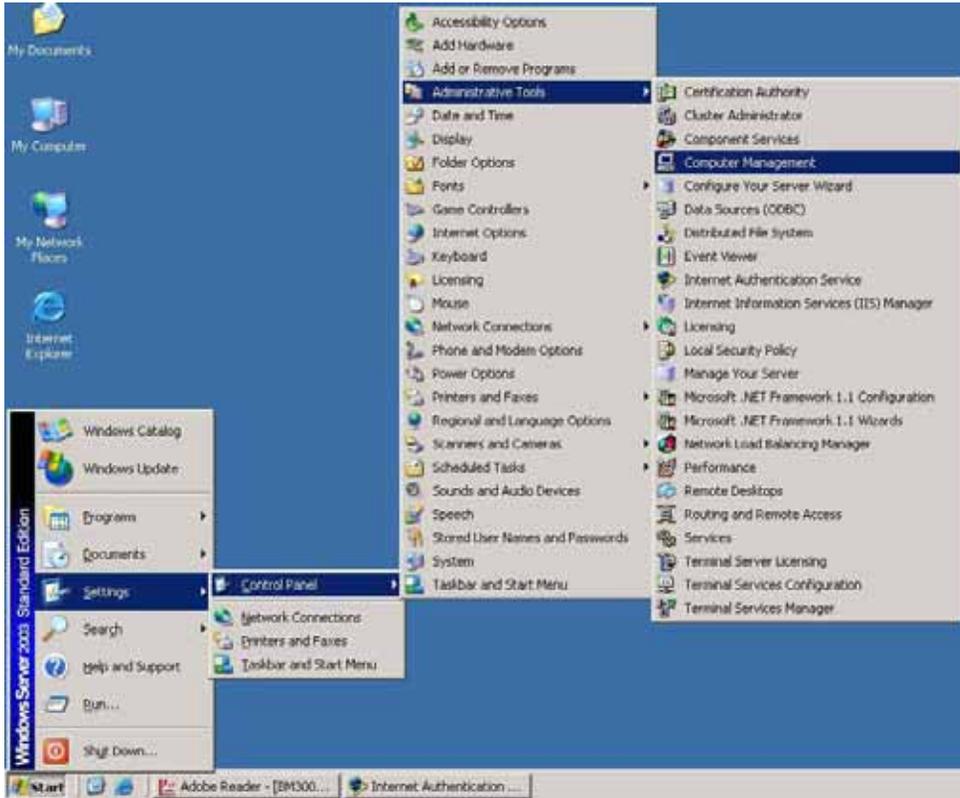
**Add RADIUS properties service-type**

Step17. Click **Edit Profile** , select **Authentication** , and check **Unencrypted authentication (PAP , SPAP)** .



**Edit RADIUS service-type dial-in property**

Step18. Add Auth User , click **Start** → **Setting** → **Control Panel**→**Administrative Tools** , select **Computer Management**



Enter computer management

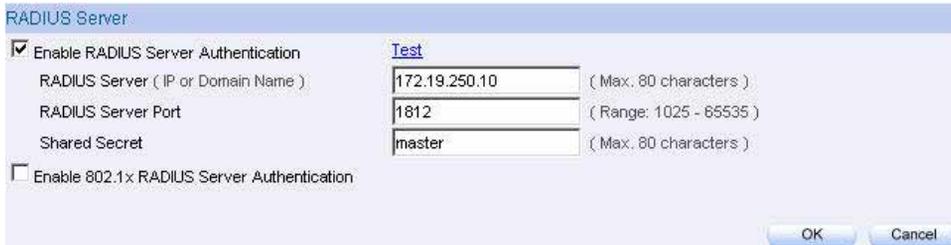
Step19. Right click on **Users** , select **New User** .



**Add new user**

Step20. Complete the Windows 2003 RADIUS Server Settings .

Step21. In **Authentication** → **RADIUS** function , enter **IP** , **Port** and **Shared Secret** . ( The setting must be the same as RADIUS server ) .



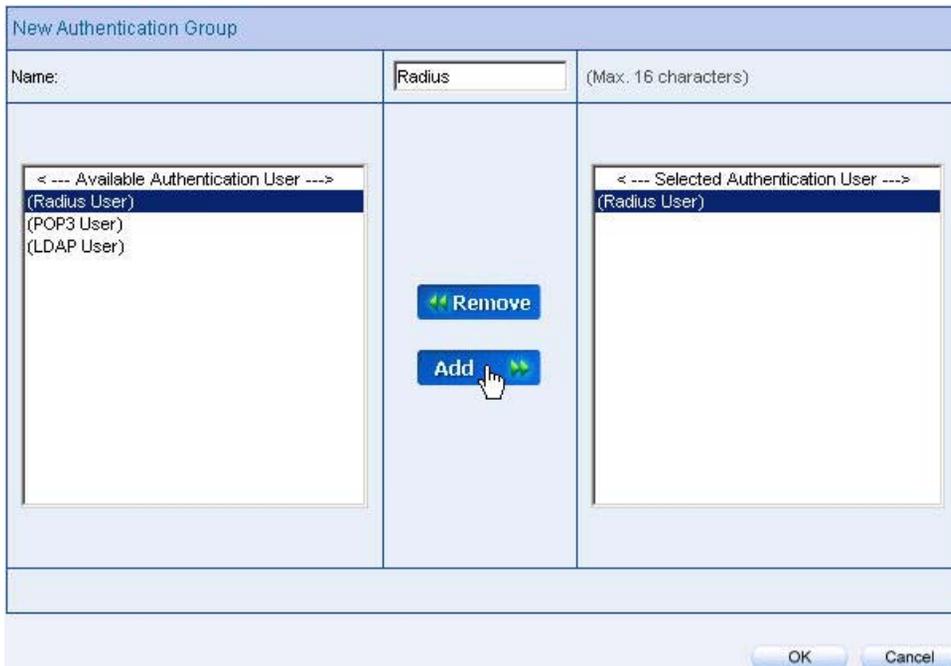
The screenshot shows a dialog box titled "RADIUS Server". It has two main sections. The first section is "Enable RADIUS Server Authentication", which is checked. Below this are three input fields: "RADIUS Server ( IP or Domain Name )" with the value "172.19.250.10" and a note "( Max. 80 characters )"; "RADIUS Server Port" with the value "1812" and a note "( Range: 1025 - 65535 )"; and "Shared Secret" with the value "master" and a note "( Max. 80 characters )". There is a "Test" button next to the "RADIUS Server" field. The second section is "Enable 802.1x RADIUS Server Authentication", which is unchecked. At the bottom right are "OK" and "Cancel" buttons.

The RADIUS server setting



Click **Test** , it can detect if the BM-2101 and RADIUS server can real working .

Step22. In **Authentication** → **User Group** , add new **Radius User** ◦



The screenshot shows a dialog box titled "New Authentication Group". At the top, there is a "Name:" field with the value "Radius" and a note "(Max. 16 characters)". Below this are two list boxes. The left list box is titled "< --- Available Authentication User --->" and contains three items: "(Radius User)", "(POP3 User)", and "(LDAP User)". The right list box is titled "< --- Selected Authentication User --->" and contains one item: "(Radius User)". Between the two list boxes are two buttons: "Remove" and "Add". A mouse cursor is pointing at the "Add" button. At the bottom right are "OK" and "Cancel" buttons.

Add new RADIUS user

Step23. In **Policy → Outgoing** , apply the **Authentication Group ( RADIUS included )** in Step22. to add the new policy .

Comment :  (Max. 64 characters)

**Add New Policy**

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	Radius
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download <input type="checkbox"/> Upload
QoS	None
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	0 MBytes ( Range: 0 - 999999 )

OK Cancel

**To add the RADIUS authentication policy**

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY			Modify Remove Pause	To 1

New Entry

**Complete the RADIUS authentication policy setting**

Step24. When the user connect to the network via the browser , it will show the authentication window . Enter the user name and password , click **OK** , then link to the network through the BM-2101

User Login	
User Authentication	
User Name	<input type="text"/> ( ex: auth_user1 )
Password	<input type="password"/>
<input type="button" value="OK"/>	

**Link to the network through the authentication window**

## 9.3 POP3

To plan the user connect to the WAN through the authentication by policy. (To use the WAN POP3 server authentication)

Step1. In **Authentication** → **POP3** , add the new settin as following

POP3 Server IP or Domain Name / Port	Configure
	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
msa.hinet.net / 110	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

POP3 server setting



Click **Test** , it can detect if the BM-2101 and POP3 server can real working .

Step2. In **Authentication** → **User Group** , add new **POP3 User** .

New Authentication Group

Name:  (Max. 16 characters)

<p>&lt; --- Available Authentication User ---&gt;</p> <ul style="list-style-type: none"><li>(Radius User)</li><li>(POP3 User)</li><li>(LDAP User)</li></ul>	<p><input type="button" value="Remove"/></p> <p><input type="button" value="Add"/></p>	<p>&lt; --- Selected Authentication User ---&gt;</p> <ul style="list-style-type: none"><li>(POP3 User)</li></ul>
---	--	--

Add new POP3 user

Step3. In **Policy** → **Outgoing** , apply Step2. (The authentication group) in to the policy

Comment :  (Max: 64 characters)

**Add New Policy**

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	POP3_Auth
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download <input type="checkbox"/> Upload
QoS	None
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	0 MBytes ( Range: 0 - 999999 )

**The POP3 server authentication in 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

**Complete the POP3 server authentication in policy setting**

Step4. When the user want to connect to the network via browser , it will show the authentication window . Enter the user name and password, click **OK** , then link to the network through the BM-2101 appliance .

User Login	
User Authentication	
User Name	<input type="text"/> ( ex: auth_user1 )
Password	<input type="password"/>
<input type="button" value="OK"/>	

**Link to the network through the authentication window**

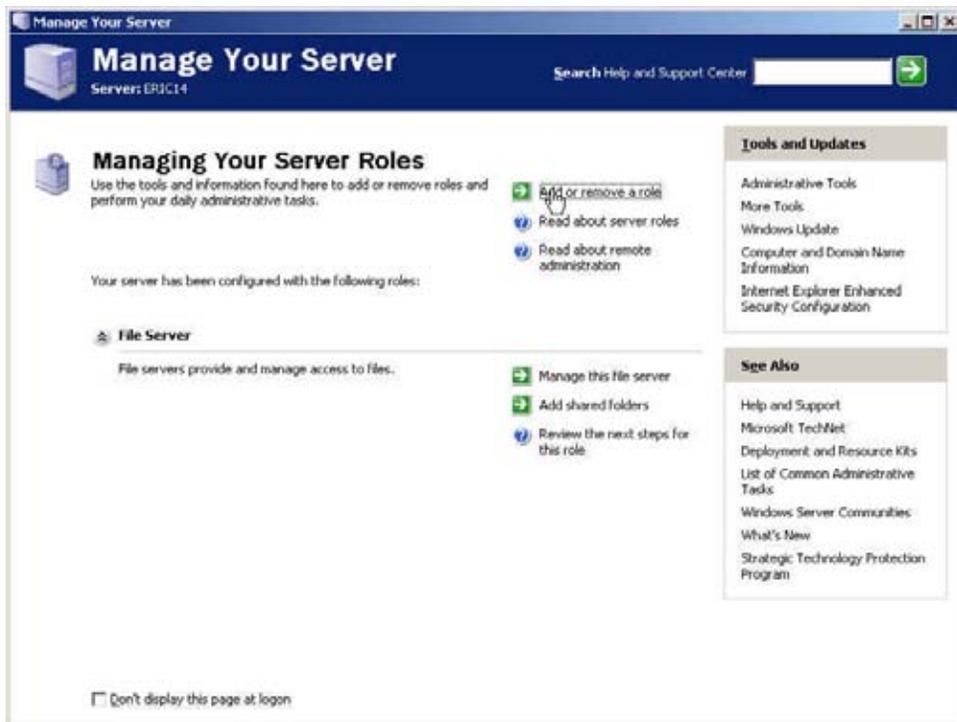
## 9.4 LDAP

To plan the user connect to the WAN through the authentication by policy (To use the WAN LDAP server ( Windows 2003 Server built-in authentication ) .

### ※ Windows 2003 LDAP Server Deployment

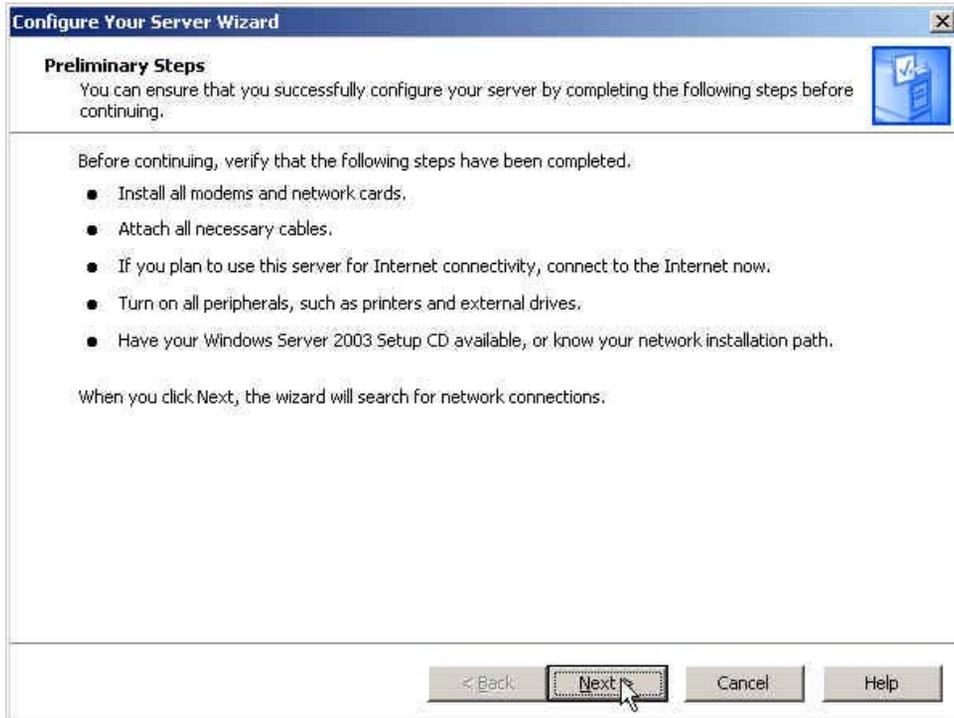
Step1. Click **Start → Program → Administrative Tools → Manage MIS engineer Server.**

Step2. In **Manage MIS engineer Server** window,click **Add or remove a role → Configure MIS engineer Server Wizard .**



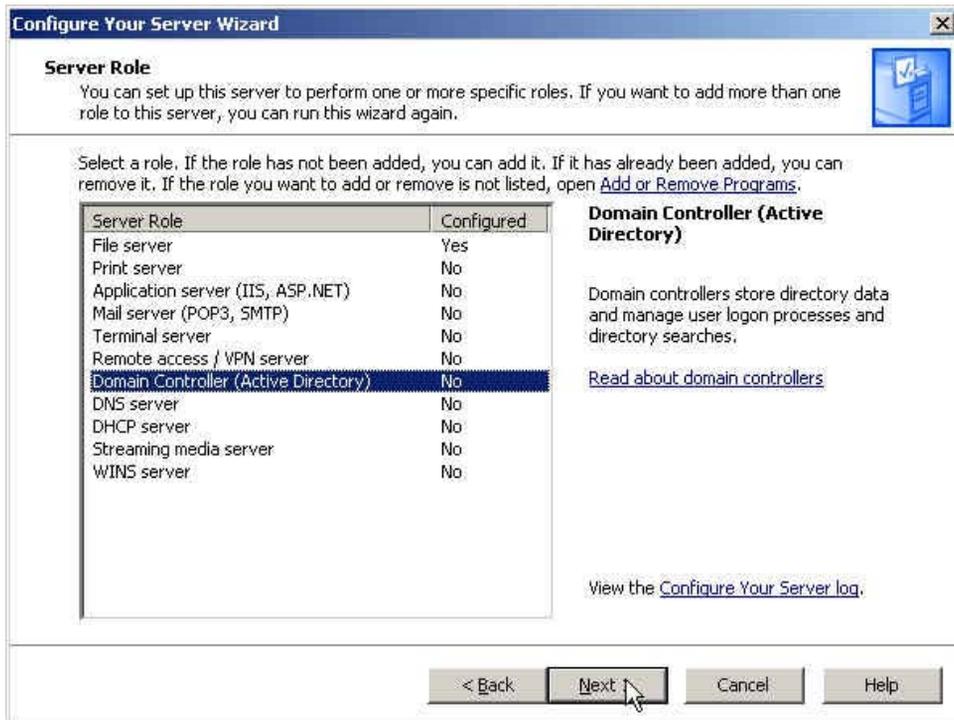
Click add or remove a role

Step3. In **Preliminary Steps** window , click **Next** .



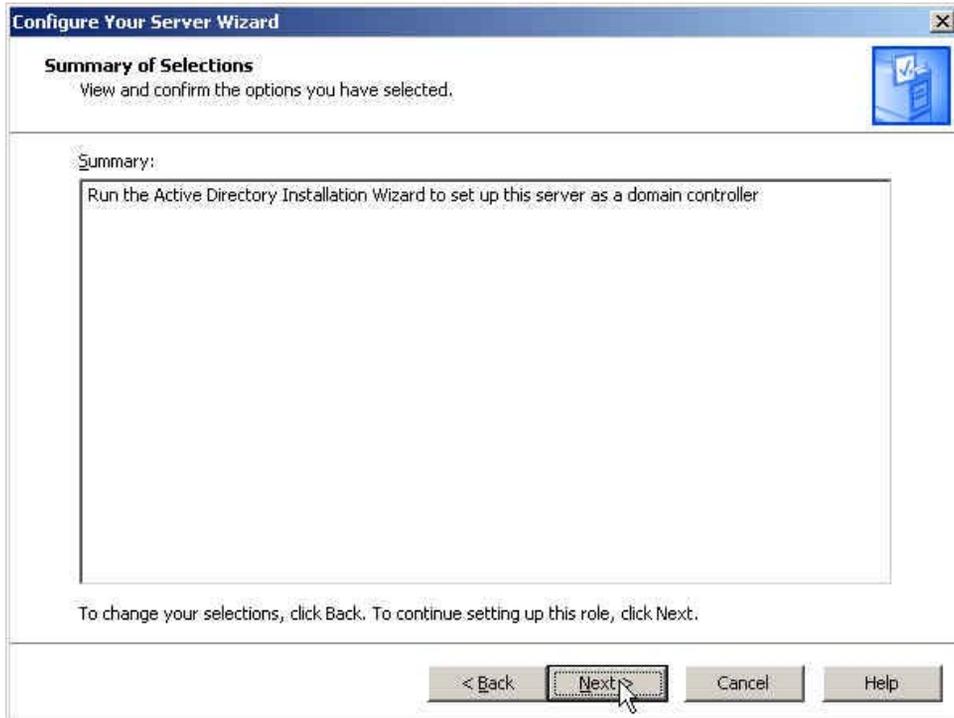
**The Preliminary steps Web UI**

Step4. In **Server Role** window, select **Active Directory** and click **Next**.



The server role window

Step5. In **Summary of Selections** window , click **Next**.



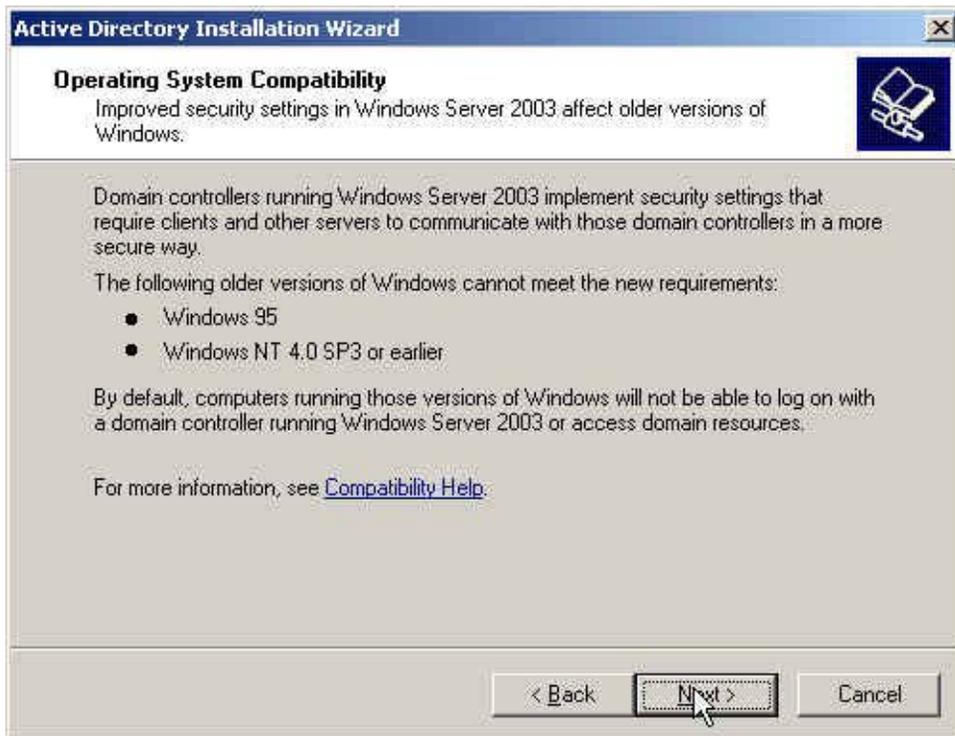
**The summary of selections window**

Step6. In **Active Directory Installation Wizard** window, click **Next**.



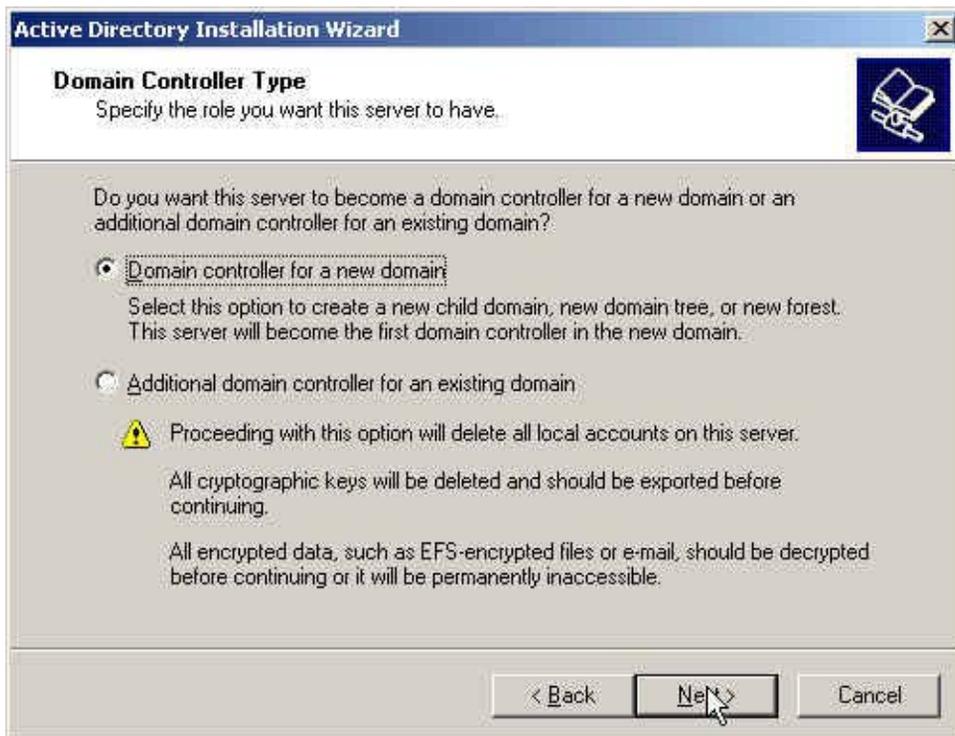
**Active directory installation wizard**

Step7. In **Operating System Compatibility** window, click **Next**.



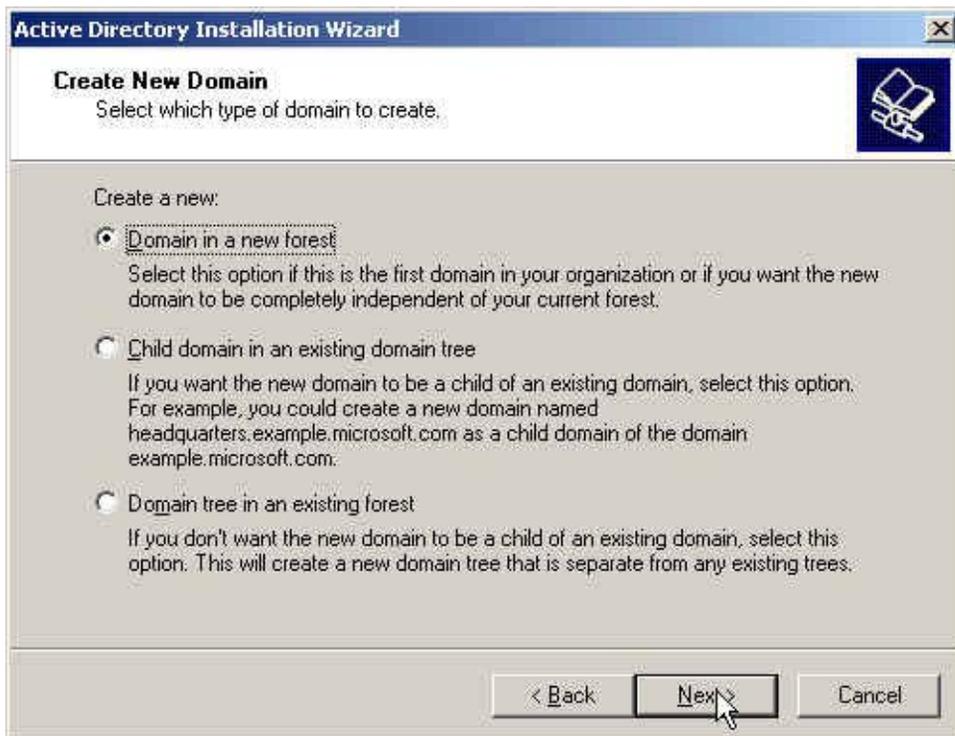
**The operating system compatibility window**

Step8. In **Domain Controller Type** window, select **Domain controller for a new domain** click **Next**.



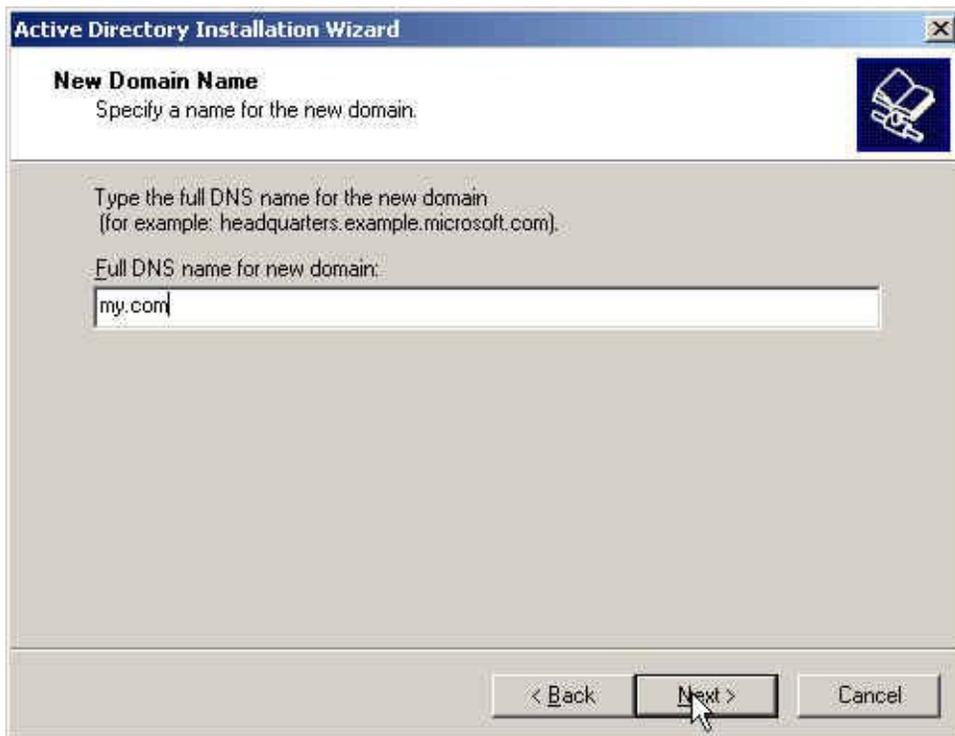
**The domain controller type window**

Step9. In **Create New Domain** window, select **Domain in a new forest**, click **Next** .



**Create new domain window**

Step10. In **New Domain Name** window , enter the **Full DNS name for new domain** , click **Next**.



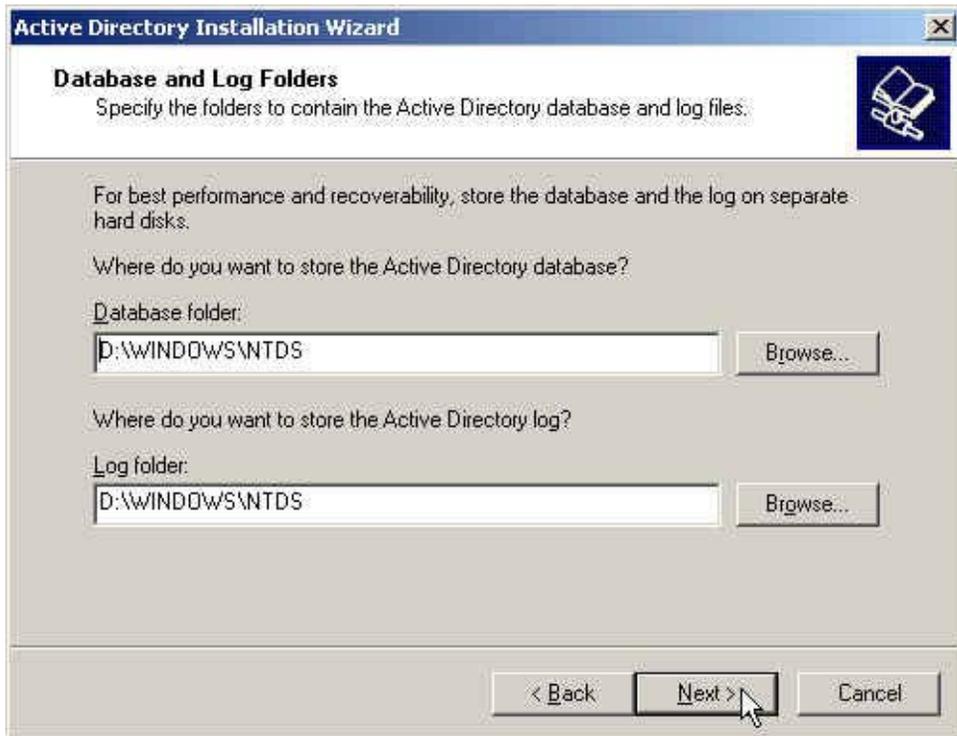
**The new domain name window**

Step11. In **NetBIOS Domain Name** window , enter the **Domain NetBIOS name** , click **Next**.



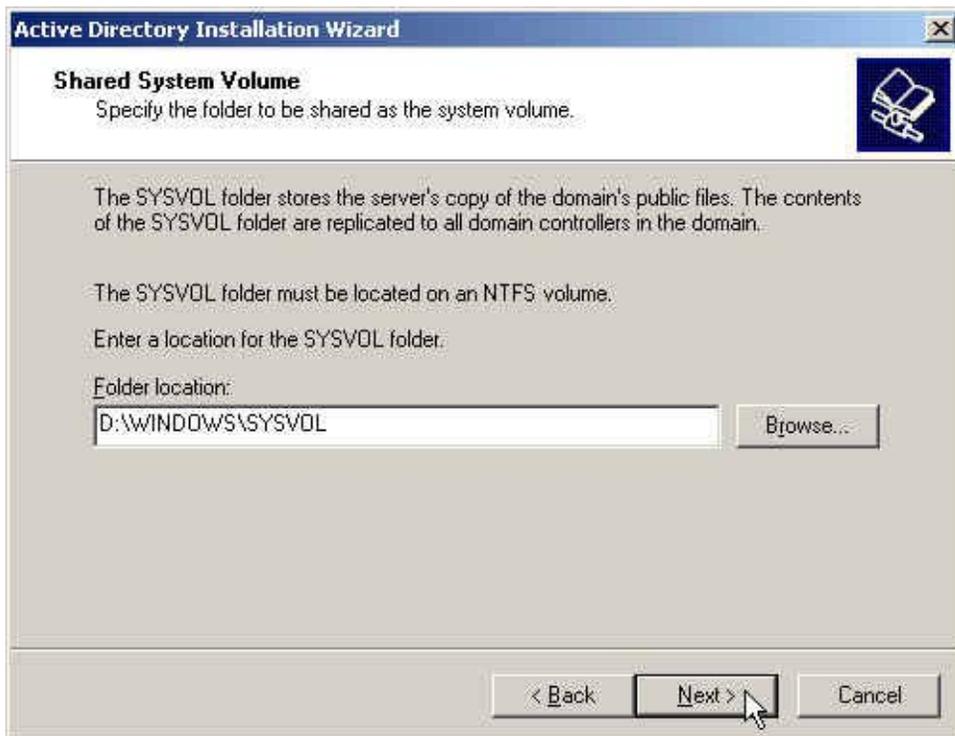
The NetBIOS domain name window

Step12. In **Database and Log Folders** window , enter the routes of **Database folder** and **Log folder** , click **Next**.



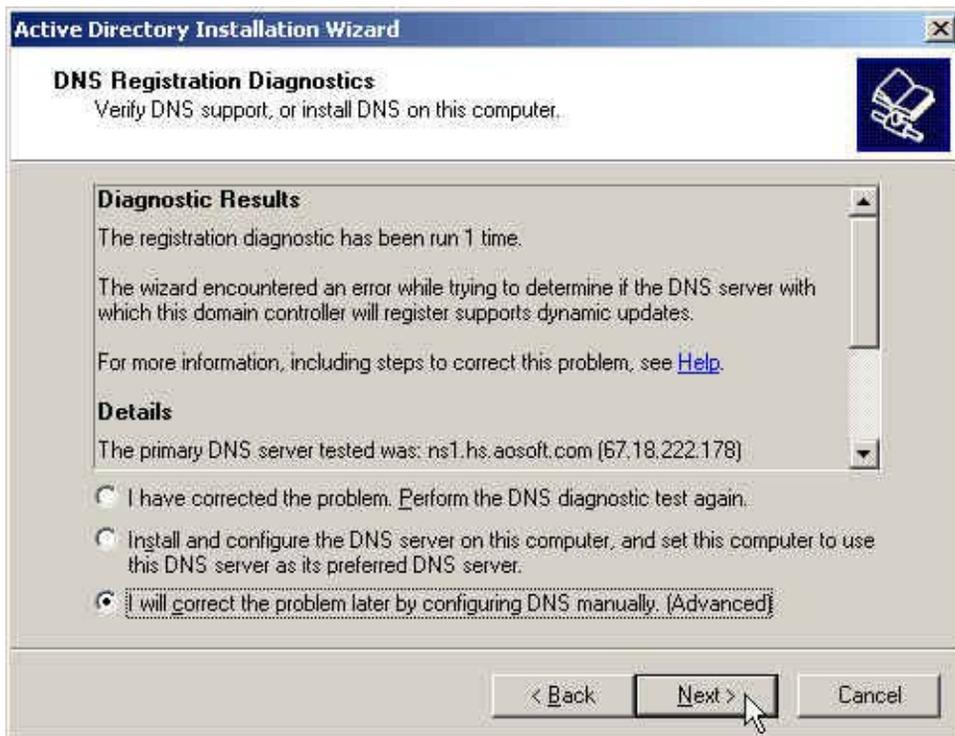
**The database and log folder window**

Step13. In **Shared System Volume** window, enter the **Folder location** , click **Next**.



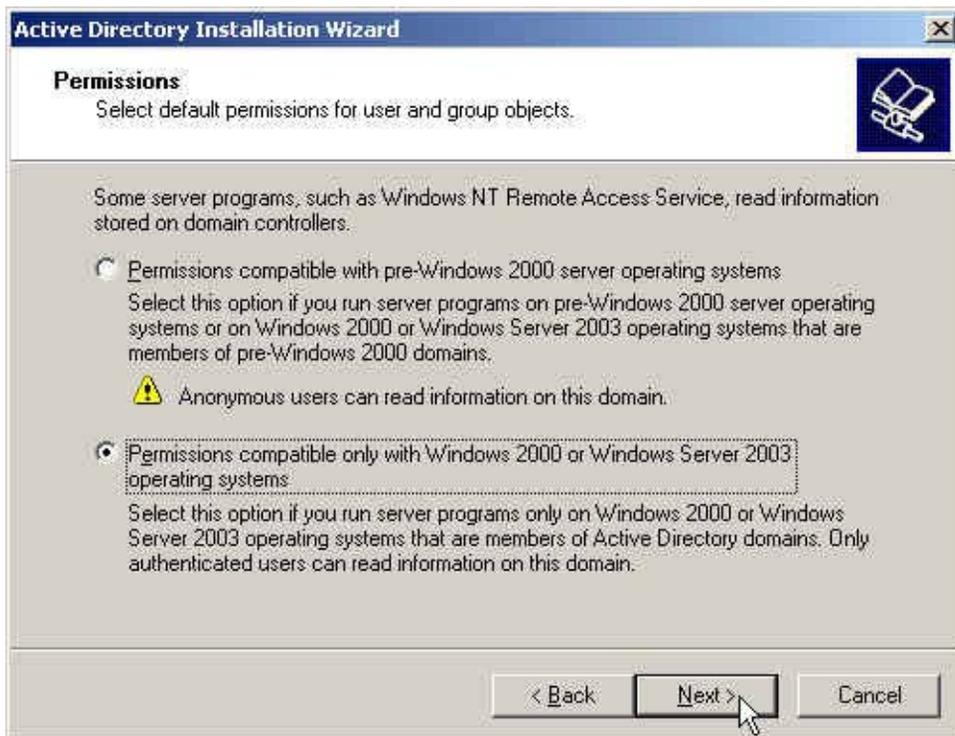
**The shared system volume window**

Step14. In **DNS Registration Diagnostics** window , select **I will correct the problem later by configuring DNS manually(Advanced)** , click **Next** .



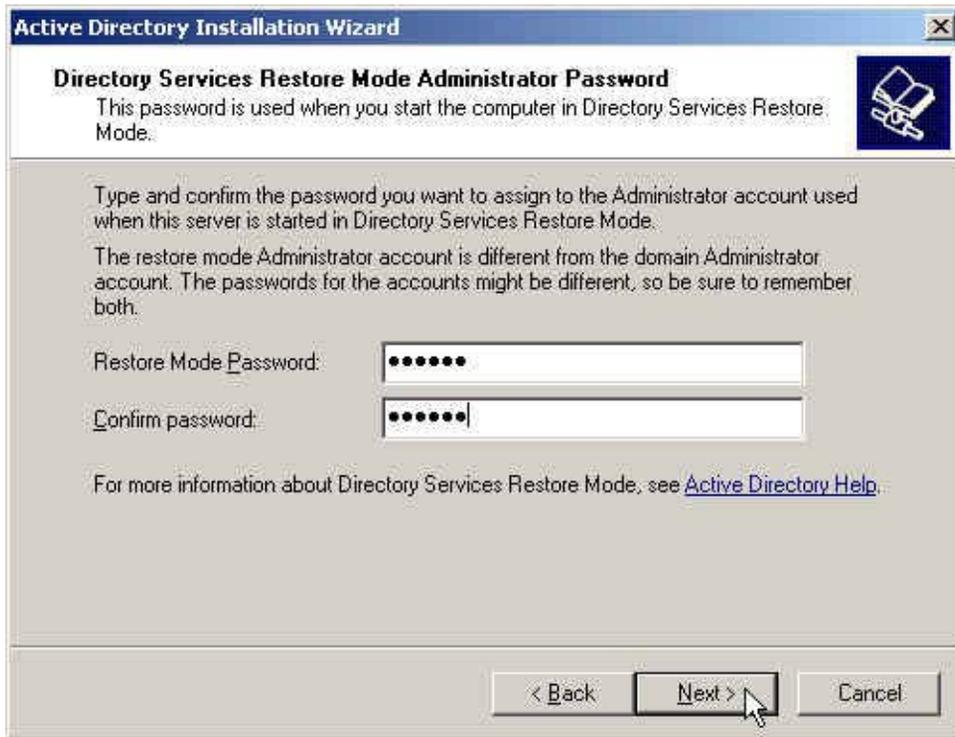
**The DNS registration diagnostics window**

Step15. In **Permissions** window , select **Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems**, click **Next** .



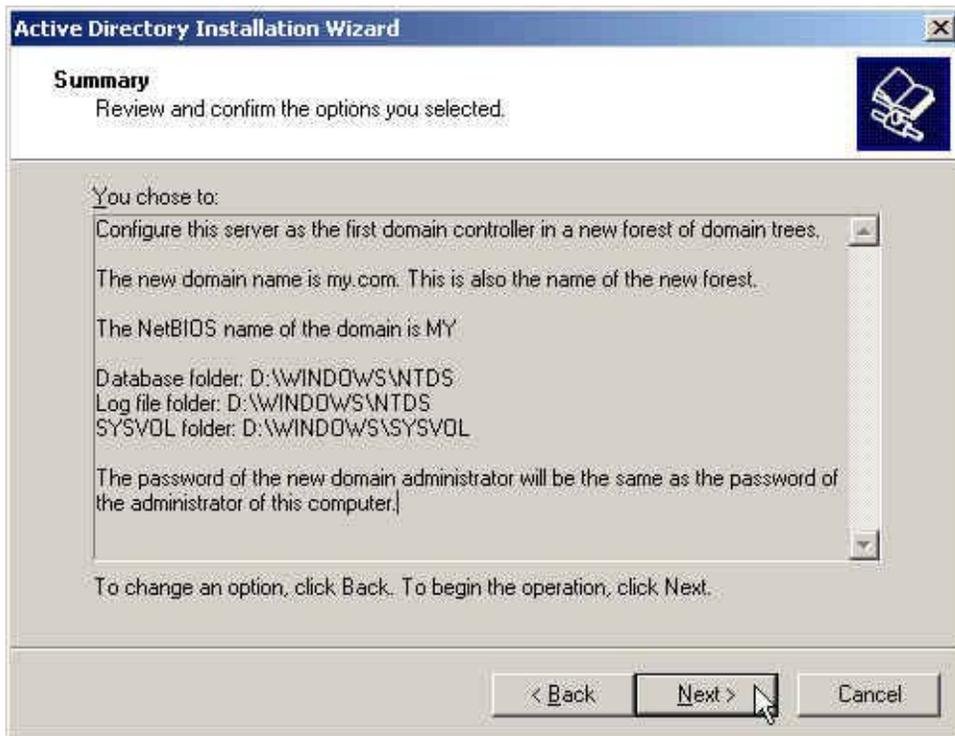
**The permissions window**

Step16. In **Directory Services Restore Mode Administrator Password** window , enter the **Restore Mode Password** and **Confirm password** , click **Next**.



The directory services restore mode administrator password window

Step17. In **Summary** window, click **Next**.



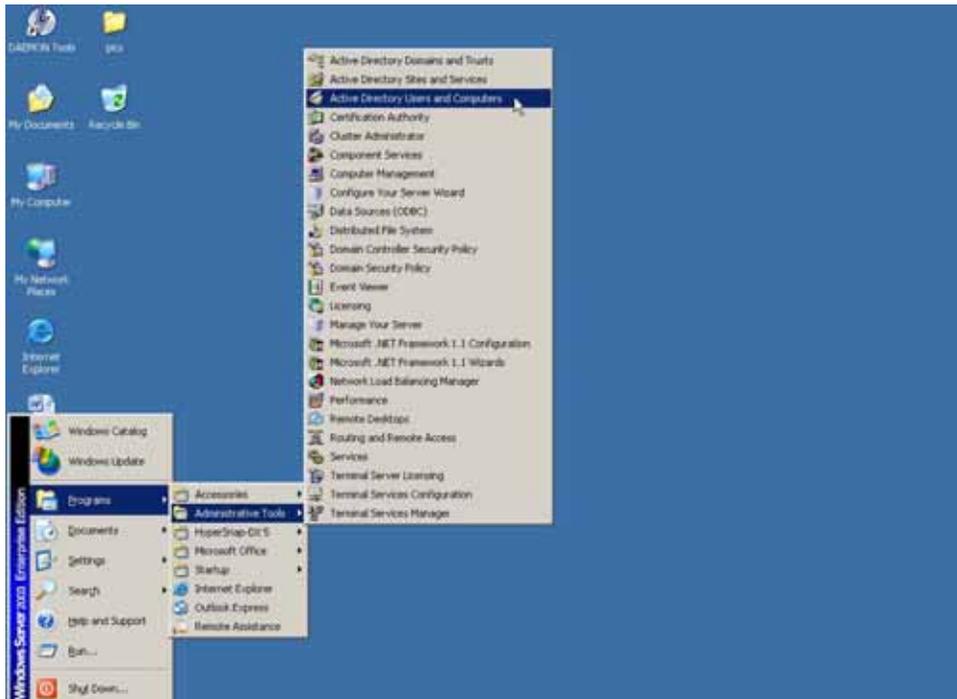
**The summary window**

Step18. Complete the Active Directory installation wizard.



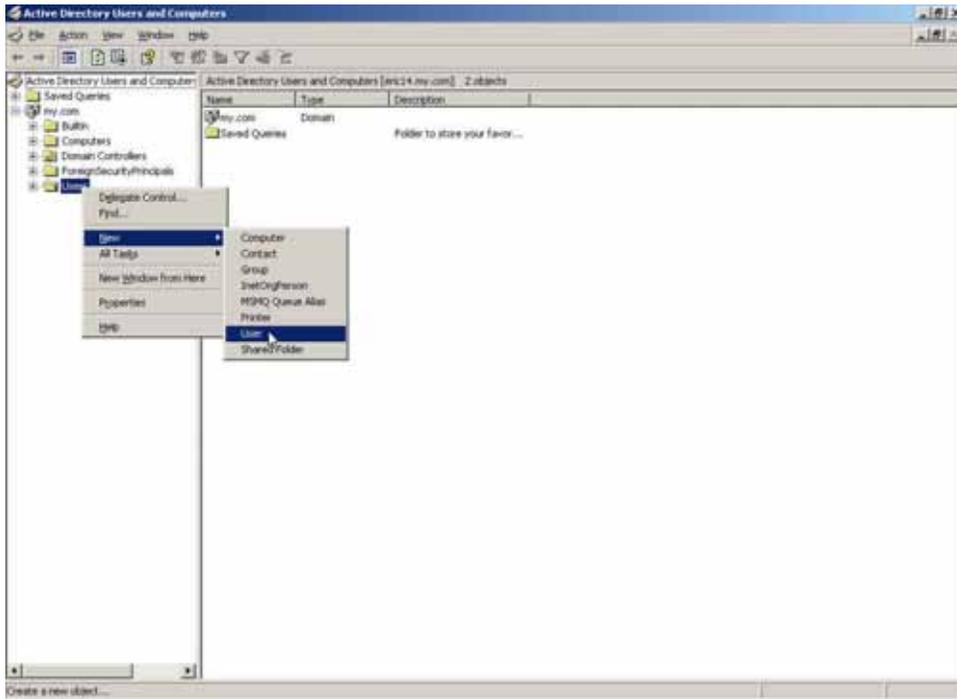
**Complete the active directory installation wizard**

Step19. Click **Start** → **Programs** → **Administrative Tools** → **Active Directory Users and Computers** .



Enable active directory users and computers

Step20. In **Active Directory Users and Computers** window , right click on the **Users** , select **New** → **User**.



**Add new active directory user**

Step21. In **New Object–User** window , enter the settings , click **Next** .

The screenshot shows a Windows-style dialog box titled "New Object - User". At the top left is a user icon and the text "Create in: my.com/Users". Below this are several input fields: "First name:", "Initials:", "Last name:", "Full name:", "User logon name:" (with a dropdown menu showing "@my.com"), and "User logon name (pre-Windows 2000):" (with "MY\' entered). At the bottom are three buttons: "< Back", "Next >", and "Cancel". A mouse cursor is pointing at the "Next >" button.

**Add new object-user setting 1**

Step22. In **New Object –User** window , enter the password , click **Next**.

**New Object - User**

Create in: my.com/Users

Password: [masked]

Confirm password: [masked]

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

< Back   Next >   Cancel

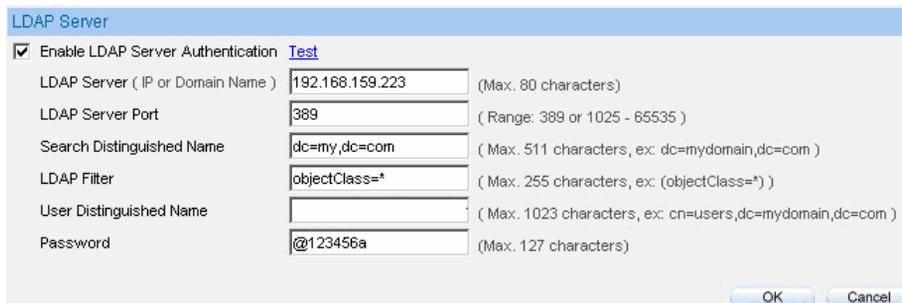
The new object – user setting 2

Step23. Complete to add the user.



Complete to add the object user

Step24. In **Authentication** → **LDAP** , enter the following setting:

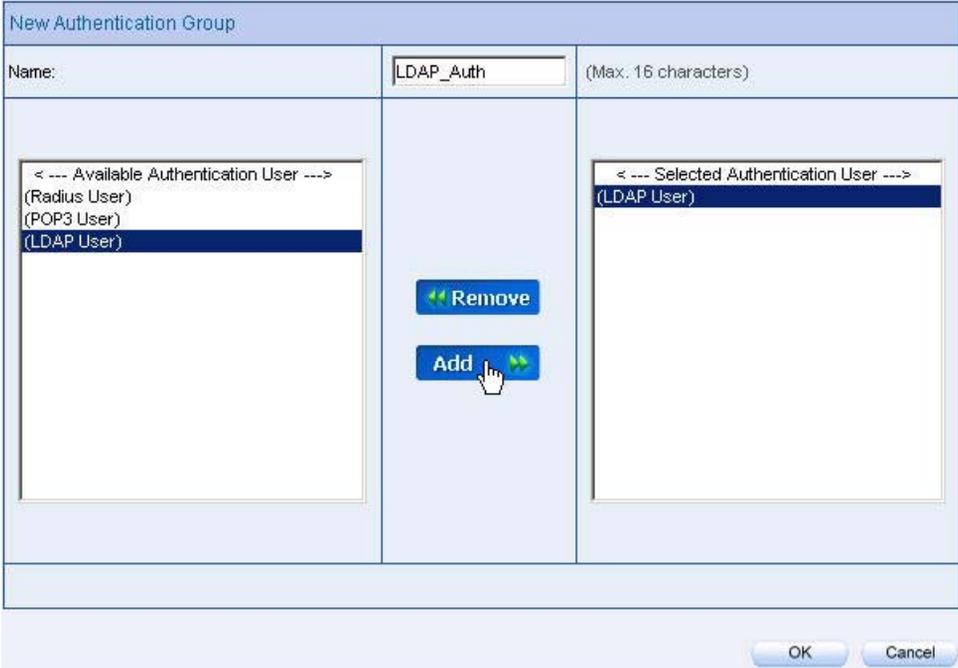


The LDAP server setting



Click **Test** , it can detect if the BM-2101 and LDAP server can real working .

Step25. In Authentication → User Group , add LDAP User.



Add new LDAP user

Step26. In **Policy** → **Outgoing** , apply Step25. (the authentication group) in to the policy setting .

Comment :  (Max. 64 characters)

**Add New Policy**

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	LDAP_Auth
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download <input type="checkbox"/> Upload
QoS	None
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	0 MBytes ( Range: 0 - 999999 )

**The LDAP server authentication in 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

**Complete the LDAP server authentication in policy setting**

Step27. When the user want to connect to the network , it will show the authentication window . Enter the user name and password , click **OK**, then link to the network through the BM-2101 appliance

User Login	
User Authentication	
User Name	<input type="text"/> ( ex: auth_user1 )
Password	<input type="password"/>
<input type="button" value="OK"/>	

**Link to the network through the authentication**

# Content Blocking

The content blocking included the **URL , Script , P2P , IM , Download and Upload.**

1. **URL** : The MIS engineer can decide to open or limit the specific web site through the complete domain name, keywords and wildcards . ( ~ and \* ) .
2. **Script** : The access competency of popup , ActiveX , Java , cookie in the blocking URL .
3. **Download** : To limit the competency of downloading the specific extension files and media files from the http or ftp protocol.
4. **Upload** : To limit the competency of uploading the specific extension files and media files from the http or ftp protocol.

## Content blocking terms

### URL String

- The domain name restricted by the BM-2101 appliance which can decide to allow or limit the competency to use the domain.

### Popup

- Can block the popup window when browsing the web site .

### ActiveX

- Can block the ActiveX packets from the web site .

### Java

- Can block the Java packets from the web site .

### Cookie

- Can block the cookie packets from the web site .

### Audio and Video Types

- Can limit the user to transfer the audio and video files through http or ftp.

### Extension

- Can limit the user to transfer the extension files through http or ftp .

### All Types

- Can limit the user to transfer the audio , video and specific extension files through http or ftp .

We set 4 environments.

No.	Range	The Application Environments
Example. 1	<b>URL</b>	Only permit the LAN user to access the data in specific web site .
Example. 2	<b>Script</b>	To limit the LAN user to access the script data in the web site .
Example. 3	<b>Download</b>	To limit the LAN user to download the extension files , video and audio files in the internet through http or ftp .
Example. 4	<b>Upload</b>	To limit the LAN user to upload the extension files , video and audio files in the internet through http or ftp .

## 10.1 URL

### Only permit the LAN user to access the data in specific web site .

The way to use the content blocking :

Symbol : ~ , the symbol means to open ; \* , the symbol means the Wildcards .

To limit the user not to enter the specific web site . : In add new URL string , enter the complete domain name or keywords in the forbidden web site . For example : [www.kcg.gov.tw](http://www.kcg.gov.tw) or gov .

To permit the user to enter the specific web site :

1. First of all , enter the complete **Domain Name** or **Keywords** in to the URL blocking setting , and add the symbol “ ~ “ which represents permitted to enter . For example , ~www.kcg.gov.tw or ~gov .
2. Complete all the setting of opened web site , add the new URL blocking policy to forbid all the web site . Type the Wildcard of \* in the URL string to forbid all .



Attention ! The forbidden command must be placed in the end of all the setting process . If the MIS engineer want to add the URL to opened , he has to remove all the forbidden command then enter the new domain name . After complete all the process , he has to enter all the forbidden command again .

Step1. In **Content Blocking** → **URL** , add the following setting :

- Click **New Entry** .
- **URL String** , enter ~yahoo. Click **OK** .
- Click **New Entry** .
- **URL String**, enter ~google . Click **OK** .
- Click **New Entry** .
- **URL String** , enter \* . Click **OK** .
- Complete the URL setting .

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"/>

**The URL setting**

Step2. In **Policy → Outgoing** , apply the **Content Blocking** setting in to the policy .

Comment :  (Max. 64 characters)

**Add New Policy**

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input checked="" type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download <input type="checkbox"/> Upload
QoS	None
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	0 MBytes ( Range: 0 - 999999 )

OK Cancel

The URL content blocking setting in policy

Step3. In **Policy → Outgoing** , complete the setting to permit the user can only access the data in specific web site through the policy.

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY			Modify Remove Pause	To 1

New Entry

Completer the URL content blocking setting in policy



The user can only browse the domain name of “ yahoo” and “google” in the web site through the policy.

## 10.2 Script

To limit the LAN user to access the script data in the web site .

Step1. In **Content Blocking** → **Script** , select the following setting :

- Select **Popup** .
- Select **ActiveX** .
- Select **Java** .
- Select **Cookie** .
- Click **OK** .
- Complete the script setting



**The script setting**

Step2. In Policy → Outgoing , apply the **Script Content Blocking Setting** in to policy :

Comment :  (Max. 64 characters)

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input checked="" type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download <input type="checkbox"/> Upload
QoS	None
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	0 MBytes ( Range: 0 - 999999 )

OK Cancel

The script content blocking in policy setting

Step3. In Policy → Outgoing , to complete the settings to limit the LAN user accessing the script data in the web site through the policy :

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	✔	❌	Modify Remove Pause	To 1

New Entry

Complete the script content blocking settings



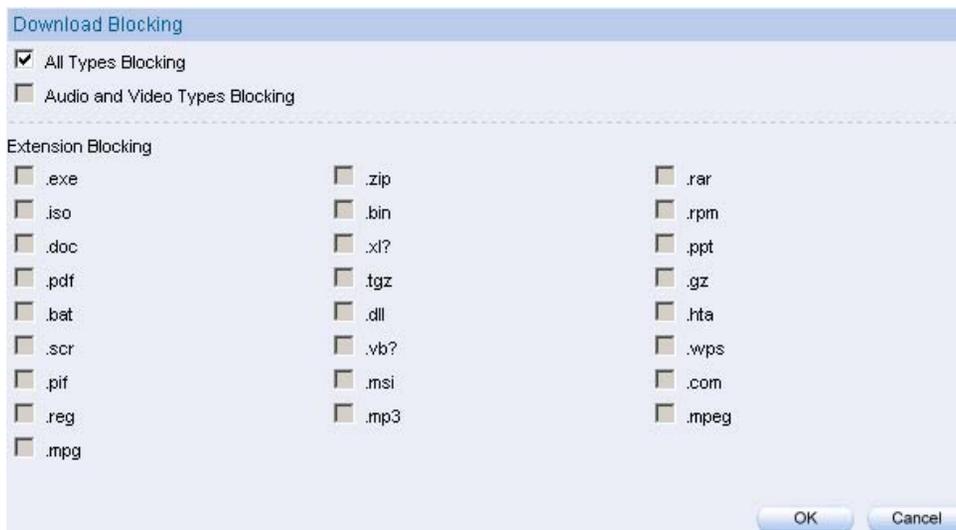
The user can not use the specific function in the web site (For example , JAVA , cookie...) when browsing the web pages through the policy . This function can forbid the user to browse the stock exchange web site and so on .( The browser can not display the market summary charts)

## 10.3 Download

To limit the LAN user to download the extension files , video and audio files in the internet through http or ftp .

Step1. In **Content Blocking**→ **Download** , set the following settings :

- Select **ALL Types** .
- Click **OK** .
- Complete the download setting .



The download setting

Step2. In **Policy** → **Outgoing**, apply the **Download Content Blocking** settings in to the policy .

Comment :  (Max. 64 characters)

[Add New Policy](#)

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input checked="" type="checkbox"/> Download <input type="checkbox"/> Upload
QoS	None
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	0 MBytes ( Range: 0 - 999999 )

The download content block setting in policy

Step3. In **Policy** → **Outgoing** , complete the settings to limit the LAN user to transfer the video and audio files and specific extention files in the network .

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

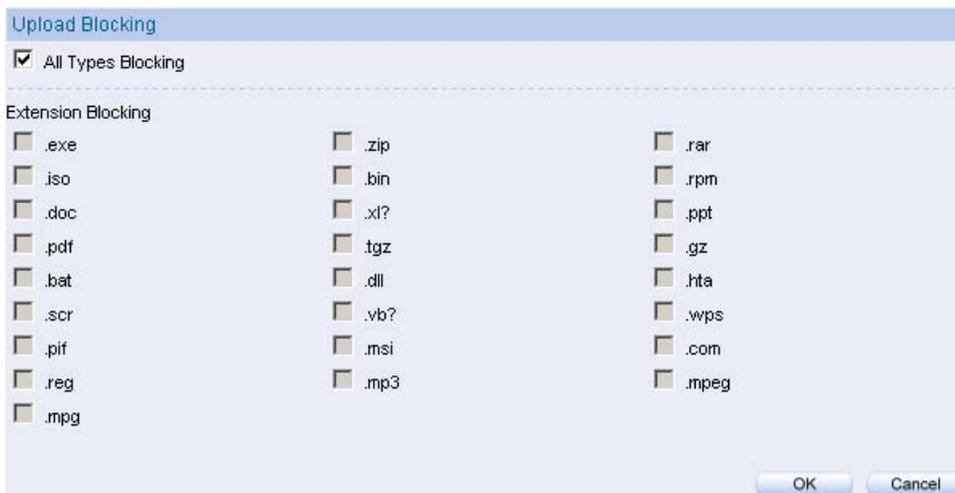
Complete the download content blocking setting in policy

## 10.4 Upload

To limit the LAN user to upload the extension files , video and audio files in the internet through http or ftp .

Step1. In **Content Blocking**→ **Upload Blocking** , set the following settings :

- Select **ALL Types Blocking**.
- Click **OK** .
- Complete the upload setting.



The upload setting

Step2. In **Policy → Outgoing**, apply the **Upload Content Blocking** settings in to the policy . :

Comment :  (Max: 64 characters)

[Add New Policy](#)

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download <input checked="" type="checkbox"/> Upload
QoS	None
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	0 MBytes ( Range: 0 - 999999 )

OK   Cancel

The upload content block setting in policy

Step3. In **Policy → Outgoing** , complete the settings to limit the LAN user to upload the video and audio files and specific extension files in the network . :

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

Complete the upload content blocking setting in policy

## Chapter 11

# IM/P2P Blocking

MIS engineer can limit user to use IM and P2P software by using IM / P2P Blocking function.

1. **IM** : Set the login privilege of **MSN Messenger, Yahoo Messenger, ICQ Messenger, QQ Messenger and Skype Messenger**.
2. **P2P** : Set the use privilege of **eDonkey, Bit Torrent, WinMX, Foxy, KuGoo, AppleJuice, Audio Galaxy, Direct Connect, iMesh, MUTE, Thunder 5**.

## Setting

### IM/P2P Signature Definitions

- System can update the IM / P2P signature definitions every one hour, or user can manually update it instantly. System will show the update time and version of IM / P2P signature definitions.

### IM Blocking

- Set the login privilege of MSN Messenger, Yahoo Messenger, ICQ Messenger, QQ Messenger and Skype Messenger.

### P2P Blocking

- Set the use privilege of eDonkey, Bit Torrent, WinMX, Foxy, KuGoo, AppleJuice, AudioGalaxy, Direct Connect, iMesh, MUTE and Thunder 5.

We set two examples :

No.	Range	Environment
Ex.1	<b>IM</b>	Limit internal user transfer messages, files and media files by IM software.
Ex.2	<b>P2P</b>	Limit internal user access internet resources by P2P software.

## 11.1 Example

Limit internal user transfer messages, files and media files by IM software.

Step1. In **IM / P2P Blocking** → **Setting**, add the following settings :

- Click **New Entry**
- Enter the **Name** called **IM\_Blocking**.
- Select **MSN Messenger, Yahoo Messenger, ICQ Messenger, QQ Messenger and Skype Messenger**.
- Click **OK**.
- Complete the settings

**Add IMP2P Blocking**

Name:  (Max. 16 characters)

**Instant Messaging**

MSN Messenger       Yahoo Messenger       ICQ Messenger  
 QQ Messenger       Skype Messenger

**Peer-to-Peer Application**

Edonkey       Bit Torrent       WinMX  
 Foxy       KuGoo       AppleJuice  
 AudioGalaxy       DirectConnect       iMesh  
 MUTE

OK Cancel

**IM blocking setting**

**IMP2P Signature Definitions**

The latest update time : 06/08/16 10:06:53 (Update signature definitions every one hour)  
The newest version: 1.0.1 (Signature definitions updated at 06/08/11 15:43:47 )  
Update signature definitions immediately (Use TCP port: 80 and UDP port: 53) [Update Now](#) [Test](#)

**IMP2P Blocking**

Total entry : 1

Name	IM	P2P	Configure
IM_Blocking	MSN, Yahoo, ICQ...	---	<b>In Use</b>

New Entry

**Complete the IM blocking setting**

Step2. In **Policy** → **Outgoing**, add one policy applied to IM blocking setting.

Comment :  (Max. 64 characters)

**Add New Policy**

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3 <input type="checkbox"/> WAN4
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P Blocking	IM_Blocking
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	<input type="text" value="0"/> KBytes ( Range: 0 - 999999 )
Quota Per Day	<input type="text" value="0"/> MBytes ( Range: 0 - 999999 )

**Set the policy applied to IM blocking setting**

Step3. In **Policy** → **Outgoing**, complete the policy setting of limit internal user to transfer messages, files and media files.

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

**Complete the policy setting of IM blocking**

Limit internal user access internet resources by P2P software.

Step1. In **IM / P2P Blocking** → **Setting**, add the following settings :

- Click **New Entry**.
- Enter the **Name** of P2P\_Blocking.
- Select **eDonkey, Bit Torrent, WinMX, Foxy, KuGoo, AppleJuice, AudioGalaxy, DirectConnect, iMesh, MUTE and Thunder 5**.
- Click **OK**.
- Complete the settings

**Add IM / P2P Blocking**

Name:  (Max. 16 characters)

**Instant Messaging**

MSN Messenger       Yahoo Messenger       ICG Messenger

QQ Messenger       Skype Messenger

---

**Peer-to-Peer Application**

Edonkey       Bit Torrent       WinMX

Foxy       KuGoo       AppleJuice

AudioGalaxy       DirectConnect       iMesh

MUTE       Thunder5

**P2P blocking setting**

**IM/P2P Signature Definitions**

The latest update time : 06/08/16 10:06:53 (Update signature definitions every one hour)

The newest version: 1.0.1 (Signature definitions updated at 06/08/11 15:43:47 )

Update signature definitions immediately (Use TCP port: 80 and UDP port: 53) [Update Now](#) [Test](#)

---

**IM/P2P Blocking**

Total entry : 2

Name▼	IM	P2P	Configure
IM_Blocking	MSN,Yahoo,ICQ...	---	<input type="button" value="In Use"/>
P2P_Blocking	---	Edonkey,Bit Torrent,WinMX...	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

**Complete the P2P blocking setting**

Step2. In **Policy → Outgoing**, add one policy applied to P2P blocking setting.

Comment :  (Max. 64 characters)

**Add New Policy**

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3 <input type="checkbox"/> WAN4
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P Blocking	P2P_Blocking
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	<input type="text" value="0"/> KBytes ( Range: 0 - 999999 )
Quota Per Day	<input type="text" value="0"/> MBytes ( Range: 0 - 999999 )

**Set the policy applied to P2P blocking**

Step3. In **Policy → Outgoing**, complete the policy setting of limit internal user to access internet resources by P2P software :

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

**Complete the Policy setting of P2P blocking**



Use P2P will seriously occupy network bandwidth and it can change its service port. So the MIS engineer not only set the service port in **Service**, but also need to set **IM / P2P Blocking** → **P2P Blocking**.

# Virtual Server

When the MIS engineer apply the network connection from the ISP provider , the provided real IP is usually not enough to give to all the users . Normally , the MIS engineer can use the private IP address transfer to the real IP address via the BM-2101's NAT (Network Address Translation) function , in order to give the sufficient IP address to every user . If the MIS engineer set the server which provide the external service in LAN , then the external user can not link to the internal private IP address .

According to this problem , the MIS engineer can use the BM-2101 's virtual server function to solve the problem . The so called virtual server is to map the real IP address to the private IP address via the BM-2101 appliance.

The virtual server also includes the features , called **One to Many** map function. It means one real IP address can map to the private IP address in four LAN servers which provide the same service . It is because the virtual server can provide the **Load Balance** function which can provide the proper bandwidth to the LAN server group depends on the sessions . In other words , the functin can reduce the problem of **System Crash and bandwidth distribution** , to make the server can work more efficiently .

In this Chapter , we will make the introduction of **Mapped IP** and **Server 1/2/3/4** .

**Mapped IP** : The LAN IP address is a kind of private IP address which is transferred via the NAT ( Network Address Translation ) . So the external user can not directly link to the private IP address . In other words , the external user has to link the BM-2101's external **real IP address**, then map to the internal private IP address via the BM-2101 appliance . That means the external real IP address mapped to the LAN private IP address.

**Server 1/2/3/4 Interface** : It is almost the same as the IP mapped function . The difference is that the virtual server use the **one to many** IP mapped . That means one real IP address mapped to 1~4 LAN private IP address. The virtual server also provide the service items as the same in the **Service** function .

## **Virtual Server**

### **WAN IP**

- The external IP address ( Real IP Address ) .

### **Mapped To Virtual IP**

- The WAN real IP address mapped to the LAN server private IP address .

### **Virtual Server Real IP**

- The virtual server mapped to the WAN IP address.

### **Service**

- The service provided by the virtual server .

### **WAN Port**

- The external port provided by the virtual server . If the selected service using only single port , then the MIS engineer can change its external port . ( For example , the MIS engineer can modify the http port to be 8080 ; If the external user want to browse the web site , then he must change the port . )

### **Server Virtual IP**

- The virtual IP address which the virtual server mapped to.

We set 4 environments.

No .	Range	The Application Environment
Example 1	<b>Mapped IP</b>	To make the single internal server which provides the services of FTP, web, mail, can real working by the policy .
Example 2	<b>Virtual Server</b>	Use the virtual server instead of many of the internal server which only provide single service by policy management. (For example , use the web service ) .
Example 3	<b>Virtual Server</b>	The external user use the VoIP to communicate to the internal user. ( VoIP service port : TCP 1720 , TCP 15328-15333 , UDP 15328-15333 )
Example 4	<b>Virtual Server</b>	Use the virtual server instead of many of the internal server which provide the same services by policy management.(For example , use the HTTP , POP3 , SMTP , DNS service group)

## The Deployment

To apply two ADSL lines included the static IP address .

( WAN1 static IP is 61.11.11.10 ~ 61.11.11.14 )

( WAN2 static IP is 211.22.22.18 ~ 211.22.22.30 )

## 12.1 Example

To make the single internal server which provides the services of FTP, web, mail, can real working by the policy .

Step1. Sets one LAN server which provide the multiple services . The network adapter IP setting is 192.168.1.100 , and the DNS setting correspond to the WAN DNS server .

Step2. In **Address** → **LAN** , add the following settings :

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		<input type="button" value="In Use"/>
Main_Server	192.168.1.100/255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>

The server setting in address

Step3. In **Virtual Server** → **Mapped IP** , add the following settings :

- Click **New Entry** .
- **WAN IP**, enter 61.11.11.12 ( Or click **Assist** to select ) .
- **Map To Virtual IP** , enter 192.168.1.100 .
- Click **OK** .
- Complete the mapped IP setting

Add New Mapped IP	
WAN IP	61.11.11.12 <input type="button" value="Assist"/> WAN1
Map To Virtual IP	192.168.1.100

The mapped IP setting

Step4. In **Service → Group** , to group the services ( DNS , FTP , HTTP , POP3 , SMTP... ) provided by the server . Add the new mail service group which can send the mail to external .

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

New Entry

Fig. 11-3 The service group setting

Step5. In **Policy → Incoming** , add the new policy included Step 3 , Step 4 .

Source	Destination	Service	Action	Option	Configure			Move
Outside_Any	Mapped IP(61.11.11.12)	Main_Service	✓				Modify Remove Pause	To 1

New Entry

Complete the incoming setting in policy

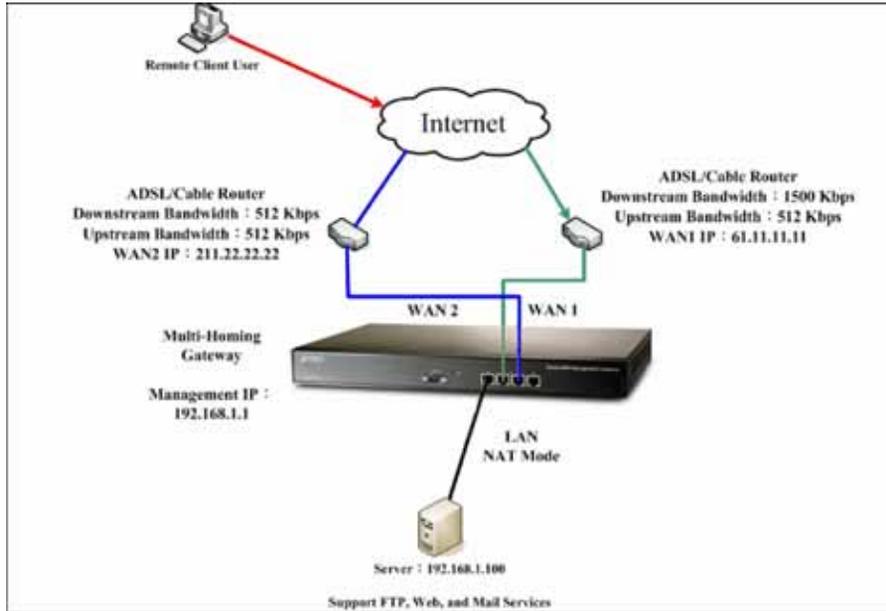
Step6. In **Policy → Outgoing** , add the new policy included Step2, Step 4, it can make the server send the e-mail to external mail server via the mail service .

Source	Destination	Service	Action	Option	Configure			Move
Main_Server	Outside_Any	Mail_Service	✓				Modify Remove Pause	To 1

New Entry

Complete the outgoing setting in policy

Step7. Complete the IP mapped setting which provided the multiple services to external.



Set up the single server environment which provided the multiple services via IP mapped



When the MIS engineer set the IP mapped by policy , it is strongly recommended not to select **ANY** in **Service** function. Because that may cause the IP mapped user be attacked .

Use the virtual server instead of many of the internal server which only provide single service by policy management. (For example , use the web service ) .

Step1. To set up many LAN server which provide the web service. The IP address are 192.168.1.101 , 192.168.1.102 , 192.168.1.103 , 192.168.1.104 .

Step2. In **Virtual Server** → **Server 1** , add the new following settings :

- Click **Virtual Server Real IP** → Click **Here to configure** .
- **Virtual Server Real IP**, enter 211.22.22.23 ( Or click **Assist** to select ) .
- Click **OK** .
- Click **New Entry** .
- **Service** , select HTTP(80) .
- External service port , enter 8080 .
- **Load Balance Server 1** , enter 192.168.1.101 .
- **Load Balance Server 2** , enter 192.168.1.102 .
- **Load Balance Server 3** , enter 192.168.1.103 .
- **Load Balance Server 4** , enter 192.168.1.104 .
- Click **OK** .
- Complete the virtual server setting.

Add New Virtual Server IP	
Virtual Server Real IP	211.22.22.23
	WAN2
	<a href="#">Assist</a>
OK Cancel	

The virtual server IP setting

Virtual Server Configuration	
Virtual Server Real IP	211.22.22.23
Service	HTTP (80)
External Service Port	8080
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
OK Cancel	

The virtual server configuration

Step3. In **Policy** → **Incoming** , add the new policy include Step 2 ( The virtual server setting

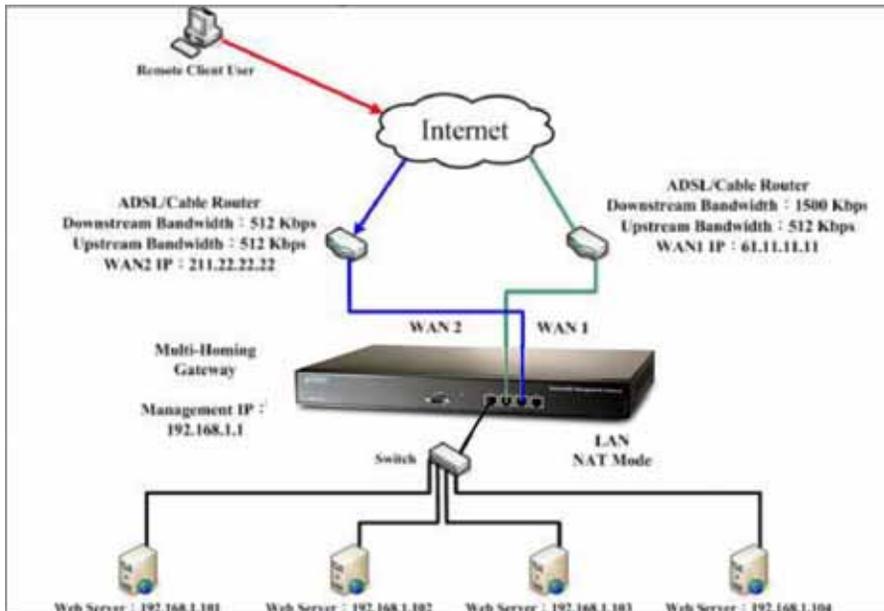
Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server1(211.22.22.23)	HTTP(8080)	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 ▾

Complete the virtual server setting in the policy



If the external user want to link to the homepage provided by the web server , then the user has to modify the port into 8080.

Step4. Make the virtual server can provide the single service to external.



Use the virtual server instead of many internal server to provide the single service

The external user use the VoIP to communicate to the internal user. ( VoIP service port : TCP 1720 , TCP 15328-15333 , UDP 15328-15333 )

Step1. To set the LAN VoIP , its IP address is 192.168.1.100 .

Step2. In **Address** → **LAN** , add the new following setting :

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		<input type="button" value="In Use"/>
VoIP	192.168.1.100/255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>

**The LAN address setting**

Step3. In **Service** → **Custom** , add new VoIP service group :

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

**Add the custom service**

Step4. In **Virtual Server** → **Server 1** , add the new following settings :

- **Virtual Server Real IP** → **click here to configure** .
- **Virtual Server Real IP**, enter 61.11.11.12 ( Or click **Assist** to select ) .
- Click **OK** .
- Click **New Entry** .
- **Service** , select (Custom Service)VoIP\_Service .
- **External Service Port** , auto set From-Service(Custom).
- **Load Balance Server 1** , enter 192.168.1.100.
- Click **OK** .
- Complete the virtual server setting

**The virtual server real IP setting**

Load Balance Server	Server Virtual IP
1	192.168.1.100
2	
3	
4	

**The virtual server setting**



If the **Custom Service** only use **single port** , the MIS engineer can modify the external port in **Virtual Server** ; Contrarily , when the **Custom Service** use **more than one port** , the MIS engineer can not modify the external service port in **Virtual Server** .

Step5. In **Policy → Incoming** , add the new policy included Step4 . ( The virtual server setting ) :

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server1(61.11.11.12)	VoIP_Service	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 ▾

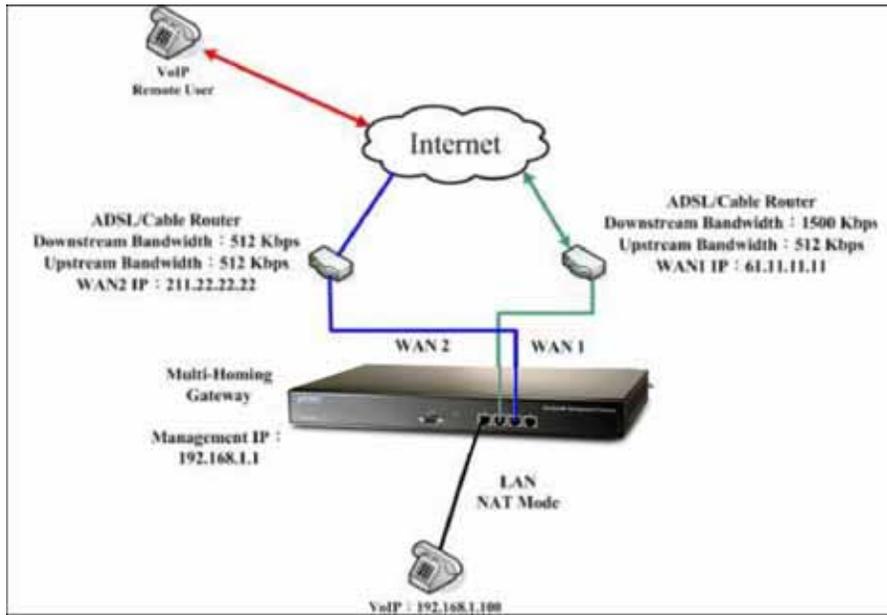
**Complete the virtual server setting in policy**

Step6. In **Policy → Outgoing** , complete the setting of LAN user use VoIP to communicate to external user :

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

**Complete the VoIP setting in policy**

Step7. Make the virtual server provide the communication service between the internal and external user



The deployment of using the communication service between the internal and external user via the virtual server

Use the virtual server instead of many of the internal server which provide the same services by policy management (For example , use the HTTP , POP3 , SMTP , DNS service group).

Step1. Sets many LAN server which provide multiple services , its network adapter IP address are 192.168.1.101 , 192.168.1.102 , 192.168.1.103 , 192.168.1.104 , and the DNS is correspond to the external DNS server .

Step2. In **Address → LAN and LAN Group** , add the new following setting :

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		<b>In Use</b>
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

**The setting of server mapped to name**

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

New Entry

**The LAN server group setting**

Step3. In **Service → Group** , group the service. And add the new policy of service group for the server which can send the mails to external.

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

New Entry

**Add new service group**

Step4. In **Virtual Server** → **Server 1** , add the new following settings :

- **Virtual Server Real IP** → **click here to configure**
- **Virtual Server Real IP**, enter 211.22.22.23 ( Or click **Assist** to select ) .
- Click **OK** .
- Click **New Entry** .
- **Service** , select (Group Service) Main\_ Service .
- **External Service Port** , auto set From-Service(Group) .
- **Load Balance Server** , enter the server virtual IP .
- Click **OK** .
- Complete the virtual server setting

Add New Virtual Server IP	
Virtual Server Real IP	211.22.22.23
	WAN2 <a href="#">Assist</a>
OK Cancel	

**The virtual server real IP setting**

Virtual Server Configuration	
Virtual Server Real IP	211.22.22.23
Service	(Group Service)Main_Service
External Service Port	From-Service(Group) ( Range: 1 - 65535 )
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
OK Cancel	

**The virtual server setting**

Step5. In **Policy → Incoming** , add the new policy included Step4 ( The virtual server setting ) :

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server1(211.22.22.23)	Main_Service	✔		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 ▾

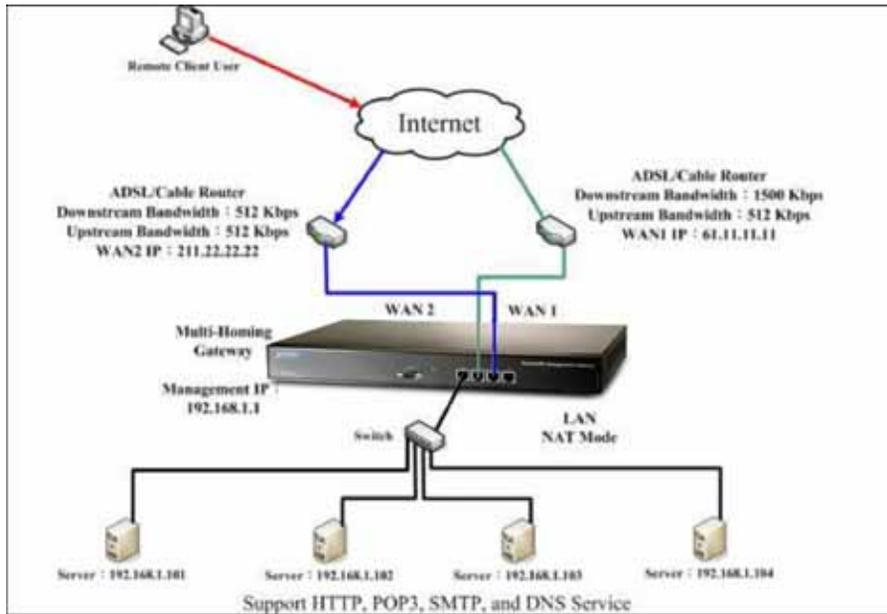
**Complete the incoming setting in policy**

Step6. In **Policy → Outgoing** , add the new policy included Step2, Step3, to make the server can send the e-mail to external mail server via the mail service.

Source	Destination	Service	Action	Option	Configure	Move
Server_Group	Outside_Any	Mail_Service	✔		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 ▾

**Complete the outgoing setting in policy**

Step7. Make the virtual server provide multiple service to external



Deployment of using the virtual server instead of many internal server which provide multiple service to external

# Policy

The BM-2101 can detect every packet pass by the devices , and to valuate if the packets can fit the policy. When the packets can qualified by the policy , the BM-2101 will allow the packets to go through the policy. In other words , if the packets can not fit the policy , then it will be blocked .

The policy parameter included the source address , destination address , service , schedule , authenticatoin user , VPN trunk , action, WAN port , traffic log , statistics , IDP , content blocking , anti-virus , Qos , MAX.concurrent sessions , quota per session and quota per day . The MIS engineer can use these parameters to set the outgoing and incoming service in data transmission by policy management.



### How to use the Policy ?

The BM-2101 can divide the Policy into 6 function depends on the data packets in different source address . The MIS engineer can easy to set the policy of source IP , source port , destination IP and destination port by data packets .

1. **Outgoing** : The source IP is in LAN and the destination IP is in WAN .The MIS engineer can set the outgoing policy included the network packets and services .
2. **Incoming** : The source IP is in WAN and the destination IP is in LAN ( For example , the IP mapped and virtual server ) . The MIS engineer can set the incoming policy included the network packets and services.
3. **WAN To DMZ** : The source IP is in WAN and the destination IP is in DMZ (For example , the IP mapped and virtul server ) .The MIS engineer can set the WAN To DMZ policy included the network packets and services .

4. **LAN To DMZ** : The source IP is in LAN and the destination IP is in DMZ . The MIS engineer can set the LAN To DMZ policy included the network packets and services .
5. **DMZ To LAN** : The source IP is in DMZ and the destination IP is in LAN . The MIS engineer can set the DMZ To LAN policy included the network packets and services .
6. **DMZ To WAN** : The source IP is in DMZ and the destination IP is in WAN . The MIS engineer can set the DMZ To WAN policy included the network packets and services .



All the packets need to be permitted by the policy in BM-2101 . The MIS engineer has to set the fitness policy in BM-2101, in order to make the LAN , WAN and DMZ connection works.



The BM-2101 's VPN function use the trunk technology by policy management , in order to monitor the packets through the data exchange.

## Policy

### Comment

- The description of policy .

### Source Address & Destination Address

- The active connection is the source IP and the passive connection is the destination IP .

### Service

- It represents the service item . The MIS engineer can select to use the system default setting or choose the **Policy Object → Service → Custom** , to use the custom setting .

### Option

- Use the icon to display as the option enabled.

Icon	Name	Definition
	Schedule	Enable the schedule autorun on certain time.
	Authentication User	Authenticatoin is enabled .
	Traffic Log	Traffic Log is enabled .
	Statistics	Statistics is enabled .
	Content Blocking	content blocking is enabled .
	Qos	Qos is enabled .

### Schedule

- Set the schedule time by policy .

## Authentication User

- User has to pass the authentication , then connect to the network by Policy .

## VPN Trunk

- To apply the IPsec and PPTP VPN into VPN trunk by policy .

## Action

- To assign the path when the data packets pass through the WAN1 , WAN2 , WAN3 or WAN4 in the BM-2101 or select to deny .

Icon	Name	Definition
	PERMIT ALL	To permit the qualified packets can go through WAN1 , WAN2.
	PERMIT WAN1	To permit the qualified Packets can pass by
	PERMIT WAN2	To permit the qualified Packets can pass by
	PERMIT VPN Trunk	To permit the VPN Trunk qualified by Policy .
	DENY	To deny the Packets qualified by Policy .
	PAUSE	To stop the Policy .

## Traffic Log

- To record all the packets pass through the policy . The MIS engineer can click  to view .

## Statistics

- Use the graphic charts to display the flow statistics .

## Content Blocking

- To manage the packet contents which applied policy .

## Qos

- To setup the MAX.Bandwidth and G.Bandwidth by policy . ( The Bandwidth is shared by the user qualified by policy . )

## MAX. Concurrent Sessions

- To assign the sessions permitted by policy . If the sessions are over the limit, then it will not build successfully .

## Quota Per Session

- To allocate the max flow ( KBtes ) in every session by policy management .

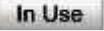
## Quota Per Day

- To allocate the max flow ( MBytes/Sec) in everyday .

## NAT

- When the packets pass through the LAN (DMZ) from external , the packets source IP will change into the BM-2101's LAN ( DMZ ) IP address .

## Pause

- If it is necessary to modify the applied option in policy management (address , Qos....) , then the MIS engineer can stop the policy and disable the  , to modify the contents .

## Move

- To click the drop down menu and change the policy sorting . ( The BM-2101 will check the passing packets depends on the policy sorting. )

We set 6 environments.

No.	Range	The Application Environment
Example. 1	<b>Outgoing</b>	To set the policy to monitor the internal user link to the network . (use traffic log , statistics and quota per session)
Example. 2	<b>Outgoing</b>	To deny the user to access the specify network resources. ( For example , the static IP and content blocking. )
Example. 3	<b>Outgoing</b>	To permitted the authenticated user can access the network resources on specific time .
Example. 4	<b>Incoming</b>	The external user use the remote control software to control the internal PCs . ( For example , pcAnywhere )
Example. 5	<b>WAN To DMZ</b>	Sets a FTP server in the DMZ by NAT mode , and to limit the external user's downstream bandwidth , MAX.concurrent sessions and quota per day.
Example. 6	<b>WAN To DMZ DMZ To WAN LAN To DMZ</b>	Sets a mail server in the DMZ by TRANSARENT mode , and to permit the internal and external user to send and receive e-mail.

\* DMZ = Demilitarized Zone

## 13.1 Example

To set the policy to monitor the internal user link to the network. (use traffic log , statistics and quota per session)

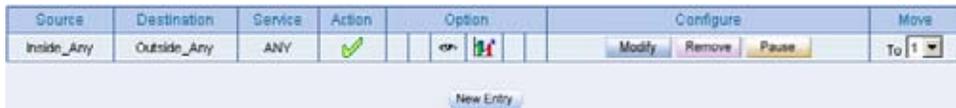
Step1. In **Policy → Outgoing** , add the following settings :

- Click **New Entry** .
- Select **Traffic Log** .
- Select **Statistics** .
- In **Quota Per Session** , enter 10KBytes/Sec .
- Click **OK** .

Comment :	<input type="text" value=""/>	(Max. 64 characters)
<b>Add New Policy</b>		
Source Address	Inside_Any ▾	
Destination Address	Outside_Any ▾	
Service	ANY ▾	
Schedule	None ▾	
Authentication User	None ▾	
VPN Trunk	None ▾	
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2	
Traffic Log	<input checked="" type="checkbox"/> Enable	
Statistics	<input checked="" type="checkbox"/> Enable	
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download <input type="checkbox"/> Upload	
QoS	None ▾	
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )	
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )	
Quota Per Session	<input type="text" value="10"/> KBytes ( Range: 0 - 999999 )	
Quota Per Day	<input type="text" value="0"/> MBytes ( Range: 0 - 999999 )	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>		

To Set the new policy

Step2. In **Policy → Outgoing** , to complete the traffic log , statistics and quota per session setting .



Complete to set the policy

Step3. In **Traffic Log Filtered** window , click [refresh] to monitor packets through the policy .

- In **Traffic Log Filtered** window , click the drop down menu at the upper left , to select the Refresh frequency .
- In **Traffic Log Filtered** , click the IP address displayed in the window , then it will filter the IP packets record .
- If the MIS engineer want to monitor all the BM-2101's packets , click **Traffic Log→ Traffic** .



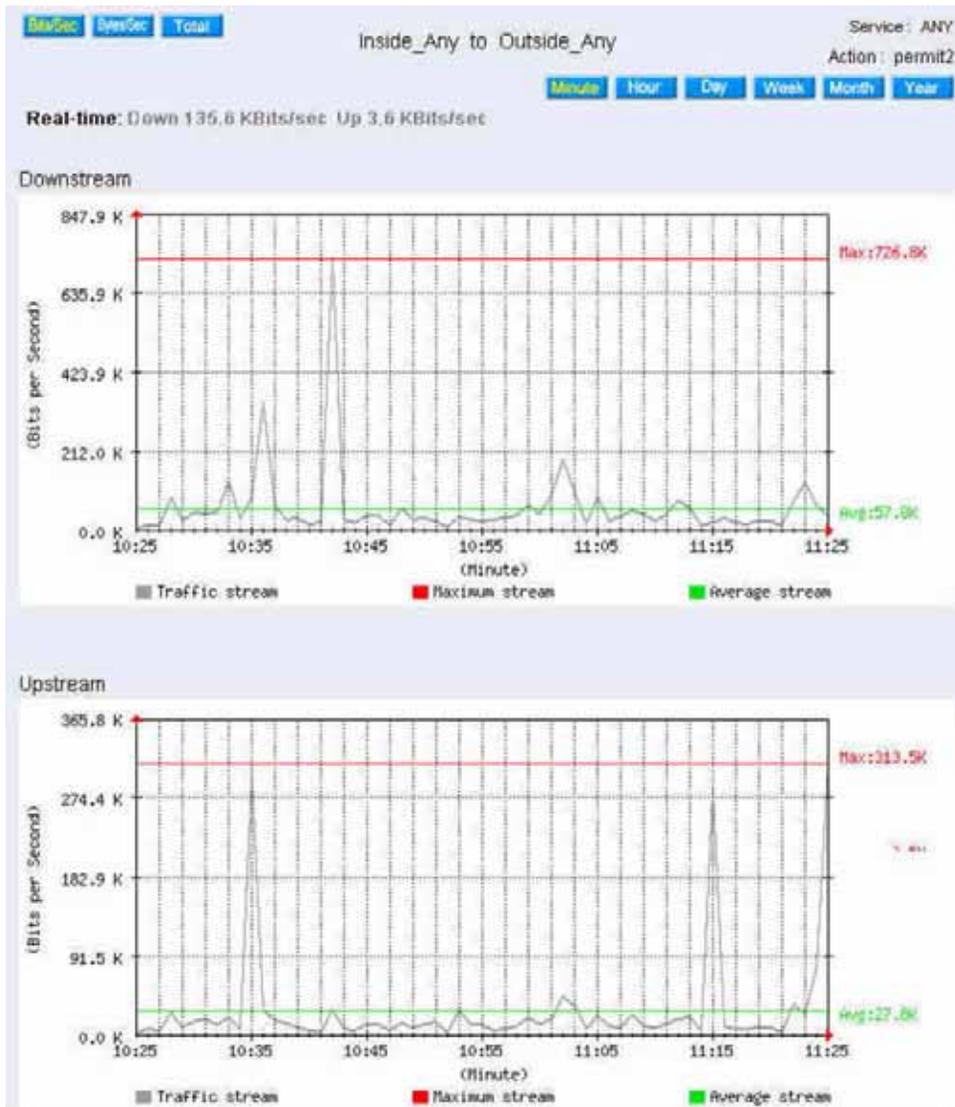
The Traffic Log Filtered window



Time	Source IP	Destination IP	Protocol	Port	Traffic	Disposition
May 22 17:19:25	192.168.139.33	192.168.139.1	TCP	3524 => 80	17 KB	✓
May 22 17:19:24	192.168.139.33	192.168.139.1	TCP	3523 => 80	7 KB	✓
May 22 17:19:19	192.168.139.30	66.102.7.99	TCP	2026 => 80 (WAN2)	48 B	✓
May 22 17:19:19	192.168.139.30	168.95.192.1	UDP	2025 => 53 (WAN2)	63 B	✓
May 22 17:19:09	192.168.139.10	163.19.1.1	UDP	38360 => 53 (WAN2)	223 B	✓
May 22 17:19:09	192.168.139.10	168.95.192.1	UDP	38360 => 53 (WAN2)	146 B	✓
May 22 17:19:08	192.168.139.10	168.95.1.1	UDP	38360 => 53 (WAN1)	73 B	✓
May 22 17:18:25	192.168.139.10	163.19.1.1	UDP	38360 => 53 (WAN2)	444 B	✓
May 22 17:18:25	192.168.139.10	168.95.192.1	UDP	38360 => 53 (WAN2)	290 B	✓
May 22 17:18:24	192.168.139.10	168.95.1.1	UDP	38360 => 53 (WAN1)	290 B	✓
May 22 17:16:50	192.168.139.10	163.19.1.1	UDP	38360 => 53 (WAN2)	444 B	✓
May 22 17:16:50	192.168.139.10	168.95.192.1	UDP	38360 => 53 (WAN2)	290 B	✓
May 22 17:16:50	192.168.139.10	168.95.1.1	UDP	38360 => 53 (WAN1)	290 B	✓
May 22 17:16:13	219.137.145.189	203.73.242.21	ICMP	---	184 B	✓
May 22 17:15:16	192.168.139.10	163.19.1.1	UDP	38360 => 53 (WAN2)	444 B	✓
May 22 17:15:16	192.168.139.10	168.95.192.1	UDP	38360 => 53 (WAN2)	290 B	✓
May 22 17:15:16	192.168.139.10	168.95.1.1	UDP	38360 => 53 (WAN1)	290 B	✓
May 22 17:14:21	192.168.139.33	192.168.139.1	TCP	3508 => 80	42 KB	✓
May 22 17:14:21	192.168.139.33	192.168.139.1	TCP	3507 => 80	91 KB	✓
May 22 17:13:43	192.168.139.10	163.19.1.1	UDP	38360 => 53 (WAN2)	444 B	✓
May 22 17:13:43	192.168.139.10	168.95.192.1	UDP	38360 => 53 (WAN2)	290 B	✓
May 22 17:12:25	192.168.139.33	192.168.139.1	TCP	3502 => 80	15 KB	✓
May 22 17:12:25	192.168.139.33	192.168.139.1	TCP	3501 => 80	67 KB	✓
May 22 17:12:10	192.168.139.10	163.19.1.1	UDP	38360 => 53 (WAN2)	221 B	✓
May 22 17:12:10	192.168.139.10	168.95.192.1	UDP	38360 => 53 (WAN2)	144 B	✓
May 22 17:12:05	192.168.139.10	168.95.1.1	UDP	38359 => 53 (WAN1)	218 B	✓
May 22 17:12:04	192.168.139.10	163.19.1.1	UDP	38359 => 53 (WAN2)	223 B	✓
May 22 17:12:04	192.168.139.10	168.95.192.1	UDP	38359 => 53 (WAN2)	146 B	✓
May 22 17:10:29	192.168.139.10	163.19.1.1	UDP	38359 => 53 (WAN2)	444 B	✓
May 22 17:10:29	192.168.139.10	168.95.1.1	UDP	38359 => 53 (WAN1)	290 B	✓
May 22 17:10:29	192.168.139.10	168.95.192.1	UDP	38359 => 53 (WAN2)	290 B	✓
May 22 17:09:57	192.168.139.30	69.25.57.140	TCP	2017 => 80 (WAN1)	6 KB	✓
May 22 17:09:57	192.168.139.30	205.180.86.14	TCP	2013 => 80 (WAN2)	2 KB	✓
May 22 17:09:42	192.168.139.30	66.102.7.147	TCP	2006 => 80 (WAN2)	14 KB	✓
May 22 17:09:37	192.168.139.30	61.219.237.250	TCP	2021 => 6969 (WAN2)	89 KB	✓
May 22 17:09:37	192.168.139.30	61.219.237.250	TCP	2020 => 6969 (WAN2)	65 KB	✓
May 22 17:09:15	192.168.139.30	59.124.51.50	TCP	2018 => 80 (WAN2)	2 KB	✓
May 22 17:09:07	192.168.139.30	211.76.137.1	TCP	2008 => 80 (WAN1)	6 KB	✓
May 22 17:09:03	192.168.139.30	61.219.34.150	TCP	2019 => 443 (WAN2)	1 KB	✓
May 22 17:08:57	192.168.139.30	204.13.83.253	TCP	2011 => 80 (WAN2)	20 KB	✓
May 22 17:08:57	192.168.139.30	204.13.83.253	TCP	2010 => 80 (WAN2)	37 KB	✓
May 22 17:08:56	192.168.139.30	216.239.63.97	TCP	2016 => 443 (WAN1)	6 KB	✓
May 22 17:08:54	192.168.139.30	168.95.192.1	UDP	2014 => 53 (WAN1)	176 B	✓
May 22 17:08:54	192.168.139.30	168.95.192.1	UDP	2015 => 53 (WAN1)	416 B	✓
May 22 17:08:53	192.168.139.30	168.95.192.1	UDP	2014 => 53 (WAN1)	63 B	✓
May 22 17:08:51	192.168.139.30	168.95.192.1	UDP	2012 => 53 (WAN2)	315 B	✓
May 22 17:08:50	192.168.139.30	168.95.1.1	UDP	2012 => 53 (WAN1)	65 B	✓

Clear

Step4. In **Monitor** → **Statistics** → **Policy** , it shows the traffic statistics through the policy .



Traffic statistics

To deny the user to access the specify network resources. ( For example , the static IP and content blocking. )

Step1. In **Content Blocking** → **URL** → **Script** → **P2P** → **IM** → **Download**→**Upload**, add the following settings :

URL String	Configure
~deu	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
~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"/>

**Content blocking setting**

**Script Blocking**

<input checked="" type="checkbox"/> Popup Blocking	<input checked="" type="checkbox"/> ActiveX Blocking
<input checked="" type="checkbox"/> Java Blocking	<input checked="" type="checkbox"/> Cookie Blocking

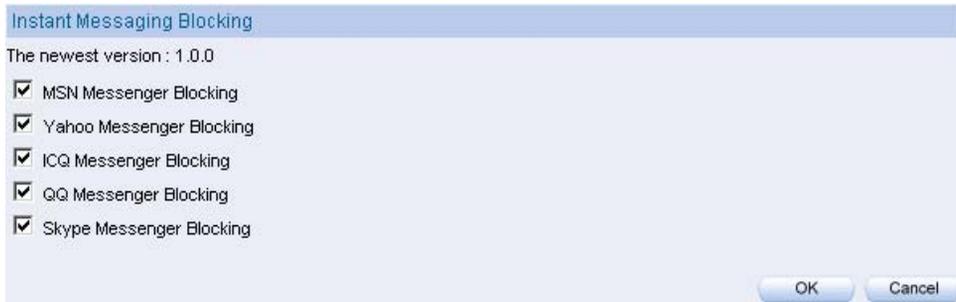
**12-7 Script setting**

**Peer-to-Peer Application**

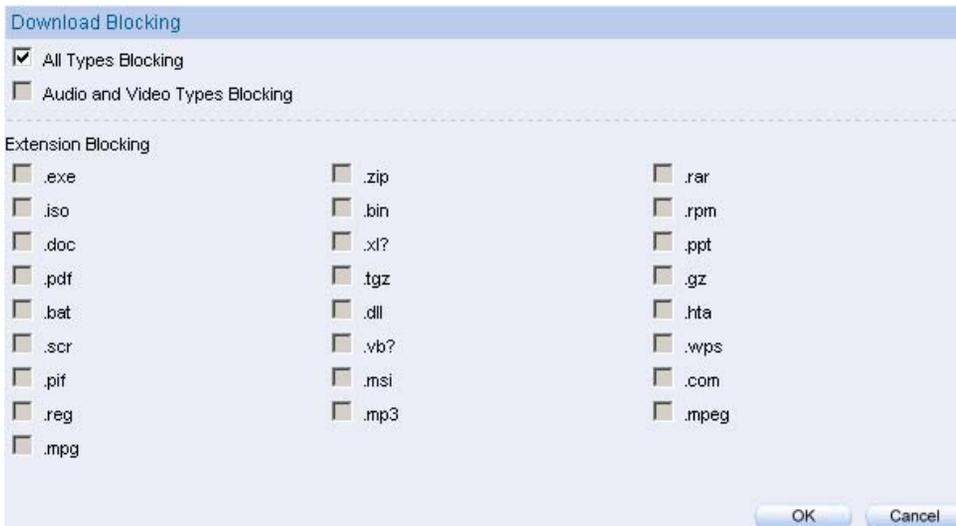
The newest version : 1.0.0

<input checked="" type="checkbox"/> eDonkey
<input checked="" type="checkbox"/> Bit Torrent
<input checked="" type="checkbox"/> WinMX
<input checked="" type="checkbox"/> Foxy
<input checked="" type="checkbox"/> KuGoo

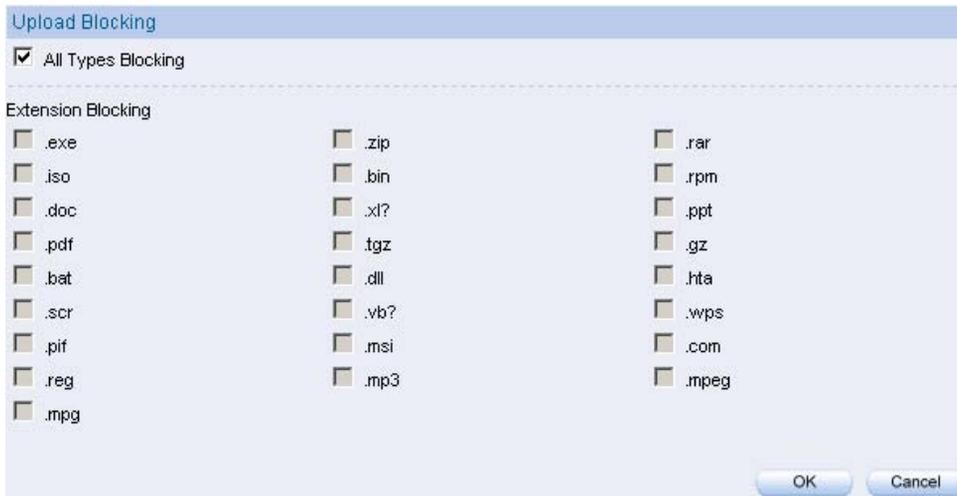
**Peer-to -Peer application setting**



### IM setting



### Download setting



**Upload setting**



1. The MIS engineer can limit the user to browse only specific web site through the content blocking by policy management.
2. The Script policy setting can deny the user to use the specific function , for example Java , cookie , market exchange web site .
3. The Peer to Peer application policy can limit the user to use the Peer to Peer applicatoin , for example , eDonkey , BT , WinMX .
4. The IM policy can limit the user to use the MSN messenger , Yahoo messenger , ICQ, QQ and Skype by transferring the Video and Audion files , messages and documents .
5. The Download policy can limit the user to access the Video and Audio files , extension files via the HTTP and FTP.

Step2. In **Address**→**WAN and WAN Group** , add the following settings :

Name	IP / Netmask	Configure
Outside_Any	0.0.0.0/0.0.0.0	<input type="button" value="In Use"/>
Remote_Server1	61.219.38.98/255.255.255.255	<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"/>

**Set the WAN IP 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"/>

**Group the WAN**



The MIS engineer can customize to group the address and apply it to policy.

Step3. In **Policy → Outgoing** , add the following settings :

- Click **New Entry** .
- **Destination Address** , select **WAN\_Group** set in Step2 . ( Use the IP to block . )
- **Action , WAN Port** , select **DENY ALL** .
- Click **OK** .

Comment :  (Max. 64 characters)

Add New Policy	
Source Address	Inside_Any
Destination Address	WAN_Group
Service	ANY
Schedule	None
Authentication User	None
VPN Trunk	None
Action, WAN Port	<input type="checkbox"/> PERMIT ALL <input checked="" type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download <input type="checkbox"/> Upload
QoS	None
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	0 MBytes ( Range: 0 - 999999 )

OK Cancel

**Set the policy included blocking function**

Step4. In **Policy → Outgoing** , add the following settings :

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

Comment :  (Max. 64 characters)

Add New Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Schedule	None ▾
Authentication User	None ▾
VPN Trunk	None ▾
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input checked="" type="checkbox"/> URL <input checked="" type="checkbox"/> Script <input checked="" type="checkbox"/> P2P <input checked="" type="checkbox"/> IM <input checked="" type="checkbox"/> Download <input checked="" type="checkbox"/> Upload
QoS	None ▾
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	0 MBytes ( Range: 0 - 999999 )

**To set the content blocking policy**

Step5. Complete to set the policy to deny users access the network resources

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	WAN_Group	ANY	✘		Modify Remove Pause	To 1
Inside_Any	Outside_Any	ANY	✔	⊖	Modify Remove Pause	To 2

[New Entry](#)

**Complete to set the policy to deny users access the network resources .**



The DENY action can block the packets correspond to the policy .The MIS engineer can move the policy to first priority , to limit users link to the specific IP address .

To permitted the authenticated user can access the network resources on specific time.

Step1. In **Schedule** , add the following settings:

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

**Add new schedule**

Step2. In **Authentication** → **User** and **User Group** , add the following settings:

Name	Member	Radius	POP3	Configure
laboratory	joy, john, jack			<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>

**The authentication user group setting**



The MIS engineer can use the group function in **Authentication** and **Service** , to easily set the policy .

Step3. In **Policy** → **Outgoing** , add the following setting :

- Click **New Entry** .
- **Authentication User** , select laboratory .
- **Schedule** , select WorkingTime .
- Click **OK**

Comment :  (Max. 64 characters)

**Add New Policy**

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	WorkingTime
Authentication User	laboratory
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download <input type="checkbox"/> Upload
QoS	None
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	0 MBytes ( Range: 0 - 999999 )

OK Cancel

To set the authentication and schedule policy

Step4. Complete the setting to permitte the user can access the network resources on specific time via the authentication .

Source	Destination	Service	Action	Option	Configurs	Move
Inside_Any	Outside_Any	ANY			Modify Remove Pause	To 1

New Entry

Complete to set the authentication and schedule policy

The external user use the remote control software to control the internal PCs . ( For example , pcAnywhere )

Step1. To set up a LAN PC remoted by the external PC , the server virtual IP is 192.168.1.2 .

Step2. In **Virtual Server** → **Server 1** , add the following settings :

Virtual Server Real IP

Total entry : 1

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

**Set the virtual server**

Step3. In **Policy** → **Incoming** , add the following settings :

- Click **New Entry** .
- **Destination Address** , select Virtual Server 1(61.11.11.12) .
- **Service** , select PC-Anywhere(5631-5632) .
- Click **OK**

Comment :  (Max. 64 characters)

Add New Policy	
Source Address	Outside_Any ▾
Destination Address	Virtual Server 1(61.11.11.12) ▾
Service	PC-Anywhere(5631-5632) ▾
Schedule	None ▾
VPN Trunk	None ▾
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT <input type="checkbox"/> DENY
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	None ▾
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	0 MBytes ( Range: 0 - 999999 )
NAT	<input type="checkbox"/> Enable

OK Cancel

To set the policy of LAN PC remotod by the external PC

Step4. Complete to set the policy of LAN PC remotod by the external PC .

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server1(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 ▾

New Entry

Complete to set the policy of LAN PC remotod by the external PC

Set a FTP server in the DMZ by NAT mode , and to limit the external user's downstream bandwidth , MAX.concurrent sessions and quota per day.

Step1. In **DMZ** , to set up a FTP server and the server virtual IP is 192.168.3.2 .  
 ( The DMZ interface address is 192.168.3.1/24 )

Step2. In **Virtual Server** → **Server 1** , add the following settings :

Virtual Server Real IP

Total entry : 1

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

Set the virtual server correspond to FTP server



In Policy → Incoming or WAN To DMZ , it is strongly recommended not to select the Service to be ANY , to avoid the internal PC be attacked.

Step3. In **QoS** , add the following settings :

Total entry : 1

Name	WAN	Downstream Bandwidth	Upstream Bandwidth	Priority	Configure
FTP_Qos	1	G.Bandwidth = 100 Kbps M.Bandwidth = 500 Kbps	G.Bandwidth = 50 Kbps M.Bandwidth = 200 Kbps	Middle	<input type="button" value="Modify"/>
	2	G.Bandwidth = 500 Kbps M.Bandwidth = 512 Kbps	G.Bandwidth = 50 Kbps M.Bandwidth = 60 Kbps		<input type="button" value="Remove"/>

Set the Qos

Step4. In **Policy** → **WAN To DMZ** , add the following settings :

- Click **New Entry** .
- **Destination Address** , select Virtual Server 1(61.11.11.12) .
- **Service** , select FTP(21) .
- **QoS** , select FTP\_QoS .
- **MAX . Concurrent Sessions** , enter 100 .
- **Quota Per Day** , enter 100000 Mbytes .
- Click **OK**

Comment :  (Max. 64 characters)

Add New Policy	
Source Address	Outside_Any ▾
Destination Address	Virtual Server 1(61.11.11.12) ▾
Service	FTP(21) ▾
Schedule	None ▾
VPN Trunk	None ▾
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT <input type="checkbox"/> DENY
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	FTP_QoS ▾
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	10 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	100000 MBytes ( Range: 0 - 999999 )
NAT	<input type="checkbox"/> Enable

OK Cancel

Add new policy

Step5. Limit users access the DMZ server services and network resources .

Source	Destination	Service	Action	Option	Configura	Move
Outside_Any	Virtual Server1(61.11.11.12)	FTP(21)	✔	⊗	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 ▾

New Entry

Complete to set the policy

Sets a mail server in the DMZ by TRANSARENT mode , and to permit the internal and external user to send and receive e-mail.

Step1. In **DMZ** , to set a mail server , and the IP is 61.11.11.12 . The DNS set to correspond to the external DNS server .

Step2. In **Address → DMZ** , add the following settings :

Name	IP / Netmask	MAC Address	Configure
DMZ_Any	0.0.0.0/0.0.0.0		<b>In Use</b>
Mail_Server	61.11.11.12/255.255.255.255	00:4B:54:55:E1:07	Modify Remove

New Entry

To set the mail server correspond to the IP address

Step3. In **Service → Group** , add the following settings :

Group name	Service	Configure
E-mail	DNS,POP3,SMTP	Modify Remove

New Entry

To set up the service group included the POP3 , SMTP and DNS

Step4. In Policy → WAN To DMZ , add the following settings :

- Click **New Entry** .
- **Destination Address** , select Mail\_Server .
- **Service** , select E-mail .
- Click **OK** .

Comment :  (Max. 64 characters)

Add New Policy	
Source Address	Outside_Any ▾
Destination Address	Mail_Server ▾
Service	E-mail ▾
Schedule	None ▾
VPN Trunk	None ▾
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT <input type="checkbox"/> DENY
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	None ▾
MAX. Concurrent Sessions Per IP	0 <input type="text"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 <input type="text"/> ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 <input type="text"/> KBytes ( Range: 0 - 999999 )
Quota Per Day	0 <input type="text"/> MBytes ( Range: 0 - 999999 )
NAT	<input type="checkbox"/> Enable

OK Cancel

To set the WAN To DMZ mail service policy

Step5. Complete to set the WAN To DMZ mail service policy

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 ▾

Complete to set the WAN To DMZ mail service policy

Step6. In **Policy** → **LAN To DMZ** , add the following settings :

- Click **New Entry** .
- **Destination Address** , select **Mail\_Server** .
- **Service** , select **E-mail** .
- Click **OK**

Comment :  (Max. 64 characters)

Add New Policy	
Source Address	Outside_Any ▾
Destination Address	Mail_Server ▾
Service	E-mail ▾
Schedule	None ▾
VPN Trunk	None ▾
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT <input type="checkbox"/> DENY
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	None ▾
MAX. Concurrent Sessions Per IP	0 <input type="text"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 <input type="text"/> ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 <input type="text"/> KBytes ( Range: 0 - 999999 )
Quota Per Day	0 <input type="text"/> MBytes ( Range: 0 - 999999 )
NAT	<input type="checkbox"/> Enable

To set the LAN To DMZ mail service policy

Step7. Complete to set the LAN To DMZ mail service policy.

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 to set the LAN To DMZ mail service policy

Step8. In Policy → DMZ To WAN , add the following settings :

- Click **New Entry** .
- **Destination Address** , select Mail\_Server .
- **Service** , select E-mail .
- Click **OK**

Comment :  (Max. 64 characters)

**Add New Policy**

Source Address	Mail_Server
Destination Address	Outside_Any
Service	E-mail
Schedule	None
Authentication User	None
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download <input type="checkbox"/> Upload
QoS	None
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	0 MBytes ( Range: 0 - 999999 )

OK Cancel

To set the DMZ To WAN Mail service policy

Step9. Complete to set the DMZ To WAN mail service policy .

Source	Destination	Service	Action	Option	Configures	Move
Mail_Server	Outside_Any	E-mail	✔		Modify Remove Pause	To 1

New Entry

Complete to set the DMZ To WAN mail service policy

## Chapter 14

# Anomaly Flow IP

When the BM-2101 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.

## 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 keep 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-2101. If over the setting value, then BM-2101 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-2101. If over the setting value, then BM-2101 will define it to be attacked.
  - ◆ **SYN Flood Threshold Blocking Time (Per Source IP )** : The BM-2101 will block the packets from the attack source IP according to the time setting. After the blocking time, the BM-2101 will re-calculate the total SYN flow from every source IP , if over the setting value, then BM-2101 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-2101. If over the setting value, then BM-2101 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-2101. If over the setting value, then BM-2101 will define it to be attacked.
  - ◆ **ICMP Flood Threshold Blocking Time ( Per Source IP )** : The BM-2101 will block the packets from the attack source IP according to the time setting. After the blocking time, the BM-2101 will re calculate the total ICMP flow from every source IP , if over the setting value, then BM-2101 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-2101. If over the setting value, then BM-2101 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-2101. If over the setting value, then BM-2101 will define it to be attacked.
  - ◆ **Udp Flood Threshold Blocking Time ( Per Source IP )** : The BM-2101 will block the packets from the attack source IP according to the time setting. After the blocking time, the BM-2101 will re calculate the total UDP flow from every source IP , if over the setting value, then BM-2101 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 pretend the legal user to pass through the BM-2101.

### **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 packes, 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 wich 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-2101 will instantly show the message in **Virus-infected IP** and **Attack Events**. If the MIS engineer enable the function in **System → E-mail alert notification** , then the BM-2101 will automatically send the notification to the MIS engineer. **Enable the SNMP → SNMP Trap**, can show the message on the SNMP Trap client software .

## 14.1 Example

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 100 sessions/sec)**
- **Select Enable Virus-infected IP Blocking ( Blocking Time 60 seconds)**
- **Select Enable E-Mail alert notification.**
- **Select Enable Snmp Trap 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 - 999 )

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

Enable E-Mail Alert Notification

Enable SNMP Trap Alert Notification

Enable NetBIOS Alert Notification      IP Address of Administrator

Enable Co-Defense System

Switch Model       IP Address of switch

Username  (Max. 32 characters)

Password  (Max. 32 characters)

---

**DoS / Anti-Attack Setting**

Sasser Block       MSBlaster Block

Code Red Block       Nimda Block

Detect SYN Attack      SYN Flood Threshold (Total)  Pkts/Sec

SYN Flood Threshold (Per Source IP)  Pkts/Sec

SYN Flood Threshold Blocking Time (Per Source IP)  Seconds

Detect ICMP Flood      ICMP Flood Threshold (Total)  Pkts/Sec

ICMP Flood Threshold (Per Source IP)  Pkts/Sec

ICMP Flood Threshold Blocking Time (Per Source IP)  Seconds

Detect UDP Flood      UDP Flood Threshold (Total)  Pkts/Sec

UDP Flood Threshold (Per Source IP)  Pkts/Sec

UDP Flood Threshold Blocking Time (Per Source IP)  Seconds

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
<input type="button" value="New Entry"/>		

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



Enable **Co-Defense System** , then the BM-2101 can send the defense message to the assigned **Switch Model**.

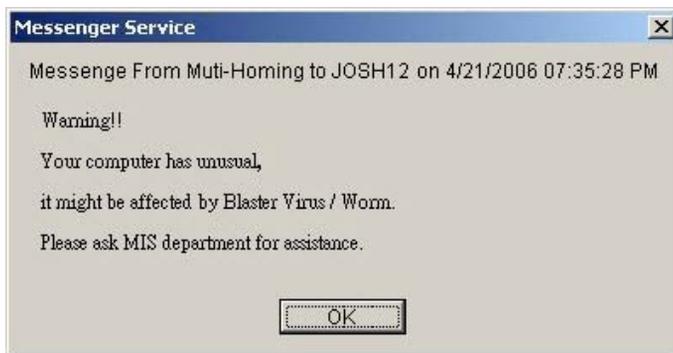


Add **Non-detected IP** , these specific IP is not controlled this function the tube.

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 : 100			
Interface	Virus-infected IP	MAC	Alarm Time
LAN	192.168.189.30		2006-04-21 19:35:28

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



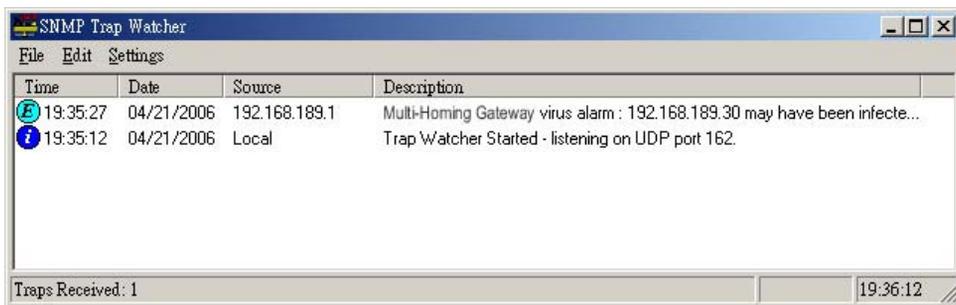
**Send the NetBIOS Alert notification to the virus-infected PC**



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

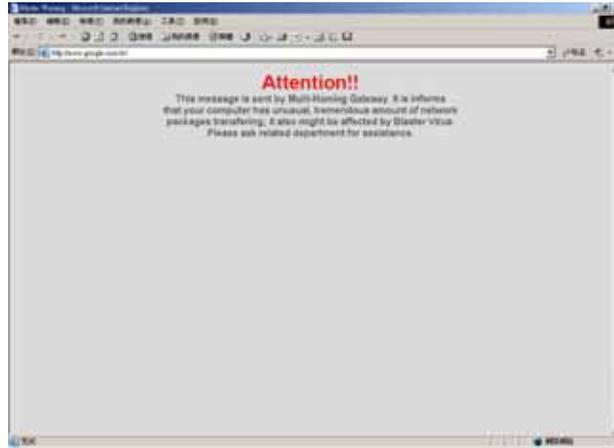
Step3. Enable the **System → E-Mail alert notification** , then the BM-2101 will send the mail notice to the MIS engineer.

Step4. If enable the **SNMP → SNMP Trap**, then the Bandwidth Management Gateway will show the message on the SNMP Trap client software.



**The SNMP Trap client receive the virus alert by the client software**

Step5. When internal user PC got virus – infected , the BM-2101 will show the alert message at first time ( If the virus-infected user can not solve the problem then the BM-2101 will restrict the virus-infected user and it will make the link speed slow and will not show any alert message again.)



Show the alert message

Step6. Enable the **Anomaly Flow → Attack Event** , then the BM-2101 shows the attack information in detail.

Time	Event
May 25 14:57:59	The system has detected the attack of TCP port scan , suspected to be 59.33.66.2
May 25 14:57:53	The system has detected the attack of TCP port scan , suspected to be 60.22.3.6
May 25 14:57:49	The system has detected the attack of TCP port scan , suspected to be 100.36.99.11
May 25 14:57:47	The system has detected the attack of TCP port scan , suspected to be 100.36.99.11
May 25 14:57:45	The system has detected the attack of TCP port scan , suspected to be 100.36.99.11
May 25 14:57:42	The system has detected the attack of TCP port scan , suspected to be 100.36.99.11
May 25 14:57:26	The system has detected the attack of TCP port scan , suspected to be 60.22.3.6
May 25 14:57:24	The system has detected the attack of TCP port scan , suspected to be 60.22.3.6
May 25 14:57:20	The system has detected the attack of TCP port scan , suspected to be 60.22.3.6
May 25 14:57:04	The system has detected the attack of TCP port scan , suspected to be 59.33.66.2
May 25 14:57:02	The system has detected the attack of TCP port scan , suspected to be 59.33.66.2
May 25 14:56:55	The system has detected the attack of TCP port scan , suspected to be 59.33.66.2

**Anomaly Flow IP attack event**

# Monitor

**Log** , includes the information of traffic, event, and connection.

MIS engineer can set the **Traffic** parameters in **Policy** , or select **View Log & Report Privilege** in **System. Log** function can specifically record the data packets contents by **Policy** setting. **Traffic** function can also record the BM-2101 destination and source data packets by **System** setting.

**Event** , record the BM-2101 system configuration of the modified contents , users , time , parameters and the log in IP address.

**Connection** , record all the BM-2101 connecting information. MIS engineer can easily to know the status depends on the connecting information when the problems happened .



### How to use Monitor ?

- (一) **Traffic** , MIS engineer can view the connection status includes time, source IP , destination IP and disposition. BM-2101 can backup the traffic log and refresh the online record on specific time period.
- (二) **Event** , if BM-2101 detected some events happened , MIS engineer can know the events description and backup it.
- (三) **Connection** , can record the connection status by this function.
- (四) **Log Backup** , MIS engineer can set the BM-2101 to automatically send the email alarm of traffic and events or instantly send the log to syslog server.

We set 4 monitoring environments.

No.	Range	The Application Environment
Example. 1	<b>Traffic</b>	View the user's used Protocol and Port , to access the internal and external resources via BM-2101
Example. 2	<b>Event</b>	View the status of MIS engineer log into BM-2101 poccus the managemnt and external interface.
Example. 3	<b>Connection</b>	View the external interface record of bandwidth management .
Example. 4	<b>Log Backup</b>	MIS engineer can receive or save the record results from the BM-2101

## 15.1 Traffic

View the user's used Protocol and Port , to access the internal and external resources via BM-2101

Step1 **Policy → DMZ To WAN** , add the following settings :

Comment :  (Max. 64 characters)

Add New Policy	
Source Address	DMZ_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2
Traffic Log	<input checked="" type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download <input type="checkbox"/> Upload
QoS	None
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	0 MBytes ( Range: 0 - 999999 )

OK Cancel

Traffic setting in policy

Step2 **Policy → DMZ To WAN** , complete the traffic setting in policy :

Source	Destination	Service	Action	Option	Configure	Move
DMZ_Any	Outside_Any	ANY			Modify Remove Pause	To 1

New Entry

Complete the DMZ To WAN traffic setting in policy

Step3 **Monitor** → **Traffic** , it shows the packets traffic through policy.

1 / 573 Next

🔍

Time	Source IP	Destination IP	Protocol	Port	Traffic	Disposition
Jun 12 09:24:06	61.218.156.18	59.124.36.163	UDP	40146 ⇌ 1153 (WAN2)	152 B	✔
Jun 12 09:24:06	220.130.75.206	59.124.36.163	TCP	4363 ⇌ 80 (WAN2)	60 B	✔
Jun 12 09:24:06	61.66.11.89	59.124.36.163	UDP	58896 ⇌ 1153 (WAN1)	152 B	✔
Jun 12 09:24:06	84.56.157.121	59.124.36.163	TCP	3651 ⇌ 80 (WAN1)	60 B	✔
Jun 12 09:24:06	60.248.76.120	59.124.36.163	UDP	34765 ⇌ 1153 (WAN1)	152 B	✔
Jun 12 09:24:05	172.19.100.77	202.43.193.120	UDP	1206 ⇌ 3478 (WAN2)	56 B	✔
Jun 12 09:24:05	211.75.150.78	59.124.36.163	UDP	37295 ⇌ 1153 (WAN1)	152 B	✔
Jun 12 09:24:05	61.66.11.89	59.124.36.163	UDP	58896 ⇌ 1153 (WAN1)	152 B	✔
Jun 12 09:24:05	202.132.79.183	59.124.36.163	UDP	60356 ⇌ 1153 (WAN2)	152 B	✔
Jun 12 09:24:05	172.19.1.101	211.22.160.20	UDP	2000 ⇌ 2000 (WAN2)	92 B	✔
Jun 12 09:24:04	192.192.12.72	59.124.36.163	UDP	60748 ⇌ 1153 (WAN1)	152 B	✔
Jun 12 09:24:04	211.72.35.151	59.124.36.163	UDP	60631 ⇌ 1153 (WAN2)	152 B	✔
Jun 12 09:24:04	60.248.233.162	59.124.36.163	UDP	44628 ⇌ 1153 (WAN2)	152 B	✔
Jun 12 09:24:04	202.39.75.196	59.124.36.163	UDP	34135 ⇌ 1153 (WAN2)	152 B	✔
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1841 ⇌ 80 (WAN2)	1 KB	✔
Jun 12 09:24:03	172.19.50.7	59.120.157.147	TCP	1840 ⇌ 80 (WAN2)	102 KB	✔
Jun 12 09:24:03	172.19.50.7	59.120.157.147	TCP	1839 ⇌ 80 (WAN2)	57 KB	✔
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1838 ⇌ 80 (WAN2)	1 KB	✔
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1837 ⇌ 80 (WAN2)	1 KB	✔
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1836 ⇌ 80 (WAN2)	18 KB	✔
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1835 ⇌ 80 (WAN2)	11 KB	✔
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1834 ⇌ 80 (WAN2)	7 KB	✔
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1833 ⇌ 80 (WAN2)	8 KB	✔
Jun 12 09:24:03	172.19.50.7	202.3.163.37	TCP	1832 ⇌ 80 (WAN2)	8 KB	✔
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1831 ⇌ 80 (WAN2)	4 KB	✔
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1830 ⇌ 80 (WAN2)	39 KB	✔
Jun 12 09:24:03	172.19.50.7	216.239.63.189	TCP	1827 ⇌ 80 (WAN2)	2 KB	✔
Jun 12 09:24:03	61.220.123.194	59.124.36.163	TCP	1236 ⇌ 80 (WAN1)	92 B	✔
Jun 12 09:24:03	61.220.123.194	59.124.36.163	TCP	1239 ⇌ 80 (WAN1)	60 B	✔
Jun 12 09:24:03	211.75.221.109	59.124.36.163	TCP	32885 ⇌ 80 (WAN1)	92 B	✔
Jun 12 09:24:03	211.75.221.109	59.124.36.163	TCP	32886 ⇌ 80 (WAN1)	60 B	✔
Jun 12 09:24:03	59.120.196.26	59.124.36.163	UDP	54276 ⇌ 1153 (WAN1)	152 B	✔
Jun 12 09:24:03	172.19.100.77	202.43.193.120	UDP	1206 ⇌ 3478 (WAN2)	56 B	✔
Jun 12 09:24:03	61.222.38.230	59.124.36.163	UDP	32834 ⇌ 1153 (WAN2)	152 B	✔
Jun 12 09:24:02	60.248.26.226	59.124.36.163	UDP	40548 ⇌ 1153 (WAN2)	152 B	✔
Jun 12 09:24:02	211.22.190.105	59.124.36.163	UDP	35275 ⇌ 1153 (WAN1)	152 B	✔
Jun 12 09:24:02	172.19.100.111	69.192.202.107	TCP	1068 ⇌ 10475 (WAN2)	24 KB	✔
Jun 12 09:24:02	61.219.223.2	59.124.36.163	UDP	54661 ⇌ 1153 (WAN1)	152 B	✔
Jun 12 09:24:02	203.65.83.67	59.124.36.163	TCP	45645 ⇌ 80 (WAN1)	60 B	✔
Jun 12 09:24:02	172.19.20.15	71.204.25.55	UDP	27124 ⇌ 39219 (WAN2)	134 B	✔
Jun 12 09:24:02	172.19.50.7	64.233.167.111	TCP	1648 ⇌ 995 (WAN2)	48 B	✔
Jun 12 09:24:01	61.152.188.66	59.124.36.163	UDP	54404 ⇌ 1153 (WAN1)	152 B	✔
Jun 12 09:24:01	60.248.231.186	59.124.36.163	UDP	60458 ⇌ 1153 (WAN1)	152 B	✔
Jun 12 09:24:01	61.221.67.114	59.124.36.163	TCP	1164 ⇌ 80 (WAN1)	92 B	✔
Jun 12 09:24:01	210.202.39.210	59.124.36.163	UDP	38237 ⇌ 1153 (WAN1)	152 B	✔
Jun 12 09:24:01	61.221.67.114	59.124.36.163	TCP	1165 ⇌ 80 (WAN1)	60 B	✔
Jun 12 09:24:01	172.19.100.111	207.237.44.102	UDP	43145 ⇌ 41250 (WAN2)	133 B	✔
Jun 12 09:24:01	211.75.42.220	59.124.36.163	TCP	1178 ⇌ 80 (WAN1)	92 B	✔
Jun 12 09:24:01	211.75.42.220	59.124.36.163	TCP	1179 ⇌ 80 (WAN1)	60 B	✔
Jun 12 09:24:01	61.63.11.253	59.124.36.163	UDP	39184 ⇌ 1153 (WAN2)	152 B	✔

Clear

1 / 573 Next

The traffic log Web UI

Step4 Click **Source IP** or **Destination IP** in Fig. 14-3, it shows the Protocol , Port and Traffic information.

1 / 1  
Refresh manually

Time	Source IP	Destination IP	Protocol	Port	Traffic	Disposition
Jun 8 14:35:11	60.248.26.226	59.124.36.163	UDP	45125 => 1153 (WAN2)	152 B	✓
Jun 8 14:35:02	60.248.26.226	59.124.36.163	UDP	45116 => 1153 (WAN2)	152 B	✓
Jun 8 14:34:25	60.248.26.226	59.124.36.163	UDP	45103 => 1153 (WAN2)	152 B	✓
Jun 8 14:33:00	60.248.26.226	59.124.36.163	UDP	45082 => 1153 (WAN2)	152 B	✓
Jun 8 14:31:52	60.248.26.226	59.124.36.163	UDP	45062 => 1153 (WAN2)	152 B	✓
Jun 8 14:30:58	60.248.26.226	59.124.36.163	UDP	45048 => 1153 (WAN2)	152 B	✓
Jun 8 14:30:09	60.248.26.226	59.124.36.163	UDP	45047 => 1153 (WAN2)	152 B	✓
Jun 8 14:29:12	60.248.26.226	59.124.36.163	UDP	45020 => 1153 (WAN2)	152 B	✓
Jun 8 14:28:51	60.248.26.226	59.124.36.163	UDP	45012 => 1153 (WAN2)	152 B	✓
Jun 8 14:26:58	60.248.26.226	59.124.36.163	UDP	44996 => 1153 (WAN2)	152 B	✓
Jun 8 14:26:43	60.248.26.226	59.124.36.163	UDP	44984 => 1153 (WAN2)	152 B	✓
Jun 8 14:25:00	60.248.26.226	59.124.36.163	UDP	44980 => 1153 (WAN2)	152 B	✓
Jun 8 14:24:25	60.248.26.226	59.124.36.163	UDP	44912 => 1153 (WAN2)	152 B	✓
Jun 8 14:24:22	60.248.26.226	59.124.36.163	UDP	44912 => 1153 (WAN2)	152 B	✓
Jun 8 14:23:19	60.248.26.226	59.124.36.163	UDP	44851 => 1153 (WAN2)	152 B	✓
Jun 8 14:23:10	60.248.26.226	59.124.36.163	UDP	44832 => 1153 (WAN2)	152 B	✓
Jun 8 14:22:34	60.248.26.226	59.124.36.163	UDP	44823 => 1153 (WAN2)	152 B	✓
Jun 8 14:19:24	60.248.26.226	59.124.36.163	UDP	44759 => 1153 (WAN2)	152 B	✓
Jun 8 14:18:28	60.248.26.226	59.124.36.163	UDP	44736 => 1153 (WAN2)	152 B	✓
Jun 8 14:16:51	60.248.26.226	59.124.36.163	UDP	44695 => 1153 (WAN2)	152 B	✓
Jun 8 14:14:45	60.248.26.226	59.124.36.163	UDP	44618 => 1153 (WAN2)	152 B	✓

The IP address traffic log Web UI

Step5 Click **Clear** , it shows the confirm window, then click **OK**. All the records will be deleted in BM-2101.

1 / 573 Next

Time	Source IP	Destination IP	Protocol	Port	Traffic	Disposition
Jun 12 09:24:06	61.218.156.18	59.124.36.163	UDP	40146 => 1153 (WAN2)	152 B	✓
Jun 12 09:24:06	220.130.75.206	59.124.36.163	TCP	4363 => 80 (WAN2)	60 B	✓
Jun 12 09:24:06	61.66.11.89	59.124.36.163	UDP	58896 => 1153 (WAN1)	152 B	✓
Jun 12 09:24:06	84.56.157.121	59.124.36.163	TCP	3651 => 80 (WAN1)	60 B	✓
Jun 12 09:24:06	60.248.76.120	59.124.36.163	UDP	34765 => 1153 (WAN1)	152 B	✓
Jun 12 09:24:05	172.19.100.77	202.43.193.120	UDP	1206 => 3478 (WAN2)	56 B	✓
Jun 12 09:24:05	211.75.150.78	59.124.36.163	UDP	37295 => 1153 (WAN1)	152 B	✓
Jun 12 09:24:05	61.66.11.89	59.124.36.163	UDP	58896 => 1153 (WAN1)	152 B	✓
Jun 12 09:24:05	202.132.79.183	59.124.36.163	UDP	60356 => 1153 (WAN2)	152 B	✓
Jun 12 09:24:05	172.19.1.101	211.22.160.20	UDP	2000 => 2000 (WAN2)	92 B	✓
Jun 12 09:24:04	192.192.12.72	59.124.36.163	UDP	60748 => 1153 (WAN1)	152 B	✓
Jun 12 09:24:04	211.72.35.151	59.124.36.163	UDP	60631 => 1153 (WAN2)	152 B	✓
Jun 12 09:24:04	60.248.233.162	59.124.36.163	UDP	44626 => 1153 (WAN2)	152 B	✓
Jun 12 09:24:04	202.39.75.196	59.124.36.163	UDP	34135 => 1153 (WAN2)	152 B	✓
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1841 => 80 (WAN2)	1 KB	✓
Jun 12 09:24:03	172.19.50.7	59.120.157.147	TCP	1840 => 80 (WAN2)	102 KB	✓
Jun 12 09:24:03	172.19.50.7	59.120.157.147	TCP	1839 => 80 (WAN2)	57 KB	✓
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1838 => 80 (WAN2)	1 KB	✓
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1837 => 80 (WAN2)	1 KB	✓
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1836 => 80 (WAN2)	18 KB	✓
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1835 => 80 (WAN2)	11 KB	✓
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1834 => 80 (WAN2)	7 KB	✓
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1833 => 80 (WAN2)	8 KB	✓
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1832 => 80 (WAN2)	8 KB	✓
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1831 => 80 (WAN2)	4 KB	✓
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1830 => 80 (WAN2)	39 KB	✓
Jun 12 09:24:03	172.19.50.7	216.239.63.189	TCP	1827 => 80 (WAN2)	2 KB	✓
Jun 12 09:24:03	61.220.123.194	59.124.36.163	TCP	1236 => 80 (WAN1)	92 B	✓
Jun 12 09:24:03	61.220.123.194	59.124.36.163	TCP	1239 => 80 (WAN1)	60 B	✓
Jun 12 09:24:03	211.75.221.109	59.124.36.163	TCP	32885 => 80 (WAN1)	92 B	✓
Jun 12 09:24:03	211.75.221.109	59.124.36.163	TCP	32886 => 80 (WAN1)	60 B	✓
Jun 12 09:24:03	59.120.196.26	59.124.36.163	UDP	54276 => 1153 (WAN1)	152 B	✓
Jun 12 09:24:03	172.19.100.77	202.43.193.120	UDP	1206 => 3478 (WAN2)	56 B	✓
Jun 12 09:24:03	61.222.38.230	59.124.36.163	UDP	32834 => 1153 (WAN2)	152 B	✓
Jun 12 09:24:02	60.248.26.226	59.124.36.163	UDP	40548 => 1153 (WAN2)	152 B	✓
Jun 12 09:24:02	211.22.198.105	59.124.36.163	UDP	35275 => 1153 (WAN1)	152 B	✓
Jun 12 09:24:02	172.19.100.111	69.192.202.107	TCP	1068 => 10475 (WAN2)	24 KB	✓
Jun 12 09:24:02	61.219.223.2	59.124.36.163	UDP	54661 => 1153 (WAN1)	152 B	✓
Jun 12 09:24:02	203.65.83.67	59.124.36.163	TCP	45645 => 80 (WAN1)	60 B	✓
Jun 12 09:24:02	172.19.20.15	71.204.25.55	UDP	27124 => 39219 (WAN2)	134 B	✓
Jun 12 09:24:02	172.19.50.7	64.233.167.111	TCP	1840 => 995 (WAN2)	48 B	✓
Jun 12 09:24:01	61.162.188.66	59.124.36.163	UDP	54404 => 1153 (WAN1)	152 B	✓
Jun 12 09:24:01	60.248.231.186	59.124.36.163	UDP	60458 => 1153 (WAN1)	152 B	✓
Jun 12 09:24:01	61.221.67.114	59.124.36.163	TCP	1164 => 80 (WAN1)	92 B	✓
Jun 12 09:24:01	210.202.39.210	59.124.36.163	UDP	38237 => 1153 (WAN1)	152 B	✓
Jun 12 09:24:01	61.221.67.114	59.124.36.163	TCP	1165 => 80 (WAN1)	60 B	✓
Jun 12 09:24:01	172.19.100.111	207.237.44.102	UDP	43145 => 41250 (WAN2)	133 B	✓
Jun 12 09:24:01	211.75.42.220	59.124.36.163	TCP	1178 => 80 (WAN1)	92 B	✓
Jun 12 09:24:01	211.75.42.220	59.124.36.163	TCP	1179 => 80 (WAN1)	60 B	✓
Jun 12 09:24:01	61.63.11.253	59.124.36.163	UDP	39184 => 1153 (WAN2)	152 B	✓

Microsoft Internet Explorer  
Are you sure you want to clear all data?  
OK Cancel

Clear

1 / 573 Next

Delete all the traffic log

Step6 Click **Clear** , it shows the confirm window, then click **OK**. All the records will be deleted in BM-2101.

1 / 573 Next

Time	Source IP	Destination IP	Protocol	Port	Traffic	Disposition
Jun 12 09:24:06	61.218.156.18	59.124.36.163	UDP	40146 => 1153 (WAN2)	152 B	✓
Jun 12 09:24:06	220.130.75.208	59.124.36.163	TCP	4363 => 80 (WAN2)	60 B	✓
Jun 12 09:24:06	61.66.11.89	59.124.36.163	UDP	58896 => 1153 (WAN1)	152 B	✓
Jun 12 09:24:06	84.56.157.121	59.124.36.163	TCP	3651 => 80 (WAN1)	60 B	✓
Jun 12 09:24:06	60.248.76.120	59.124.36.163	UDP	34765 => 1153 (WAN1)	152 B	✓
Jun 12 09:24:05	172.19.100.77	202.43.193.120	UDP	1206 => 3478 (WAN2)	56 B	✓
Jun 12 09:24:05	211.75.150.78	59.124.36.163	UDP	37295 => 1153 (WAN1)	152 B	✓
Jun 12 09:24:05	61.66.11.89	59.124.36.163	UDP	58896 => 1153 (WAN1)	152 B	✓
Jun 12 09:24:05	202.132.79.183	59.124.36.163	UDP	60366 => 1153 (WAN2)	152 B	✓
Jun 12 09:24:05	172.19.1.101	211.22.160.20	UDP	2000 => 2000 (WAN2)	92 B	✓
Jun 12 09:24:04	192.192.12.72	59.124.36.163	UDP	60748 => 1153 (WAN1)	152 B	✓
Jun 12 09:24:04	211.72.35.151	59.124.36.163	UDP	60631 => 1153 (WAN2)	152 B	✓
Jun 12 09:24:04	60.248.233.162	59.124.36.163	UDP	44626 => 1153 (WAN2)	152 B	✓
Jun 12 09:24:04	202.39.75.196	59.124.36.163	UDP	34135 => 1153 (WAN2)	152 B	✓
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1841 => 80 (WAN2)	1 KB	✓
Jun 12 09:24:03	172.19.50.7	59.120.157.147	TCP	1840 => 80 (WAN2)	102 KB	✓
Jun 12 09:24:03	172.19.50.7	59.120.157.147	TCP	1839 => 80 (WAN2)	57 KB	✓
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1838 => 80 (WAN2)	1 KB	✓
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1837 => 80 (WAN2)	1 KB	✓
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1836 => 80 (WAN2)	18 KB	✓
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1835 => 80 (WAN2)	11 KB	✓
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1834 => 80 (WAN2)	7 KB	✓
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1833 => 80 (WAN2)	8 KB	✓
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1832 => 80 (WAN2)	8 KB	✓
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1831 => 80 (WAN2)	4 KB	✓
Jun 12 09:24:03	172.19.50.7	202.3.173.222	TCP	1830 => 80 (WAN2)	39 KB	✓
Jun 12 09:24:03	172.19.50.7	216.239.63.189	TCP	1827 => 80 (WAN2)	2 KB	✓
Jun 12 09:24:03	61.220.123.194	59.124.36.163	TCP	1236 => 80 (WAN1)	92 B	✓
Jun 12 09:24:03	61.220.123.194	59.124.36.163	TCP	1239 => 80 (WAN1)	60 B	✓
Jun 12 09:24:03	211.75.221.109	59.124.36.163	TCP	32885 => 80 (WAN1)	92 B	✓
Jun 12 09:24:03	211.75.221.109	59.124.36.163	TCP	32886 => 80 (WAN1)	60 B	✓
Jun 12 09:24:03	59.120.196.26	59.124.36.163	UDP	54276 => 1153 (WAN1)	152 B	✓
Jun 12 09:24:03	172.19.100.77	202.43.193.120	UDP	1206 => 3478 (WAN2)	56 B	✓
Jun 12 09:24:03	61.222.38.230	59.124.36.163	UDP	32834 => 1153 (WAN2)	152 B	✓
Jun 12 09:24:02	60.248.26.226	59.124.36.163	UDP	40548 => 1153 (WAN2)	152 B	✓
Jun 12 09:24:02	211.22.198.105	59.124.36.163	UDP	35275 => 1153 (WAN1)	152 B	✓
Jun 12 09:24:02	172.19.100.111	69.192.202.107	TCP	1068 => 10475 (WAN2)	24 KB	✓
Jun 12 09:24:02	61.219.223.2	59.124.36.163	UDP	54661 => 1153 (WAN1)	152 B	✓
Jun 12 09:24:02	203.65.83.67	59.124.36.163	TCP	45645 => 80 (WAN1)	60 B	✓
Jun 12 09:24:02	172.19.20.15	71.204.25.55	UDP	27124 => 39219 (WAN2)	134 B	✓
Jun 12 09:24:02	172.19.50.7	64.233.167.111	TCP	1840 => 995 (WAN2)	48 B	✓
Jun 12 09:24:01	61.162.188.66	59.124.36.163	UDP	54404 => 1153 (WAN1)	152 B	✓
Jun 12 09:24:01	60.248.231.186	59.124.36.163	UDP	60458 => 1153 (WAN1)	152 B	✓
Jun 12 09:24:01	61.221.67.114	59.124.36.163	TCP	1164 => 80 (WAN1)	92 B	✓
Jun 12 09:24:01	210.202.39.210	59.124.36.163	UDP	38237 => 1153 (WAN1)	152 B	✓
Jun 12 09:24:01	61.221.67.114	59.124.36.163	TCP	1165 => 80 (WAN1)	60 B	✓
Jun 12 09:24:01	172.19.100.111	207.237.44.102	UDP	43145 => 41250 (WAN2)	133 B	✓
Jun 12 09:24:01	211.75.42.220	59.124.36.163	TCP	1178 => 80 (WAN1)	92 B	✓
Jun 12 09:24:01	211.75.42.220	59.124.36.163	TCP	1179 => 80 (WAN1)	60 B	✓
Jun 12 09:24:01	61.63.11.253	59.124.36.163	UDP	39184 => 1153 (WAN2)	152 B	✓

Microsoft Internet Explorer

Are you sure you want to clear all data?

OK Cancel

Clear

1 / 573 Next

Delete all the traffic log

## 15.2 Event

View the status of the WAN interface and the MIS engineer action as he log into the BM-2101 appliance.

Step1. **Monitor** → **Event** , it shows the status of MIS engineer log into BM-2101 to process the management and external interface.

Step2. Click **Download** → **File Download** → **Save**.

Step3. Click **Clear** , it shows the confirm window, then click **OK**. All the records will be deleted in BM-2101

## 15.3 Connection

View the external interface connection record as process the bandwidth management.

Step1. **Monitor**→**Connection** , it shows the external interface connection status in BM-2101.

Time	Connection Log
May 24 20:55:02	Terminating on signal 15.
May 24 20:55:02	ipcp: down
May 24 20:55:02	Script /etc/ppp/ip-down started (pid 12631)
May 24 20:55:02	Couldn't increase MTU to 1500
May 24 20:55:02	Couldn't increase MRU to 1500
May 24 20:55:02	Script /etc/ppp/ip-down finished (pid 12631), status = 0x0
May 24 20:55:02	Connection terminated.
May 24 20:55:02	Connect time 0.5 minutes.
May 24 20:55:02	Sent 70620 bytes, received 92827 bytes.
May 24 20:55:02	Doing disconnect
May 24 20:55:02	Exit.
May 24 20:55:03	pppd 2.4.1 started by root, uid 0
May 24 20:55:03	tdb_store failed: Invalid tdb context
May 24 20:55:03	Sending PADI
May 24 20:55:03	HOST_UNIQ successful match
May 24 20:55:04	HOST_UNIQ successful match
May 24 20:55:04	Got connection: d31
May 24 20:55:04	pads
May 24 20:55:04	Connecting PPPoE socket: 00:90:1a:40:09:87 310d eth3 0x80a4d20
May 24 20:55:04	using channel 8
May 24 20:55:04	Couldn't allocate PPP unit 2 as it is already in use
May 24 20:55:04	Using interface ppp2
May 24 20:55:04	tdb_store failed: Invalid tdb context
May 24 20:55:04	Connect: ppp2 <-> eth3
May 24 20:55:04	Couldn't increase MTU to 1500
May 24 20:55:04	Couldn't increase MRU to 1500
May 24 20:55:04	lcp_reqci: returning CONFACK.
May 24 20:55:04	ipcp: returning Configure-ACK
May 24 20:55:04	ipcp: up
May 24 20:55:04	local IP address 59.112.69.62
May 24 20:55:04	remote IP address 59.112.64.254
May 24 20:55:04	Script /etc/ppp/ip-up started (pid 12803)
May 24 20:55:04	Script /etc/ppp/ip-up finished (pid 12803), status = 0x0

**Connection records**

Step2. Click **Download** → **File Download** → **Save**.

Time	Connection Log
May 24 20:55:02	Terminating on signal 15.
May 24 20:55:02	ipcp: down
May 24 20:55:02	Script /etc/ppp/ip-down started (pid 12631)
May 24 20:55:02	Couldn't increase MTU to 1500
May 24 20:55:02	Couldn't increase MRU to 1500
May 24 20:55:02	Script /etc/ppp/ip-down finished (pid 12631), status = 0x0
May 24 20:55:02	Connection terminated.
May 24 20:55:02	Connect time 0.5 minutes.
May 24 20:55:02	Sent 70620 bytes, received 92827 bytes.
May 24 20:55:02	Doing disconnect
May 24 20:55:02	Exit.
May 24 20:55:03	pppd 2.4.0
May 24 20:55:03	tldb_store
May 24 20:55:03	Sending F
May 24 20:55:03	HOST_UN
May 24 20:55:04	HOST_UN
May 24 20:55:04	Got conn
May 24 20:55:04	pads
May 24 20:55:04	Connecti
May 24 20:55:04	using cha
May 24 20:55:04	Couldn't a
May 24 20:55:04	Using inte
May 24 20:55:04	tldb_store
May 24 20:55:04	Connect:
May 24 20:55:04	Couldn't in
May 24 20:55:04	Couldn't increase MRU to 1500
May 24 20:55:04	lcp_reqci: returning CONFACK.
May 24 20:55:04	ipcp: returning Configure-ACK
May 24 20:55:04	ipcp: up
May 24 20:55:04	local IP address 59.112.69.62
May 24 20:55:04	remote IP address 59.112.64.254
May 24 20:55:04	Script /etc/ppp/ip-up started (pid 12803)
May 24 20:55:04	Script /etc/ppp/ip-up finished (pid 12803), status = 0x0

**File Download** ✕

Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: local7.log  
 File type: Text Document  
 From: 192.168.111.1

Would you like to open the file or save it to your computer?

Always ask before opening this type of file

**Save the connection log files**

Step3. Click **Clear** , it shows the confirm window, then click **OK**. All the records will be deleted in BM-2101.

Time	Connection Log
May 24 20:55:02	Terminating on signal 15.
May 24 20:55:02	ipcp: down
May 24 20:55:02	Script /etc/ppp/ip-down started (pid 12631)
May 24 20:55:02	Couldn't increase MTU to 1500
May 24 20:55:02	Couldn't increase MRU to 1500
May 24 20:55:02	Script /etc/ppp/ip-down finished (pid 12631), status = 0x0
May 24 20:55:02	Connection terminated.
May 24 20:55:02	Connect time 0.5 minutes.
May 24 20:55:02	Sent 70620 bytes, received 92827 bytes.
May 24 20:55:02	Doing disconnect
May 24 20:55:02	Exit.
May 24 20:55:03	pppd 2.4.1 started by root, uid 0
May 24 20:55:03	tdb_store failed: Invalid tdb context
May 24 20:55:03	Sending PADI
May 24 20:55:03	HOST_UNIQ successful match
May 24 20:55:04	HOST_UNIQ successful match
May 24 20:55:04	Got connection: d31
May 24 20:55:04	pads
May 24 20:55:04	Connecting PPPoE socket: 00
May 24 20:55:04	using channel 8
May 24 20:55:04	Couldn't allocate PPP unit 2 as
May 24 20:55:04	Using interface ppp2
May 24 20:55:04	tdb_store failed: Invalid tdb context
May 24 20:55:04	Connect: ppp2 <-> eth3
May 24 20:55:04	Couldn't increase MTU to 1500
May 24 20:55:04	Couldn't increase MRU to 1500
May 24 20:55:04	lcp_reqci: returning CONFACK.
May 24 20:55:04	ipcp: returning Configure-ACK
May 24 20:55:04	ipcp: up
May 24 20:55:04	local IP address 59.112.69.62
May 24 20:55:04	remote IP address 59.112.64.254
May 24 20:55:04	Script /etc/ppp/ip-up started (pid 12803)
May 24 20:55:04	Script /etc/ppp/ip-up finished (pid 12803), status = 0x0

Clear Download

**Delete all the connection log files**

## 15.4 Backup

MIS engineer can receive and save the record results from the BM-2101.

Step1. **System → Configure** , enable **E-mail Alert Notification** and enter the e-mail settings



The screenshot shows the 'E-mail Setting' configuration window. It has a blue header bar with the title 'E-mail Setting'. Below the header, there is a checked checkbox labeled 'Enable E-mail Alert Notification'. Underneath, there are several fields for configuration: 'Sender Address (Required by some ISPs)' with the value 'sender@mydomain.c' and a note '( ex: sender@mydomain.com )'; 'SMTP Server' with the value 'mail.mydomain.com' and a note '( ex: mail.mydomain.com )'; 'E-mail Address 1' with the value 'user1@mydomain.cc' and a note '( ex: user1@mydomain.com )'; 'E-mail Address 2' with the value 'user2@mydomain.cc' and a note '( ex: user2@mydomain.com )'; and a 'Mail Test' button.

**E-mail setting**

Step2. **Monitor → Backup → enable log mail support**. Click **OK**.



The screenshot shows the 'Log Mail Configuration' window. It has a blue header bar with the title 'Log Mail Configuration'. Below the header, there is a checked checkbox labeled 'Enable Log Mail Support'. Underneath, there is a note: 'When Log Full (300Kbytes), Multi-Homing Gateway Appliance sends Log'. Below this note, there are three rows of configuration: 'From SMTP Server' with the value 'mail.mydomain.com'; 'To E-mail Address 1' with the value 'user1@mydomain.com'; and 'E-mail Address 2' with the value 'user2@mydomain.com'.

**Log mail configuration**



Select **Enable E-mail Log** , BM-2101 sends e-mail log when log full 300kbytes then clear all the online log.

Step3. **Monitor** → **Backup** → **Syslog setting** :

- Select **Enable Syslog Messages**.
- Enter the IP in **Syslog host IP address**.
- Enter the Syslog receive Port number in **Syslog host Port**.
- Click OK.
- Complete the setting.

Syslog Setting

Enable Syslog Messages

Syslog Host IP Address  ( ex: 192.168.1.61 )

Syslog Host Port  ( ex: 514 )

OK Cancel

**Syslog setting**

## Chapter 16

# Accounting Report

MIS engineer can use **Accounting Report** to view all the internal and external user's network accessing activities ( Includes the policy and VPN ). **Accounting Report** can record user's upstream/downstream , first packet/last packet/duration , service and also provides the IP traffic and distribution charts.

## Setting

### Setting

- Enable the account report , to record the inbound and outbound information in BM-2101

Accounting Report includes **Outbound** and **Inbound**.

Outbound Accounting Report



Account report can record any downstream /upstream service traffic used by LAN and DMZ user via BM-2101

### User User

- Display LAN and DMZ user 's accounting report.

## Site Site

- Display external server accounting report.

## Service Service

- Accounting report can record the service traffic used by LAN or DMZ user via BM-2101

### Inbound Accounting Report



Account report can record any service downstream /upstream traffic used from external user to LAN or DMZ user via BM-2101

## User User

- Display the external user's accounting report.

## Site Site

- Display the LAN and DMZ server accounting report.

## Service Service

- Accounting report can record the service traffic used from external user to LAN or DMZ server via BM-2101.

## 16.1 Outbound

Step1 **Accounting Report → Outbound** , click **User** , it shows the accounting report of send/retrieve packets in downstream , upstream, first packet , last packet , duration from the external server to access user IP address in BM-2101.

- **User** : To view the needed record, and every 50 records to be a page.
- Select **User** .
- **Source IP** : It is the LAN or DMZ user's IP address , click the source IP to show the user's information.
- **Downstream** : The percentage of user's traffic and total downstream from external server to access LAN or DMZ user via BM-2101.
- **Upstream** : The percentage of user's traffic and total upstream from LAN or DMZ user to access external server via BM-2101.
- **First Packet** : Record the first packet from LAN or DMZ user to access external server via BM-2101.
- **Last Packet** : Record the last packet from LAN or DMZ user to access external server via BM-2101.
- **Duration** : Record the duration ( the first packet to last packet) from LAN or DMZ user to access external server via BM-2101.
- **Total Traffic** : Accumulate every user's total downstream / upstream traffic and its percentage from LAN or DMZ user to access external server.
- **Remove** : Delete the record.
- **Reset** : Clear all records and restart the accounting report.

Top: 1 - 23 ▾

No	User	Site	Service	Source IP	Downstream	Upstream	First Packet	Last Packet	Duration	Action
1				192.168.139.30	179.3 MB 85.5%	24.0 MB 72.4%	12/20 23:02:06	12/30 20:11:23	00:21:06:17	Remove
2				HS31	12.6 MB 6.0%	2.6 MB 7.9%	12/27 20:47:50	12/28 19:04:02	22:16:12	Remove
3				HS31	8.1 MB 3.8%	2.4 MB 7.2%	12/29 22:08:10	12/30 18:36:54	20:27:44	Remove
4				NUSOFT_5006	4.6 MB 2.2%	811.1 KB 2.4%	12/29 00:17:11	12/29 10:03:47	00:46:36	Remove
5				192.168.139.10	1.7 MB 0.8%	887.2 KB 2.7%	12/20 17:24:05	12/30 20:13:20	100:02:46:16	Remove
6				JUSTIN72	1.0 MB 0.5%	733.3 KB 2.2%	12/20 17:09:53	12/27 16:53:16	60:22:43:23	Remove
7				SIMSIAN	905.0 KB 0.4%	194.6 KB 0.6%	12/26 10:58:19	12/26 11:13:13	00:14:54	Remove
8				192.168.139.71	813.3 KB 0.4%	151.1 KB 0.5%	12/21 09:52:18	12/21 10:14:47	00:22:29	Remove
9				LOCALHOST	344.3 KB 0.2%	73.0 KB 0.2%	12/21 15:43:01	12/30 18:18:53	00:02:36:52	Remove
10				192.168.139.11	165.0 KB 0.1%	149.5 KB 0.5%	12/21 16:40:51	12/26 12:11:21	40:20:30:30	Remove
11				192.168.139.9	68.9 KB 0.0%	20.8 KB 0.1%	12/22 12:38:36	12/22 12:40:46	00:11:10	Remove
12				192.168.139.20	42.5 KB 0.0%	993.6 KB 3.0%	12/26 10:53:37	12/26 10:57:52	00:04:15	Remove
13				YUOR-NAME-AND-1	29.4 KB 0.0%	73.4 KB 0.2%	12/23 00:20:10	12/23 00:20:26	00:00:07	Remove
14				192.168.139.120	21.6 KB 0.0%	10.0 KB 0.0%	12/27 14:34:48	12/27 14:34:55	00:00:07	Remove
15				192.168.139.21	14.4 KB 0.0%	4.6 KB 0.0%	12/26 10:55:42	12/26 10:55:42	00:00:00	Remove
16				JOSHI10	6.1 KB 0.0%	23.4 KB 0.1%	12/20 23:00:48	12/30 18:28:53	00:19:28:05	Remove
17				HS31	2.3 KB 0.0%	2.4 KB 0.0%	12/28 21:31:48	12/28 22:25:10	00:53:22	Remove
18				172.19.100.71	1.7 KB 0.0%	11.2 KB 0.0%	12/21 09:52:14	12/21 09:56:55	00:04:41	Remove
19				192.168.139.30	640.0 B 0.0%	4.1 KB 0.0%	12/21 16:14:49	12/29 19:42:42	80:04:27:53	Remove
20				SIMSIAN	126.0 B 0.0%	60.0 B 0.0%	12/23 09:56:55	12/23 09:56:55	00:00:00	Remove
21				HS31	0.0 B 0.0%	600.0 B 0.0%	12/29 22:08:17	12/29 22:10:34	00:02:17	Remove
22				207.46.0.60	0.0 B 0.0%	286.0 B 0.0%	12/27 14:36:00	12/27 14:36:06	00:00:06	Remove
23				192.168.139.13	0.0 B 0.0%	192.0 B 0.0%	12/30 16:45:53	12/30 16:45:53	00:00:00	Remove
Total Traffic:					209.6 MBytes	33.2 MBytes	Reporting time: Tue Jun 20 14:37:20 2006			

Reset

### Outbound accounting report

## 192.168.139.71 Information

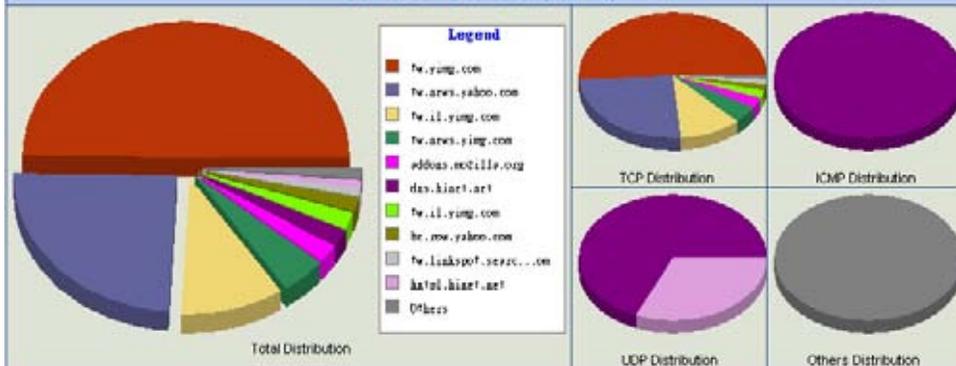
IP Address	192.168.139.71
First / Last Packet (Duration)	12/21 09:52:10 -- 12/21 10:14:47 (00:22:29)
DNS Name	
NetBIOS Name (Group)	
MAC Address (NIC Vendor)	00:0C:76:B7:97:B1 (LINKNOM)
Total Data Downstream / Upstream	813.3 KBytes / 151.1 KBytes

1 / 2 [Load](#)

Top Sites:

No	Destination IP	Downstream	TCP	UDP	ICMP	Others
1	tw.yimg.com	405.4 KB 49.9%	405.4 KB 51.3%	0.0 B 0.0%	0.0 B 0.0%	0.0 B 0.0%
2	tw.news.yahoo.com	199.7 KB 24.6%	199.7 KB 25.3%	0.0 B 0.0%	0.0 B 0.0%	0.0 B 0.0%
3	tw.it.yimg.com	83.4 KB 10.3%	83.4 KB 10.6%	0.0 B 0.0%	0.0 B 0.0%	0.0 B 0.0%
4	tw.news.yimg.com	35.6 KB 4.4%	35.6 KB 4.5%	0.0 B 0.0%	0.0 B 0.0%	0.0 B 0.0%
5	addons.mozilla.org	10.9 KB 2.3%	10.9 KB 2.4%	0.0 B 0.0%	0.0 B 0.0%	0.0 B 0.0%
6	dns.hinet.net	16.1 KB 2.0%	0.0 B 0.0%	15.7 KB 80.6%	420.0 B 100.0%	0.0 B 0.0%
7	tw.it.yimg.com	15.6 KB 1.9%	15.6 KB 2.0%	0.0 B 0.0%	0.0 B 0.0%	0.0 B 0.0%
8	bc.rtw.yahoo.com	13.4 KB 1.7%	13.4 KB 1.7%	0.0 B 0.0%	0.0 B 0.0%	0.0 B 0.0%
9	tw.linkspot.search.com	10.0 KB 1.2%	10.0 KB 1.3%	0.0 B 0.0%	0.0 B 0.0%	0.0 B 0.0%
10	http://hinat.net	7.2 KB 0.9%	0.0 B 0.0%	7.2 KB 31.4%	0.0 B 0.0%	0.0 B 0.0%
Total Traffic		813.3 KBytes	790.0 KBytes	22.9 KBytes	420.0 Bytes	0.0 Bytes

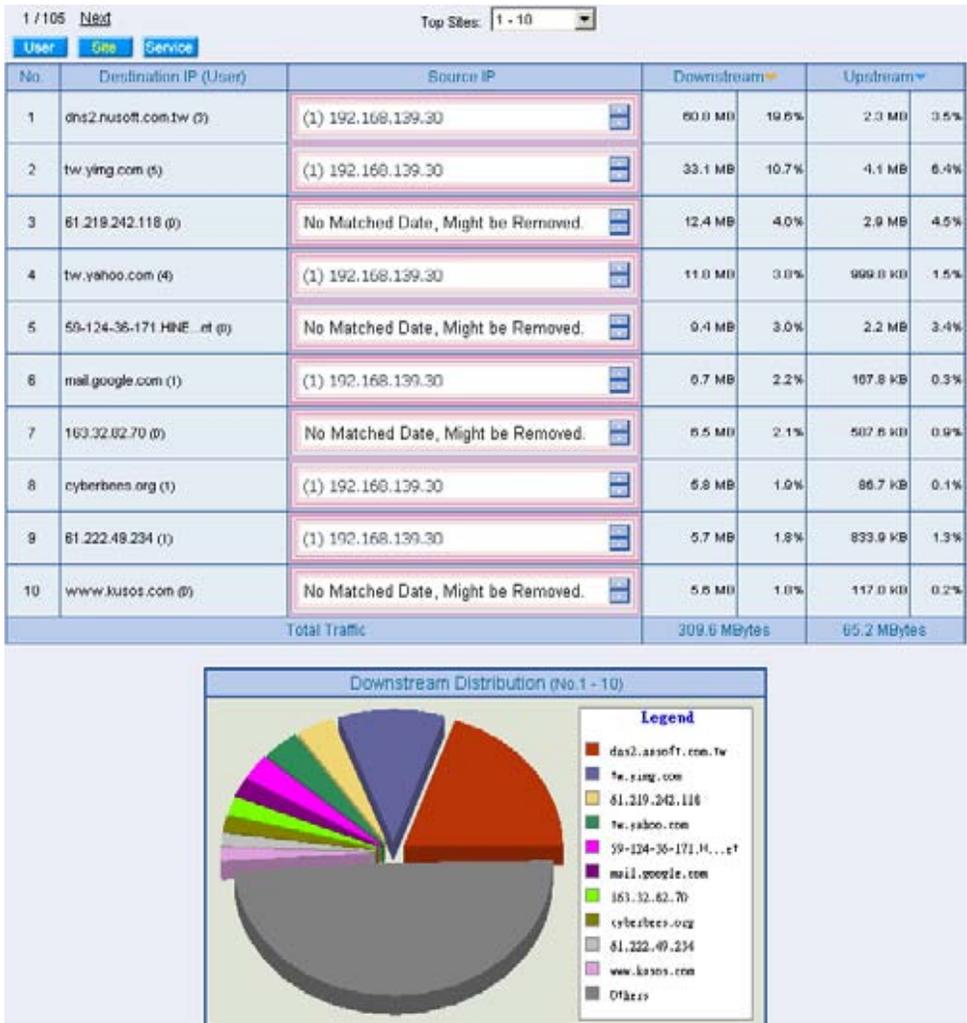
Downstream Distribution (No.1 - 10)



### Outbound use information

Step2 **Accounting Report → Outbound** , click **Site** , it shows the send / retrieve packet traffic report of downstream , upstream and downstream distribution used by external server via the BM-2101 IP address

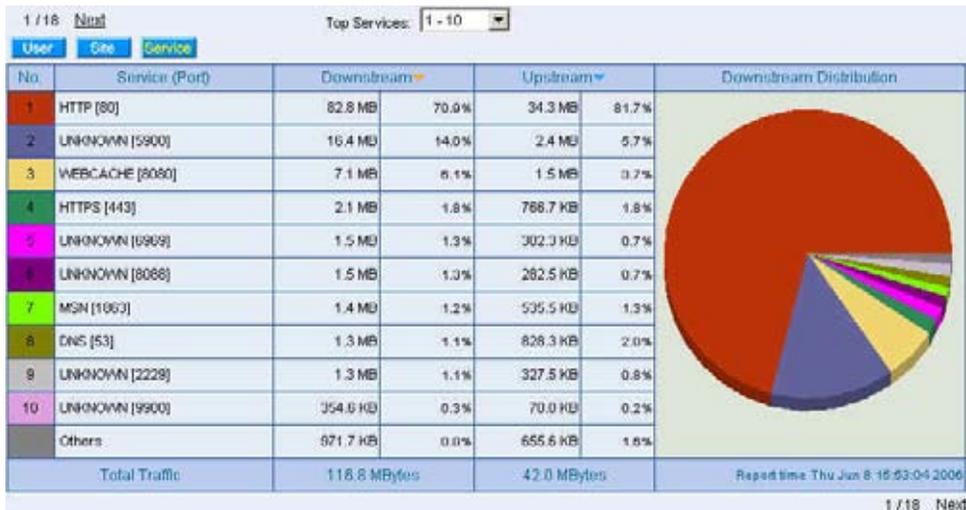
- **Site** : View the needed record , and every 10 records to be one page.
- Select  .
- **Destination IP (User)** : It means the external server IP or represents the LAN or DMZ user numbers to access the external server.
- **Source IP** : It means the LAN or DMZ user's IP address , to access the external server.
- **Downstream** : The percentage of traffic and total downstream traffic from external server to access LAN or DMZ user via BM-2101.
- **Upstream** : The percentage of traffic and total upstream traffic from LAN or DMZ user to access external server via BM-2101.
- **Total Traffic** : Accumulate every user's total downstream / upstream traffic and its percentage from LAN or DMZ user to access external server.
  
- **Downstream Distribution** : Display the distribution charts depends on the real downstream traffic.



Outbound site accounting report

Step3 **Accounting Report** → **Outbound** , click **Service** , it shows the statistics and distribution charts of user's service downstream , upstream and downstream distribution from LAN or DMZ to external server.

- **Service** : View the needed record , and every 10 records to be one page.
- Select **Service** .
- **Service (Port)** : It means the service name used from the LAN or DMZ user to access external server.
- **Downstream** : It means the percentage of traffic and total downstream traffic from external server to access LAN or DMZ user via BM-2101.
- **Upstream** : It means the percentage of traffic and total upstream traffic from LAN or DMZ user to access external server via BM-2101.
- **Total Traffic** : Accumulate every service percentage and total traffic of downstream/upstream.
- **Downstream Distribution** : Display the distribution charts depends on the real downstream traffic.



**Outbound service accounting report**

## 16.2 Inbound

Step1 **Accounting Report → Inbound** , click **User** , it shows the accounting report of send/retrieve packets in downstream , upstream, first packet , last packet duration from external server to access the user IP address in BM-2101.

- **User** : To view the needed record, and every 50 records to be a page.
- Select 
- **Source IP** : It is the external user IP address , click the source IP to show the user's information.
- **Upstream** : The percentage of user's traffic and total upstream from LAN or DMZ server to access external user via BM-2101.
- **Downstream** : The percentage of user's traffic and total downstream from external user to access LAN or DMZ server via BM-2101.
- **First Packet** : Record the first packet from external user to access LAN or DMZ server via BM-2101.
- **Last Packet** : Record the last packet from external user to access LAN or DMZ server via BM-2101.
- **Duration** : Record the duration ( the first packet to last packet) from external user to access LAN or DMZ server via BM-2101.
- **Total Traffic** : Accumulate every user's total downstream / upstream traffic and its percentage from external user to access LAN or DMZ server.
- **Remove** : Delete the record.
- **Reset** : Clear all records and restart the accounting report.

1 / 196		Next		Top Sites: 1 - 50					
User	Site	Service							
No.	Source IP	Downstream	Upstream	First Packet	Last Packet	Duration	Action		
1	61.64.192.40	43.4 MB	40.9%	214.8 MB	98.7%	12/14 00:37:21	12/30 01:48:20	100 01:11:05	Remove
2	KD HSIAN0-01	24.2 MB	26.1%	646.4 KB	0.3%	12/19 20:59:37	12/24 23:27:53	50 02:29:16	Remove
3	192.12.132.2	14.6 MB	15.0%	405.0 KB	0.2%	12/20 23:01:09	12/20 23:10:43	00:09:34	Remove
4	61-228-191...et	4.6 MB	5.0%	128.4 KB	0.1%	12/21 17:42:30	12/21 18:05:18	00:22:48	Remove
5	59-124-36...et	3.8 MB	4.1%	104.0 KB	0.0%	12/21 17:40:29	12/22 10:48:43	17:08:14	Remove
6	59-124-36...et	1.4 MB	1.5%	57.5 KB	0.0%	12/12 14:21:17	12/22 09:27:59	90 10:06:42	Remove
7	61.228.184.40	69.9 KB	0.1%	2.0 KB	0.0%	12/22 10:42:54	12/22 10:42:54	00:00:00	Remove
8	NUSOFF_5006	30.8 KB	0.0%	30.8 KB	0.0%	12/16 23:34:51	12/16 23:34:52	00:00:01	Remove
9	61.228.181.156	10.4 KB	0.0%	19.8 KB	0.0%	12/12 14:22:22	12/12 15:53:06	01:30:44	Remove
10	61.228.183.180	6.7 KB	0.0%	2.7 KB	0.0%	12/22 10:00:23	12/22 10:00:23	00:00:00	Remove
11	61.228.184.154	4.7 KB	0.0%	7.0 KB	0.0%	12/13 10:50:26	12/13 11:19:59	00:29:32	Remove
12	61-228-188...et	4.0 KB	0.0%	1.5 KB	0.0%	12/21 17:41:10	12/21 17:41:57	00:00:41	Remove
13	RON27	3.3 KB	0.0%	3.6 KB	0.0%	12/14 11:04:40	12/14 11:56:02	00:51:13	Remove
14	59.124.29.147	2.3 KB	0.0%	25.8 KB	0.0%	12/12 14:49:13	12/14 10:06:05	10 19:16:52	Remove
15	216.166.142.17	1.6 KB	0.0%	2.3 KB	0.0%	12/23 16:18:02	12/24 15:10:17	22:52:15	Remove
16	216.161.164.146	1.2 KB	0.0%	1.7 KB	0.0%	12/23 16:20:40	12/23 22:50:41	06:29:53	Remove
17	61.228.175.95	1.1 KB	0.0%	990.0 B	0.0%	12/13 11:24:41	12/13 11:26:20	00:01:39	Remove
18	221.202.225.42	1.1 KB	0.0%	1.9 KB	0.0%	12/23 16:17:31	12/23 17:31:32	01:14:01	Remove
19	216.161.164.162	1.0 KB	0.0%	1.3 KB	0.0%	12/23 18:38:51	12/24 04:01:43	09:24:52	Remove
20	216.161.164.140	952.0 B	0.0%	1.3 KB	0.0%	12/23 16:02:30	12/23 21:20:30	05:17:52	Remove
21	216.161.164.98	996.0 B	0.0%	1.3 KB	0.0%	12/21 05:41:12	12/23 21:16:20	20 15:35:00	Remove
22	63.216.76.17	896.0 B	0.0%	1.3 KB	0.0%	12/23 16:08:00	12/24 08:17:10	16:09:10	Remove
23	204.11.19.11	896.0 B	0.0%	1.1 KB	0.0%	12/23 17:28:28	12/24 09:31:23	16:04:55	Remove
24	66.172.60.66	784.0 B	0.0%	1.1 KB	0.0%	12/23 16:00:02	12/24 01:45:36	09:39:34	Remove
25	81.219.148.72	750.0 B	0.0%	770.0 B	0.0%	12/20 09:54:19	12/20 17:09:52	07:14:33	Remove
26	61-228-180...et	672.0 B	0.0%	1.1 KB	0.0%	12/12 14:21:12	12/12 14:56:49	00:35:37	Remove
27	66.172.60.32	672.0 B	0.0%	012.0 B	0.0%	12/23 16:16:23	12/23 21:10:07	04:54:44	Remove
28	59.124.17.12	668.0 B	0.0%	9.7 KB	0.0%	12/12 14:44:19	12/14 10:35:53	10 19:51:34	Remove
29	63.236.161.8	616.0 B	0.0%	1.1 KB	0.0%	12/23 16:03:25	12/23 19:50:18	03:46:53	Remove
30	216.161.164.111	560.0 B	0.0%	760.0 B	0.0%	12/23 16:04:29	12/23 20:46:12	04:41:44	Remove
31	216.161.164.190	560.0 B	0.0%	760.0 B	0.0%	12/23 16:39:47	12/24 00:17:25	07:37:38	Remove
32	63.216.76.11	448.0 B	0.0%	739.0 B	0.0%	12/21 05:48:55	12/23 21:18:48	20 15:26:53	Remove
33	66.172.60.5	418.0 B	0.0%	668.0 B	0.0%	12/23 16:27:52	12/27 19:02:07	40 02:34:10	Remove
34	216.11.202.12	440.0 B	0.0%	567.0 B	0.0%	12/27 16:48:01	12/27 16:59:20	00:11:19	Remove
35	59.124.123.83	427.0 B	0.0%	793.0 B	0.0%	12/12 14:23:00	12/12 15:16:46	00:55:30	Remove
36	59.124.30.217	437.0 B	0.0%	3.0 KB	0.0%	12/12 14:59:26	12/14 10:32:19	10 19:32:53	Remove
37	59.36.61.194	433.0 B	0.0%	625.0 B	0.0%	12/12 14:56:23	12/12 14:56:23	00:00:00	Remove
38	60.124.166.36	433.0 B	0.0%	1.0 KB	0.0%	12/13 11:20:01	12/14 09:59:33	22:39:32	Remove
39	63.216.76.8	392.0 B	0.0%	532.0 B	0.0%	12/23 16:28:05	12/23 16:24:41	01:56:36	Remove
40	66.172.60.38	392.0 B	0.0%	532.0 B	0.0%	12/23 17:55:16	12/24 01:17:59	07:22:43	Remove
41	216.166.142.23	392.0 B	0.0%	499.0 B	0.0%	12/23 18:02:28	12/27 10:09:06	40 01:06:38	Remove
42	216.161.164.60	336.0 B	0.0%	511.0 B	0.0%	12/23 16:02:32	12/23 22:08:40	06:06:17	Remove
43	80.170.235.89	336.0 B	0.0%	338.0 B	0.0%	12/23 16:14:35	12/23 17:13:44	00:59:09	Remove
44	82.264.54.17	328.0 B	0.0%	379.0 B	0.0%	12/23 16:56:22	12/23 16:04:44	01:00:22	Remove
45	63.216.76.14	280.0 B	0.0%	359.0 B	0.0%	12/13 13:31:37	12/23 20:06:40	100 06:35:03	Remove
46	60.211.9.170	280.0 B	0.0%	648.0 B	0.0%	12/16 11:30:17	12/16 11:43:29	00:13:12	Remove
47	172.161.80.292	280.0 B	0.0%	275.0 B	0.0%	12/23 16:03:40	12/23 16:55:43	00:52:03	Remove
48	83.46.69.94	260.0 B	0.0%	275.0 B	0.0%	12/23 16:21:17	12/23 17:04:22	00:43:05	Remove
49	207.226.112.8	260.0 B	0.0%	435.0 B	0.0%	12/23 16:22:03	12/27 19:14:11	40 02:52:00	Remove
60	66.172.60.43	280.0 B	0.0%	380.0 B	0.0%	12/23 16:32:59	12/24 00:56:00	08:23:01	Remove
Total Traffic		92.5 MBytes		217.7 MBytes		Reporting time Tue Jun 20 14:37:39 20 2006			

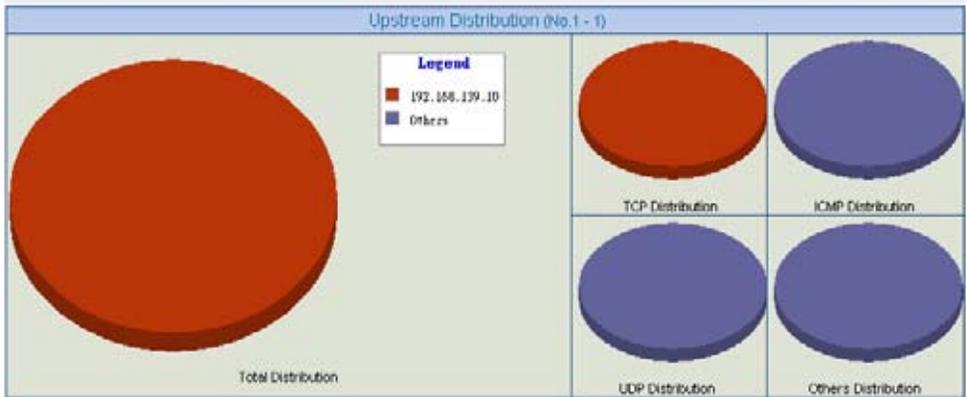
Inbound user accounting report

## 61.228.184.40 Information

IP Address	61.228.184.40
First / Last Packet (Duration)	12/22 10:42:54 -- 12/22 10:42:54 [00:00:00]
DNS Name	
NetBIOS Name (Group)	
MAC Address (NIC Vendor)	
Total Data Downstream / Upstream	2.8 KBytes / 89.9 KBytes

Top Sites: 1 - 1

No.	Destination IP	Upstream	TCP	UDP	ICMP	Others
1	192.168.139.10	89.9 KB 100.0%	89.9 KB 100.0%	0.0 B 0.0%	0.0 B 0.0%	0.0 B 0.0%
Total Traffic		89.9 KBytes	89.9 KBytes	0.0 Bytes	0.0 Bytes	0.0 Bytes



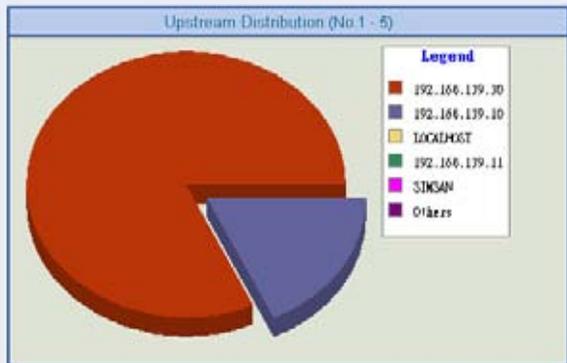
### Inbound user information

Step2 **Accounting Report → Inbound** , click **Site** , it shows the send/retrieve packet traffic report of downstream , upstream and upstream distribution used by LAN or DMZ server via the BM-2101 IP address

- **Site** : View the needed record , and every 10 records to be one page.
- Select 
- **Destination IP (User)** : It means the LAN or DMZ server IP or represents the external user numbers to access the LAN or DMZ server.
- **Source IP** : It means the external user's IP address , to access the LAN or DMZ server.
  
- **Downstream** : The percentage of traffic and total downstream traffic from external user to access LAN or DMZ server via BM-2101.
  
- **Upstream** : The percentage of traffic and total upstream traffic from LAN or DMZ server to access external user via BM-2101.
- **Total Traffic** : Accumulate every user's total downstream / upstream traffic and its percentage from external user to access LAN or DMZ server.
  
- **Upstream Distribution** : Display the distribution charts depends on the real upstream traffic.

Top Sites: 1 - 5

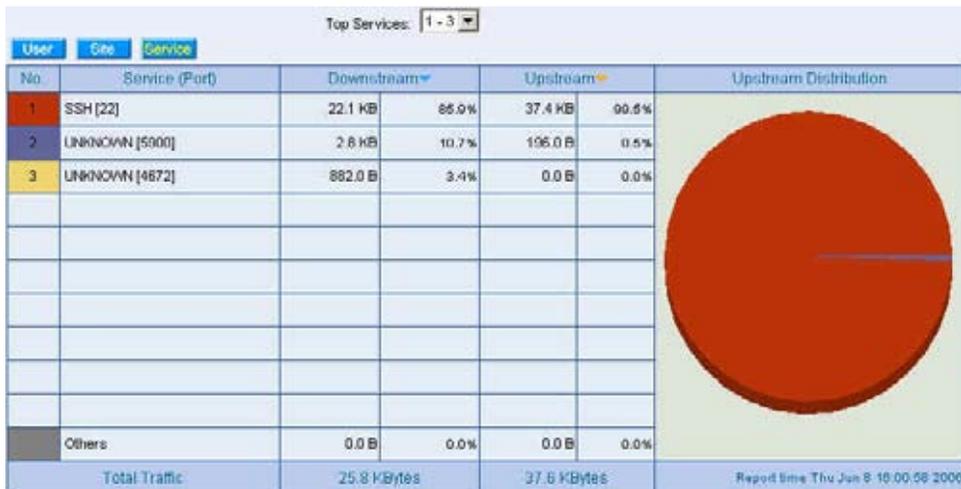
No.	Destination IP (User)	Source IP	Downstream		Upstream	
1	192.168.139.30 (478)	(1) 61.64.192.40	10.7 MB	4.9%	75.0 MB	81.9%
2	192.168.139.10 (13)	(1) 61.64.192.40	206.7 MB	95.0%	16.7 MB	18.0%
3	LOCALHOST (270)	(1) 61.228.181.156	207.3 KB	0.1%	21.0 KB	0.0%
4	192.168.139.11 (1)	(1) 192.168.183.10	60.0 B	0.0%	0.0 B	0.0%
5	SIMSAN (1)	(1) 192.168.183.34	144.0 B	0.0%	0.0 B	0.0%
Total Traffic			217.7 MBytes		82.5 MBytes	



Inbound site accounting report

Step3 **Accounting Report → Inbound** , click **Service** , it shows the statistics and distribution charts of user's service downstream , upstream and upstream distribution from external user to LAN or DMZ server.

- **Service** : View the needed record , and every 10 records to be one page.
- Select **Service**
- **Service (Port)** : It means the service name used from the external user to access LAN or DMZ server.
- **Downstream** : It means the percentage of traffic and total downstream traffic from external user to access LAN or DMZ server via BM-2101.
- **Upstream** : It means the percentage of traffic and total upstream traffic from LAN or DMZ server to access external user via BM-2101.
- **Total Traffic** : Accumulate every service percentage and total traffic of downstream/upstream.
- **Upstream Distribution** : Display the distribution charts depends on the real upstream traffic.



**Inbound service accounting report**

## Chapter 17

# Statistics

**WAN statistics** , it includes all the upstream/downstream packets pass through the **WAN interface** and traffic log in upstream/downstream

**Policy statistics** , it includes all the upstream/downstream packets pass through the **Policy** and traffic log in upstream/downstream

MIS engineer can use the statistics to easily know the status of WAN or the packet and stream in policy.

## Statistics

### Statistics charts

- Ordinate : Network stream.
- Horizontal ordinate : Time ( hour/minute ) .

### Source , Destination , Service , Action

- Record the original **Policy** setting, MIS engineer can easily know the **Policy statistics** belongs to which **Policy**.

### Time

- MIS engineer can respectively to view the statistics according to time unit of minute , hour , day , week , Month and Year.



MIS engineer can select the time unit :

1. **Minute** : Refresh the statistics charts every minute.
2. **Hour** : Refresh the statistics charts every hour.
3. **Day**: Refresh the statistics charts every day.
4. **Week** : Refresh the statistics charts every week.
5. **Month** : Refresh the statistics charts every month.
6. **Year** : Refresh the statistics charts every year.

### Bits/sec Bytes/sec Utilization Total

- MIS engineer can modify the ordinate stream unit in statistics charts.
  - ◆ Utilization : The maximum stream of BM-2101 (according to the stream setting in **Interface**.)
  - ◆ Total : Use the accumulated total stream to be the ordinate in time unit.

## 17.1 WAN

Step1 **Statistics** → **WAN** , it shows all the downstream/upstream packets and statistics pass through **WAN interface**.

- **Time** : View the statistics charts according to the unit of minute, hour , da , week , month, year.

WAN	Time
WAN 1	<a href="#">Minute</a> <a href="#">Hour</a> <a href="#">Day</a> <a href="#">Week</a> <a href="#">Month</a> <a href="#">Year</a>
WAN 2	<a href="#">Minute</a> <a href="#">Hour</a> <a href="#">Day</a> <a href="#">Week</a> <a href="#">Month</a> <a href="#">Year</a>
All WAN Interface	<a href="#">Minute</a> <a href="#">Hour</a> <a href="#">Day</a> <a href="#">Week</a> <a href="#">Month</a> <a href="#">Year</a>

The WAN statistics



The **WAN statistics** is the attached function of **WAN interface**. The **WAN statistics** will enabled when enable the **WAN interface**.

Step2. **Statistics** → **WAN** , select the WAN to view. MIS engineer can click **Minute** , to view the statistic charts results in every minute ; Click **Hour** , to view the statistic charts results in every hour. Click **Day** , to view the statistic charts results in every day. Click **Week** , to view the statistics charts results in every week. Click **Month** , to view the statistics results in every month. ; Click **Year** , to view the statistics charts results in every year.

### Step3. Statistic charts

- Ordinate : Network flow.
- Horizontal ordinate : Time (hour/minute).



[View the WAN flow](#)

## 17.2 Policy

Step1 When enable **Policy** → **Statistics** option , then the **Policy statistics charts** will enabled in **Statistics** → **Policy**.

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

The policy statistics

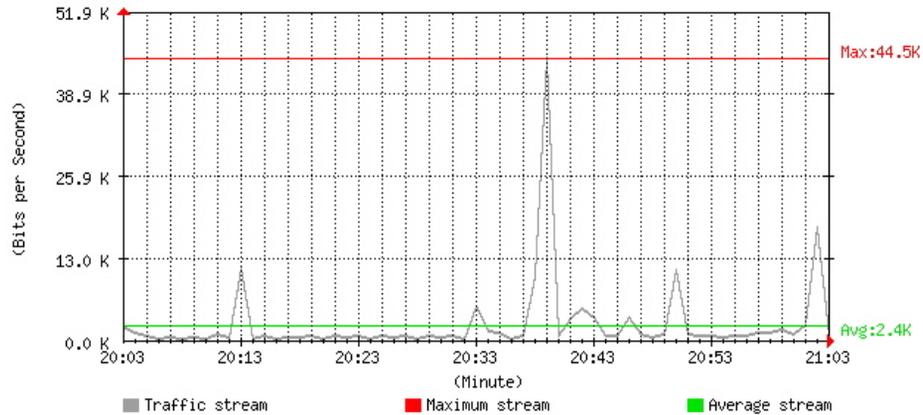


If the MIS engineer want to enable the **Policy Statistics** , then he must enable the statistic option in **Policy**.

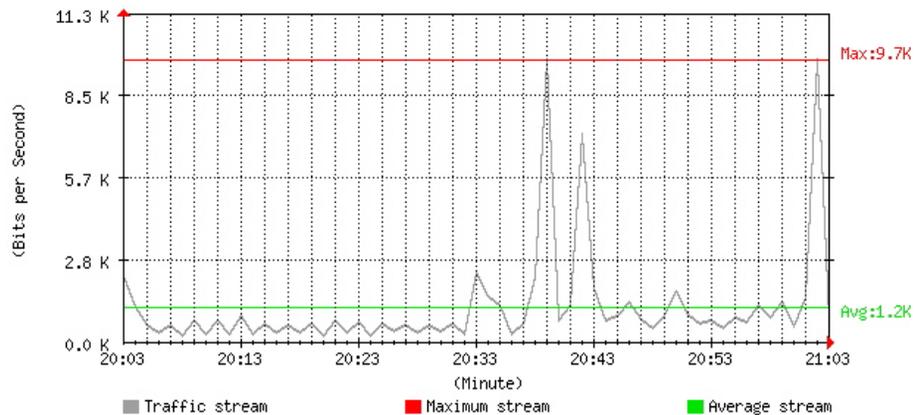
Step2. **Statistics** → **Policy** , select the policy to view. MIS engineer can click **Minute** , to view the statistic charts results in every minute ; Click **Hour** , to view the statistic charts results in every hour. Click **Day** , to view the statistic charts results in every day. Click **Week** , to view the statistics charts results in every week. Click **Month** , to view the statistics results in every month. ; Click **Year** , to view the statistics charts results in every year.

### Step3. Network flow statistic charts.

- Ordinate : Network flow.
- Horizontal ordinate : Time ( hour/minute ) .



### Upstream



[View the policy statistics charts](#)

## Chapter 18

# Diagnostic

The MIS engineer can set the BM-2101A proactively send the packets ( Ping and Traceroute ) to detects the status of WAN interface.

## 18.1 Ping

Step1. In **Diagnostic → Ping**, the MIS engineer can set the BM-2101A send the packets to specific address, to detects the status of WAN interface :

- Enter the **Destination IP / Domain name**.
- Enter the **Packet size**. ( Default setting is 32 Bytes )
- Enter **Count** value. ( Default setting is 4)
- Enter **Wait time**. ( Default setting is 1 second)
- Enter the source packets **Interface**.
- Click **OK**.

The screenshot shows a 'Ping Setting' dialog box with the following fields and values:

Field	Value	Notes
Destination IP / Domain name	www.google.com	(Max: 30 characters)
Packet size	32	Bytes ( Range: 1 - 9999 )
Count	4	( Range: 0 - 9999, 0: means unlimited )
Wait time	1	Seconds ( Range: 1 - 9999 )
Interface	WAN1	61.11.11.11

Buttons: OK, Cancel

**Ping Result**

Result
There is no message!

**Ping setting**

**Ping Setting:**

Destination IP / Domain name:  (Max: 30 characters)

Packet size:  Bytes ( Range: 1 - 9999 )

Count:  ( Range: 0 - 9999, 0 means unlimited )

Wait time:  Seconds ( Range: 1 - 9999 )

Interface:

---

**Ping Result:**

Result
PING www.l.google.com (66.249.89.104) from 59.124.36.162 : 32 bytes of data:
Reply from 66.249.89.104: bytes=32 icmp_seq=0 ttl=243 time=60.335 msec
Reply from 66.249.89.104: bytes=32 icmp_seq=1 ttl=243 time=59.604 msec
Reply from 66.249.89.104: bytes=32 icmp_seq=2 ttl=243 time=58.993 msec
Reply from 66.249.89.104: bytes=32 icmp_seq=3 ttl=243 time=59.631 msec
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/dev = 58.993/59.640/60.335/0.561 ms

**Ping results**



If the MIS engineer select **VPN** of Interface, then he must enter the local BM-2101A LAN interface IP , and enter the remote LAN IP (which can send or receive packets via VPN) in to **Destination IP / Domain name column.**

- Use the following method to detect the VPN status of local 192.168.189.X/24 segment and remote 192.168.169.X/24 segment.

**Ping Setting**

Destination IP / Domain name:  (Max. 30 characters)

Packet size:  Bytes (Range: 1 - 9999)

Count:  (Range: 0 - 9999, 0 means unlimited)

Wait time:  Seconds (Range: 1 - 9999)

Interface:

**Ping Result**

Result
PING 192.168.169.30 (192.168.169.30) from 192.168.189.1 : 32 bytes of data :
Reply from 192.168.169.30: bytes=32 icmp_seq=0 ttl=128 time=20.698 msec
Reply from 192.168.169.30: bytes=32 icmp_seq=1 ttl=128 time=20.409 msec
Reply from 192.168.169.30: bytes=32 icmp_seq=2 ttl=128 time=20.425 msec
Reply from 192.168.169.30: bytes=32 icmp_seq=3 ttl=128 time=20.444 msec
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/mdev = 20.409/20.494/20.698/0.118 ms

**The Ping results of VPN**

## 18.2 Traceroute

Step1. In **Diagnostic** → **Traceroute**, the MIS engineer can set the BM-2101 send the packets to specific address by traceroute command, to detects the status of WAN interface :

- Enter the **Destination IP / Domain name**.
- Enter the **Packet size**.( Default setting is 40 Bytes )
- Enter the **MAX Time-to-Live**.( Default setting is 30 Hops)
- Enter the **Wait time**.( Default setting is 2 seconds)
- Select the source packets **Interface**.
- Click **OK**.

Traceroute Setting	
Destination IP / Domain name	168.95.1.1 (Max: 30 characters)
Packet size	40 Bytes ( Range: 40 - 9999 )
Max Time-to-Live	30 Hops ( Range: 1 - 255 )
Wait time	2 Seconds ( Range: 2 - 9999 )
Interface	WAN1

OK Cancel

Traceroute Result	
Result	
	There is no message!

**Traceroute setting**

**Traceroute Setting**

Destination IP / Domain name:  (Max: 30 characters)

Packet size:  Bytes (Range: 40 - 9999)

Max Time-to-Live:  Hops (Range: 1 - 255)

Wait time:  Seconds (Range: 2 - 9999)

Interface:

OK Cancel

---

**Traceroute Result**

Result
traceroute to 168.95.1.1 (168.95.1.1), 30 hops max, 40 byte packets from 61.228.186.159
From 61.228.186.159
To hop 1 : IP = 59.112.64.254 round-trip min/avg/max = 19.402/19.577/19.684 ms
To hop 2 : IP = 168.95.72.2 round-trip min/avg/max = 17.476/17.678/17.942 ms
To hop 3 : IP = 203.75.232.78 round-trip min/avg/max = 17.716/19.091/21.609 ms
To hop 4 : IP = 211.22.34.2 round-trip min/avg/max = 17.679/17.796/17.972 ms
To hop 5 : IP = 211.22.35.185 round-trip min/avg/max = 17.455/17.845/18.163 ms
To hop 6 : IP = 168.95.1.1 round-trip min/avg/max = 17.712/18.269/18.988 ms
Traceroute complete

Clear

**Traceroute results**

## Chapter 19

# Wake on Lan

The MIS engineer can use the BM-2101 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 chapter, we will make the introduction of Wake on Lan.

## 19.1 Example

### Remote monitor the internal PC

Step1. The internal PC to be remote monitored, and its MAC is 00:30:4F:B7:96:3B.

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

- Click **New Entry**.
- **Name**, enter josh.
- **MAC Address**, enter 00:30:4F:B7:96:3B.
- Click **OK**.



The screenshot shows a dialog box titled "Add Wake on Lan setting". It has two input fields: "Name" with the value "josh" and a "(Max. 20 characters) Assist" link, and "MAC Address" with the value "00:30:4F:B7:96:3B". At the bottom right, there are "OK" and "Cancel" buttons.

Set the internal PC to be monitored

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

Name	MAC Address	Configure
josh		Wake Up Modify Remove

New Entry

Start up the PC

# Status

MIS engineer can easily know the status of network connection anytime. For example , the information of area network and WAN interface IP address , netmask, default gateway , DNS server IP address etc.

1. **Interface** : It shows the all the interface status in BM-2101.
2. **System Info** : It shows the CPU utilization , memory utilization and ramdisk utilization.
3. **Authentication** : It records the authentication information in BM-2101.
4. **ARP Table** : It records all the ARP information in host PC whcih connected to the BM-2101.
5. **Sessions Info** : It records all the session packets pass through BM-2101.
6. **DHCP Clients** : It records the IP address status distributed by the DHCP server in BM-2101.

## Sessions Info

### Search

- To search the record depends on the Policy , No , Source IP , Destination IP and Port in BM-2101.
  - ◆ Add the following settings :
    1. **Policy** , select All Policy.
    2. **NO**, select ALL.
    3. Click **Search**.

**Search**

Enter keyword or phrase

Policy:

NO:

Source IP:

Destination IP:

Port:  -->  (Range: 1 - 65535)

**Results**

1 / 7 [Next](#)

Search results : 320 records

Sorting by Start Time:

Search the specific record

## 20.1 Interface

Step1 **Status** → **Interface** , it shows all the interface information in BM-2101.

- **System Uptime** : The operating uptime of BM-2101.
- **Active Sessions Number** : It shows the real sessions pass through BM-2101.
- **MAC Address** : The MAC address of interface.
- **IP Address/Netmask** : The IP address and netmask of interface.
- **Rx Pkts , Err.Pkts** : It shows the received packets and error packets of interface.
- **Tx Pkts , Err.Pkts** : It shows the transferred packets and error packets.
- **Ping , HTTP , HTTPS** : It shows if the user can ping the BM-2101 interface , or enter the Web UI through HTTP and HTTPS.
- **Forwarding Mode** : It shows the interface connection mode.
- **WAN Connection** : It shows the WAN interface connection status.
- **DnS / UpS kbps** : It shows the maximum downstream / upstream bandwidth in WAN . ( MIS engineer can set the max downstream / upstream bandwidth in **Interface**)
- **DnStream Alloca.** : The BM-2101 can allocate the downstream percentage depends on the WAN interface network flow.
- **UpStream Alloca.** : The BM-2101 can allocate the upstream percentage depends on the WAN interface network flow.
- **PPPoE Con.Time** : When using the PPPoE connection , it will shows the connection uptime.
- **Default Gateway** : It shows the WAN gateway address.
- **DNS 1** : It means the DNS 1 server IP address applied from the ISP.
- **DNS 2** : It means the DNS 2 server IP address applied from the ISP.

Active Sessions Number : 41

System Uptime : 4 Day 16 Hour 51 Min 34 Sec

	LAN	WAN1	WAN2	DMZ
Forwarding Mode	NAT	Static IP	Static IP	Transparent
WAN Connection	---			---
DnS / UpS Kbps	---	100000 / 100000	100000 / 100000	---
DnStream Alloca.	---	0%	100%	---
UpStream Alloca.	---	50%	49%	---
PPPoE Con. Time	---	---	---	---
MAC Address				
IP Address	192.168.189.1	61.11.11.11	211.22.22.22	0.0.0.0
Netmask	255.255.255.0	255.255.255.0	255.255.255.0	0.0.0.0
Default Gateway	---	61.11.11.254	211.22.22.254	---
DNS1	---	168.95.192.1	168.95.192.1	---
DNS2	---	168.95.1.1	168.95.1.1	---
Rx Pkts, Err. Pkts	1081295, 0	0, 0	2109, 0	2107, 0
Tx Pkts, Err. Pkts	14374, 0	132351, 0	132232, 0	145880, 0
Ping				
HTTP				
HTTPS				

### The interface information

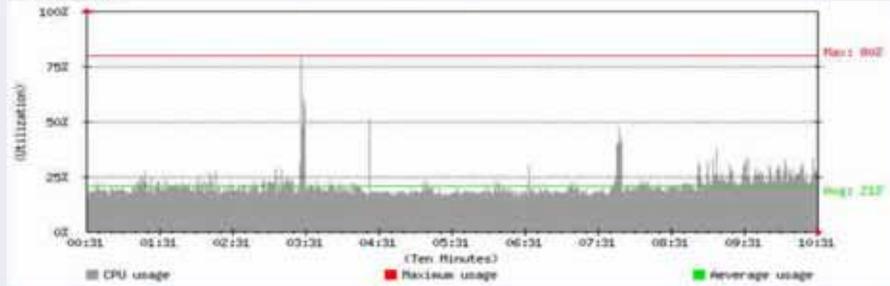
## 20.2 System Info

Step1 **Status** → **System Info** , it shows the real system information.

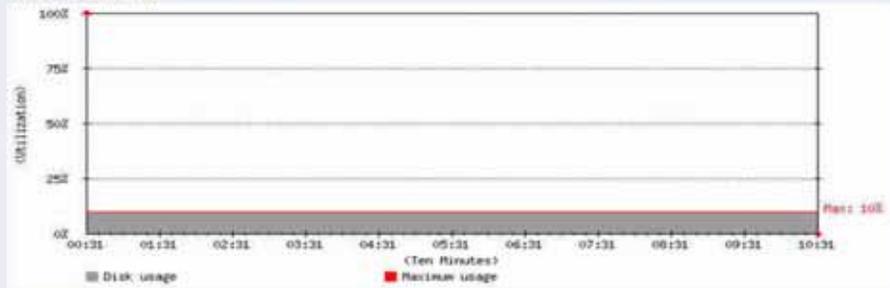
- CPU Utilization : The CPU utilization in BM-2101.
- HardDisk Utilization : The hard disk utilization in BM-2101 .
- Memory Utilization : The memory utilization in BM-2101 .
- RamDisk Utilization : The ram disk utilization in BM-2101 .

Memory Size : 1024 MB  
Hard Disk Status : ok

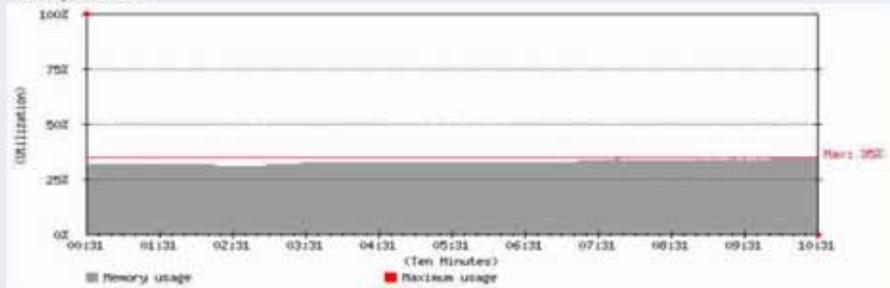
#### CPU Utilization



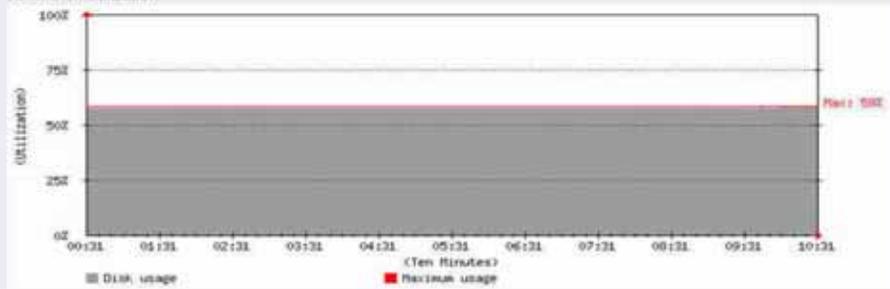
#### Hard Disk Utilization



#### Memory Utilization



#### RAM Disk Utilization



The system information

## 20.3 Authentication

Step1 **Status → Authentication** , it shows the authentication information in BM-2101.

- **IP Address** : It represents the authenticated user IP address.
- **Authentication –User Name** : It represents the authenticated login name used by authentication user.
- **Login Time** : It represents the user's login time (year / month / day / hour / minute / second.)

IP Address	Authentication-User Name	Login Time	Configure
192.168.138.30	Josh	2005/12/30 22:0:40	Remove

The authentication status Web UI



Click **Remove** , to delete the policy authenticated by BM-2101.

## 20.4 ARP Table

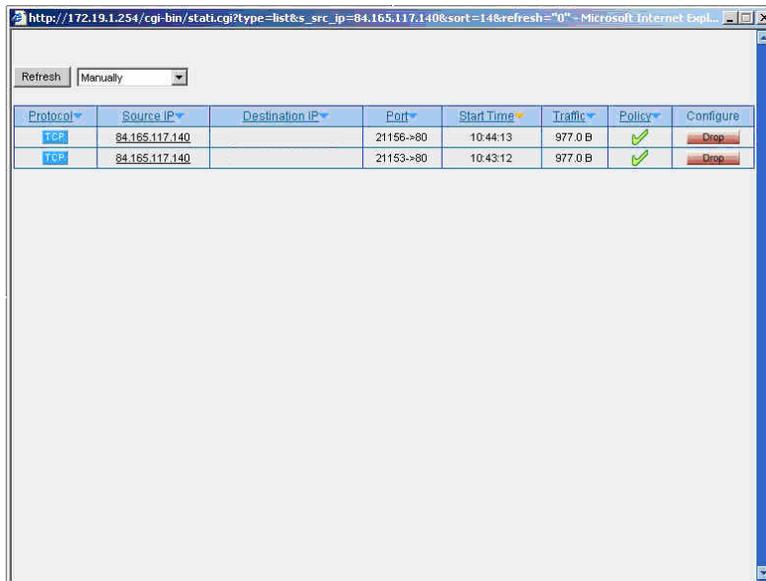
Step1 **Status → ARP Table** , it shows the information of Net BIOS name , IP address , MAC address and interface .

- **Net BIOS Name** : The PC's network identification name.
- **IP Address** : The PC's IP address.
- **MAC Address** : The computer's network adapter identification number.
- **Interface** : The computer's network interface position.

## 20.5 Sessions Info

Step1 **Status** → **Sessions Info** , and click one of the **Source IP**, then shows the information of sessions packets pass through BM-2101.

Step2 Click **Source IP** or **DestinationIP**. It shows the traffic statistics by user's IP , host name or domain name to access the network resources of pop up window.



The screenshot shows a web browser window with the URL `http://172.19.1.254/cgi-bin/stati.cgi?type=list&s_src_ip=84.165.117.140&sort=14&refresh="0"`. The page contains a table with the following data:

Protocol	Source IP	Destination IP	Port	Start Time	Traffic	Policy	Configure
TCP	84.165.117.140		21156->80	10:44:13	977.0 B	✓	Drop
TCP	84.165.117.140		21153->80	10:43:12	977.0 B	✓	Drop

Use the IP address to look up the sessions information



Click **Drop** , can immediately stop the specific session packets transferring .

## 20.6 DHCP Client

Step1 **Status → DHCP Clients** , it shows the status of IP address distributed by the DHCP server in BM-2101.

- **Net BIOS Name** : The PC's network identification name of IP address distributed by DHCP server.
- **IP Address** : The PC's dynamic IP address distributed by DHCP server.
- **MAC Address** : The computer's dynamic IP address mapped to MAC address.
- **Leased Time** : The effect date in dynamic IP address. (start date / end date) ( year / month / day / hour / minute / second ) .

NetBIOS Name	IP Address	MAC Address	Leased Time	
			Start	End
----	192.168.139.9		2005/12/30 21:56:6	2005/12/31 21:56:6
----	192.168.139.13		2005/12/30 16:45:36	2005/12/31 16:45:36
LOCALHOST	192.168.139.12		2005/12/30 16:18:31	2005/12/31 16:18:31

The DHCP Clients Web UI