Bandwidth Management Gateway

BM-2101

User's Manual

Copyright

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

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

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 DMZ	1 x 10/100Base-TX, Auto-MDI/MDI-X 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

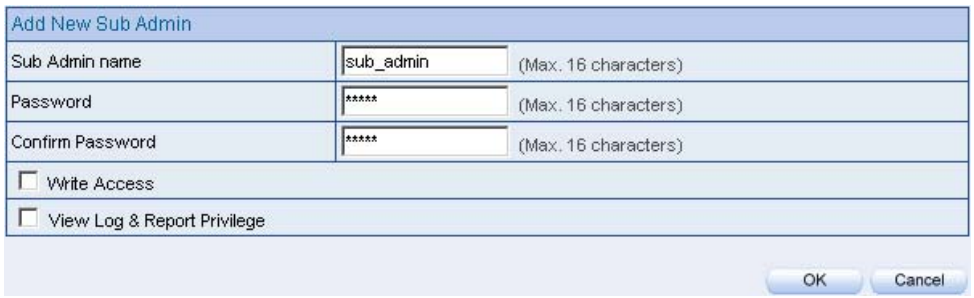
Step1. Click **Admin → New Sub-Admin** .

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.



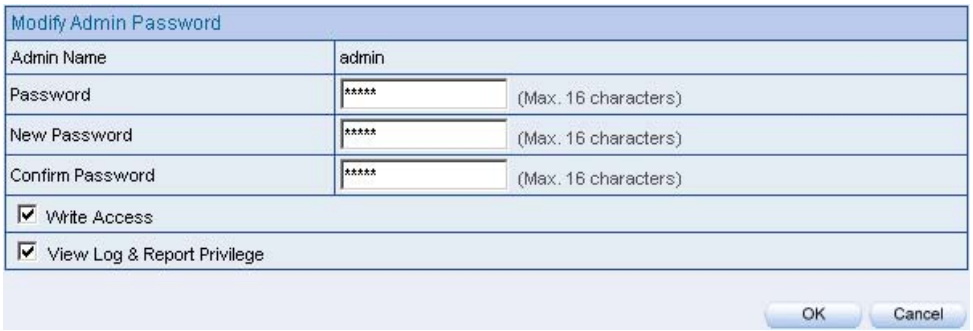
Add new sub admin

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

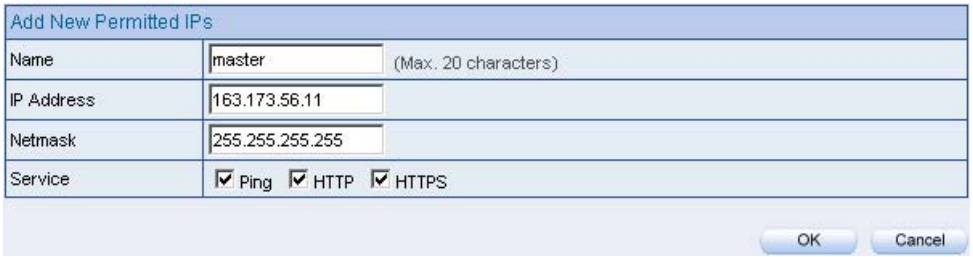


Modify admin password

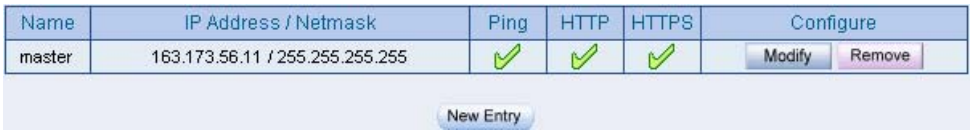
2.2 Permitted IPs

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**
- Compelte adding **Permitted IPs**



Add new Permitted IPs



Complete add new Permitted IPs

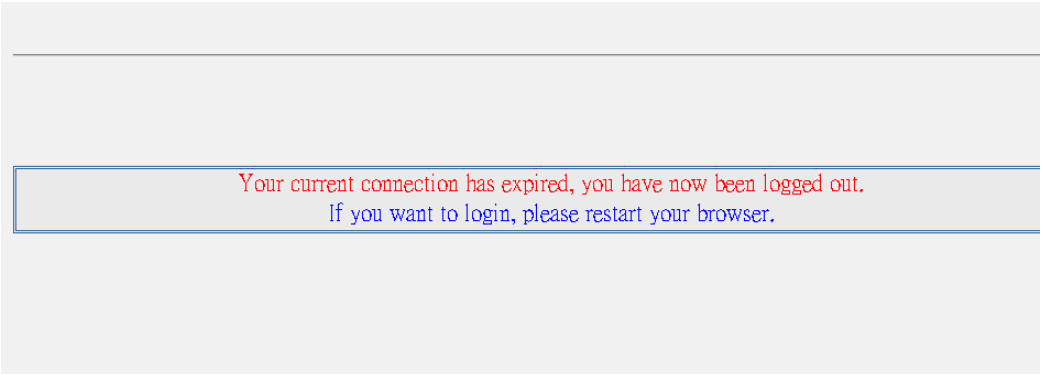
To activate Permitted IPs, click **Interface → LAN, WAN,** and **DMZ** to uncheck **Ping** ,**HTTP,** and **HTTPS**. However, **Permitted IPs** must be set before the cancellation of HTTP and HTTPS, or MIS engineer can not enter BM-2101's Web UI via the appointed interface.

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 Chaper, 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 administerator 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 occured .

Web Management

- The MIS engineeristerator 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, Customerr 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)
  Custermor 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 reserveing 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.

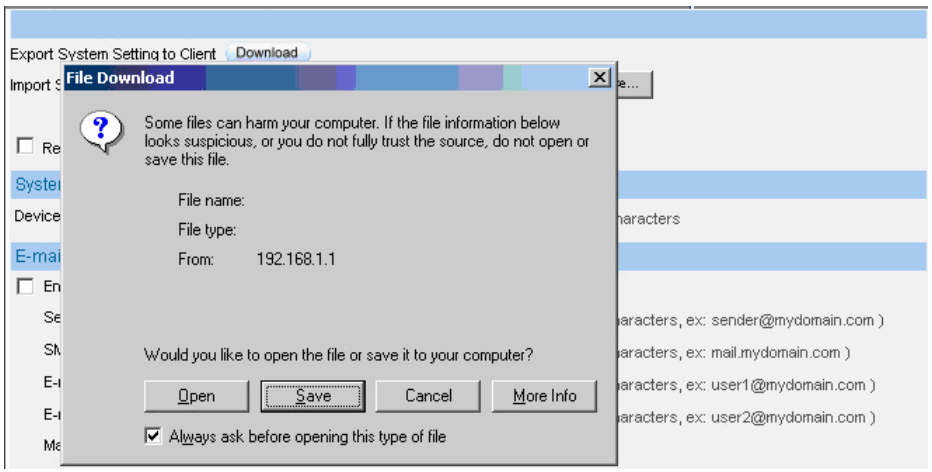
Virtual IP Address

- 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.



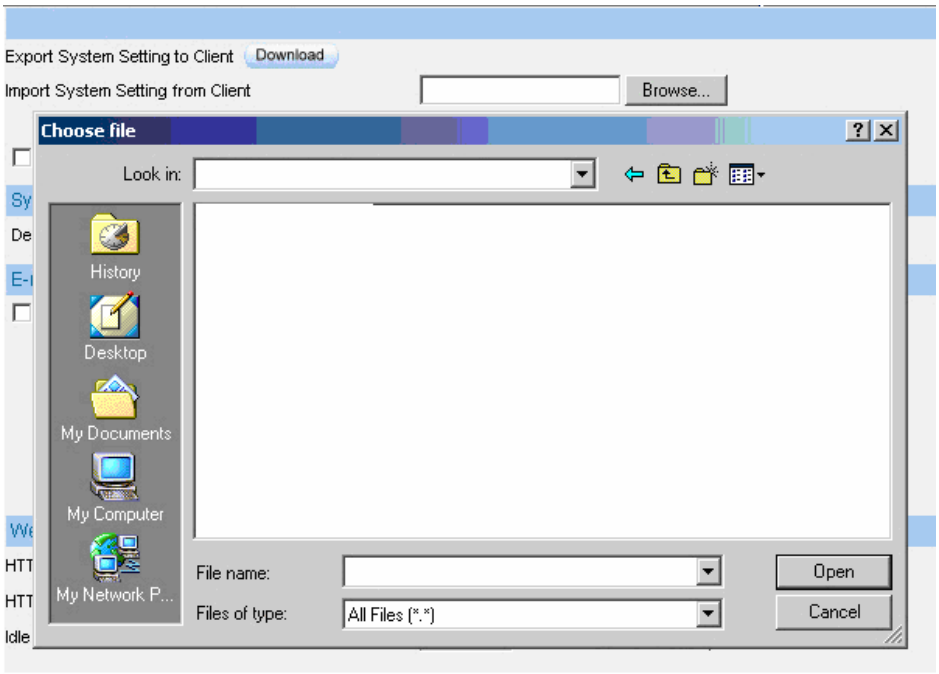
Choose the location to save files

Step1. In **Setting** window, click **Browse** near **Import System Setting from Client** .

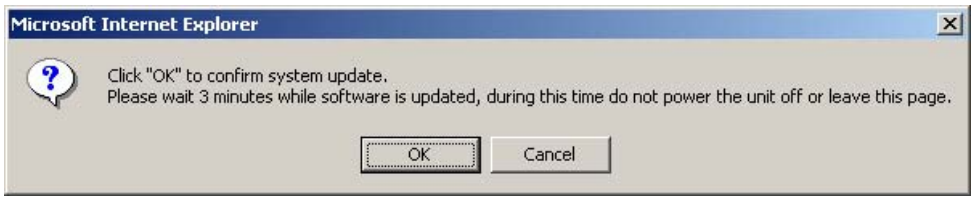
Step2. In **Choose File** window, select the previously saved settings and click **Open .**

Step3. Click **Open**, and a confirmation dialogue box pop out.

Step4. Click the **OK** to import the configuration file.



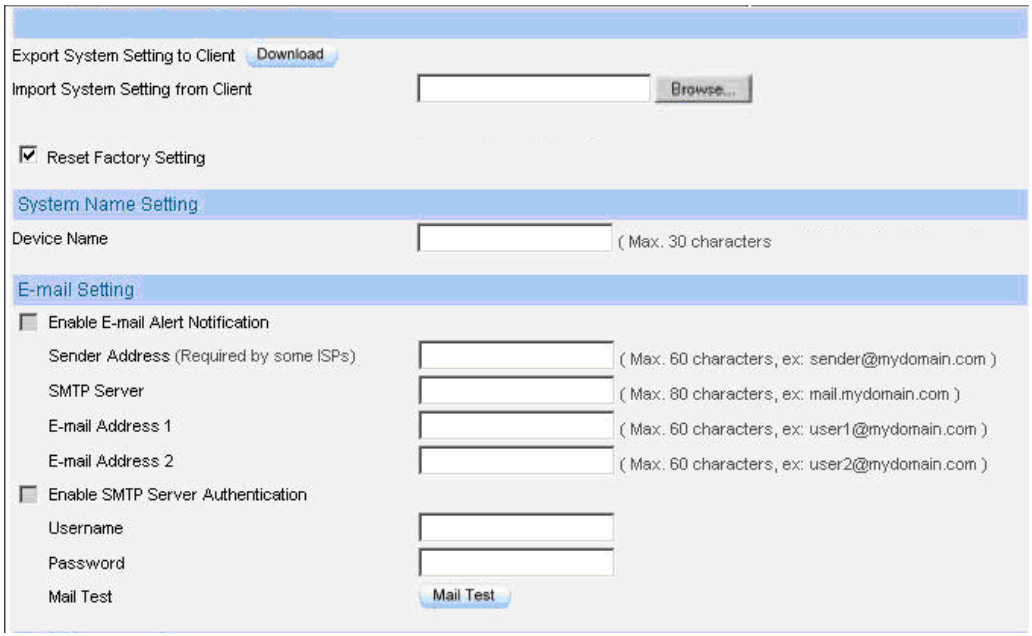
Import the file



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



Restore to factory setting

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

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

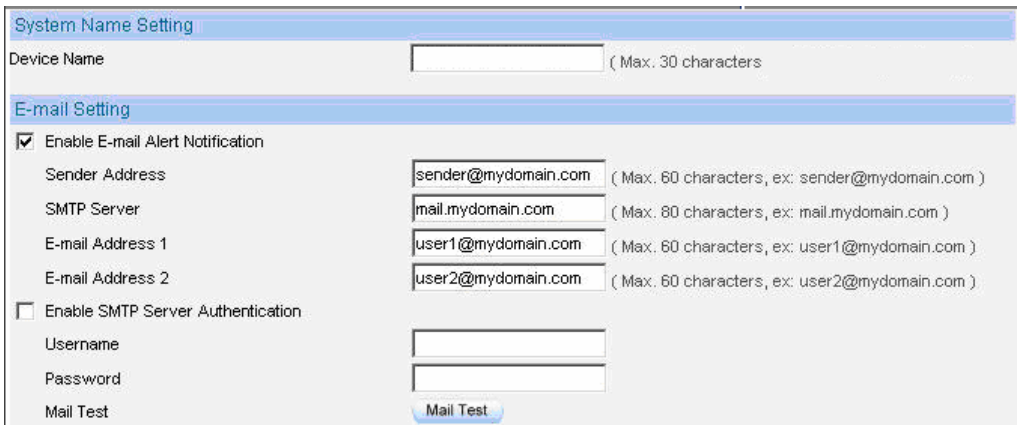
Step3. **Sender Address** : Enter the sender's email address. (Required by some ISP).

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.



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

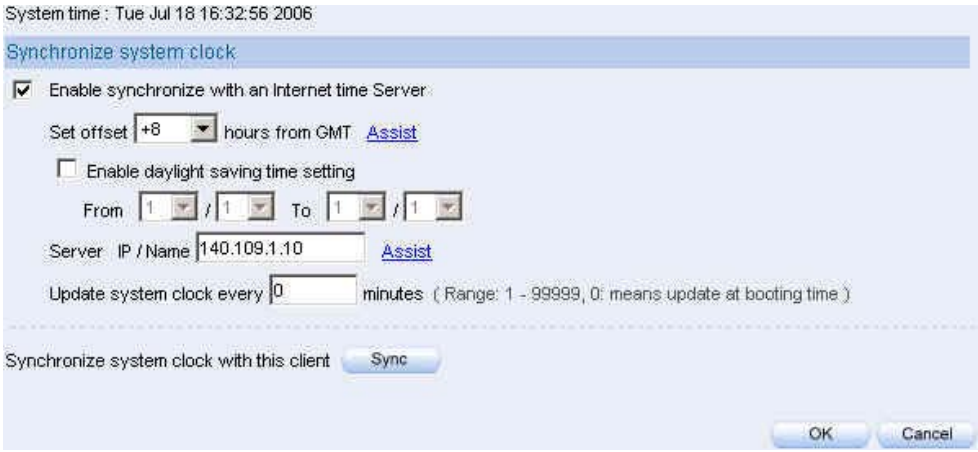
3.2 Date / Time

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.



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.

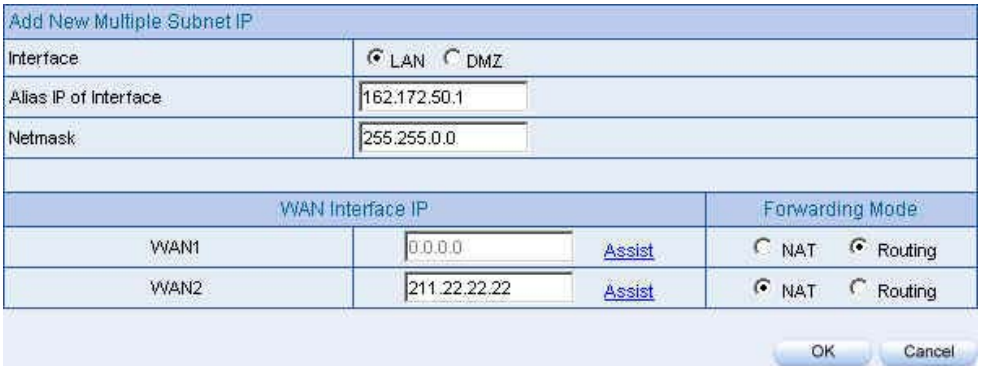
Preparations

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.

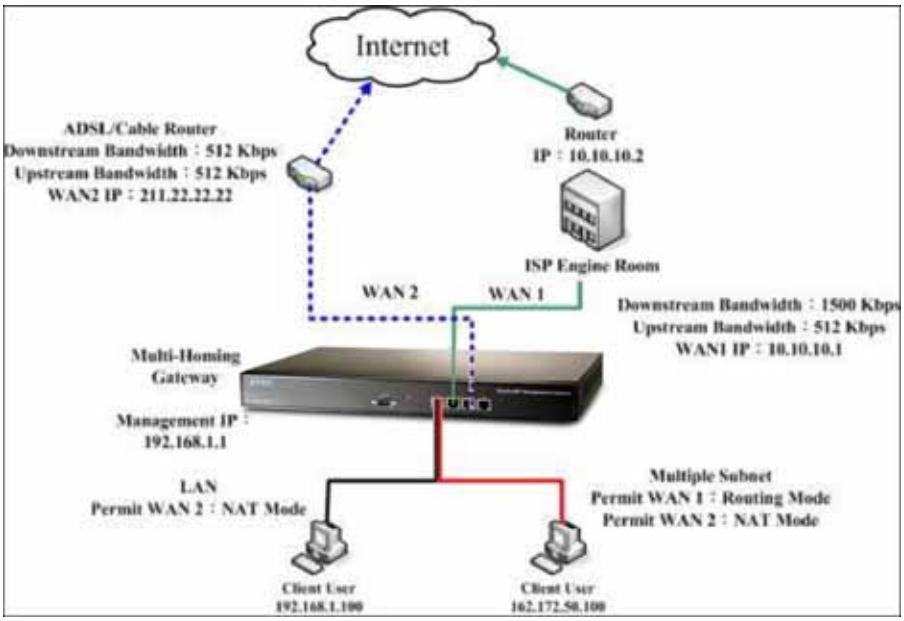


Add new multiple subnet IP

 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 usd 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 is192.168.1.1/24.

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

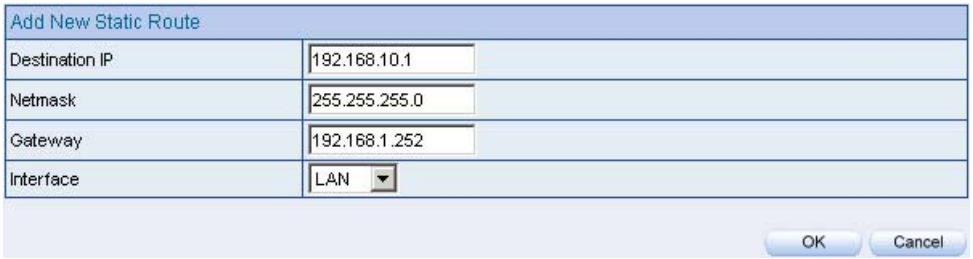
Company B

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** ：

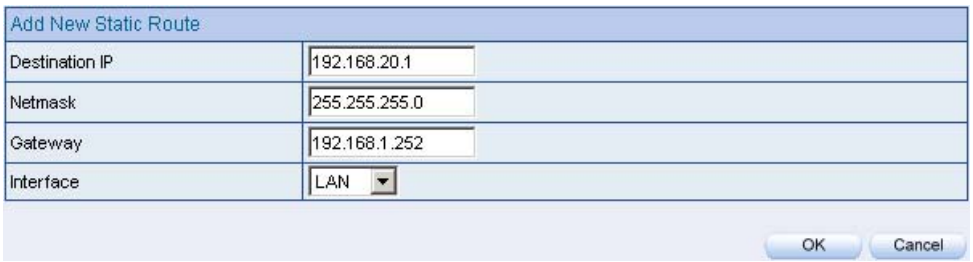
- **Destination IP** : Enter 192.168.10.1
- **Netmask** : Enter 255.255.255.0
- **Gateway** : Enter 192.168.1.252
- **Interface** : Select **LAN**.
- Click **OK**



Add new static route-1

Step2. In **Configure → Route Table**

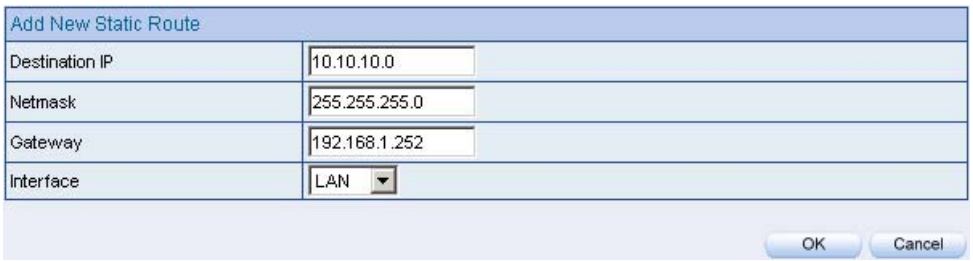
- **Destination IP**: Enter 192.168.20.1
- **Netmask**: Enter 255.255.255.0
- **Gateway** : Enter 192.168.1.252
- **Interface** : Select **LAN .**
- Click **OK**



Add new static route-2

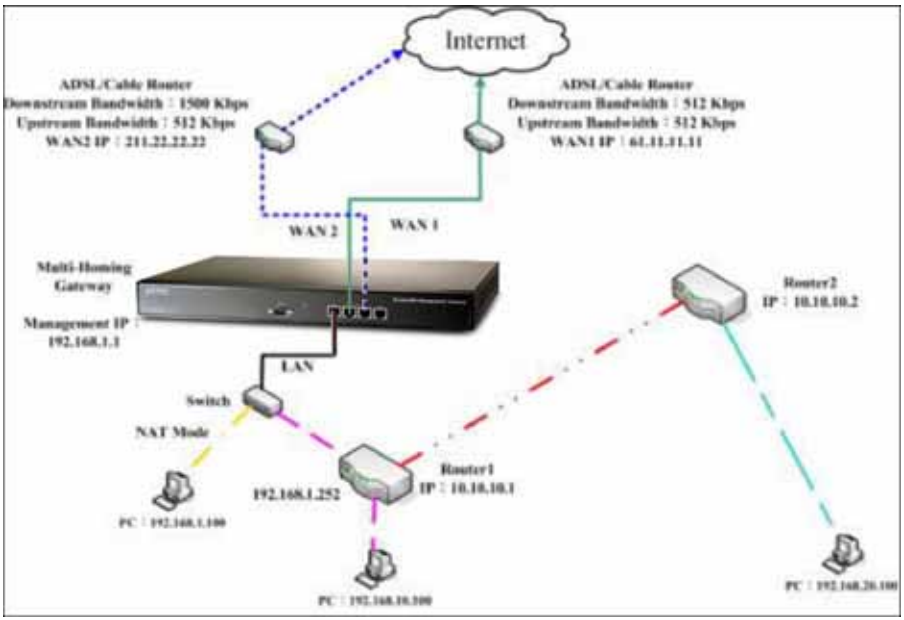
Step3. In **Configure → Route Table**：

- **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 -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.

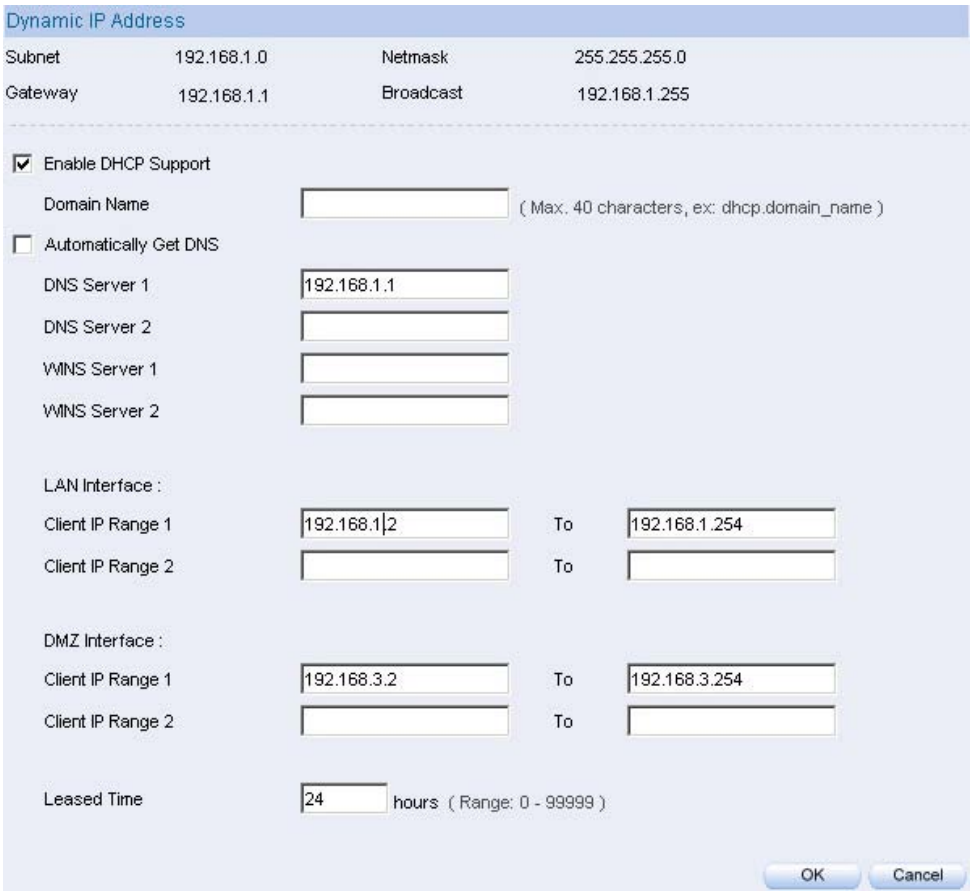


Route table environment

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 addresss, 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.



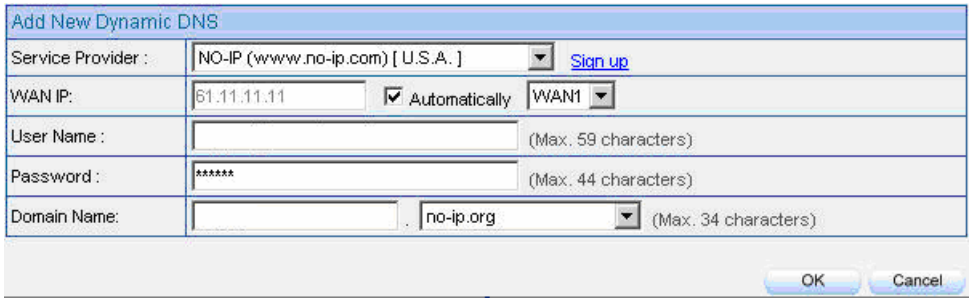
DHCP setting

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.



DDNS setting

Complete the DDNS setting

Icon				
Connotation	Connection Succeed	Wrong Password	Connecting	Errors

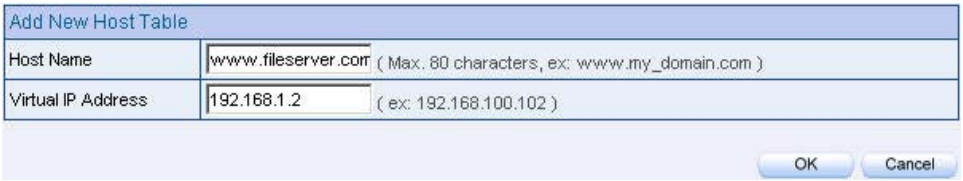
 If the MIS engineer have not apply the DDNS account, then he can choose the proper DDNS supplier, click **Sign up**, and then it will display the registeration web page.

 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



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

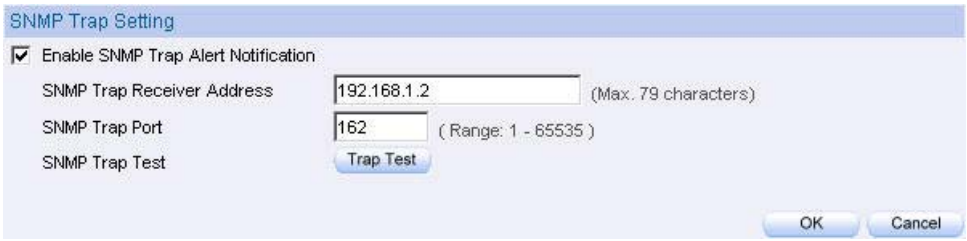
Step1. In **Configure → SNMP → Enable SNMP Agent** and enter the following setting：

- **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.

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.

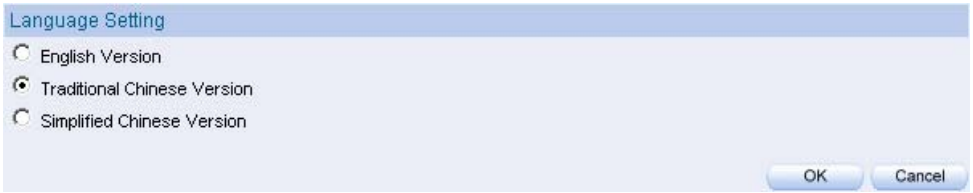


SNMP Trap setting

The MIS engineer can click Trap Test to test if SNMP Trap can wrok 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 bandwith 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 bandwdith 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.

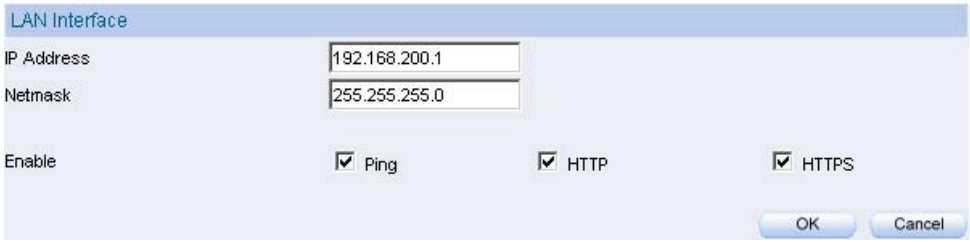
No.	Range	The Application Environment
Example 1	**LAN**	Modify the LAN interface address.
Example 2	**WAN**	Set the WAN interface address.
Example 3	**DMZ**	Set the DMZ interface address（NAT mode）.
Example 4	**DMZ**	Set the DMZ interface address（DMZ_Transparent mode）.

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 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.

Disable the WAN Interface

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

- ICMP: enter the persistant 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).

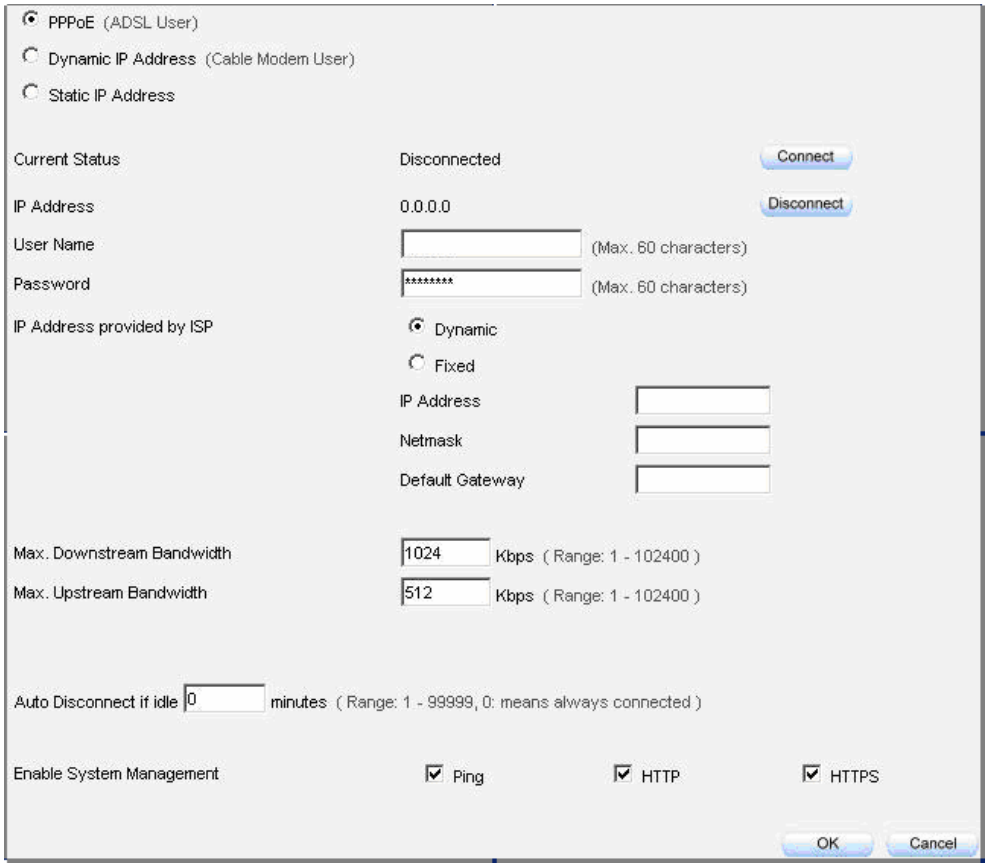
ICMP test

DNStest

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 depnds on the network bandwidth which the user applied .)
  6. Select **Ping** , **HTTP** , and **HTTPS**
  7. Click **OK .**



Select PPPoE

Balance Mode : Auto (Auto recommended)

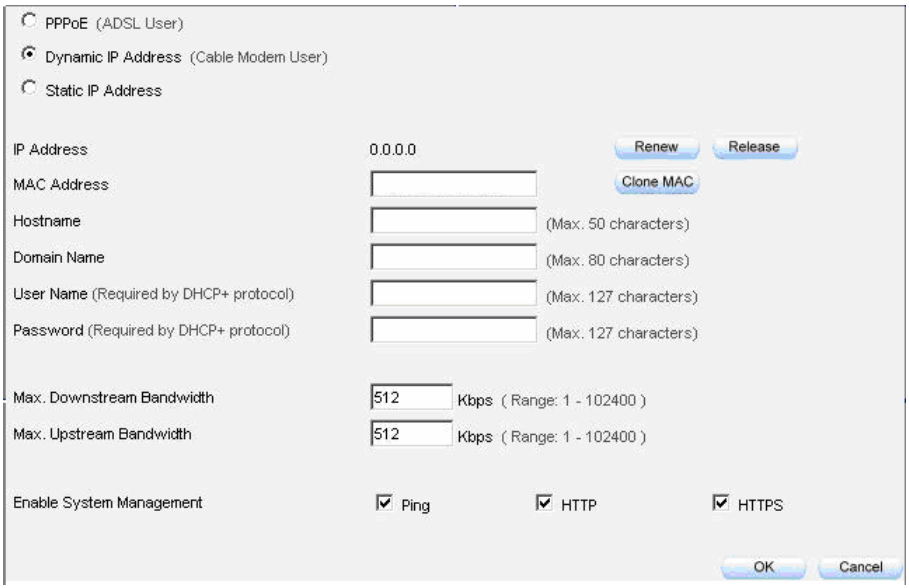
WAN No.	Connect Mode	IP Address	Saturated Connections	Ping	HTTP	HTTPS	Configure	Priority
1	PPPoE	61.228.170.252	1	✔	✔	✔	Modify	1
2	(Disable)	---	0	---	---	---	Modify	0

Complete PPPoE setting

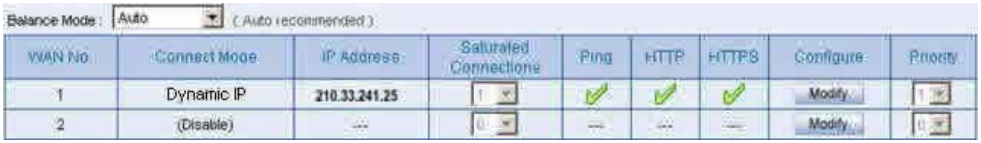
If use the PPPoE，the MIS engineer can set the WAN interface auto connect when it disconnect (it is recommended enable this function) or set the WAN interface disconect as idle.（Not Recommended）.

■ **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** .



Select Dynamic IP address

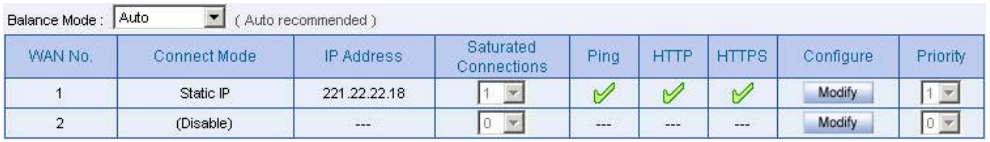


Complete to set the Dynamic IP address

■ 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**

Set the Static IP address



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 selet 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)

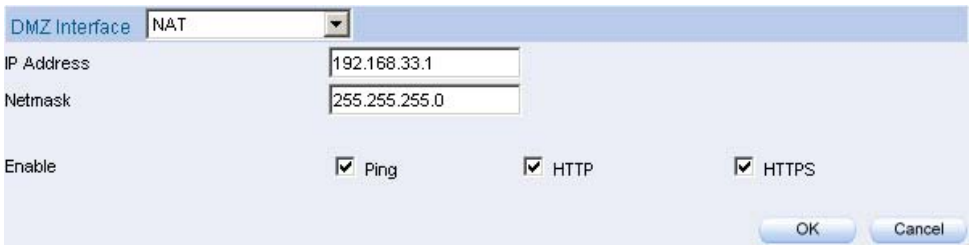
Step1. In **Interface → DMZ .**

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**



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**

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 identicy name to represent the IP address . Basically , the IP address can 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 shows 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 threee 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.

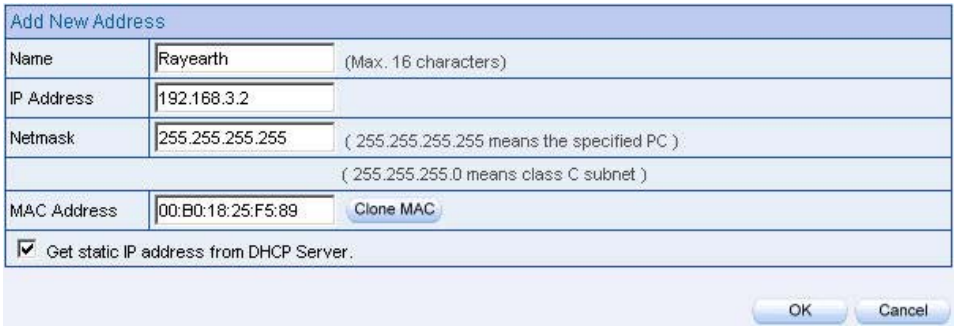
No.	Range	The Application Environment
Example 1	**LAN**	When use the DHCP, to distribute the static IPaddress to the specific user and limit the user can only access the FTP resources through policy .
Example 2	**LAN Group and WAN**	To set the policy which allow part of users connect to the remote static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

5.1 Example

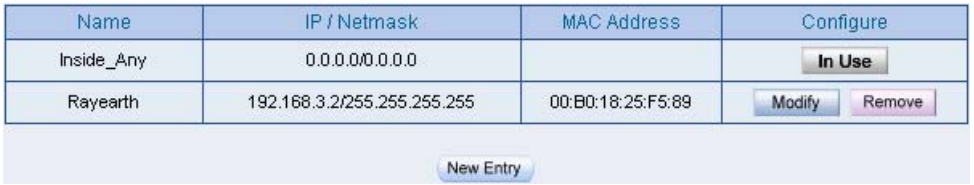
When use the DHCP, to distribute the static IPaddress to the specific user and limit the user can only access the FTP resources through policy.

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**

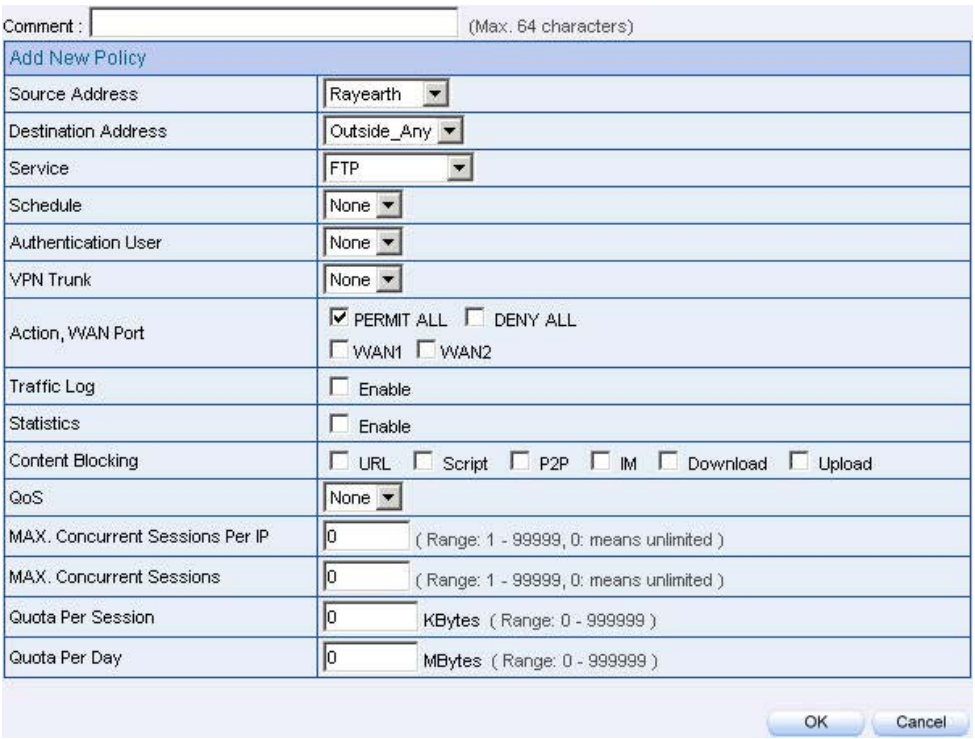


LAN address setting



Complete the LAN address setting

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



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 .

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

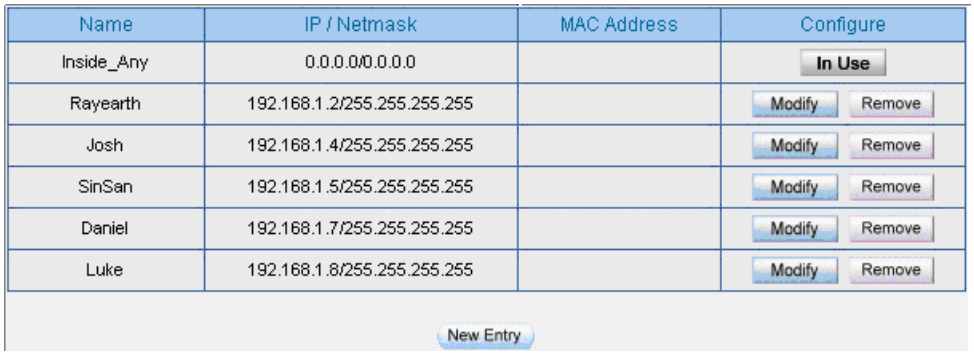
 When the MIS engineer set the Address settings , he can click Clone MAC ， in order to let the BM-2101 can automatically copy the user's network adapter MAC address .

 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 IPaddress.

Step1. Set many LAN address.



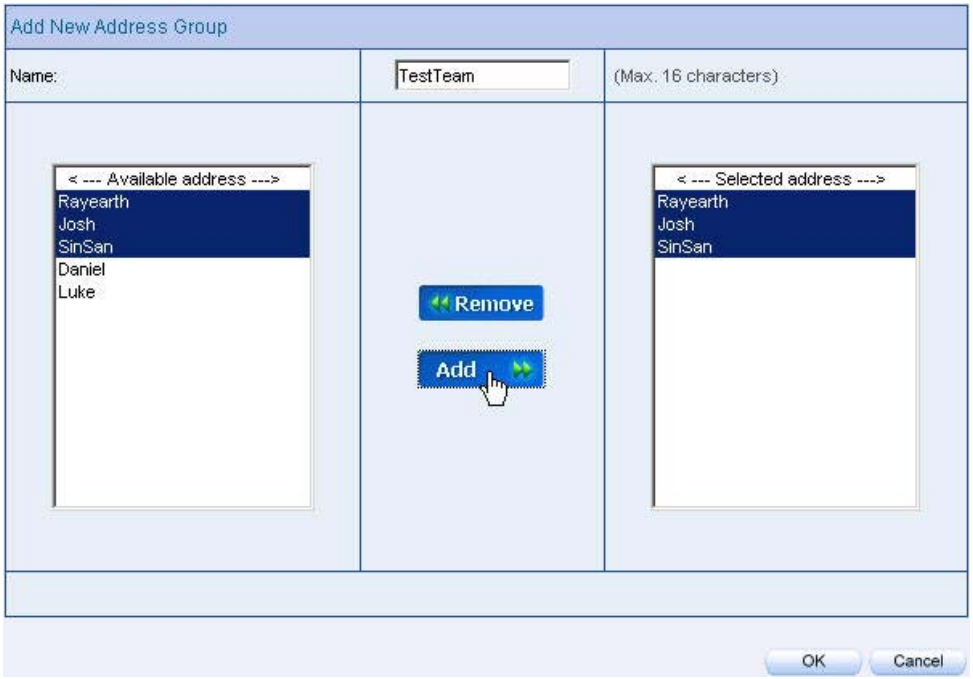
Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		In Use
Rayearth	192.168.1.2/255.255.255.255		Modify Remove
Josh	192.168.1.4/255.255.255.255		Modify Remove
SinSan	192.168.1.5/255.255.255.255		Modify Remove
Daniel	192.168.1.7/255.255.255.255		Modify Remove
Luke	192.168.1.8/255.255.255.255		Modify Remove

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** .



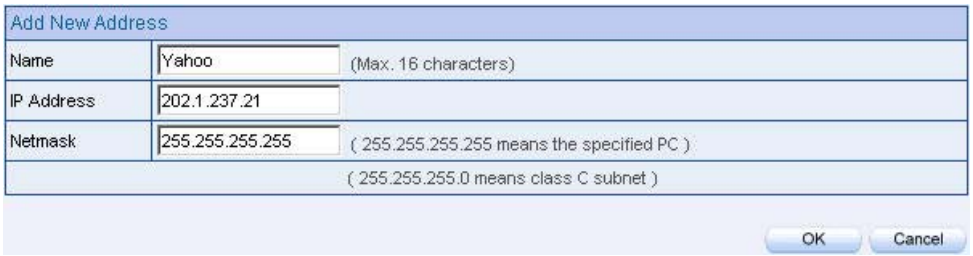
Group the LAN address

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：

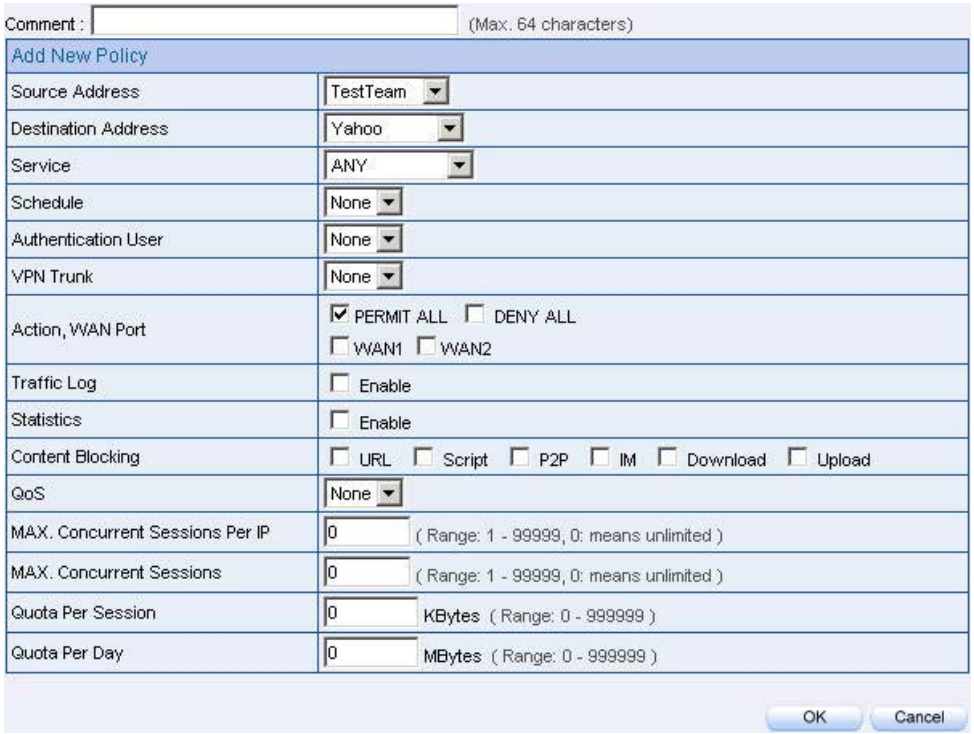
- Click **New Entry**
- Enter the remote static IP information .（**Name , IP , Netmask**）
- Click **OK**



Set the WAN address

Complete to set the WAN address

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



Apply the address setting in policy

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 (10x5=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	Any service .
TCP	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	UDP service , for example , IKE , DNS , NTP , IRC , RIP , SNMP , SYSLOG , TALK , TFTP , UDP-ANY , UUCP .
ICMP	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	**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）
Example . 2	**Group**	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		In Use
VoIP_01	192.168.1.2/255.255.255.255		Modify Remove
VoIP_02	192.168.1.3/255.255.255.255		Modify Remove
VoIP_03	192.168.1.4/255.255.255.255		Modify Remove
VoIP_04	192.168.1.5/255.255.255.255		Modify Remove

New Entry

LAN address setting

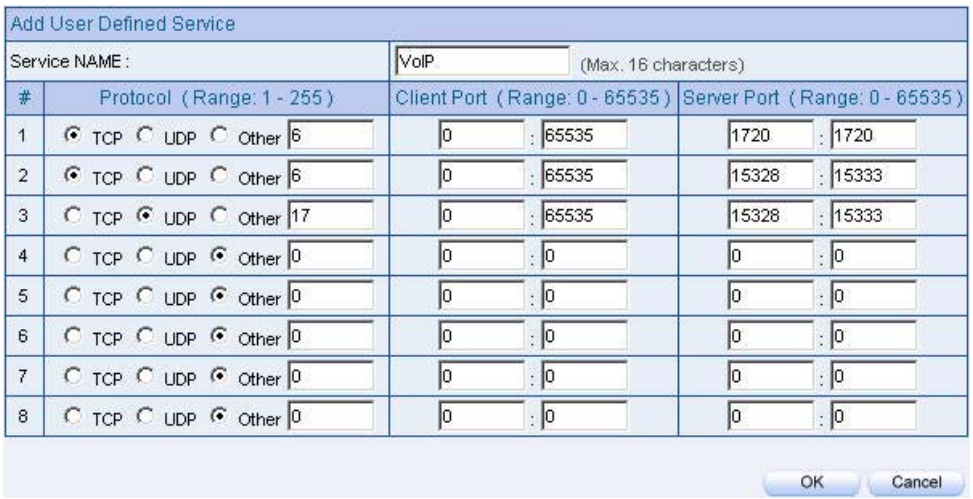
Name	Member	Configure
VoIP_Group	VoIP_01, VoIP_02, VoIP_03...	Modify Remove Pause

New Entry

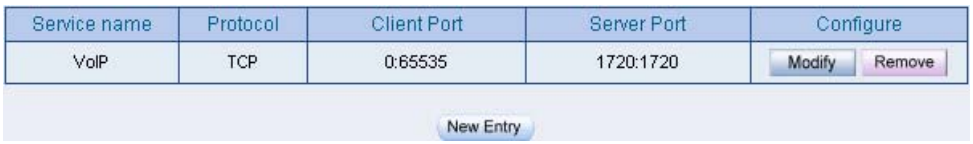
Group the LAN address

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** .



Custom setting

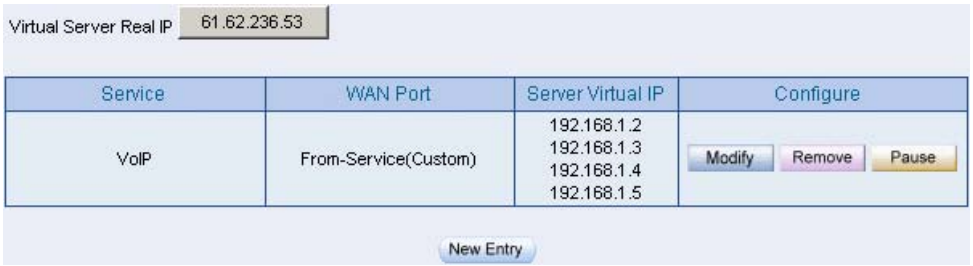


Complete the VoIP custom setting

 Normally，the default client port number is 0 to 65535. It is recommended not to modif y 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** .



Apply the service setting to virtual server

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

Complete to set the incoming VoIP policy

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

Complete to set the outgoing VoIP policy

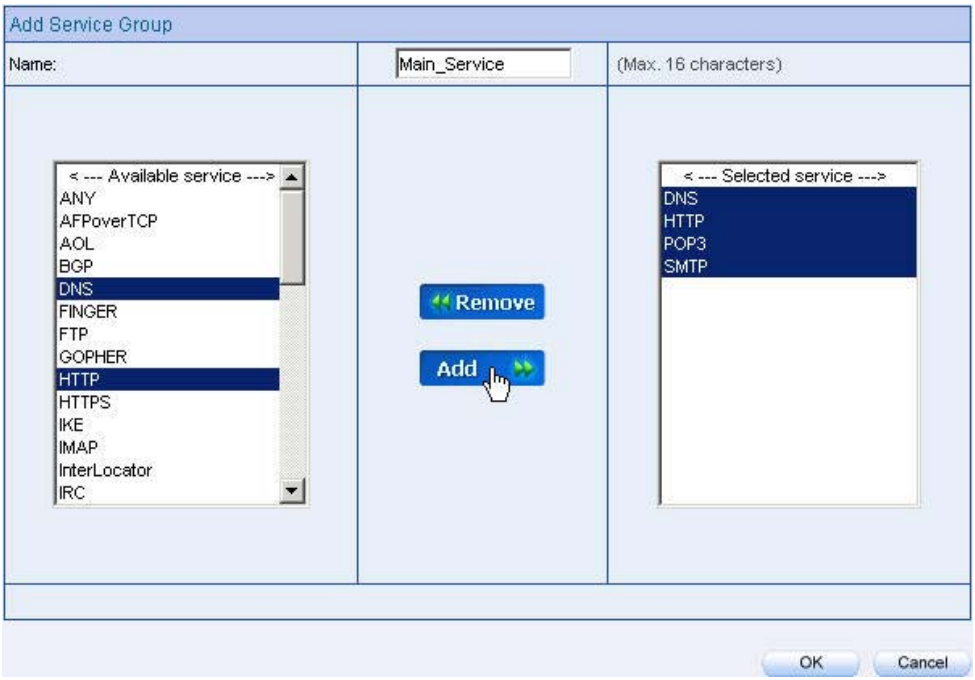
The service setting must apply to **Policy** and **Virtual Server**， to make it real working .

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

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.

LAN group setting

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

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.

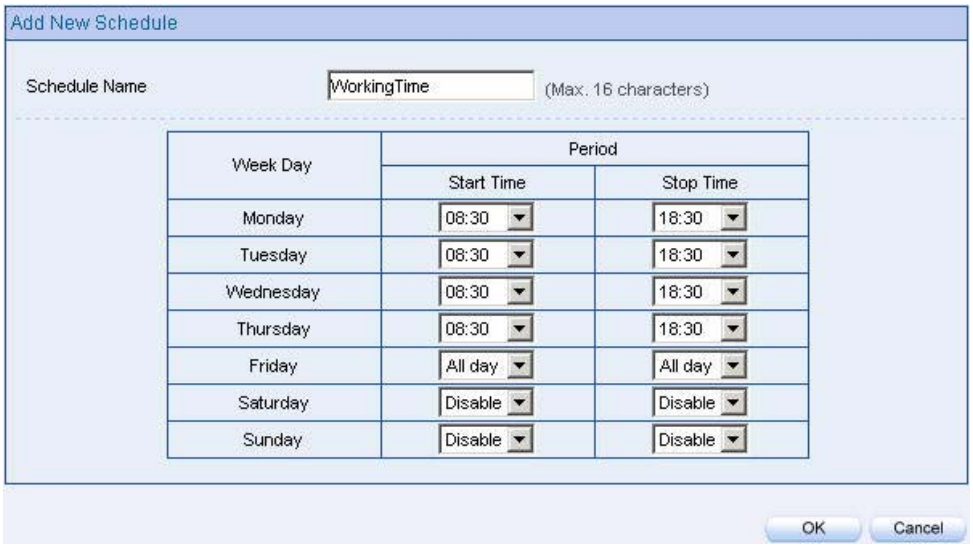
How to use Sehedule ?

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

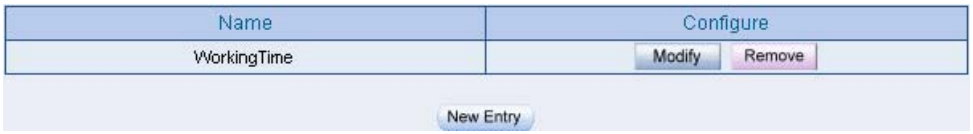
To set the valid time of LAN user can access the network data everyday through the policy management.

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**



Schedule setting



Complete the schedule setting

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

Complete to apply the schedule setting to policy

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

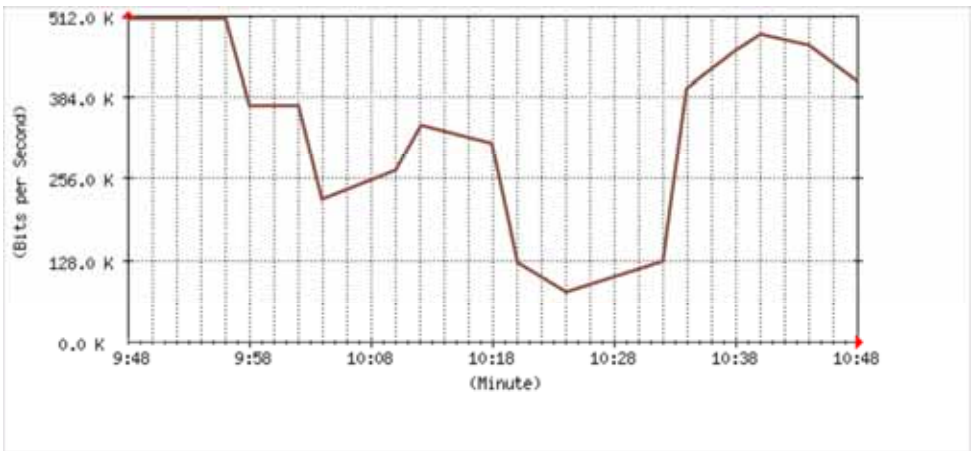
Chapter 8

QoS

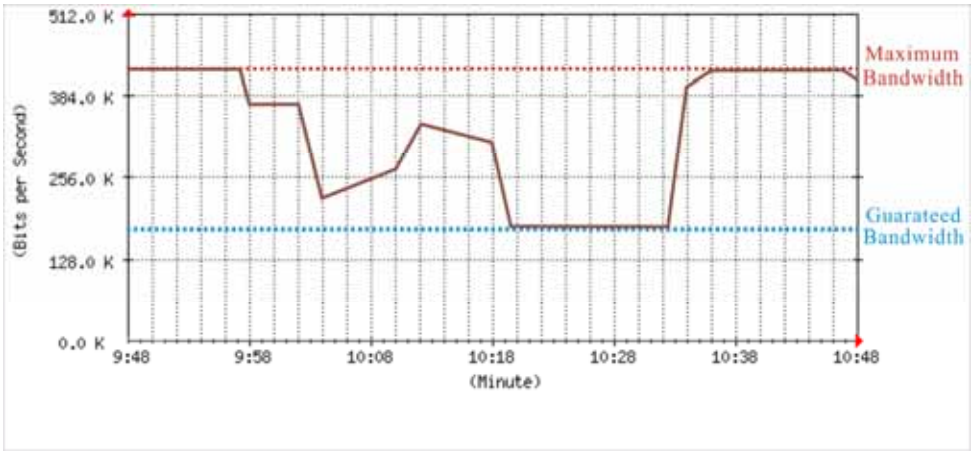
The BM-2101 appliance can manage the downstream and upstream bandwidth through the bandwidth parameter setting .

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 unuse 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

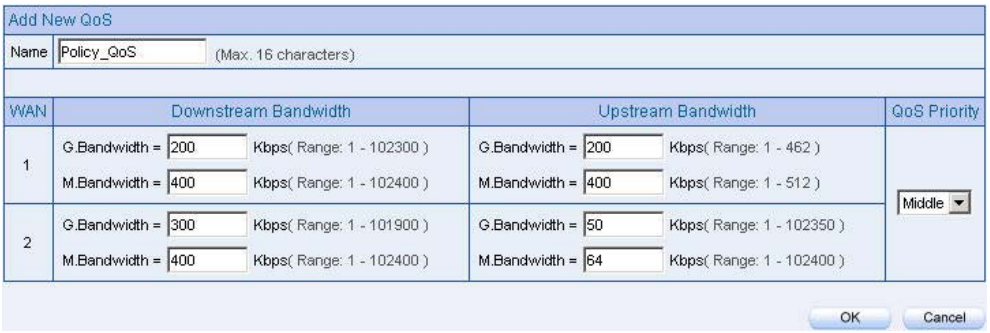
- The maximum bandwidth in QoS. The **Policy** which applied to the QoS, its bandwidth will not over the QoS Setting .

8.1 Example

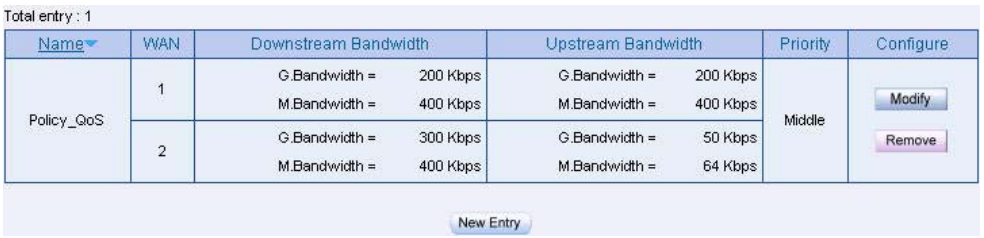
To set the Policy of the Upstream Bandwidth and Downstream Bandwidth .

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** .



QoS setting



Complete the QoS setting

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

Set the QoS policy

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 .

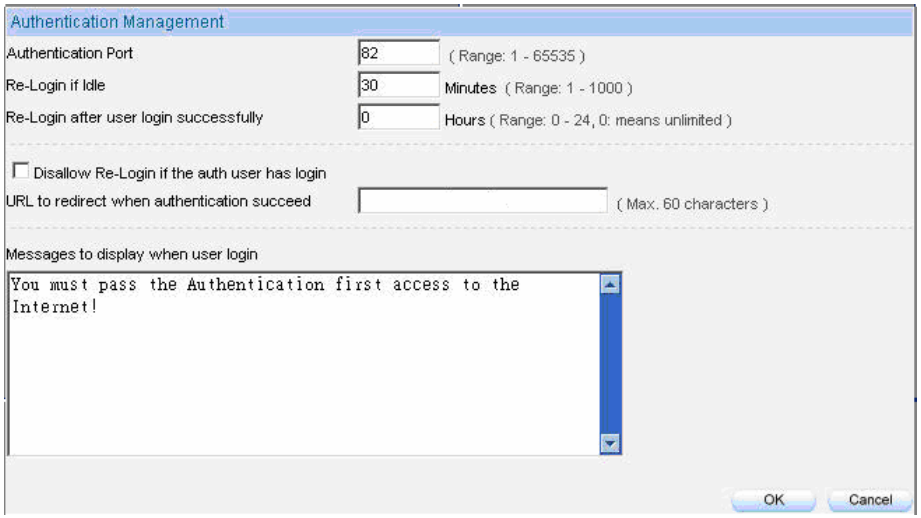
The BM-2101 appliance provided 4 authentication modes . The **User** and **User Group** built in ; others are **RADIUS** , **POP3** and **LDAP** self-built Authentication Server. The MIS engineer can use the 5 modes , to manage the authentication.

Authentication

Authentication Management

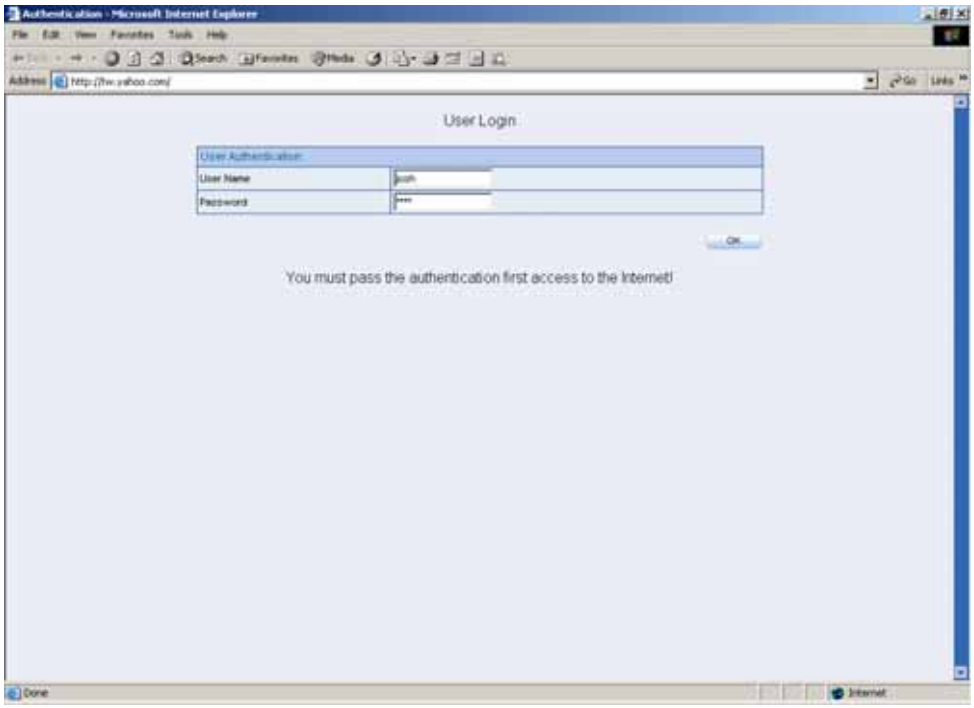
- It can provide the authentication port to the MIS engineer and the valid authentication time . (The MIS engineer has to set the Authentication function first .)
  - **Authentication Port**：When enable the Authentication, the LAN user must pass the authentication to login to the WAN. And the authentication 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 authenticaion 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 authenticaion , 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 massage in the authenication window.）

- To add the settings in the authenticaion management ：



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 .

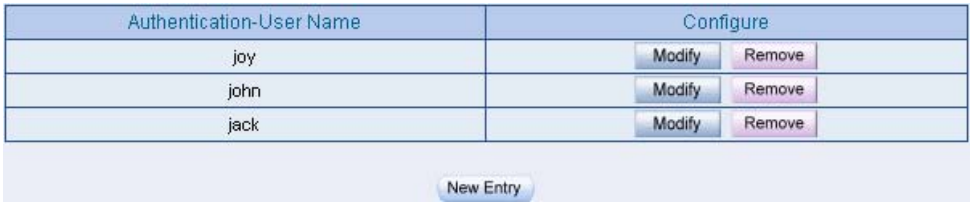
We set 4 environments.

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

9.1 User / User Group

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

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

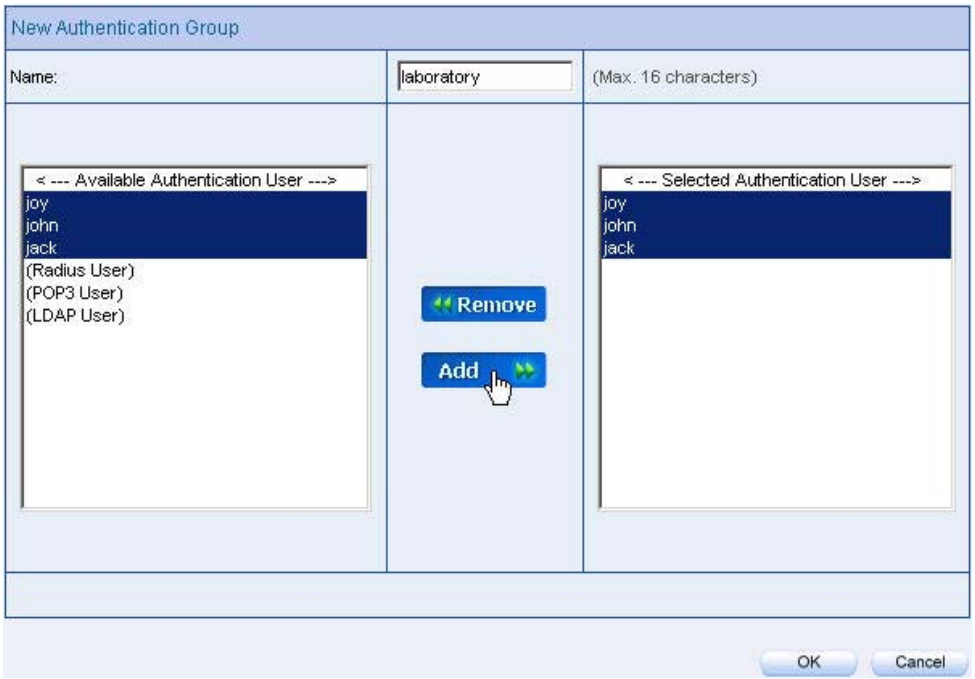


Set the authentication user

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

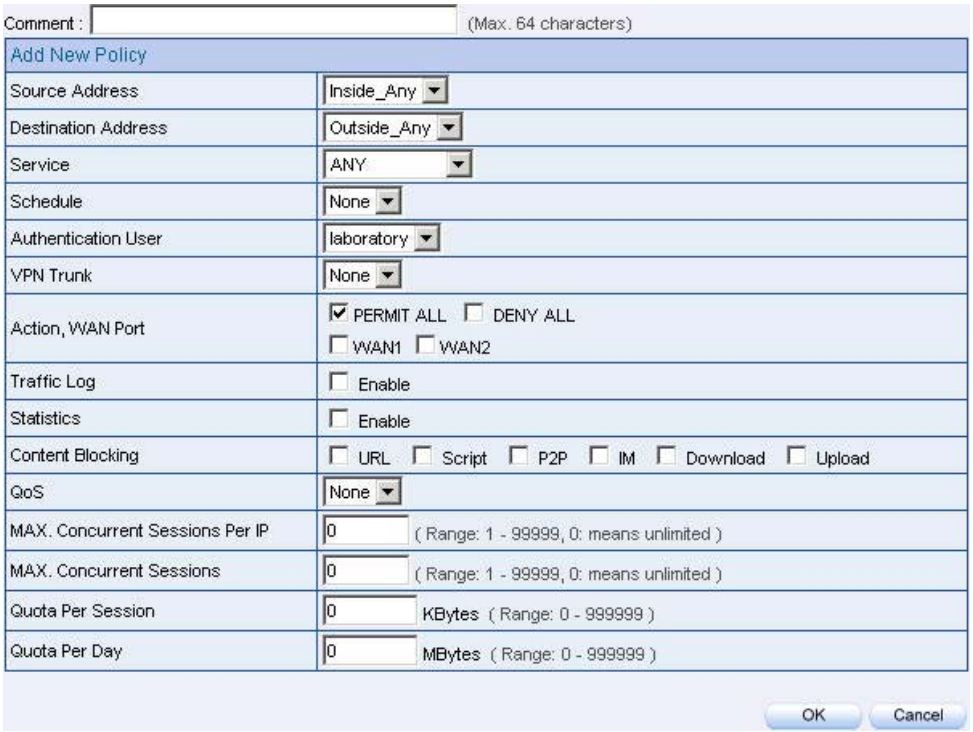
Step2. In **Authentication → User Group** , add the new setting as following：

- 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.



Authenticatoin setting

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



Authentication user policy setting

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.

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 authenticaton in policy .To use the WAN RADIUS server（Windows 2003 Server built-in authentication .）

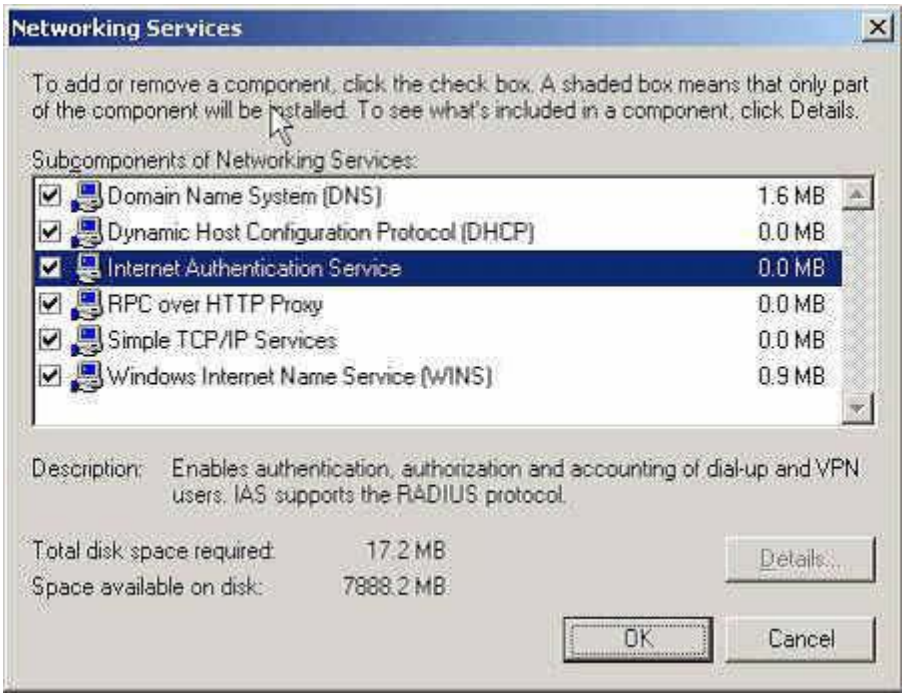
※ Windows 2003 RADIUS Server Deployment

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

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

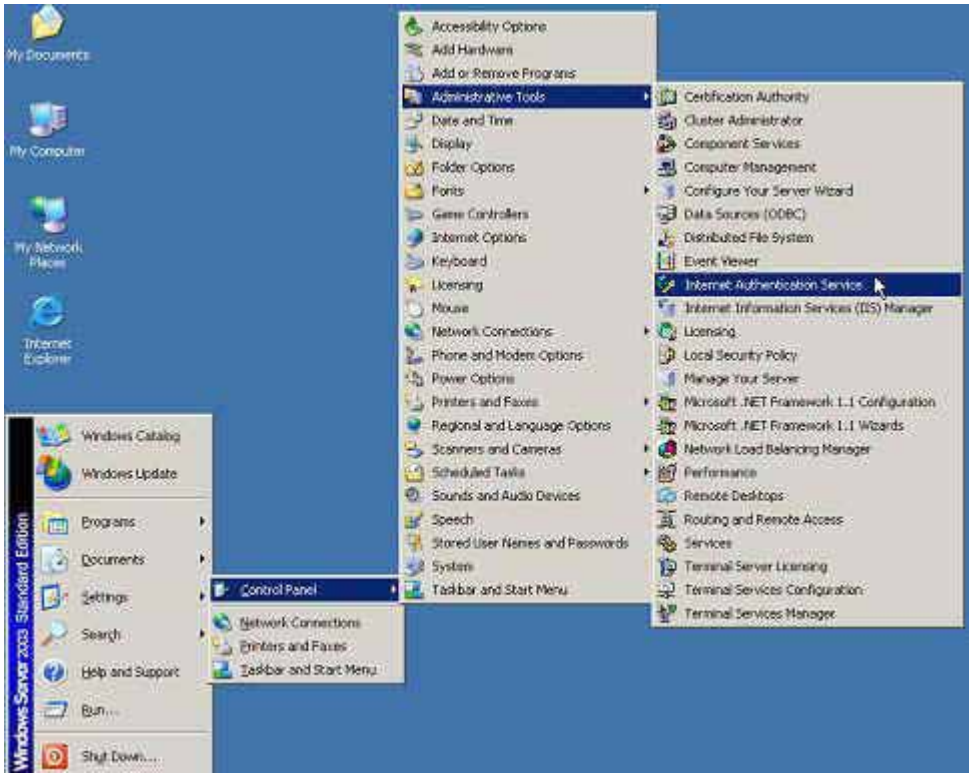
Windows Components Wizard

Step3. Select **Internet Authentication Service**



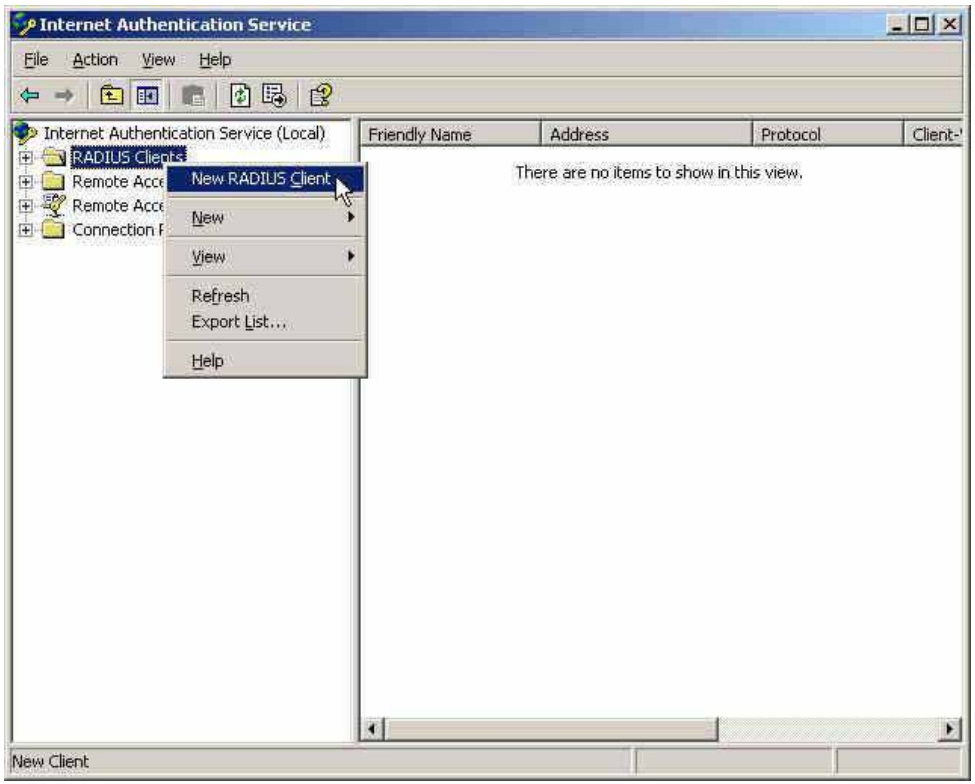
Add new network authentication service components

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



Select network authentication service

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

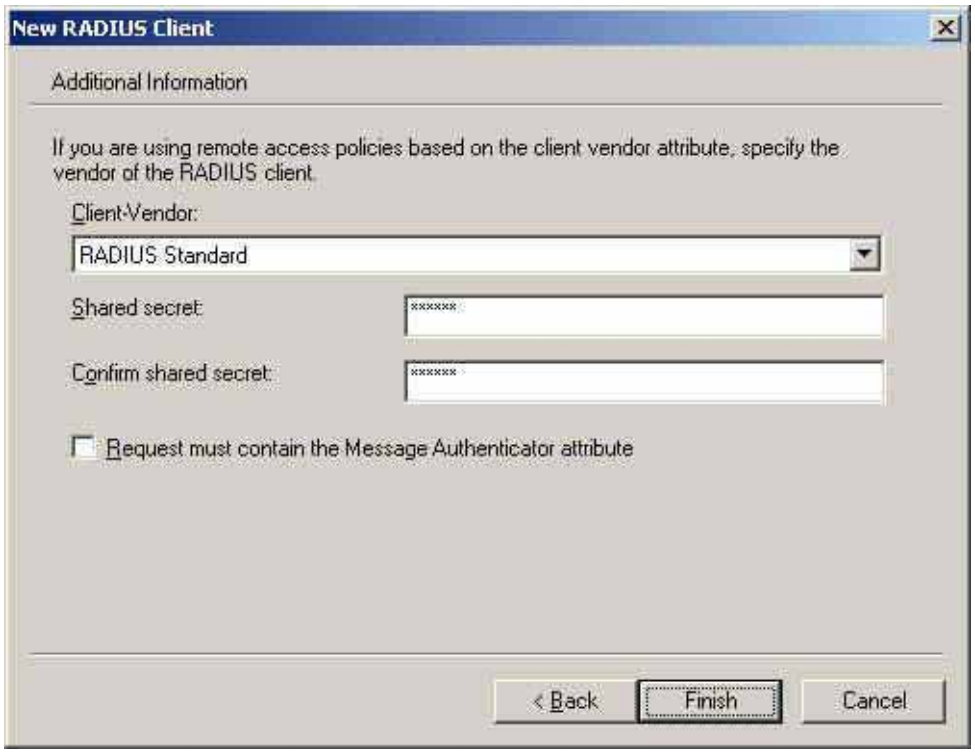


Add new RADIUS client

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

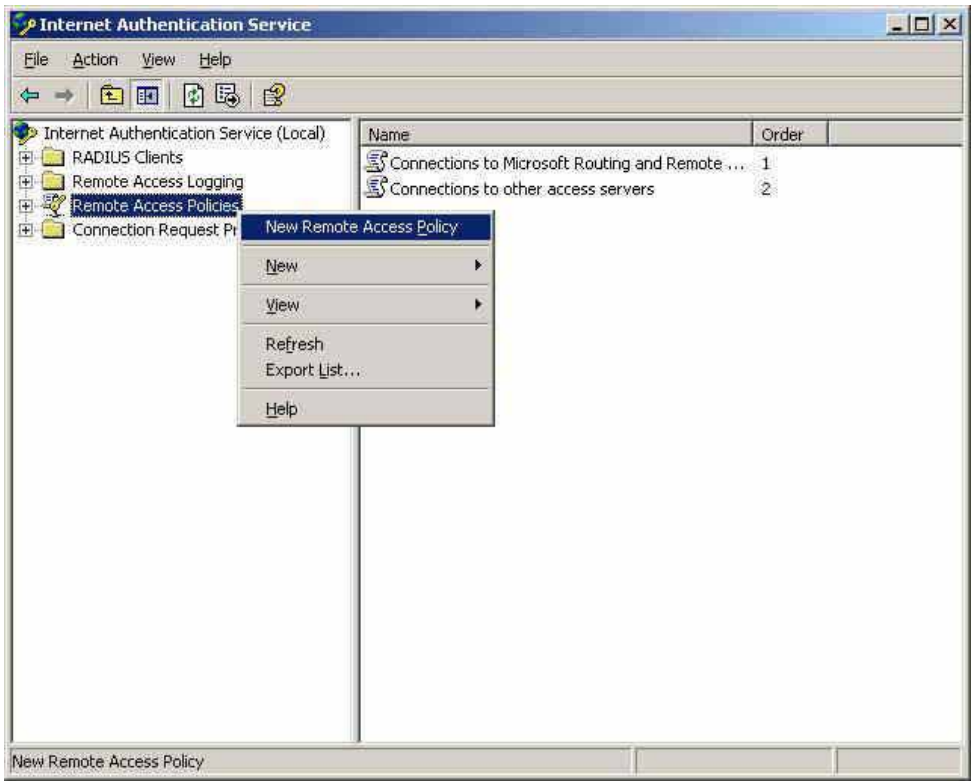
Add New RADIUS client name and IP address setting

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



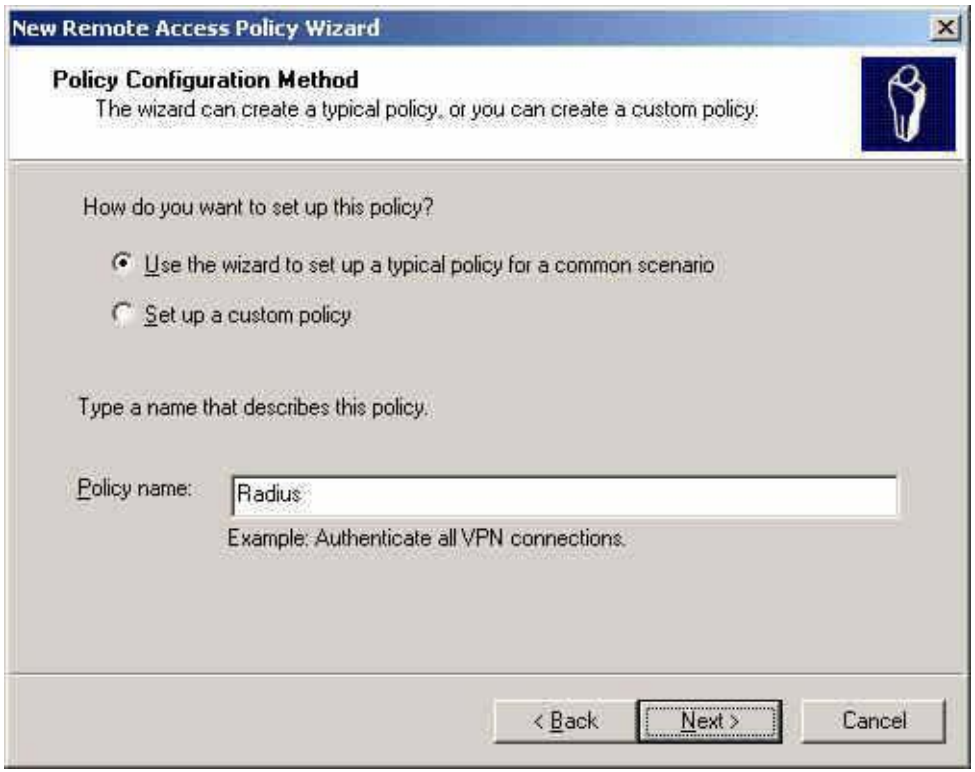
Add new RADIUS client-vendor and shared secret

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



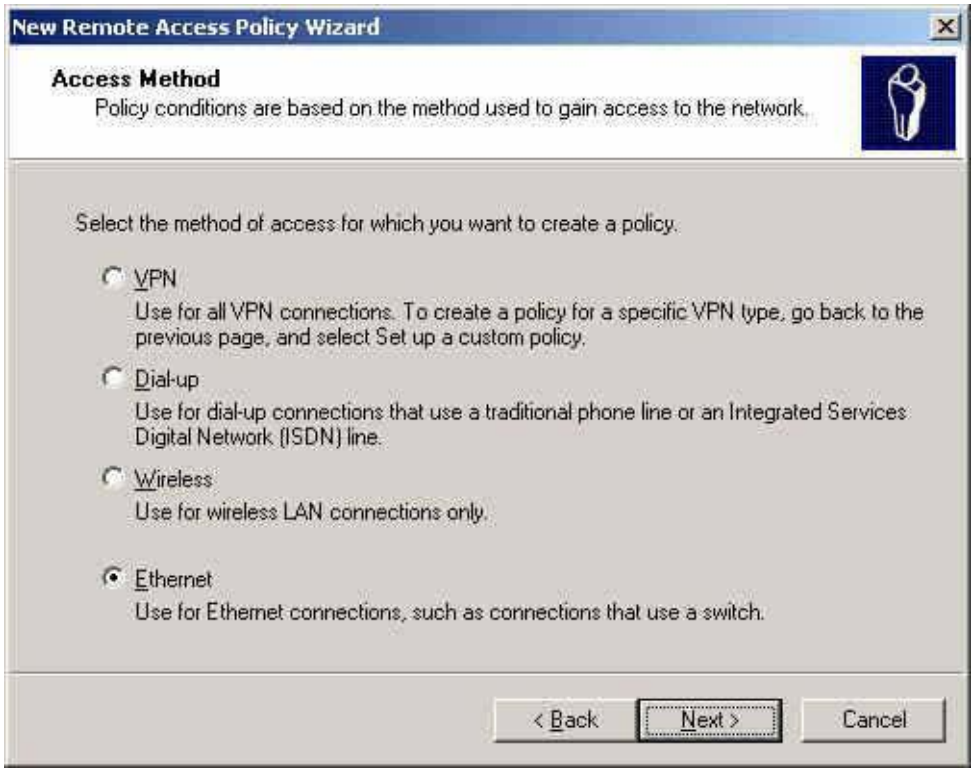
Add new romote access policies

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



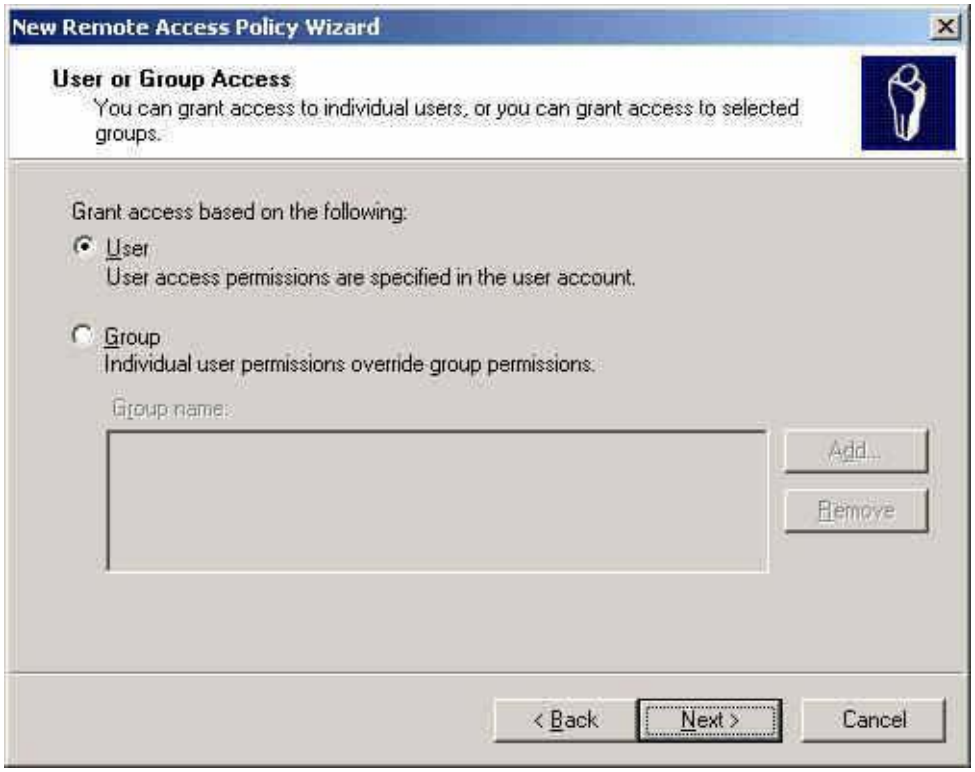
Add new romote access policies and policy name

Step10. Select **Ethernet** .



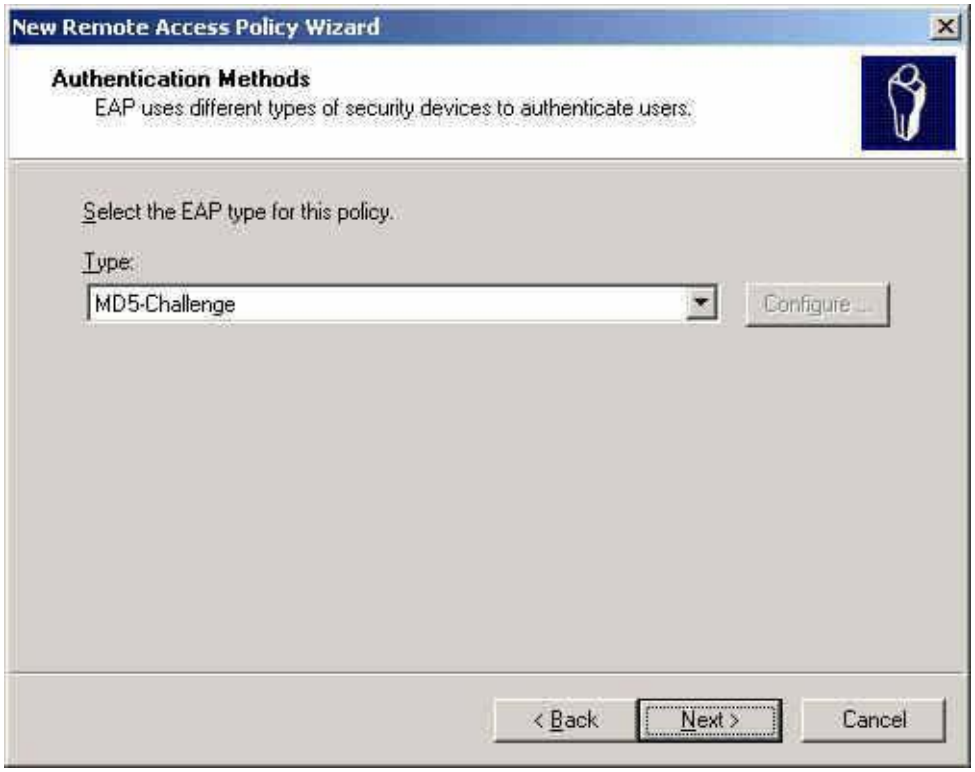
The way to add new romote access policy

Step11. Select **User**



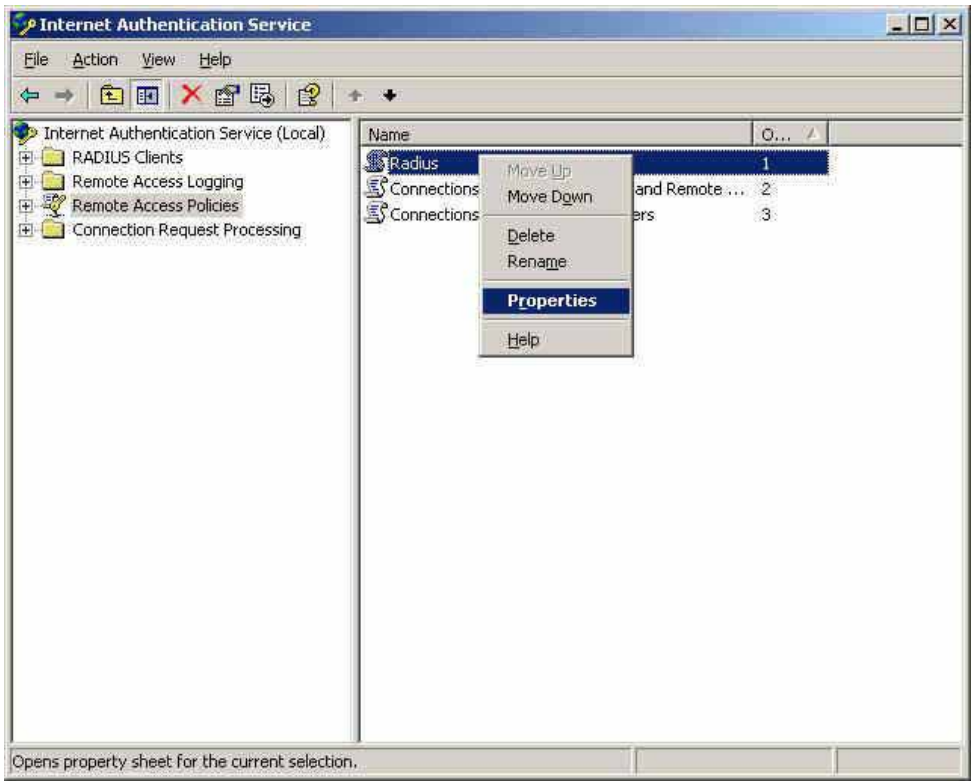
Add new romote access policy user and group

Step12. Select **MD5-Challenge**.



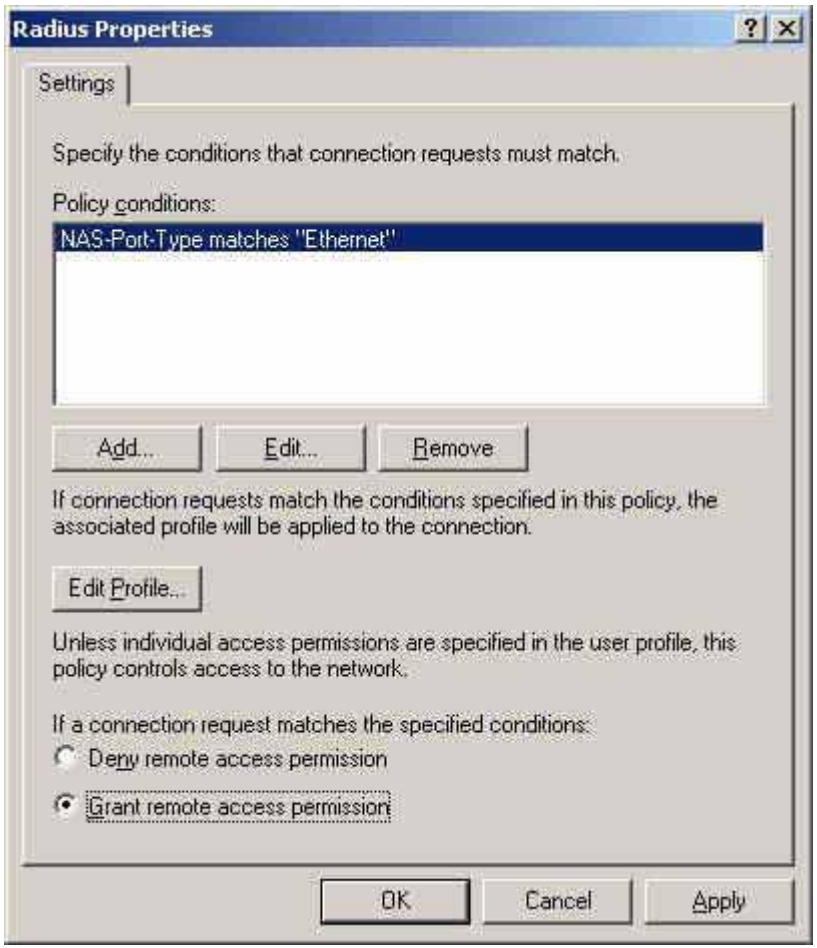
The authentication of add new romote access policy

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



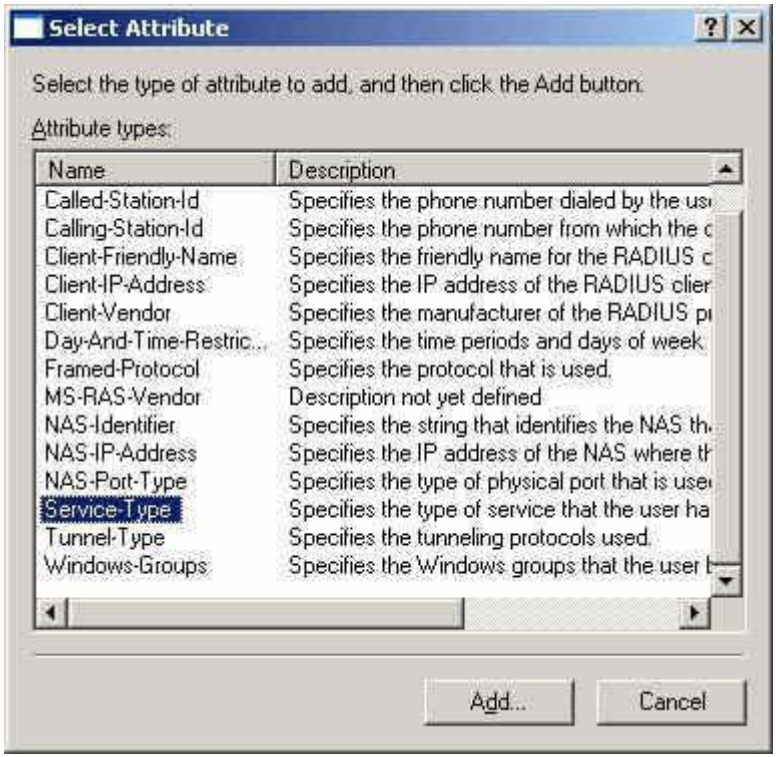
The network authentication service setting

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



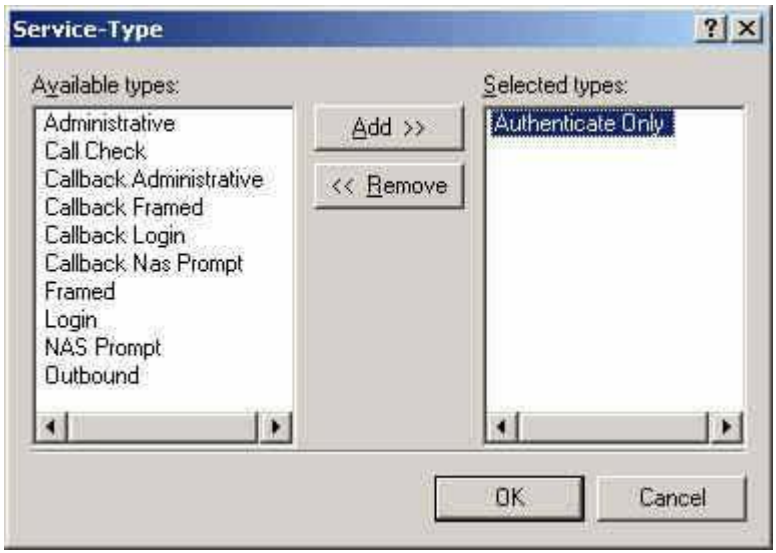
The RADIUS properties settings

Step15. **Add Service-Type**.



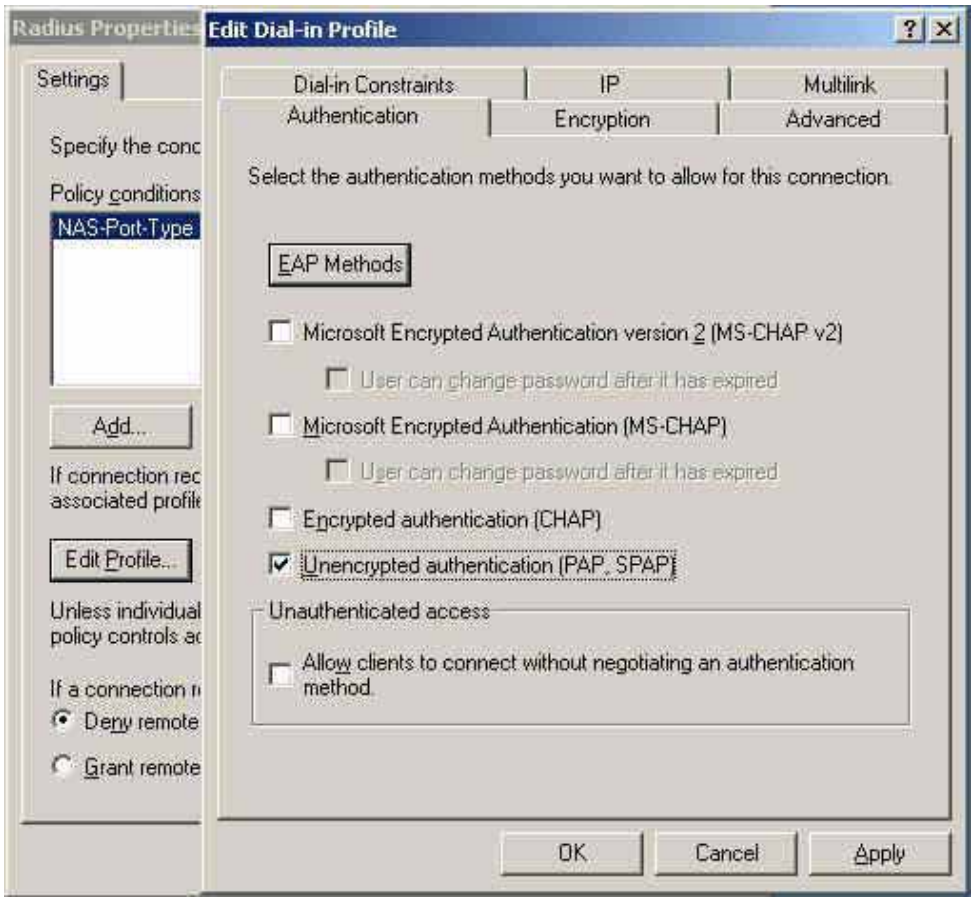
Add new RADIUS properties attribute

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



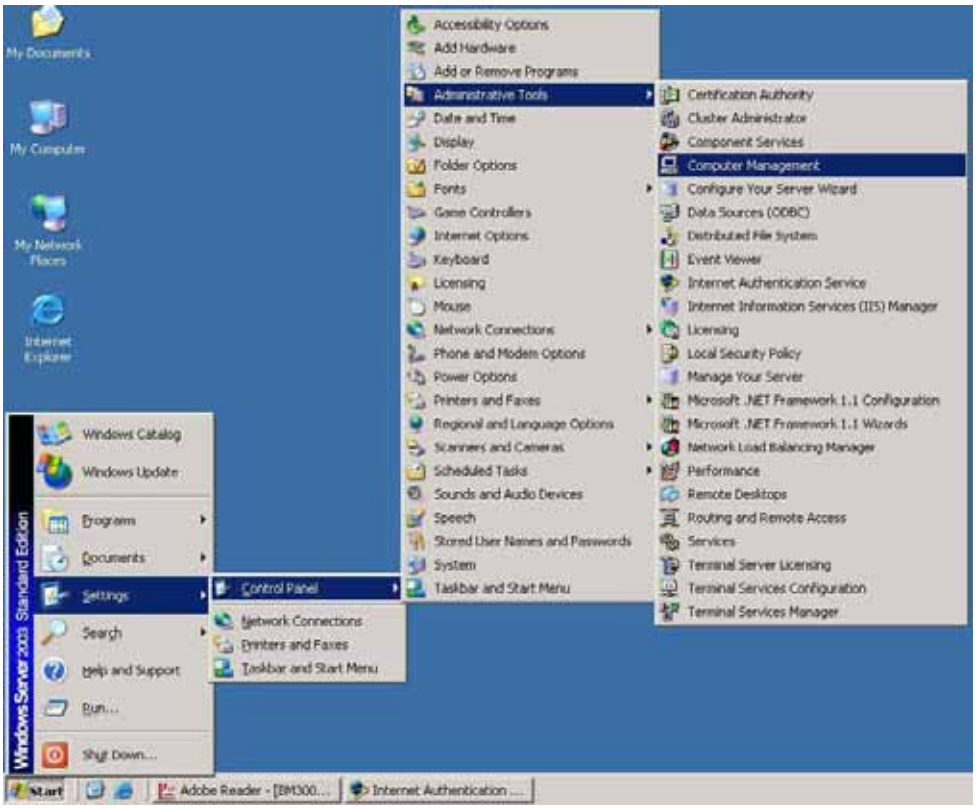
Add RADIUS properties service-type

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



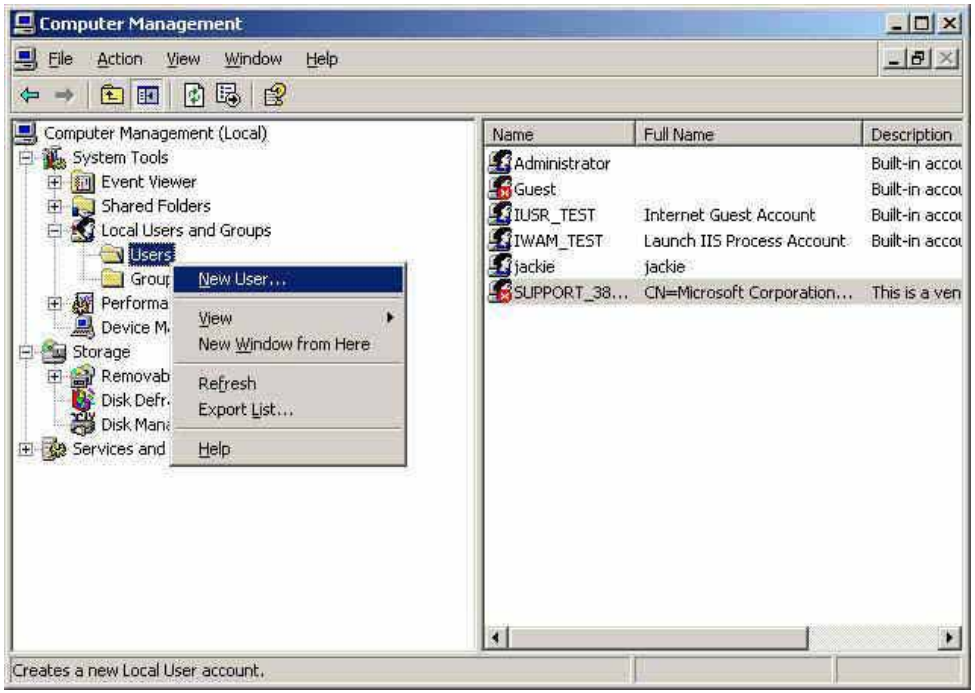
Edit RADIUS service-type dial-in property

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



Enter computer management

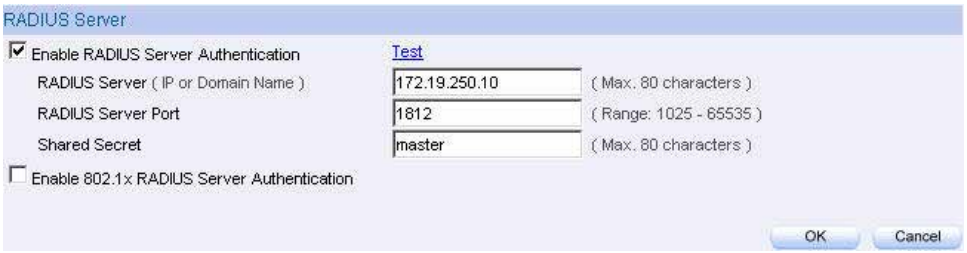
Step19. Right click on **Users** , select **New User** .



Add new user

Step20. Complete the Windows 2003 RADIUS Server Settings .

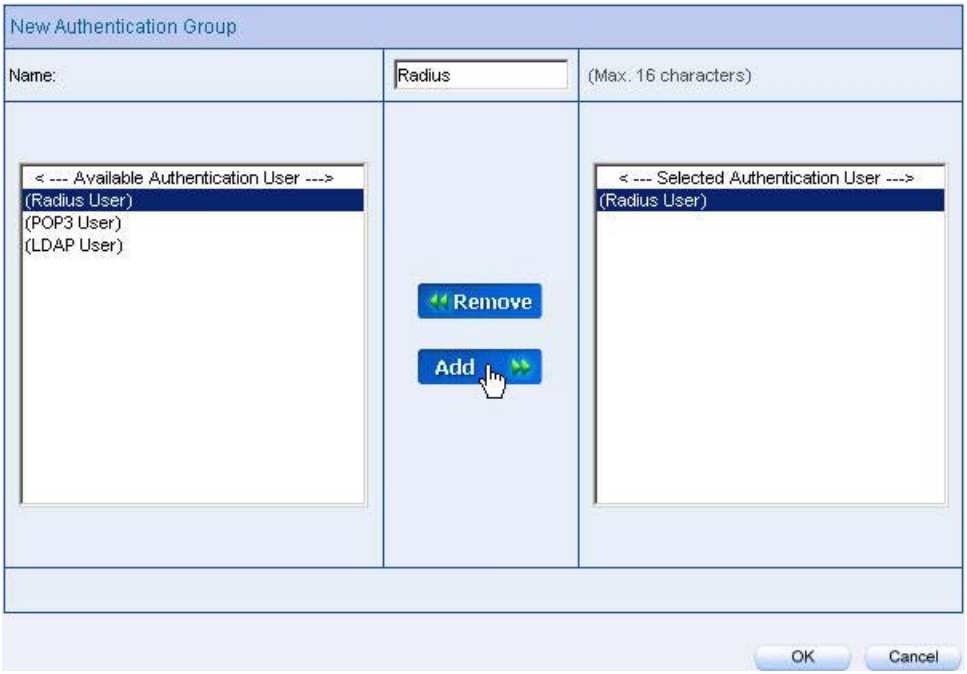
Step21. In **Authentication → RADIUS** function , enter **IP** , **Port** and **Shared Secret** . (The setting must be the same as RADIUS server) .



The RADIUS server setting

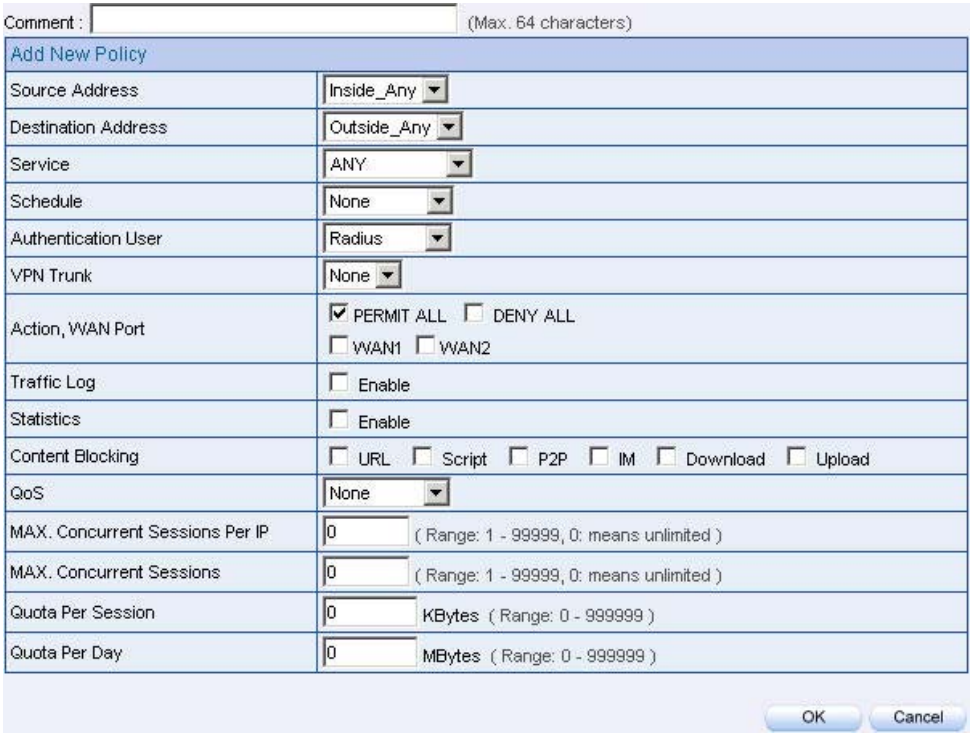
Click **Test**，it can detect if the BM-2101 and RADIUS server can real working .

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



Add new RADIUS user

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



To add the RADIUS authentication policy

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

Link to the network through the authentication window

9.3 POP3

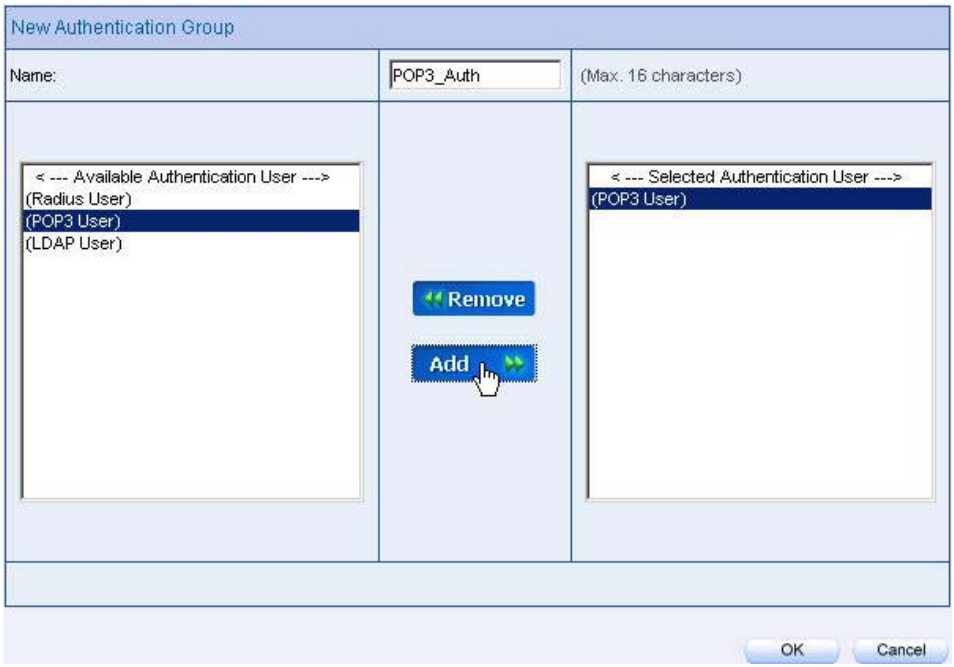
To plan the user connect to the WAN through the authenticaton by policy. (To use the WAN POP3 server authentication)

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

POP3 server setting

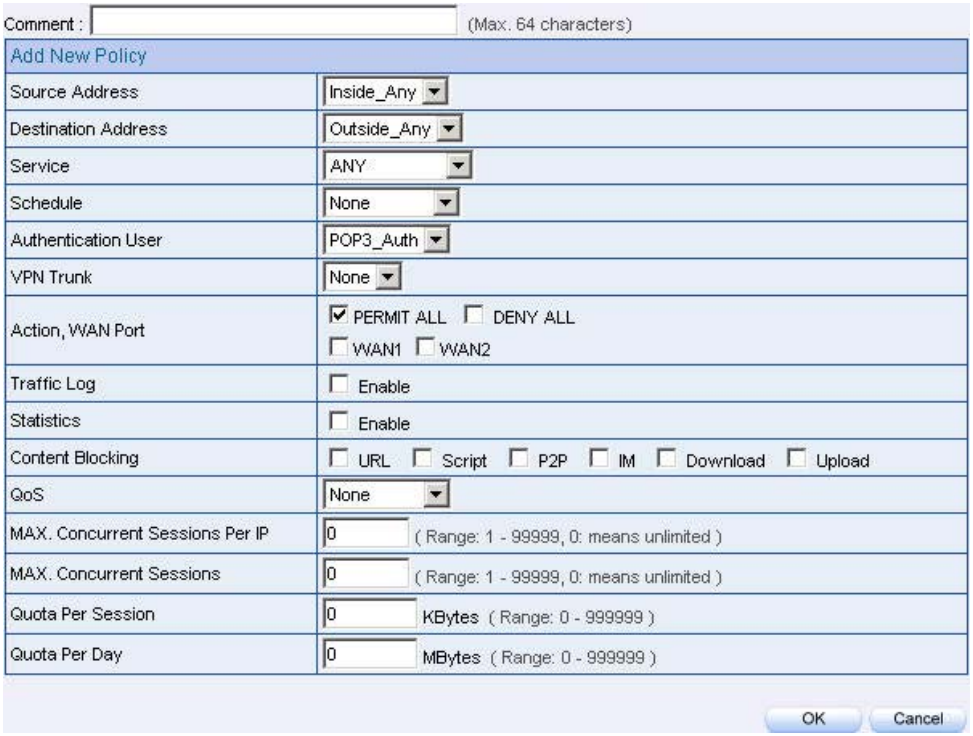
Click **Test**，it can detect if the BM-2101 and POP3 server can real working .

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



Add new POP3 user

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



The POP3 server authentication in policy setting

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 .

Link to the network through the authentication window

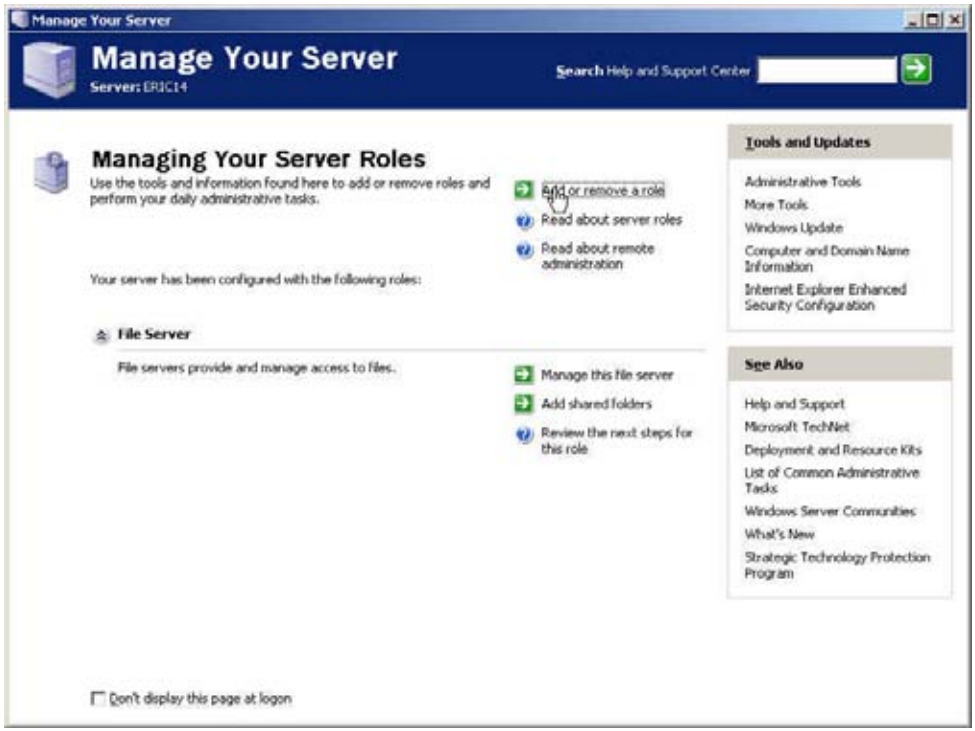
9.4 LDAP

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

※ Windows 2003 LDAP Server Deployment

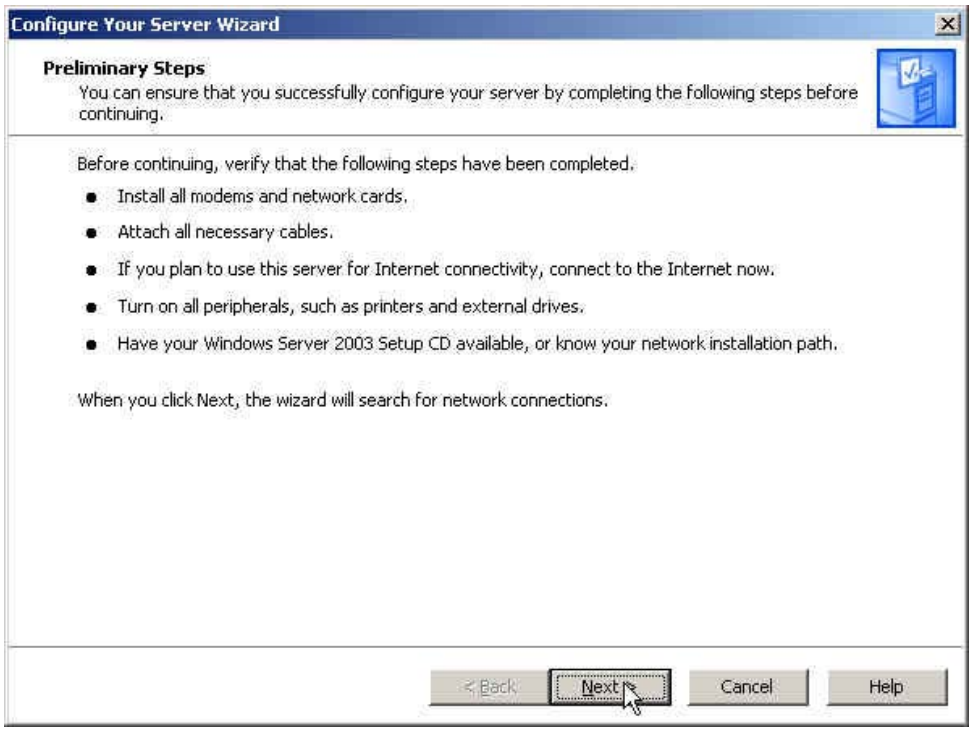
Step1. Click **Start → Program → Administrative Tools → Manage MIS engineer Server.**

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



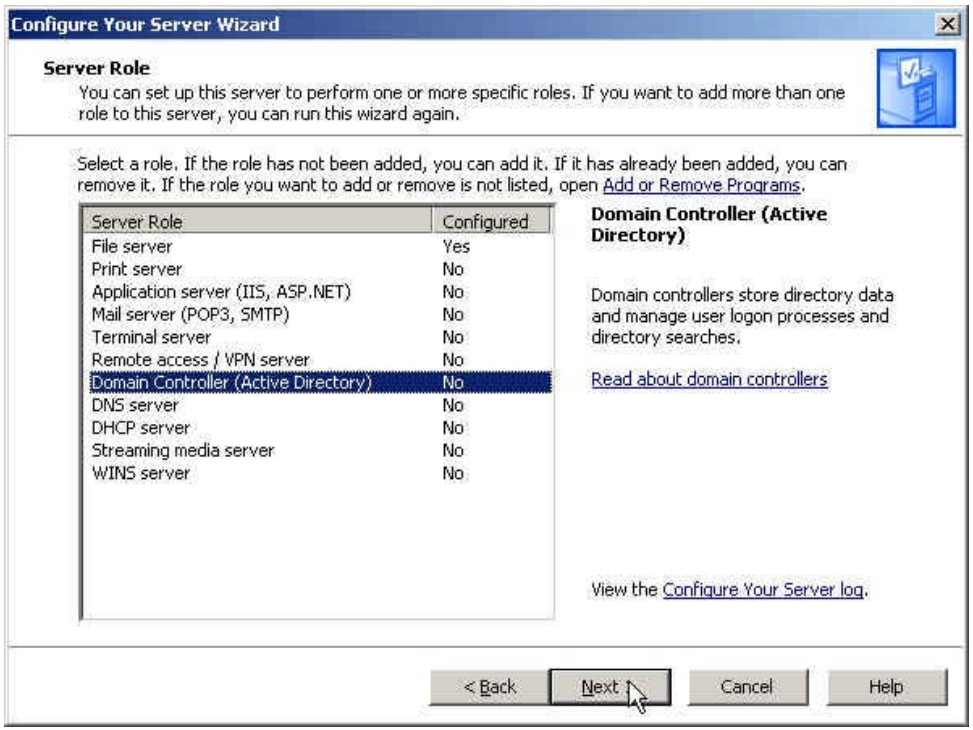
Click add or remove a role

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



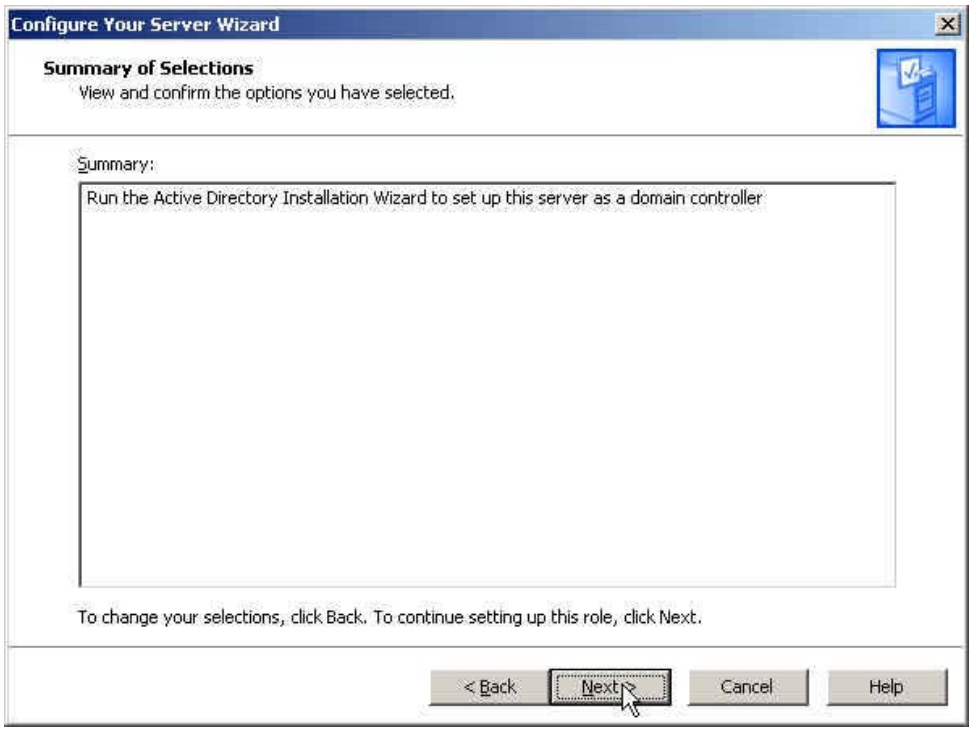
The Preliminary steps Web UI

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



The server role window

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

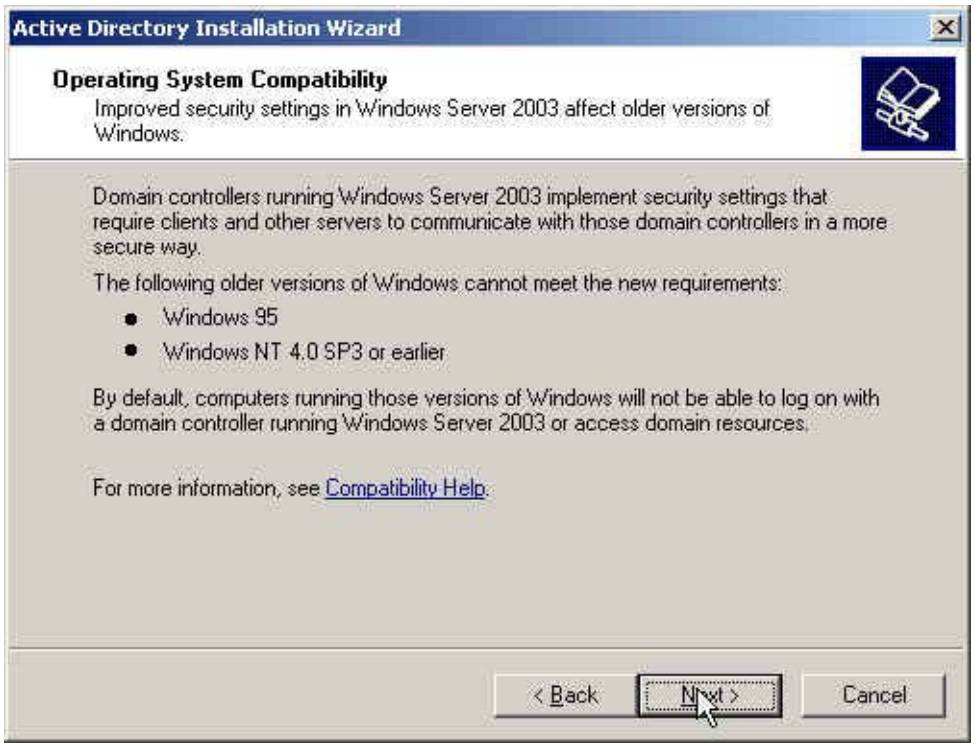


The summary of selections window

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

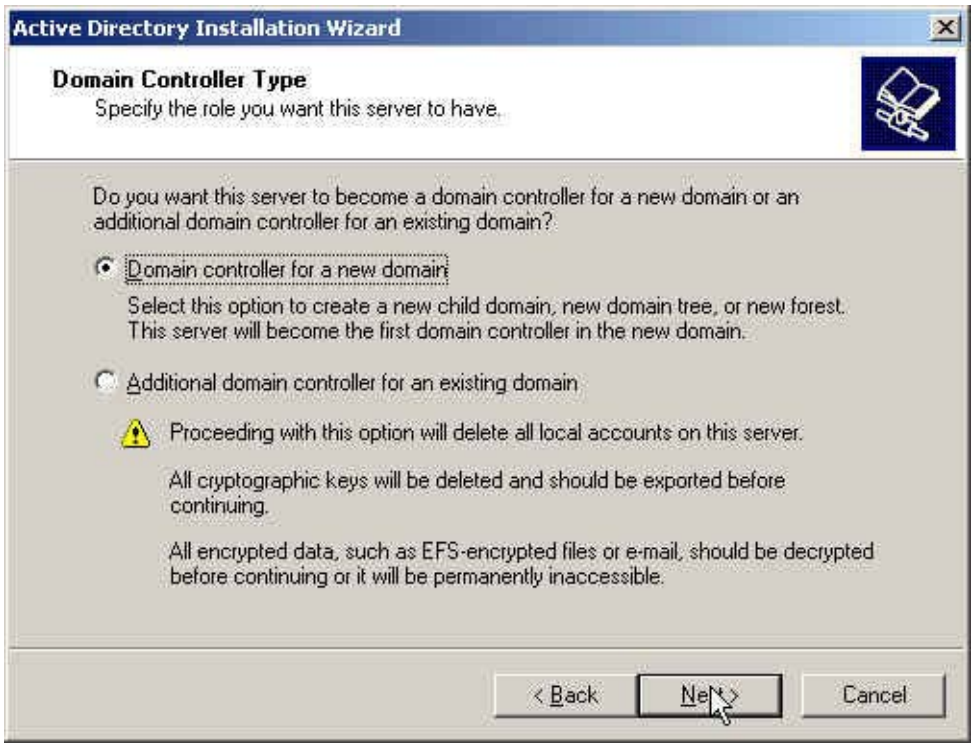
Active directory installation wizard

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



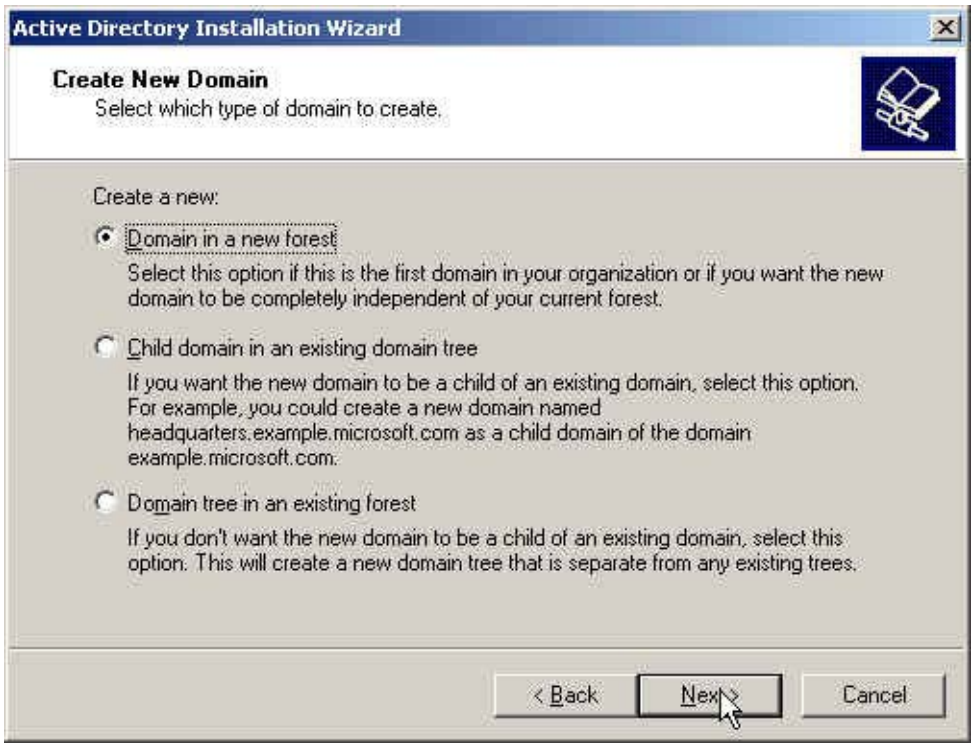
The operating system compatibility window

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



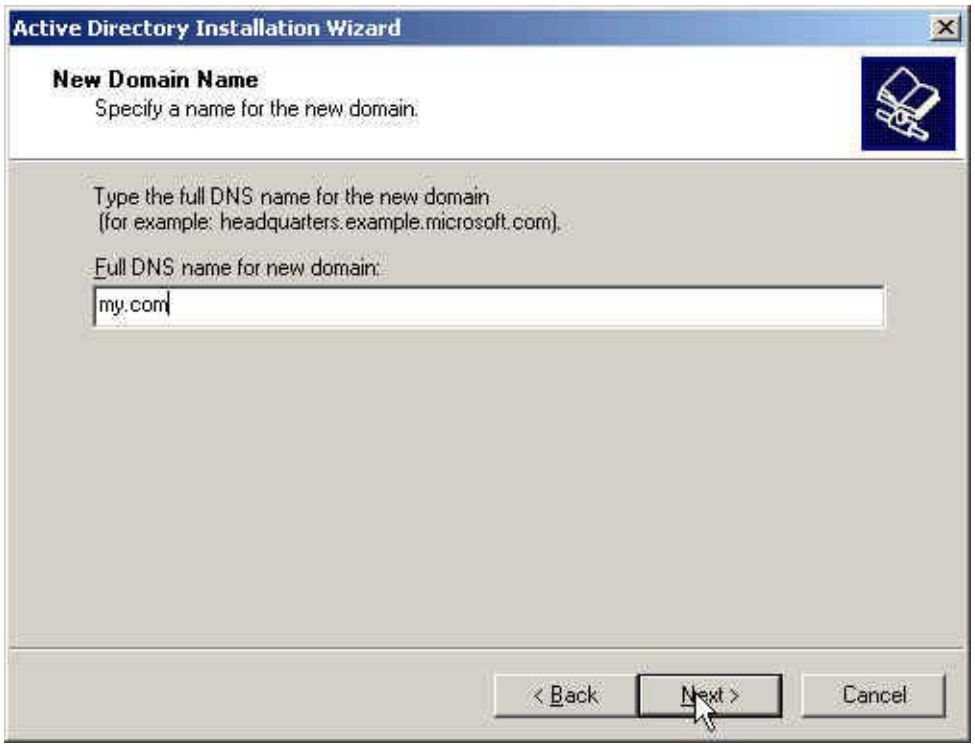
The domain controller type window

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



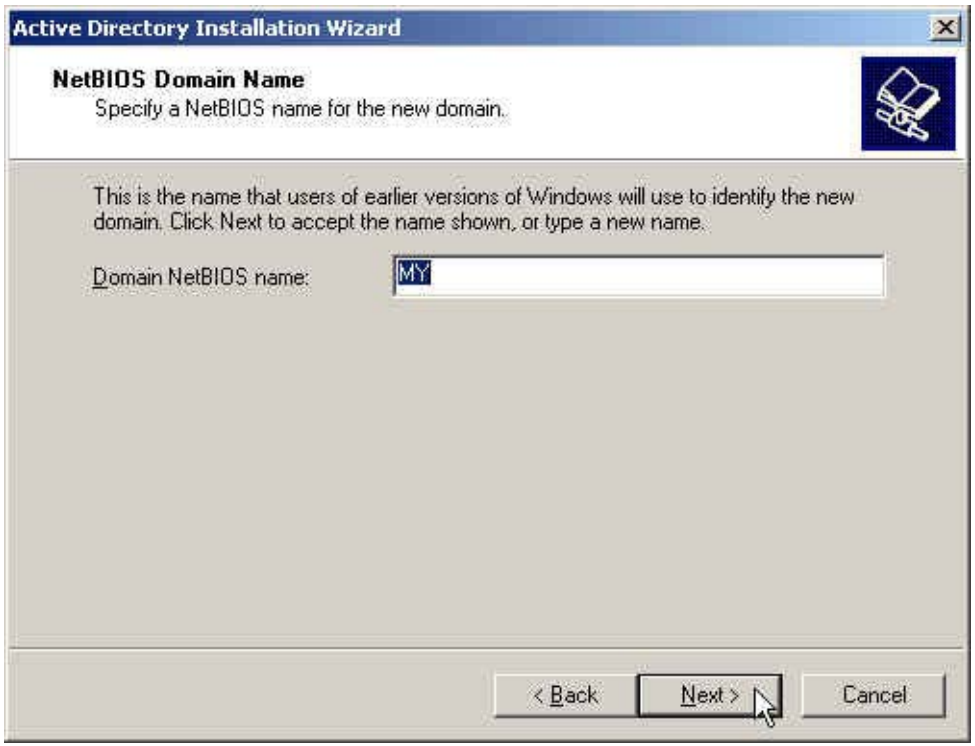
Create new domain window

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



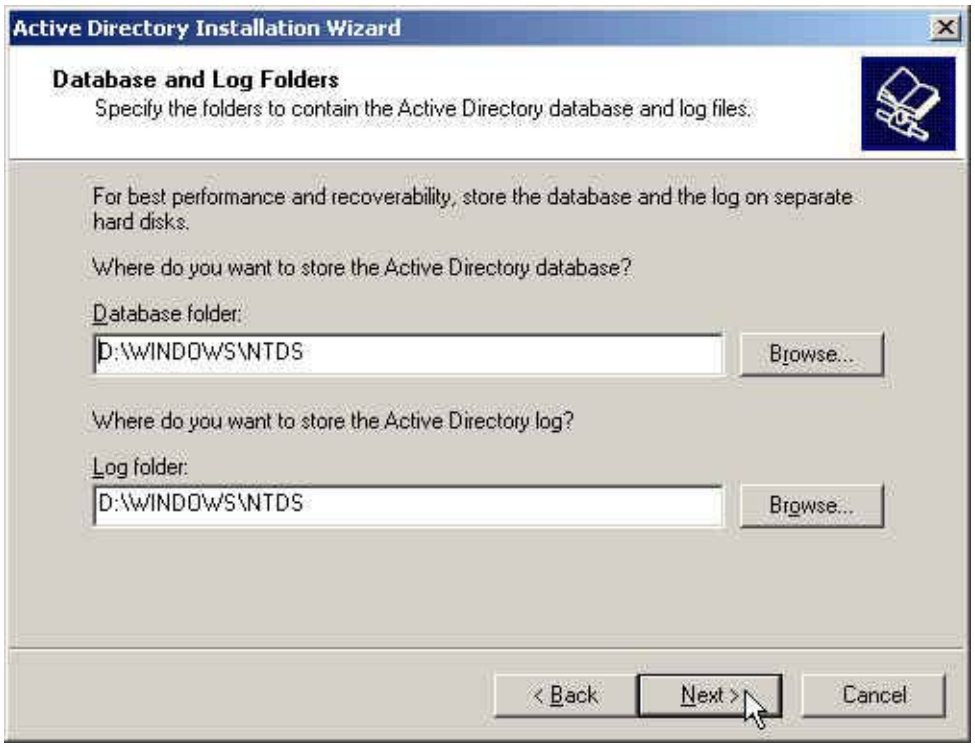
The new domain name window

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



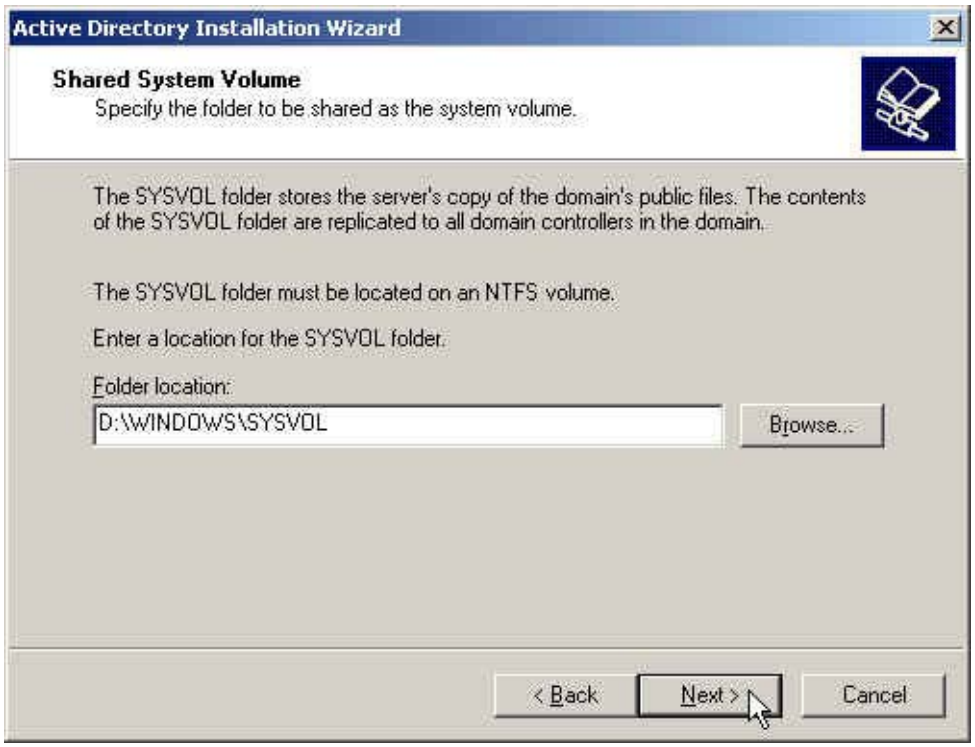
The NetBIOS domain name window

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



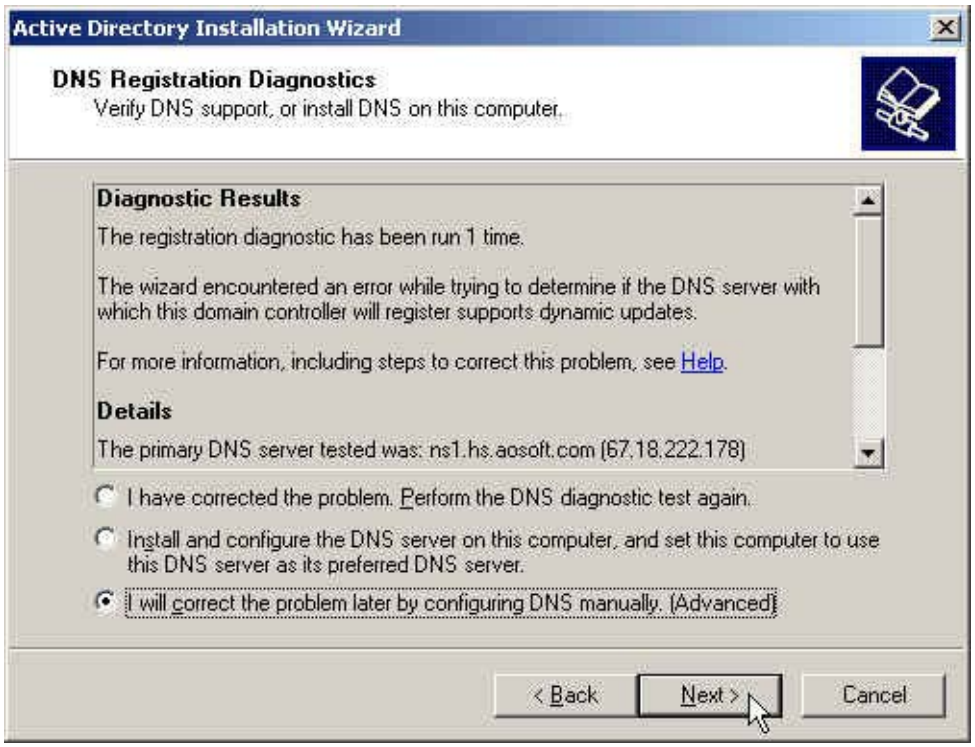
The database and log folder window

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



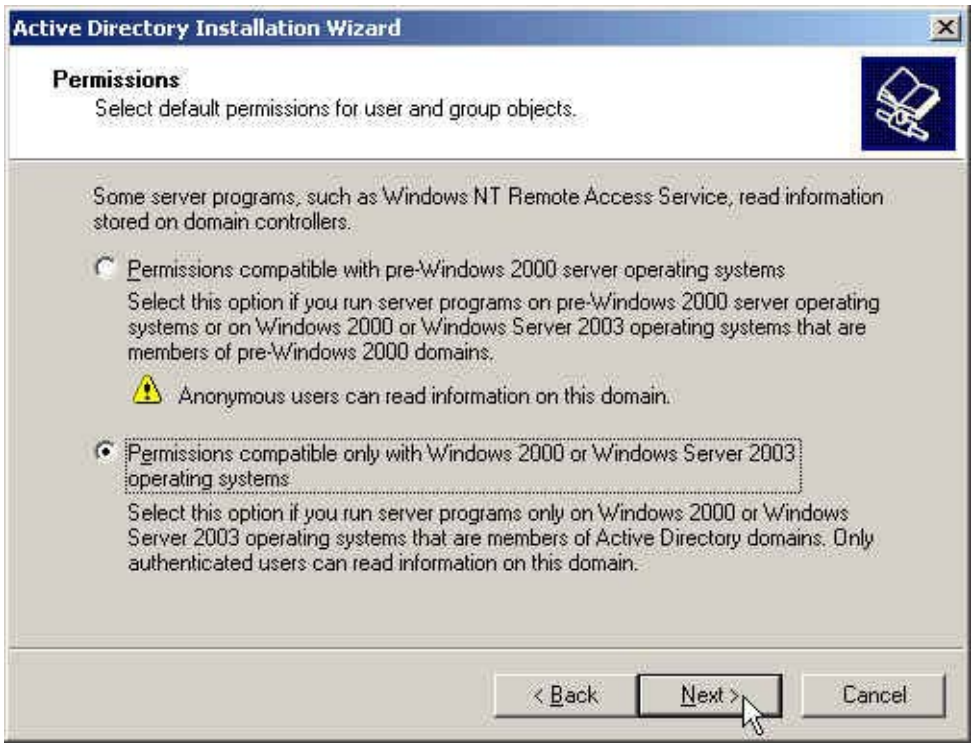
The shared system volume window

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



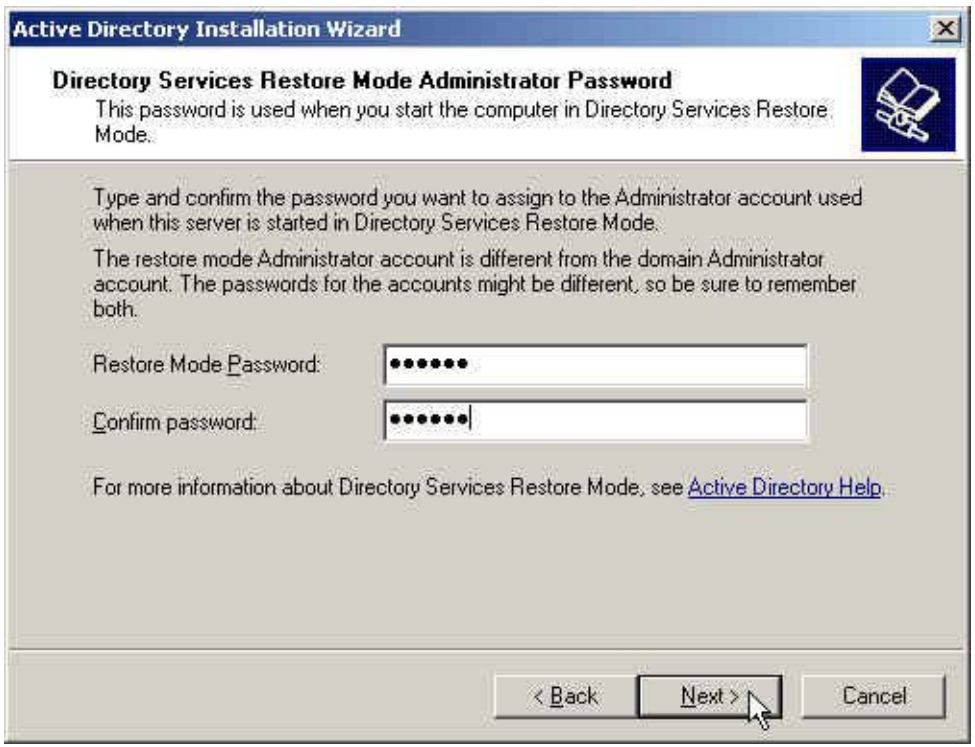
The DNS registration diagnostics window

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



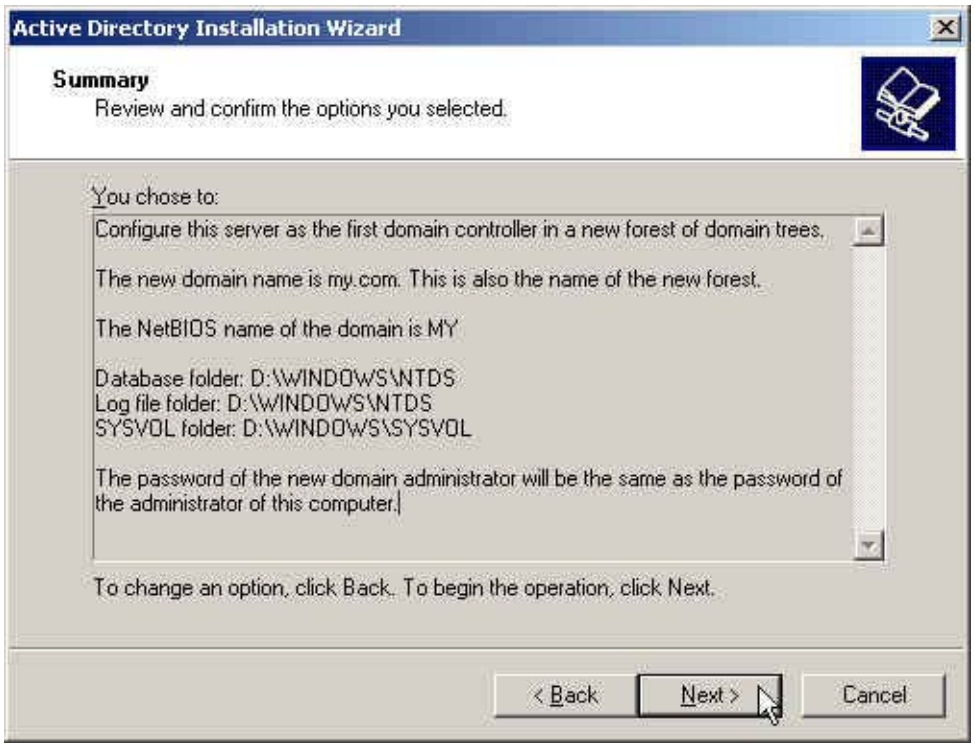
The permissions window

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**.

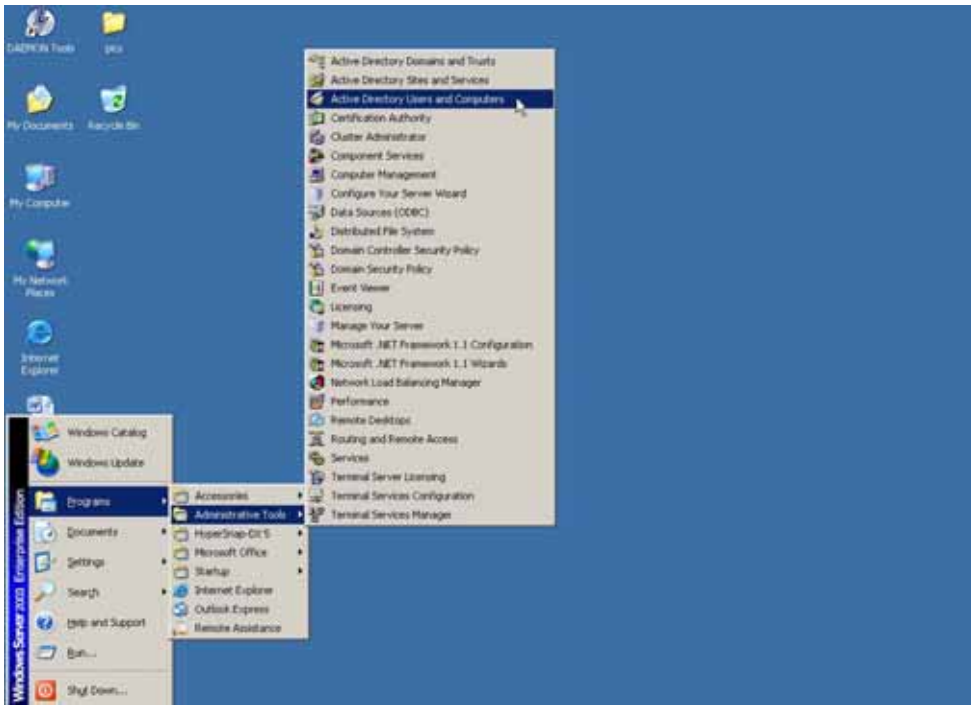


The summary window

Step18. Complete the Active Directory installation wizard.

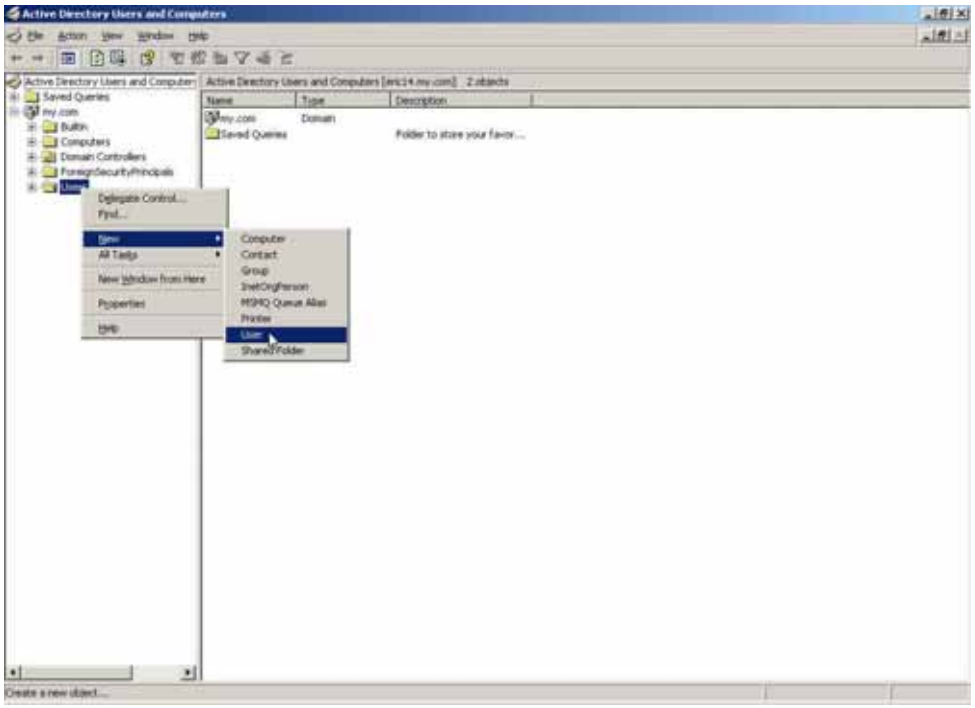
Complete the active directory installation wizard

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



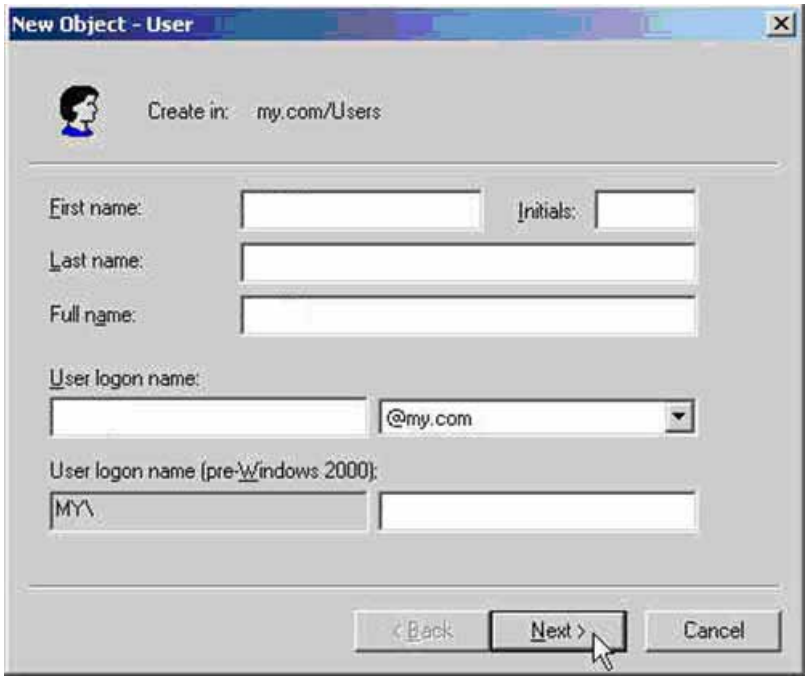
Enable active directory users and computers

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** .

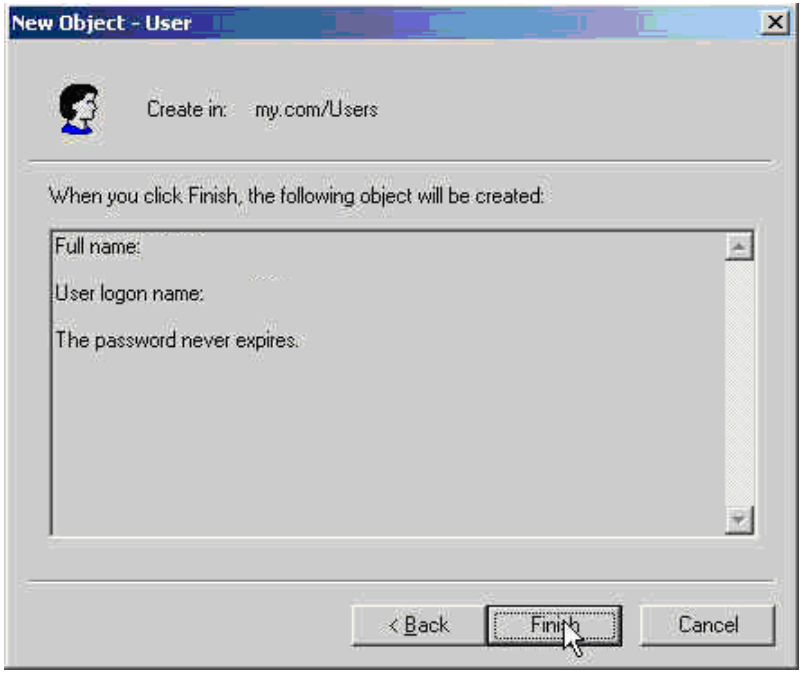


Add new object-user setting 1

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

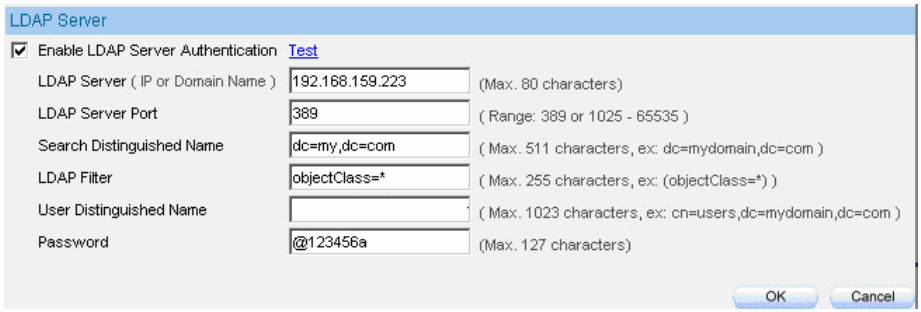
The new object – user setting 2

Step23. Complete to add the user.



Complete to add the object user

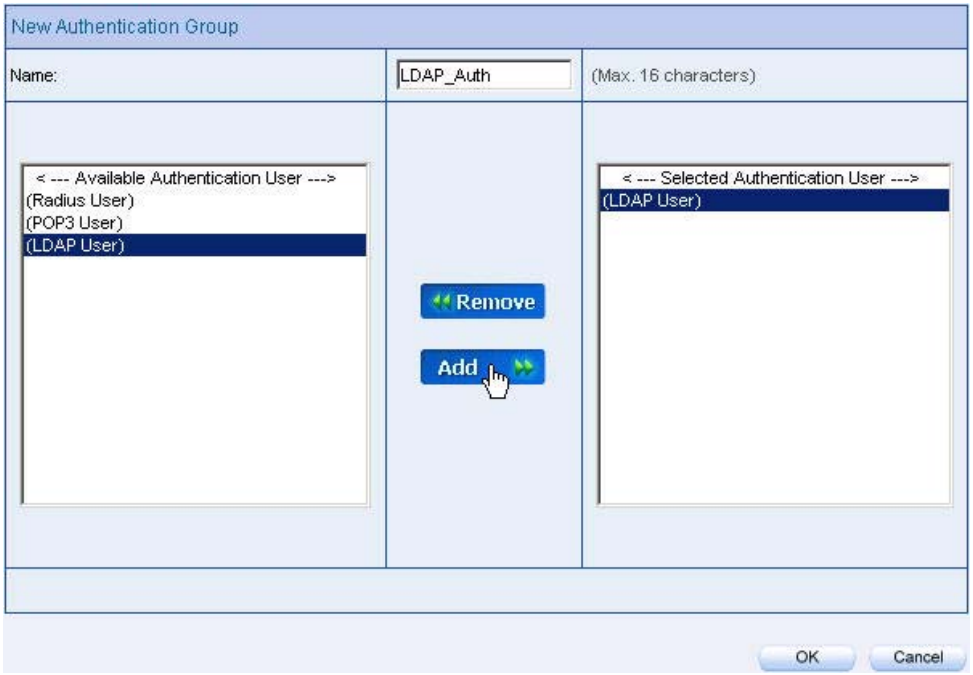
Step24. In **Authentication → LDAP** , enter the following setting:



The LDAP server setting

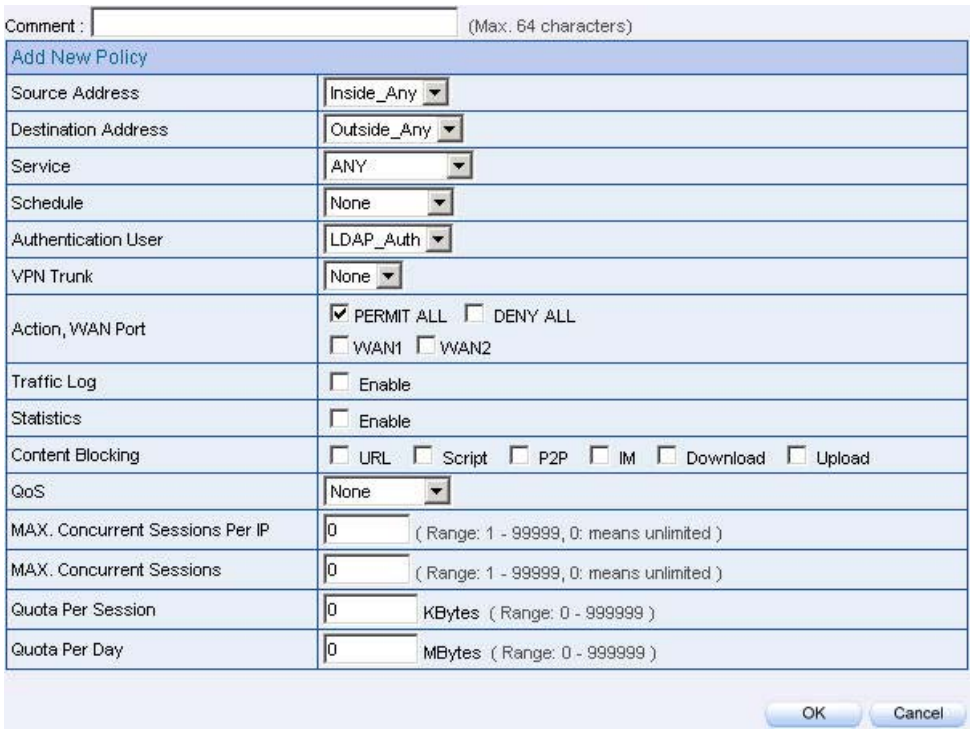
Click **Test**，it can detect if the BM-2101 and LDAP server can real working .

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 .



The LDAP server authentication in policy setting

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

Link to the network through the authentication

Chapter 10

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	**URL**	Only permit the LAN user to access the data in specific web site .
Example. 2	**Script**	To limit the LAN user to access the script data in the web site .
Example. 3	**Download**	To limit the LAN user to download the extension files , video and audio files in the intenet through http or ftp .
Example. 4	**Upload**	To limit the LAN user to upload the extension files , video and audio files in the intenet 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 meas to open； ＊ , the smbol 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 or gov .

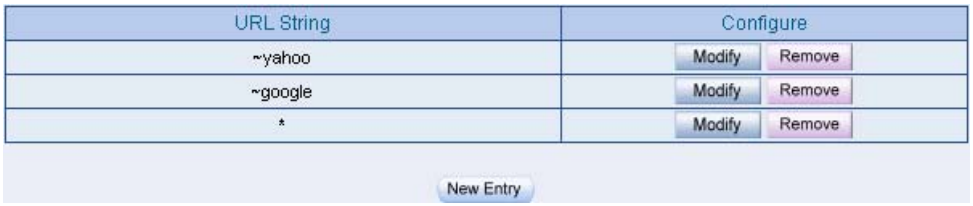
To permit the user to enter the specific web site：

1. First of all , enter the complete **Domain Name** or **Keywords** in to the URL blocking setting , and add the symbol " **~ "** which reresents 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 .

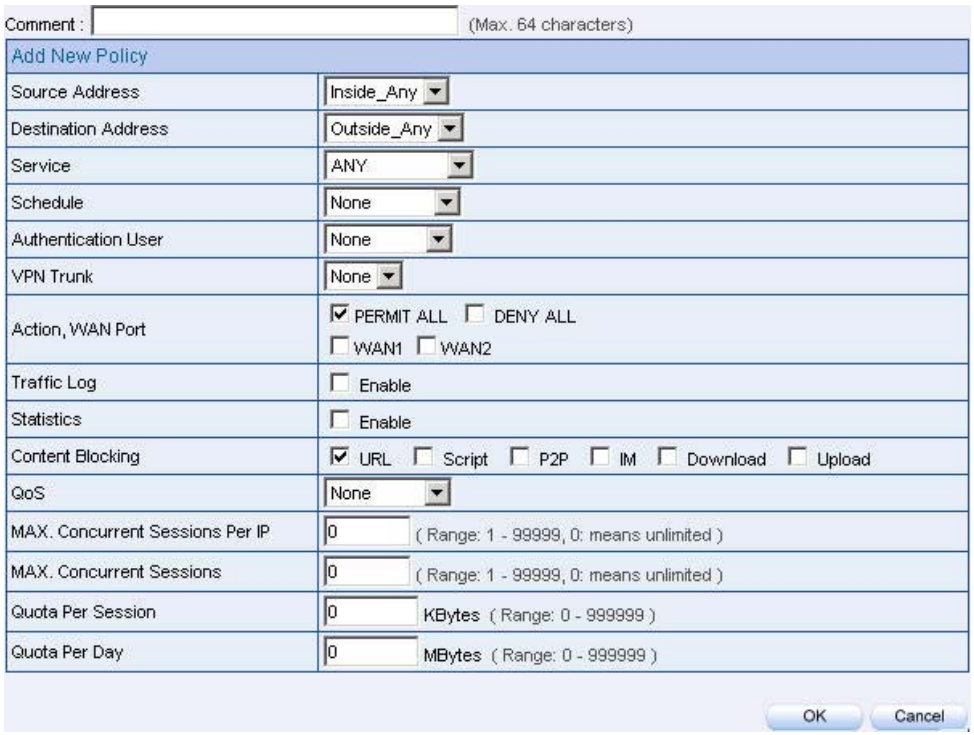
Step1. In **Content Blocking → URL** , add the following setting ：

- 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 .



The URL setting

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



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.

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

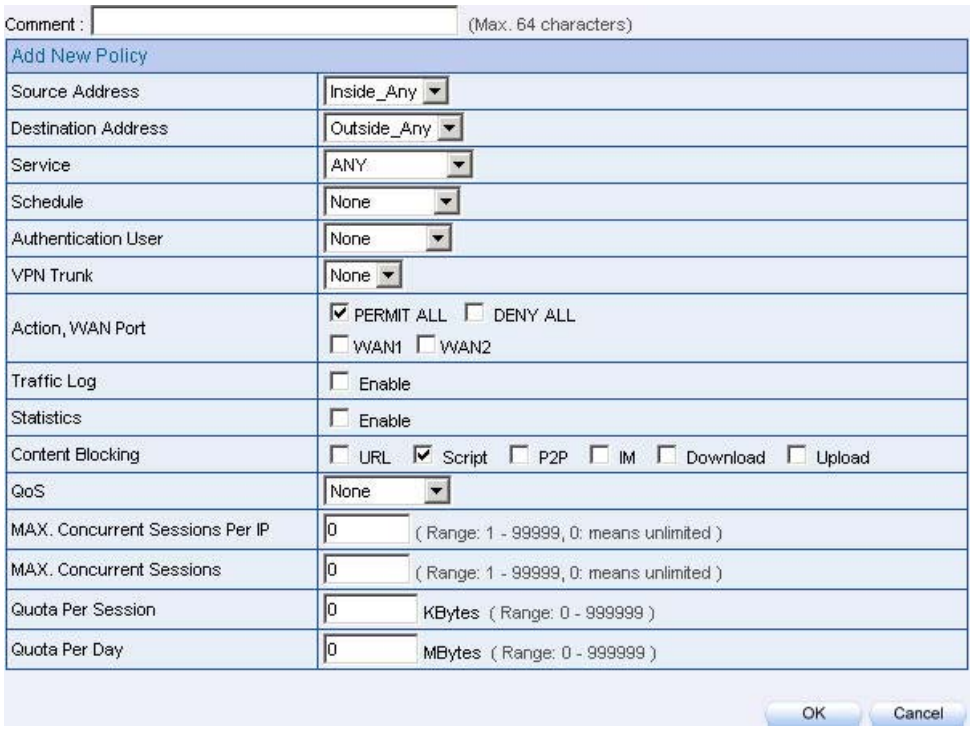
To limit the LAN user to access the script data in the web site .

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 ：



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：

Complete the script content blocking settings

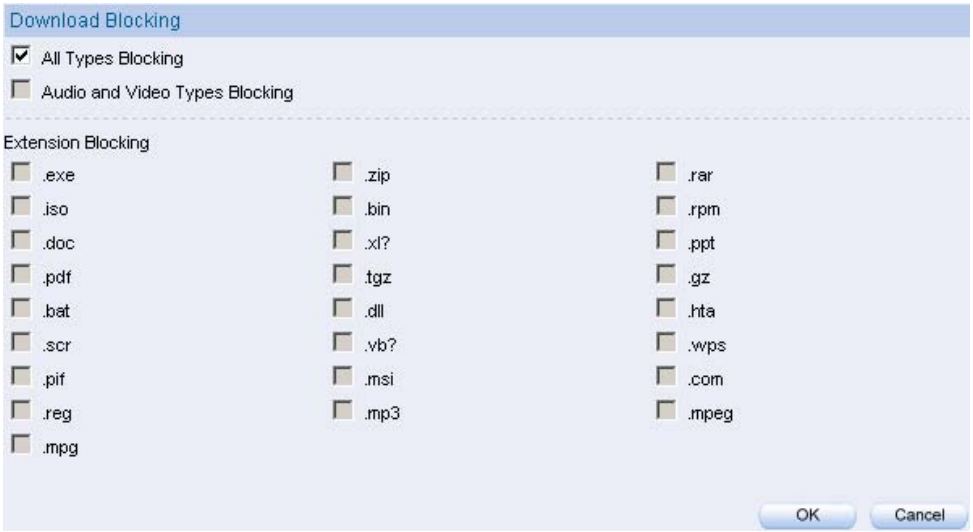
The user can not use the specific function in the web site (For example , JAVA , cookie…) when browsing the web pages through the policy . This function can forbid the user to browse the stock exchange web site and so on .(The browser can not display the market summary charts)

10.3 Download

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

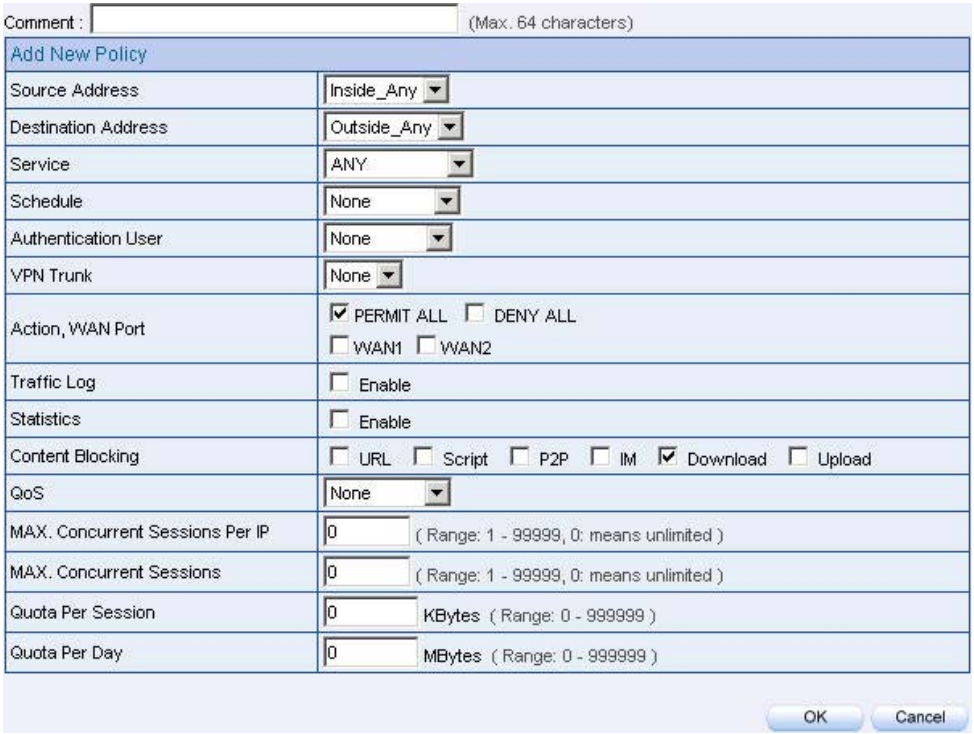
Step1. In **Content Blocking→ Download** , set the following settings ：

- 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 .



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 .

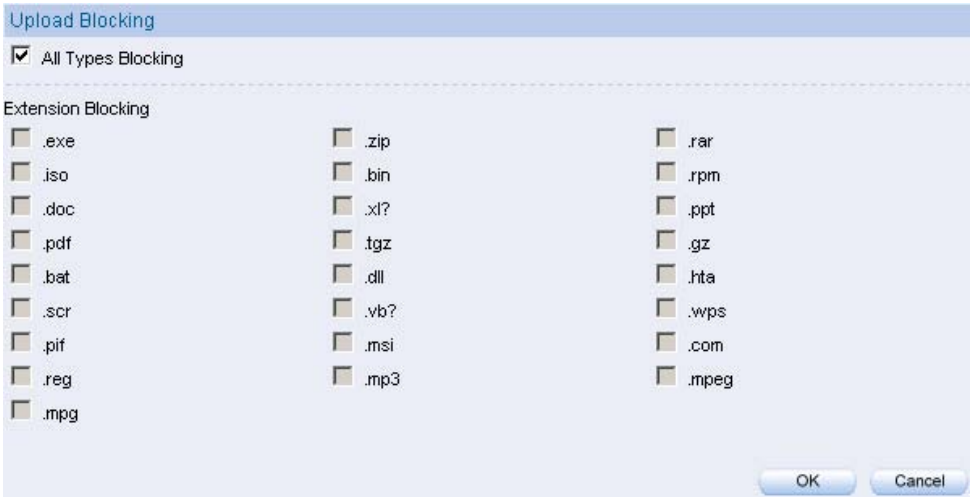
Complete the download content blocking setting in policy

10.4 Upload

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

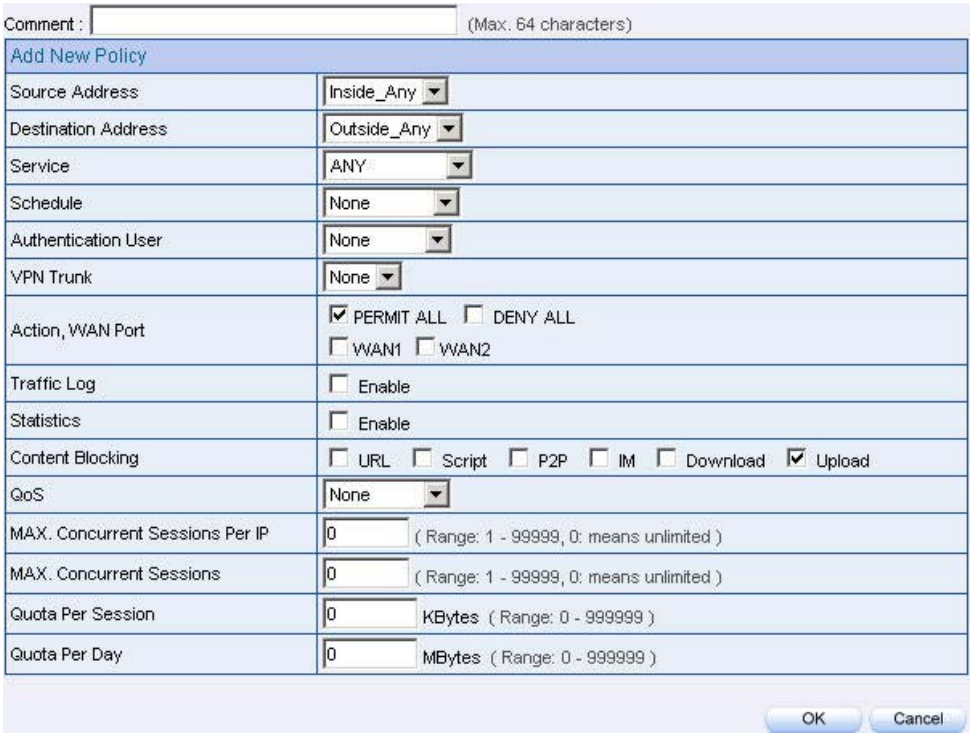
Step1. In **Content Blocking→ Upload Blocking** , set the following settings ：

- 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 . ：



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 extention files in the network . ：

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 Definitoins

- 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 :

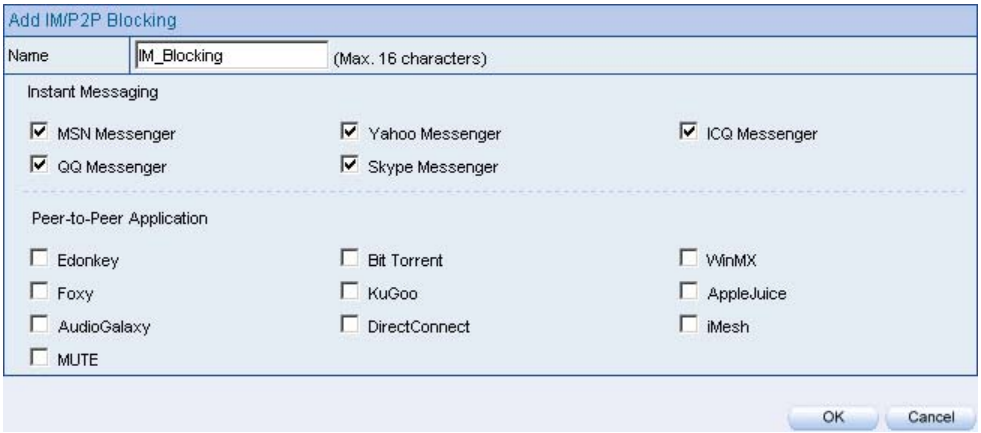
No.	Range	Environment
Ex.1	**IM**	Limit internal user transfer messages, files and media files by IM software.
Ex.2	**P2P**	Limit internal user access internet resources by P2P software.

11.1 Example

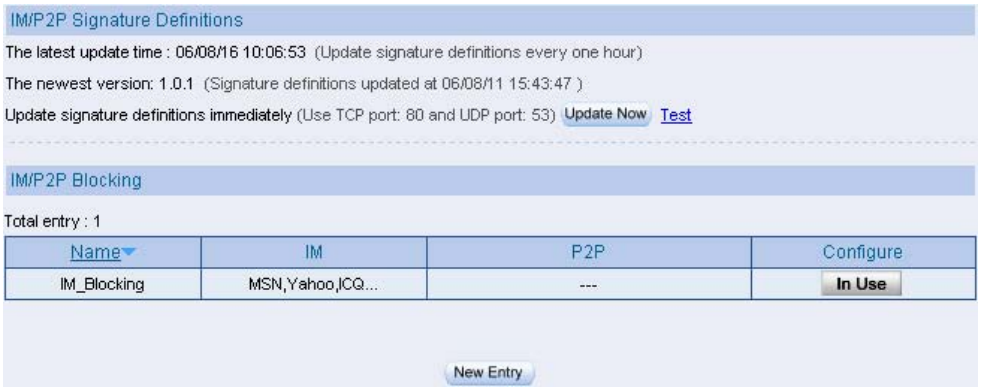
Limit internal user transfer messages, files and media files by IM software.

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

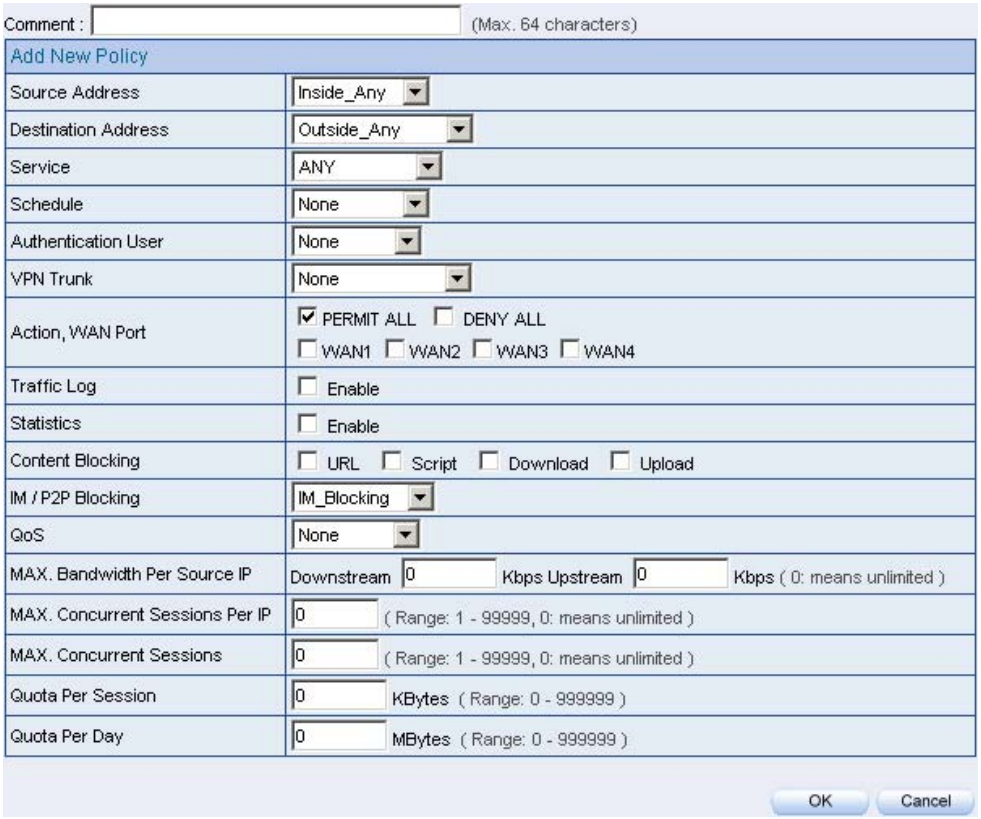


IM blocking setting



Complete the IM blocking setting

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



Set the policy applied to IM blocking setting

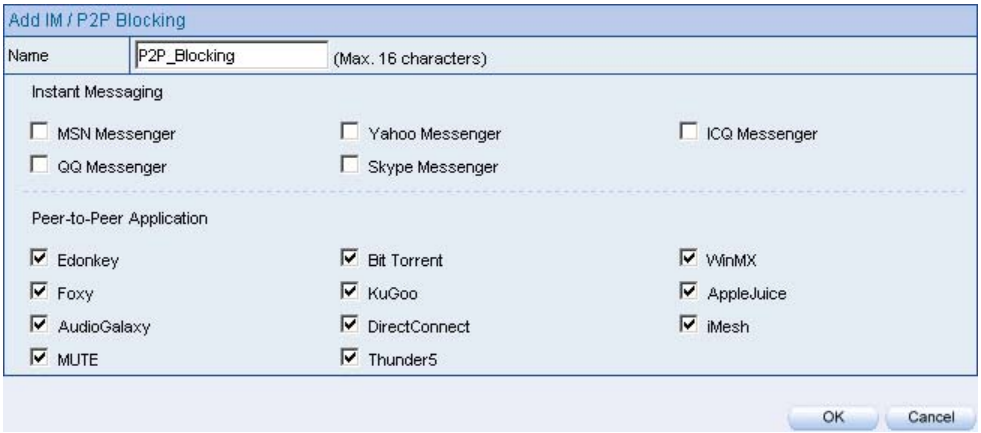
Step3. In **Policy → Outgoing** , complete the policy setting of limit internal user to transfer messages, files and media files.

Complete the policy setting of IM blocking

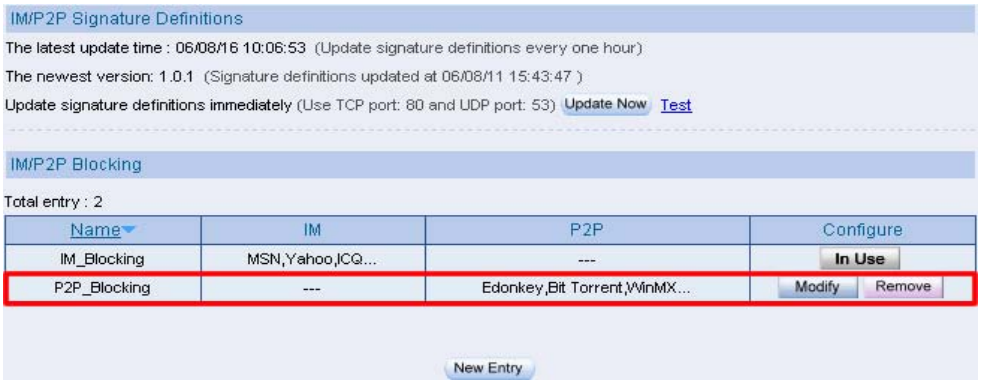
Limit internal user access internet resources by P2P software.

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

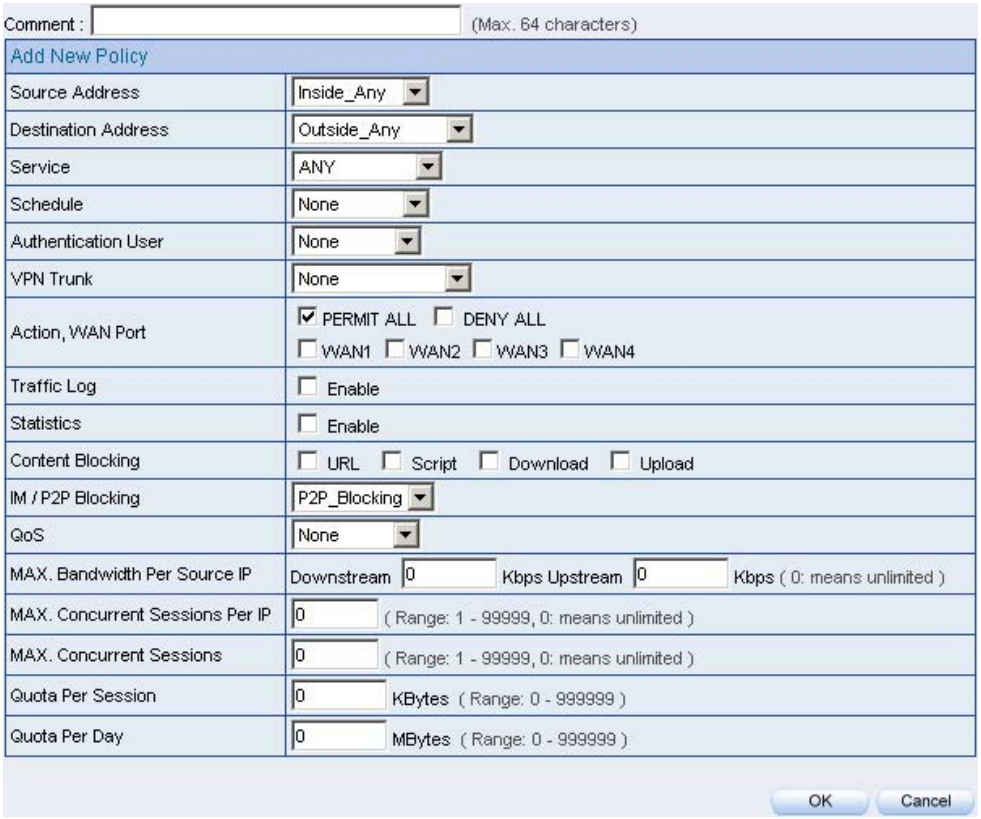


P2P blocking setting



Complete the P2P blocking setting

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



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：

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.**

Chapter 12

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 transffered 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	**Mapped IP**	To make the single internal server which provides the services of FTP, web, mail, can real working by the policy .
Example 2	**Virtual Server**	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	**Virtual Server**	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	**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)

The Deployment

To apply two ADSL lines included the static IP address .

（WAN1 static IP is 61.11.11.10 ~ 61.11.11.14）

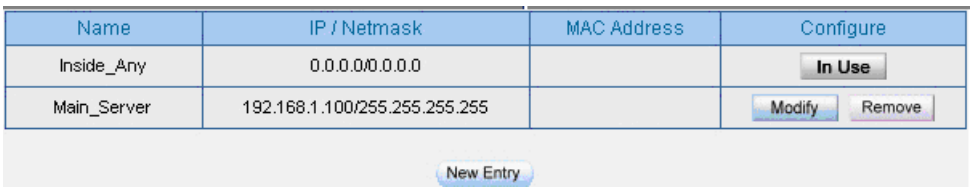
（WAN2 static IP is 211.22.22.18 ~ 211.22.22.30）

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 ：



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

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 .

Fig. 11-3 The service group setting

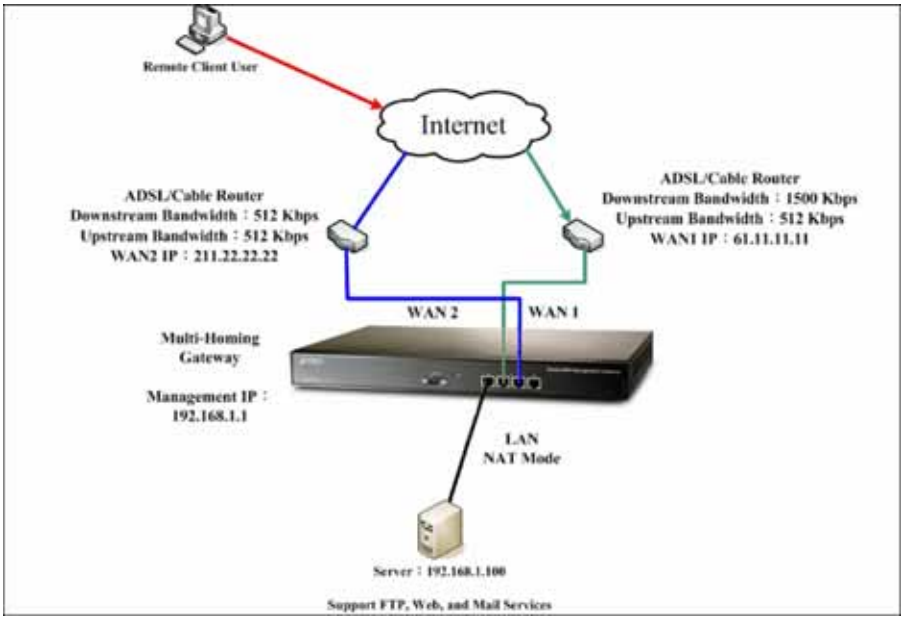
Step5. In **Policy → Incoming** , add the new policy included Step 3 , Step 4 .

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 .

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

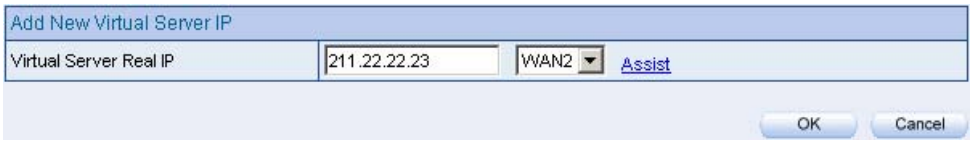
When the MIS engineer set the IP mapped by policy , it is strongly recommended not to select **ANY** in **Service** function. Because that may cause the IP mapped user be attacked .

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) .

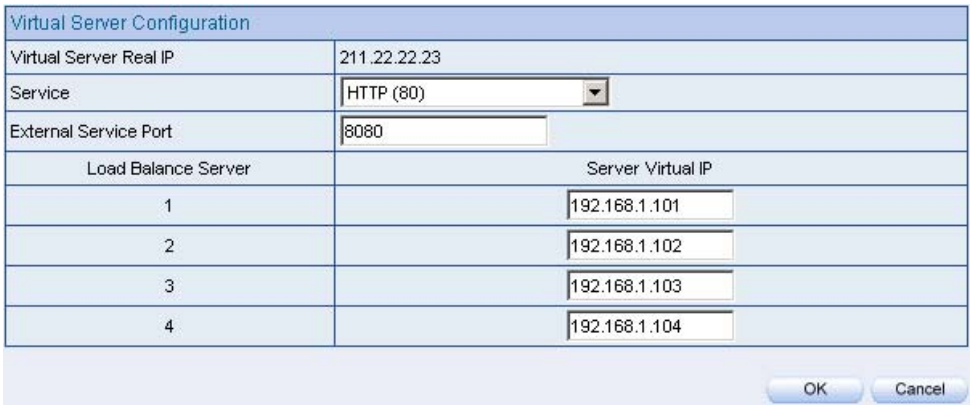
Step1. To set up many LAN server which provide the web service. The IP address are 192.168.1.101 , 192.168.1.102 , 192.168.1.103 , 192.168.1.104 .

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**, enter192.168.1.103 .
- **Load Balance Server 4** , enter 192.168.1.104 .
- Click **OK** .
- Complete the virtual server setting.



The virtual server IP setting



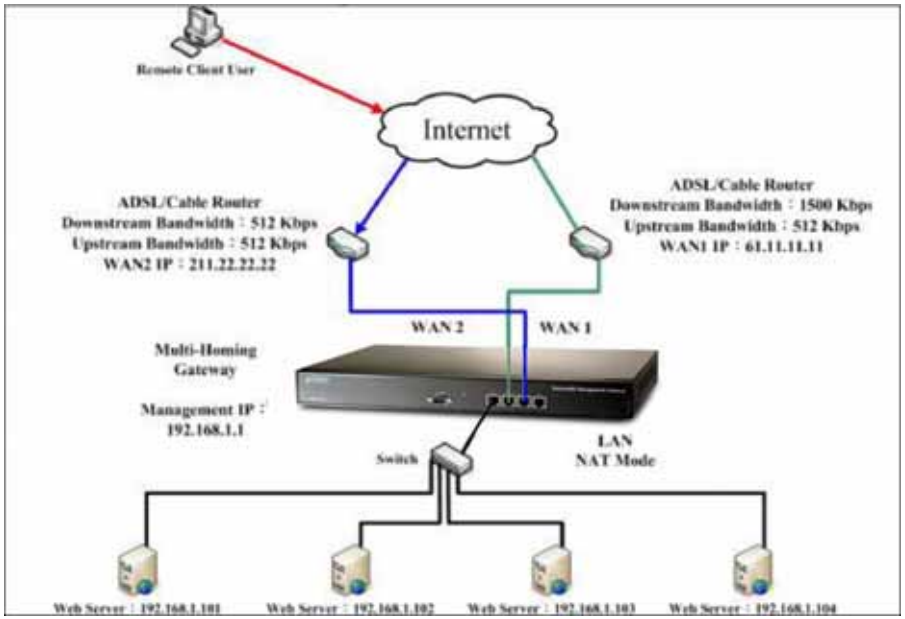
The virtual server configuration

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

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.

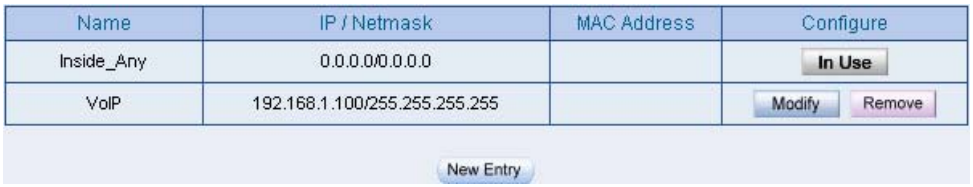


Use the virtual server instead of many internal server to provide the single service

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

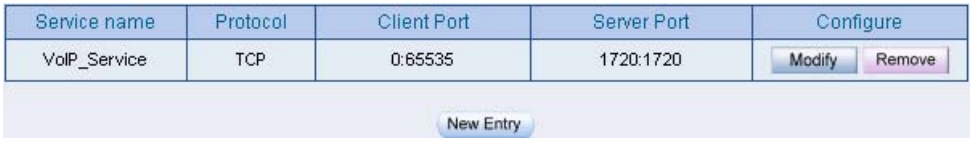
Step1. To set the LAN VoIP , its IP address is 192.168.1.100 .

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



The LAN address setting

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

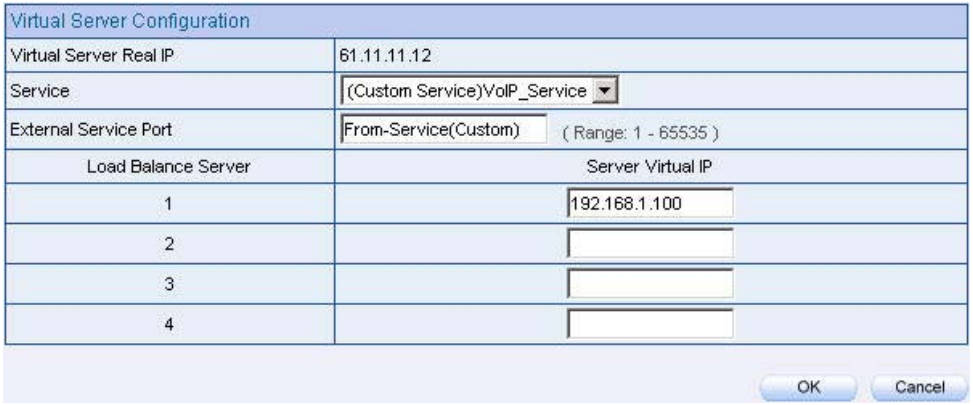


Add the custom service

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



The virtual server setting

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

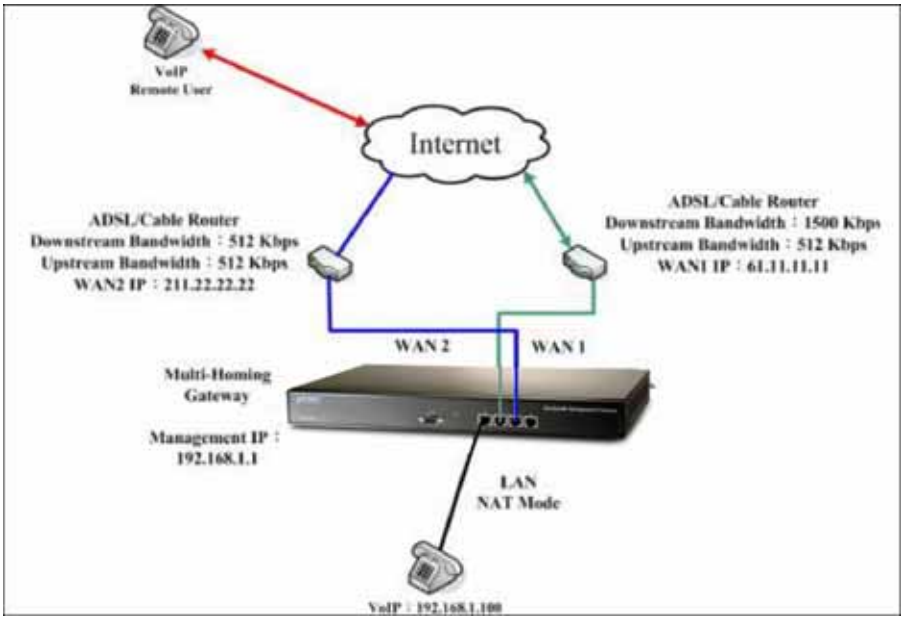
Step5. In **Policy → Incoming** , add the new policy included Step4 . (The virtual server setting)：

Complete the virtual server setting in policy

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

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		In Use
Server_01	192.168.1.101/255.255.255.255		Modify Remove
Server_02	192.168.1.102/255.255.255.255		Modify Remove
Server_03	192.168.1.103/255.255.255.255		Modify Remove
Server_04	192.168.1.104/255.255.255.255		Modify Remove

New Entry

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.

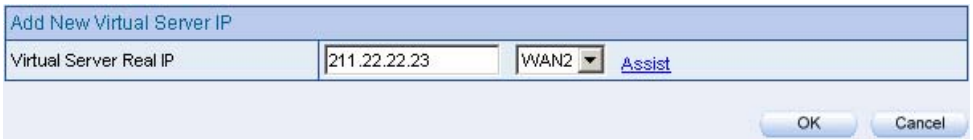
Group name	Service	Configure
Main_Service	DNS,HTTP,POP3...	Modify Remove
Mail_Service	DNS,POP3,SMTP	Modify Remove

New Entry

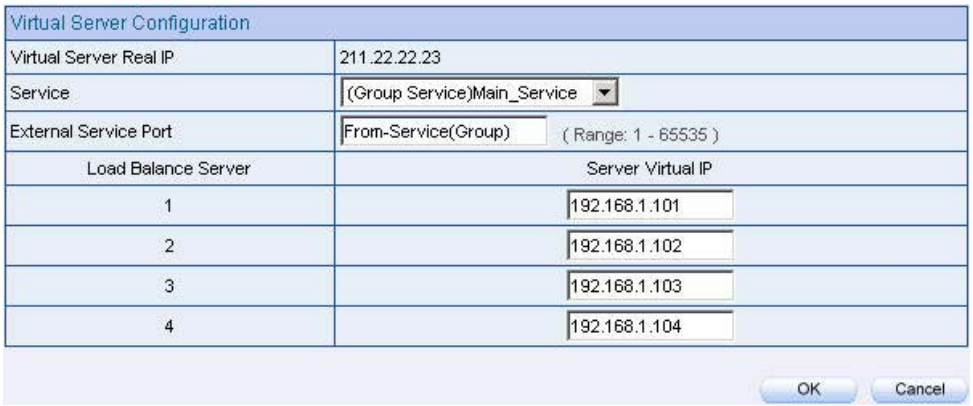
Add new service group

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



The virtual server real IP setting



The virtual server setting

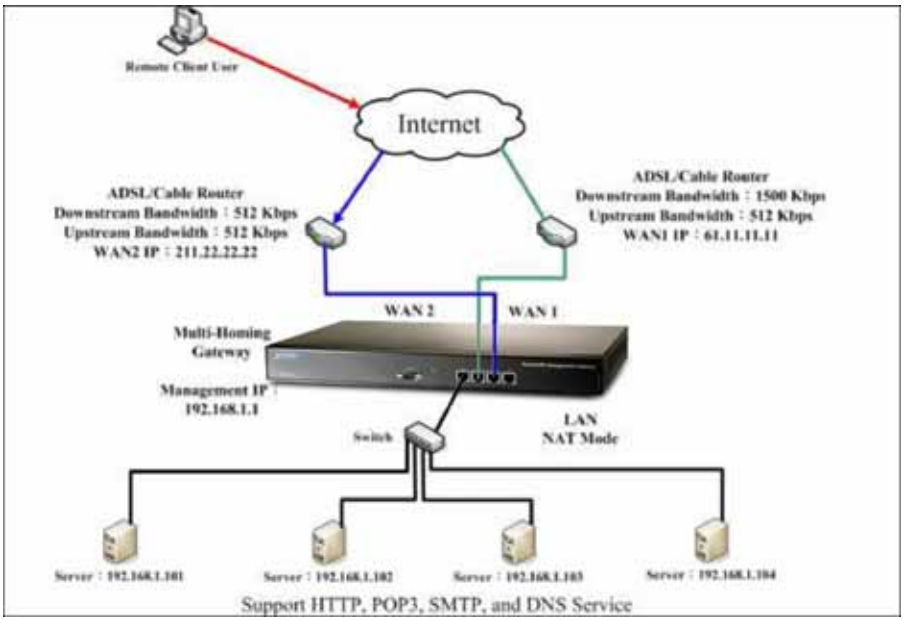
Step5. In **Policy → Incoming** , add the new policy included Step4 (The virtual server setting)：

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.

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

Chapter 13

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 successfuly .

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	**Outgoing**	To set the policy to monitor the internal user link to the network . (use traffic log , statistics and quota per session)
Example. 2	**Outgoing**	To deny the user to access the specify network resources. （For example , the static IP and content blocking.）
Example. 3	**Outgoing**	To permitted the authenticated user can access the network resources on specific time .
Example. 4	**Incoming**	The external user use the remote control software to control the internal PCs . （For example , pcAnywhere）
Example. 5	**WAN To DMZ**	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	**WAN To DMZ DMZ To WAN LAN To DMZ**	Sets a mail server in the DMZ by TRANSARENT mode , and to permit the internal and external user to send and receive e-mail.

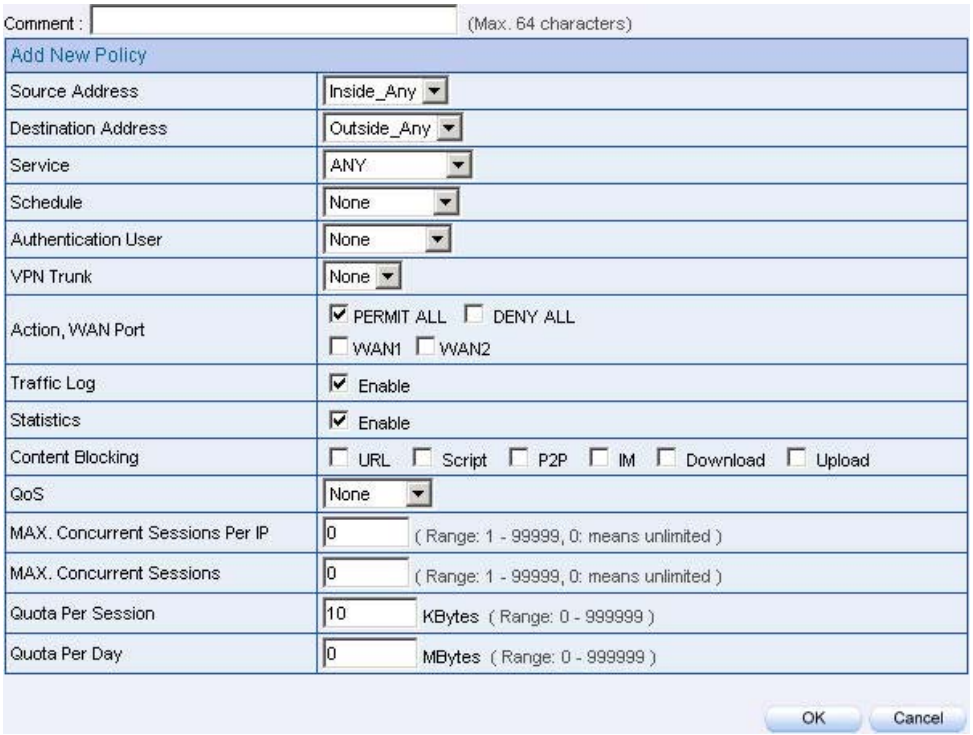
* DMZ = Demilitarized Zone

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** .



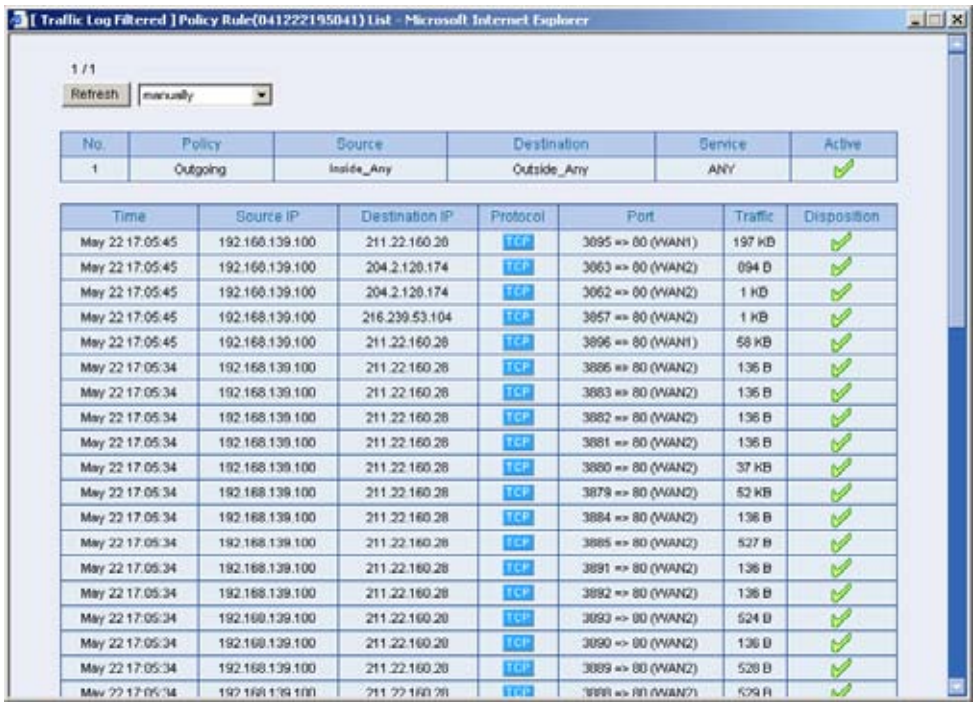
To Set the new policy

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 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

1 / 5 Next

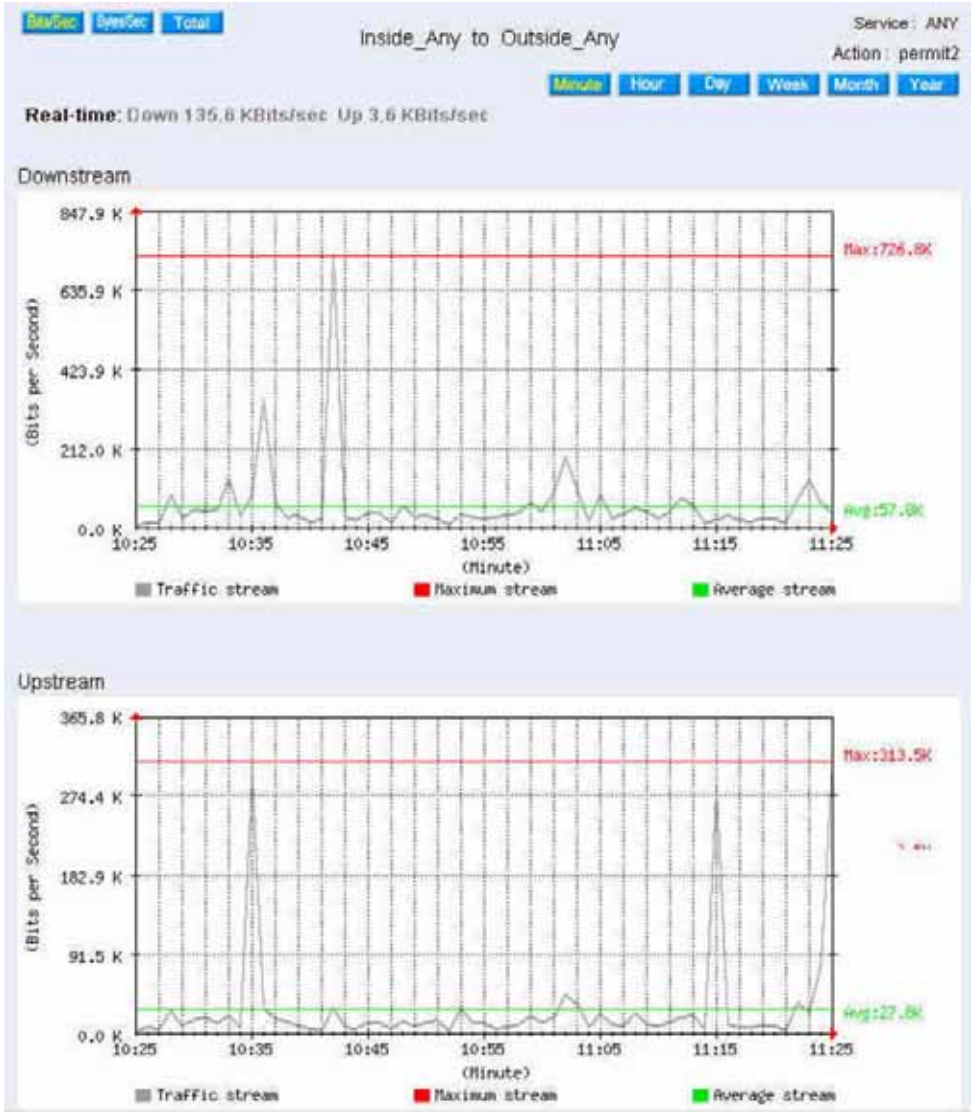
Time	Source IP	Destination IP	Protocol	Port	Traffic	Disposition
May 22 17:19:25	192.168.139.33	192.168.139.1	TCP	3524 => 80	17 KB	✓
May 22 17:19:24	192.168.139.33	192.168.139.1	TCP	3523 => 80	7 KB	✓
May 22 17:19:19	192.168.139.30	66.102.7.99	TCP	2026 => 80 (WAN2)	48 B	✓
May 22 17:19:19	192.168.139.30	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

1 / 5 Next

Traffic Log Web UI

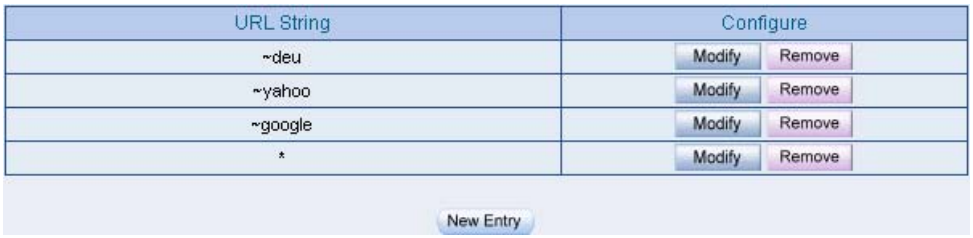
Step4. In **Monitor → Statistics → Ploicy** , it shows the traffic statistics through the policy .



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 ：

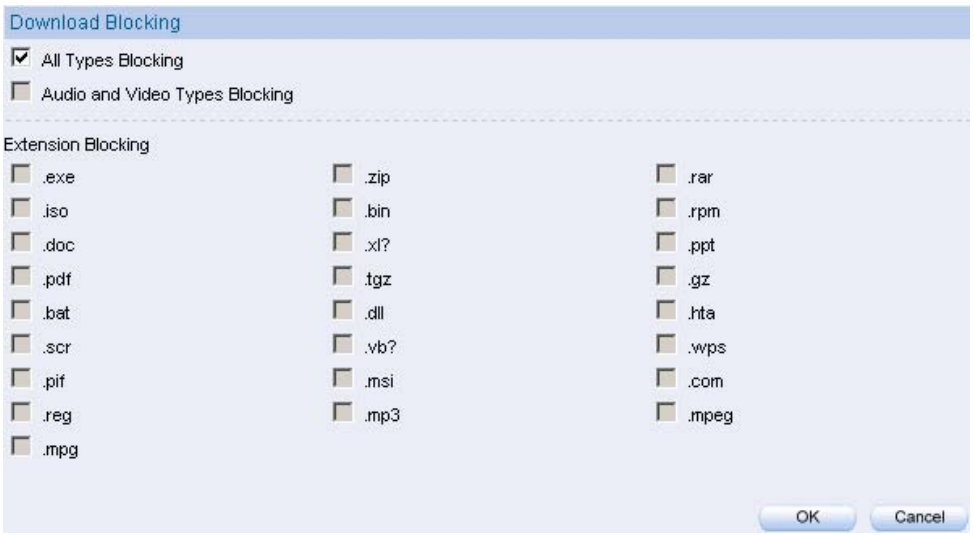


Content blocking setting

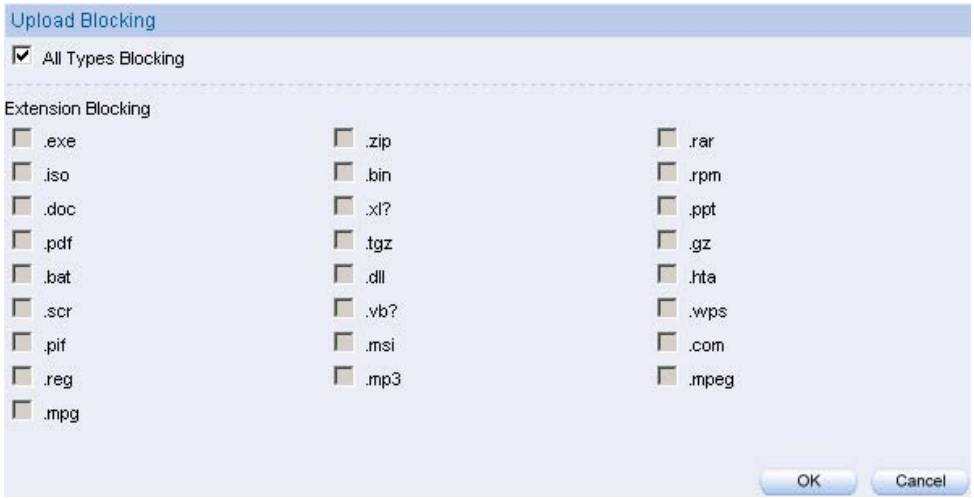
12-7 Script setting

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	In Use
Remote_Server1	61.219.38.98/255.255.255.255	Modify Remove
Remote_Server2	202.1.237.21/255.255.255.255	Modify Remove

New Entry

Set the WAN IP to block

Name	Member	Configure
WAN_Group	Remote_Server1, Remote_Server2	Modify Remove Pause

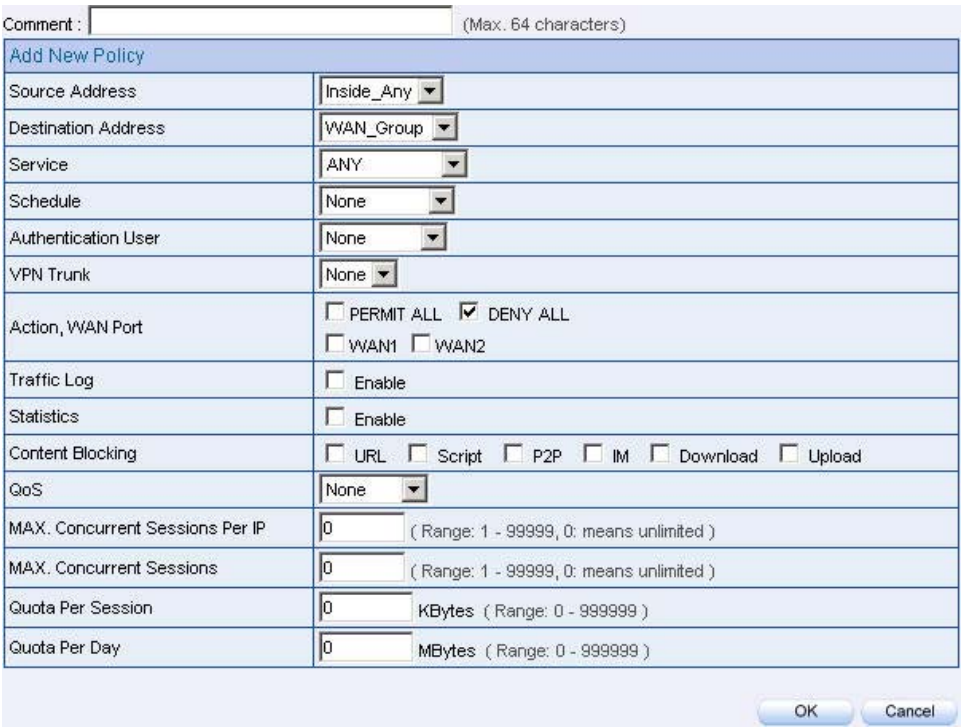
New Entry

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：

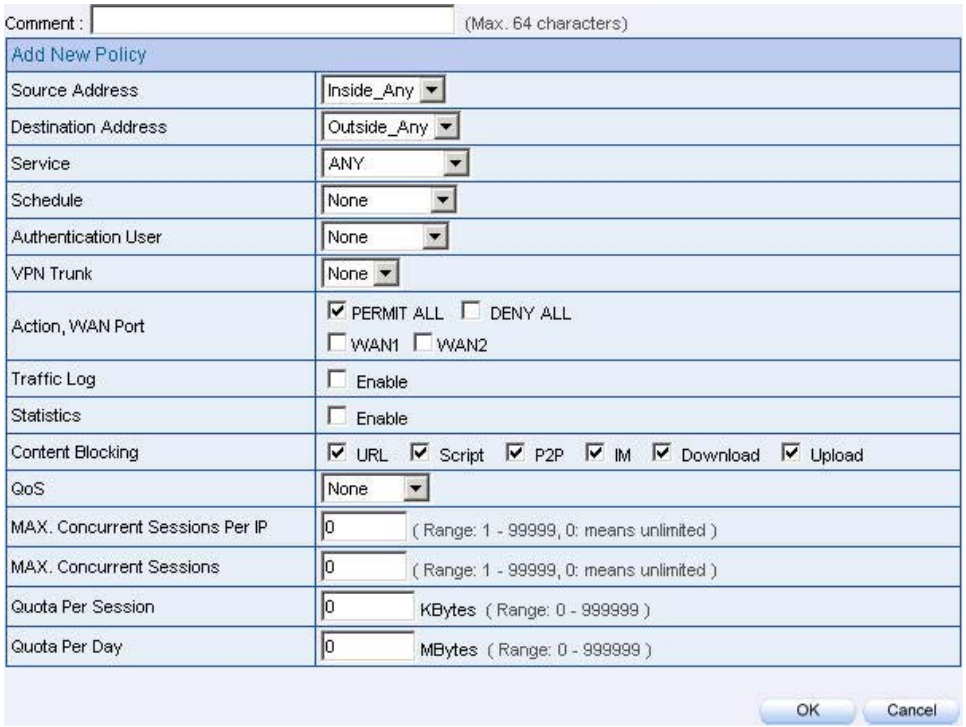
- Click **New Entry** .
- **Destination Address** , select **WAN _Group** set in Step2 . （Use the IP to block .）
- **Action , WAN Port** , select **DENY ALL** .
- Click **OK** .



Set the policy included blocking function

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

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



To set the content blocking policy

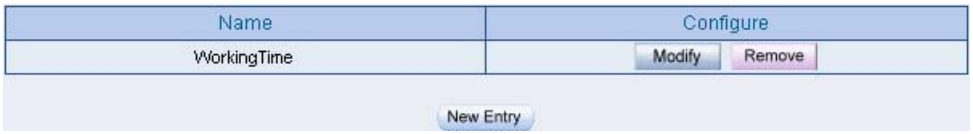
Step5. Complete to set the policy to deny users access the network resources

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 poriority , to limit users link to the specific IP address .

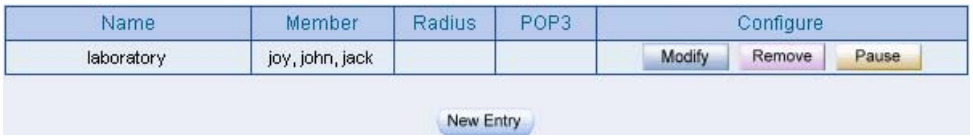
To permitted the authenticated user can access the network resources on specific time.

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



Add new schedule

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

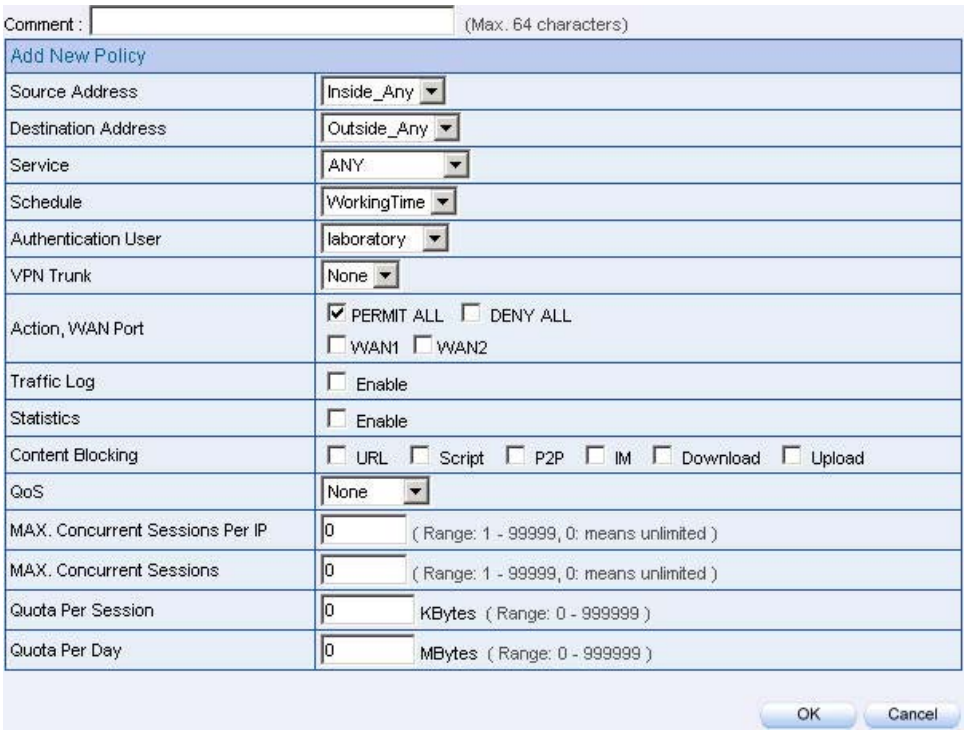


The authentication user group setting

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**



To set the authentication and schedule policy

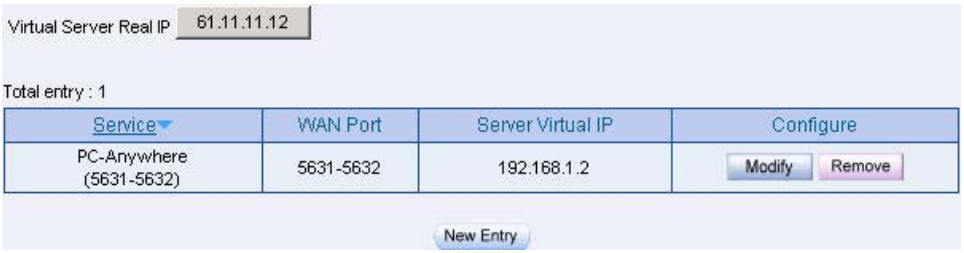
Step4. Complete the setting to permitte the user can access the network resources on specific time via the authentication .

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 .

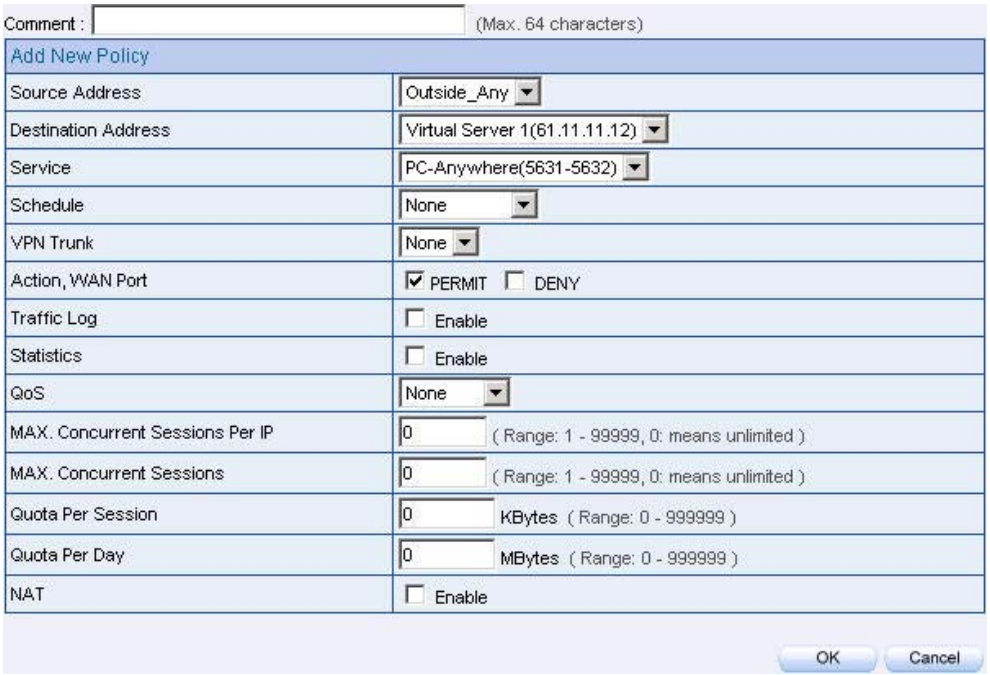
Step2. In **Virtual Server → Server 1** , add the following settings：



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**



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

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

Complete to set the policy of LAN PC remoted 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：

Set the virtual server correspond to FTP server

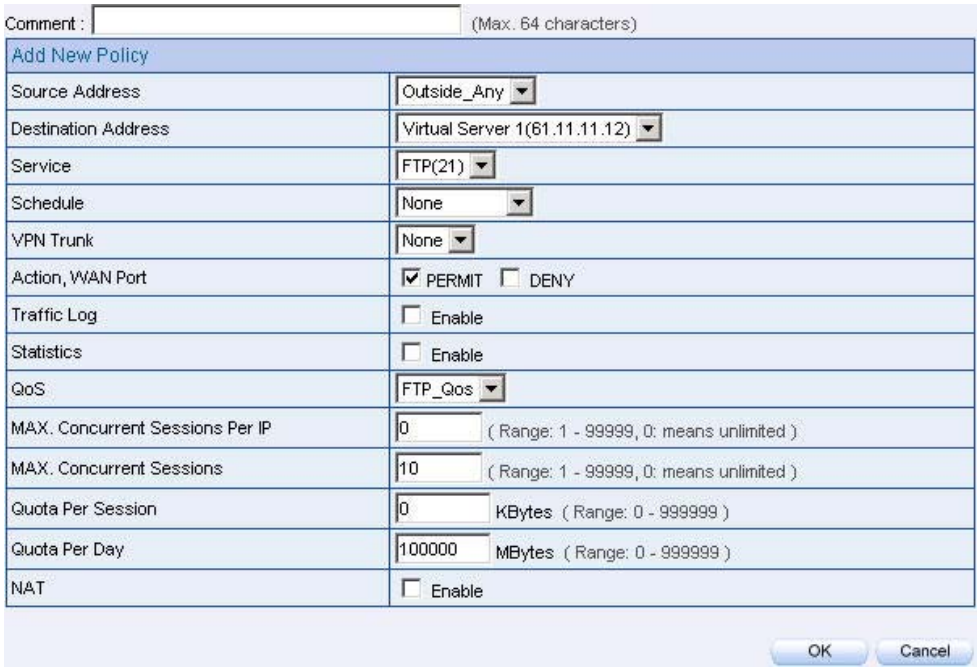
In **Policy → Incoming** or **WAN To DMZ** , it is strongly recommended not to select the **Service** to be **ANY** , to avoid the internal PC be attacked.

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

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**



Add new policy

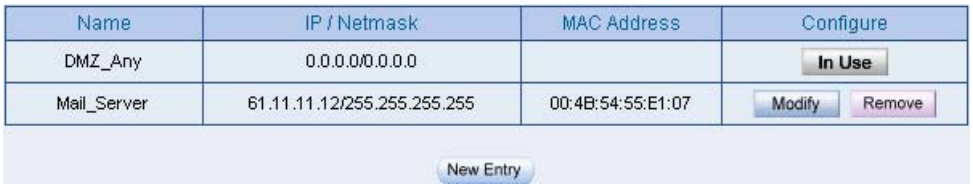
Step5. Limit users access the DMZ server services and network resources .

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：



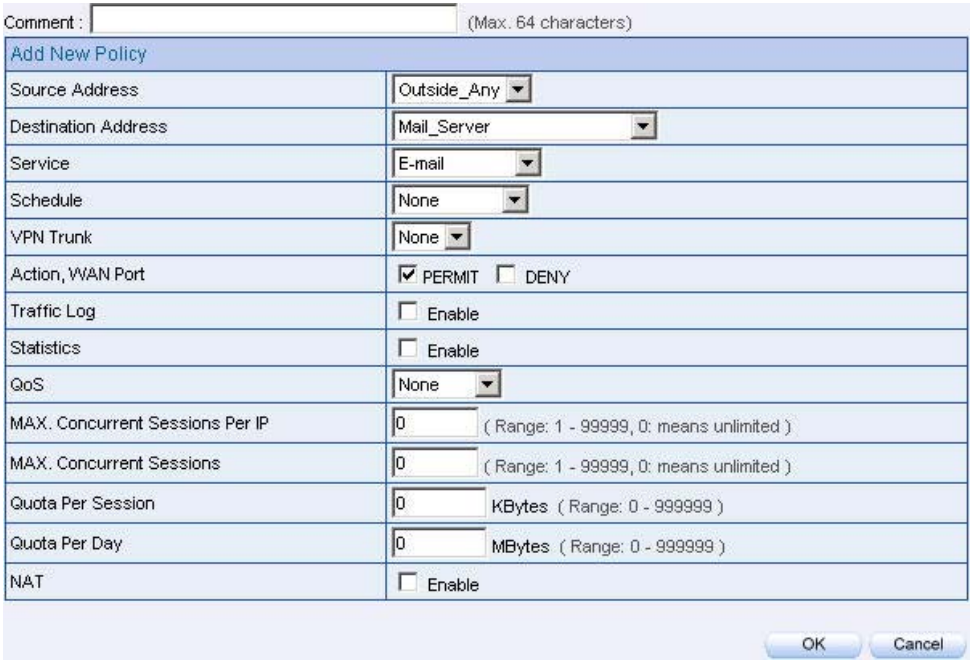
To set the mail server correspond to the IP address

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

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** .



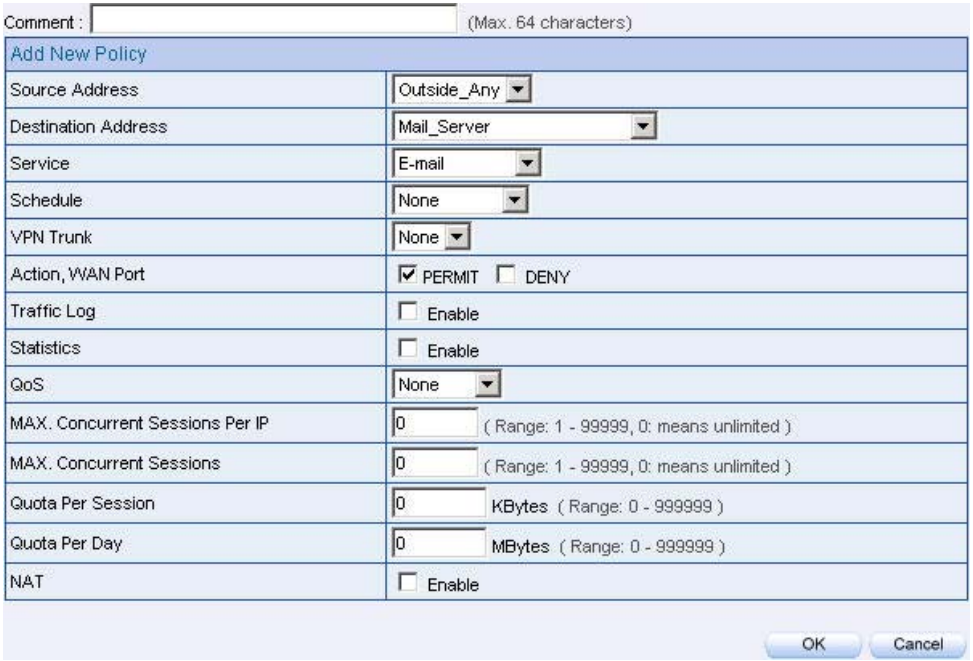
To set the WAN To DMZ mail service policy

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

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**



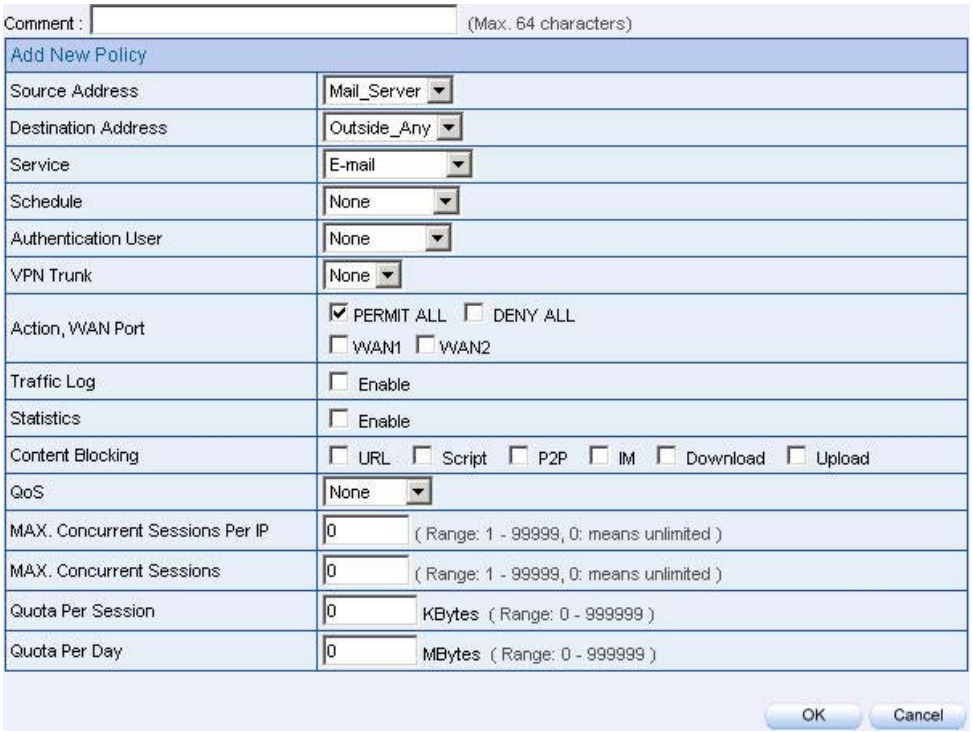
To set the LAN To DMZ mail service policy

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

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**



To set the DMZ To WAN Mail service policy

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

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 packes sent from hacker and use the Broadcast to send to ever 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 packes sent from hacker and use the Broadcast to send to ever 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 pretent 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 pretent 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.

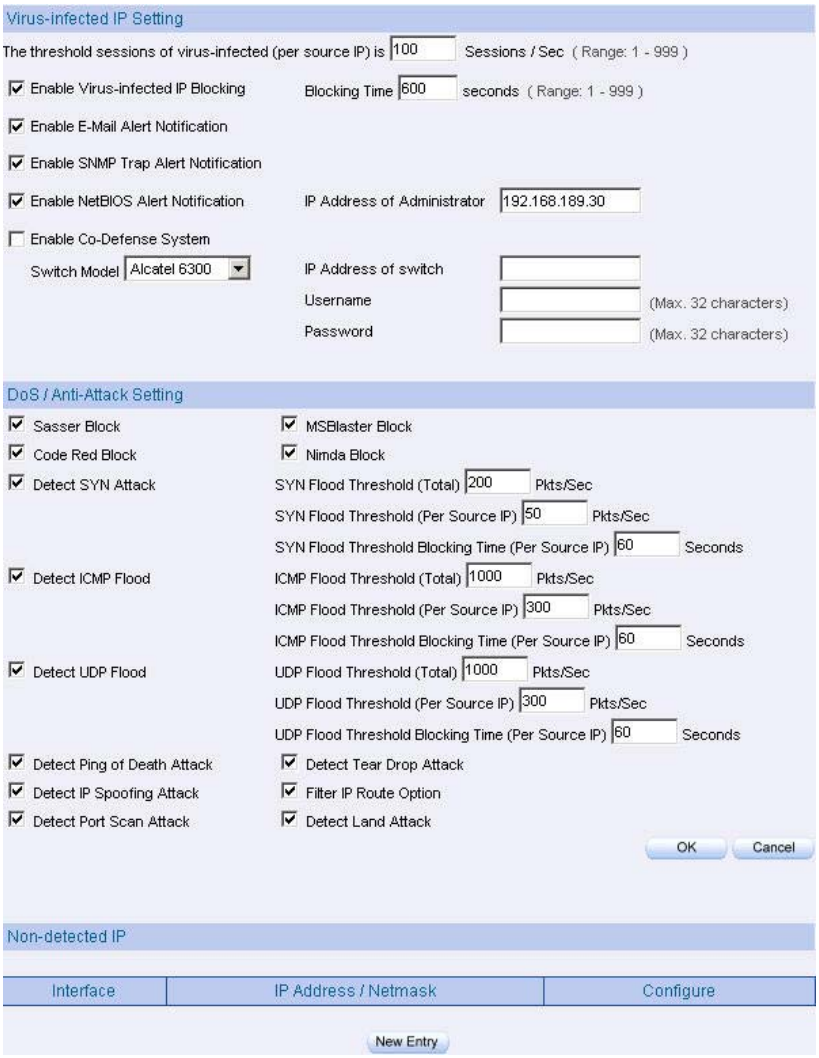
 When the MIS engineer enable the **Anomaly Flow** function, the BM-2101 will instantly show the message in **Virus-infected IP** and **Attack Events.** If the MIS engineer enable the function in **System → E-mail alert notification ,** then the BM-2101 will automatically send the notification to the 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.

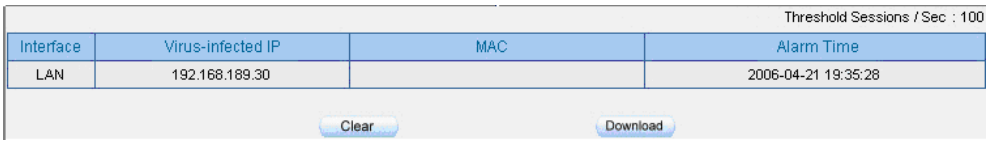


The setting of anomaly flow IP and Dos / Anti-Attack

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 → Viru-infected IP**. Or send the Net BIOS Notification to the MIS and virus-infected PC.



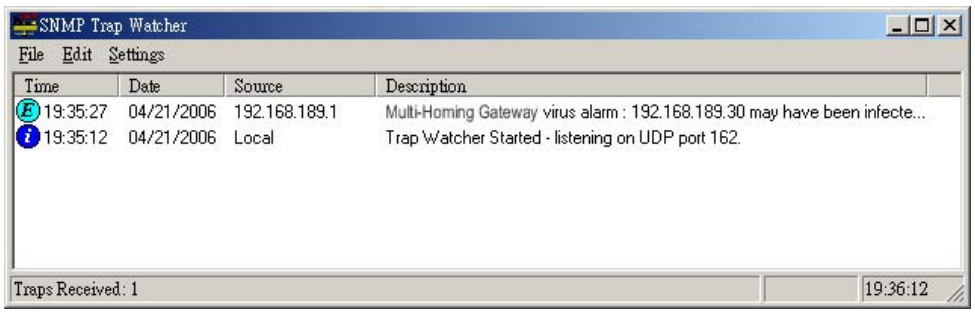
Anomaly flow IP and Virus-infected IP

Send the NetBIOS Alert notification to the virus-infected PC

Send the NetBIOS Alert Notification to the MIS engineer

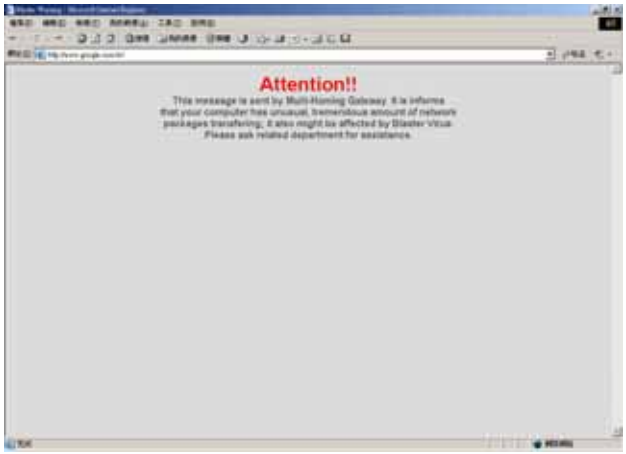
Step3. Enable the **System → E-Mail alert notification** , then the BM-2101 will send the mail notice to the MIS engineer.

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



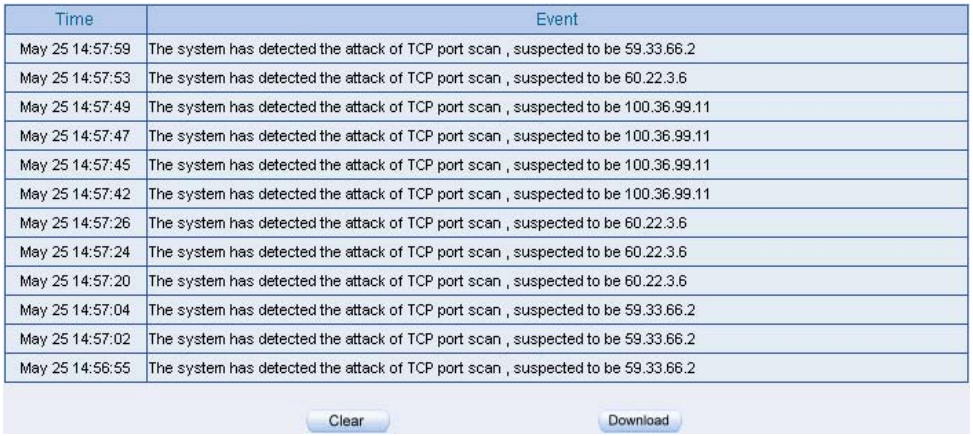
The SNMP Trap client receive the virus alert by the client software

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

Clear Download

Anomaly Flow IP attack event

Chapter 15

Monitor

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

MIS engineer can set the **Traffic** parameters in **Policy** , or select **View Log & Report Privlege** 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 conents , 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.

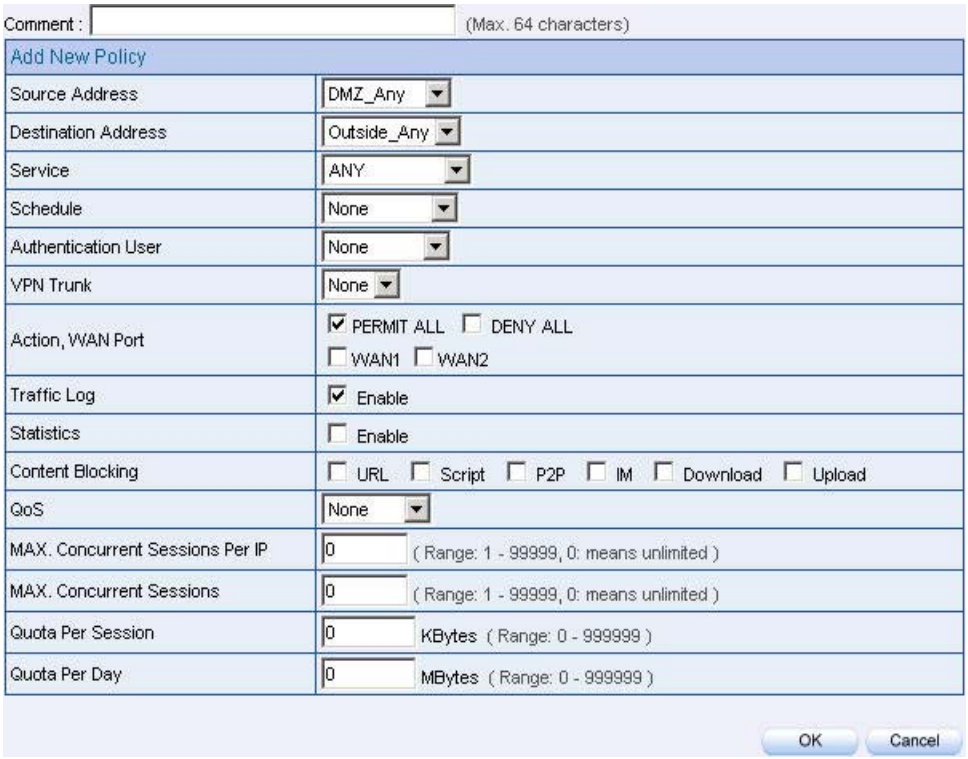
We set 4 monitoring environments.

No.	Range	The Application Environment
Example. 1	**Traffic**	View the user's used Protocol and Port , to access the internal and external resources via BM-2101
Example. 2	**Event**	View the status of MIS engineer log into BM-2101 pocess the managemnt and external interface.
Example. 3	**Connection**	View the external interface record of bandwidth management .
Example. 4	**Log Backup**	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：

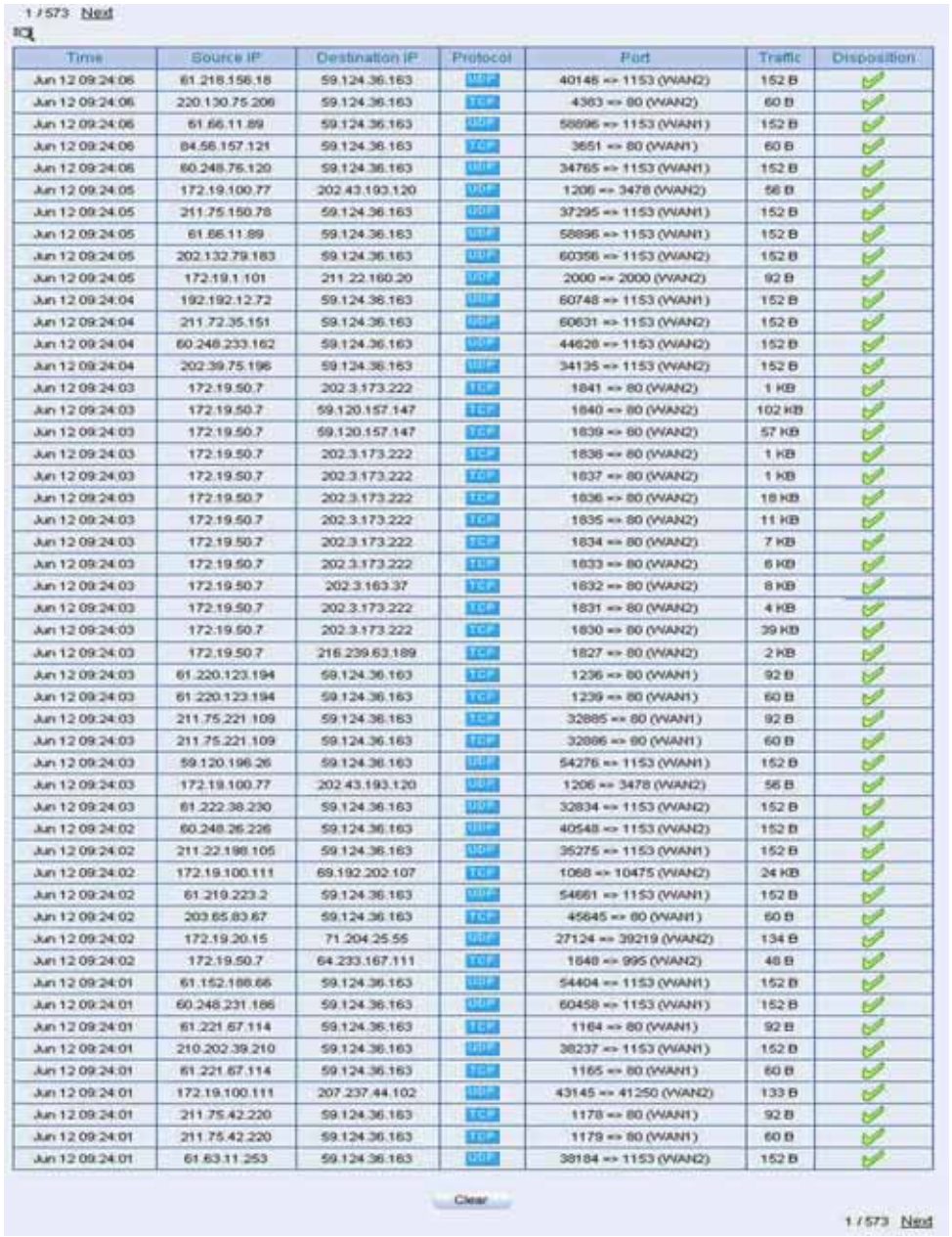


Traffic setting in policy

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

Complete the DMZ To WAN traffic setting in policy

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



1 / 573 Next

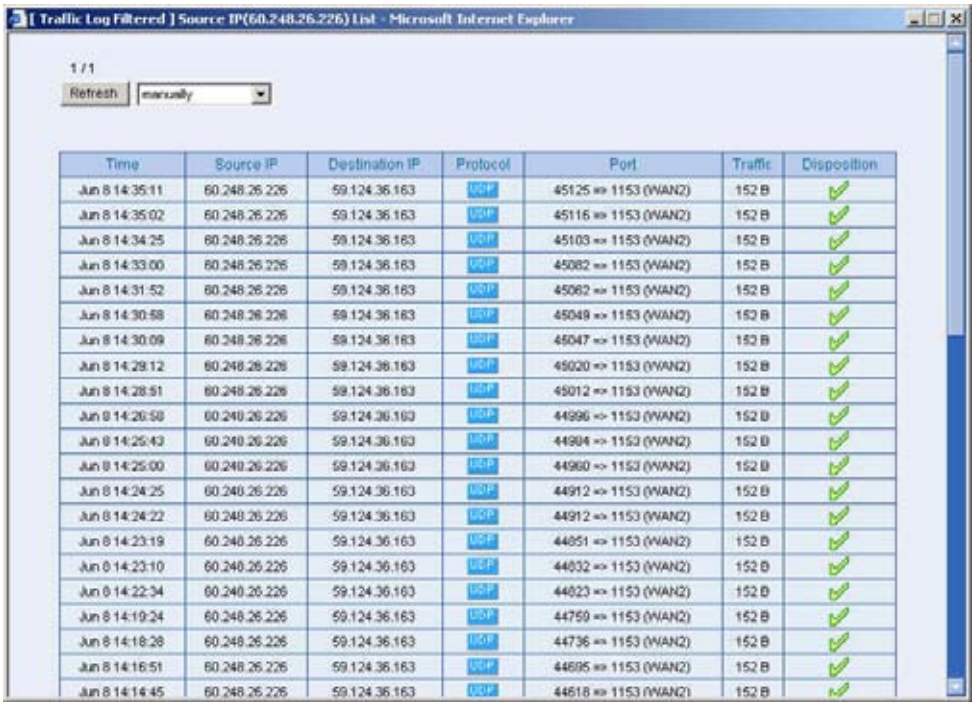
Time	Source IP	Destination IP	Protocol	Port	Traffic	Disposition
Jun 12 09:24:06	61.218.156.18	59.124.36.163	UDP	40148 => 1153 (WAN2)	152 B	✓
Jun 12 09:24:06	220.130.75.206	59.124.36.163	TCP	4363 => 80 (WAN2)	60 B	✓
Jun 12 09:24:06	61.66.11.89	59.124.36.163	UDP	58896 => 1153 (WAN1)	152 B	✓
Jun 12 09:24:06	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)	6 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	211.22.198.105	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	1848 => 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	38184 => 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.



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.

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.

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 enginer 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

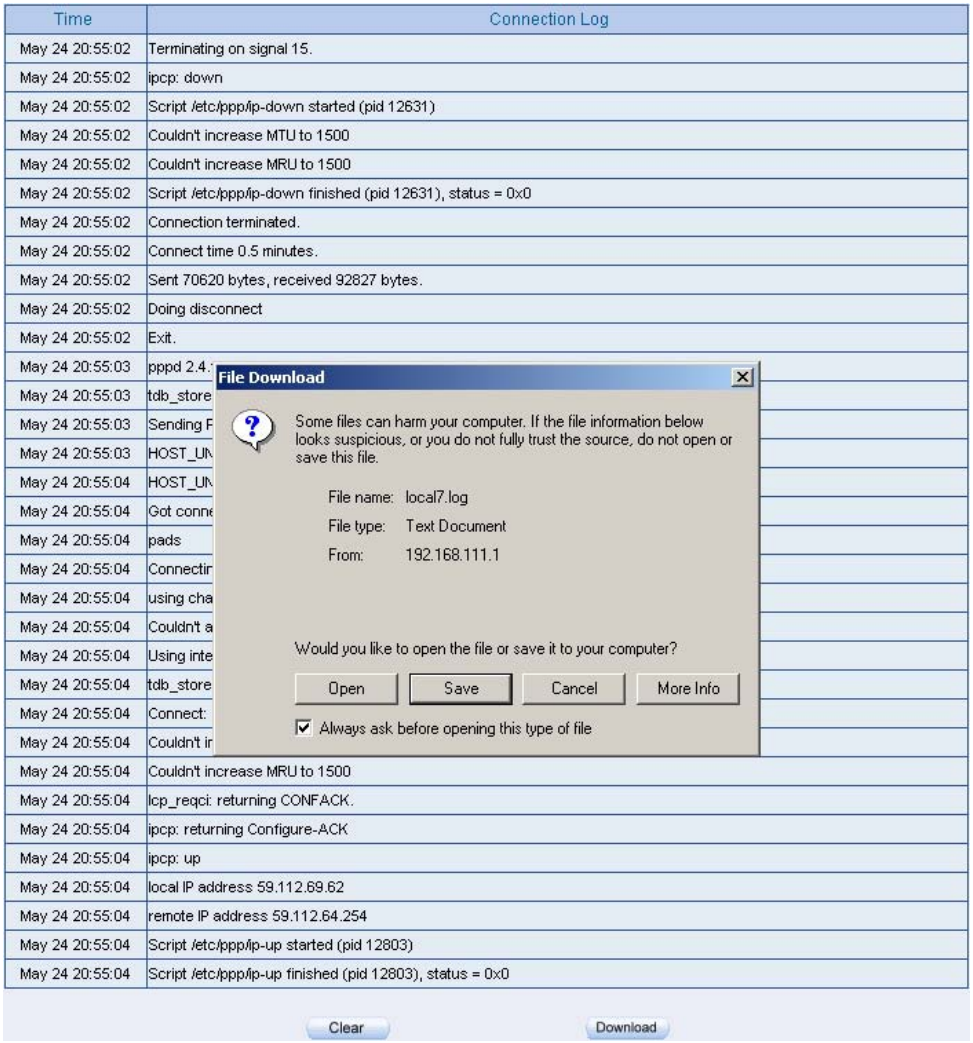
View the external interface connection record as process the bandwidth management.

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

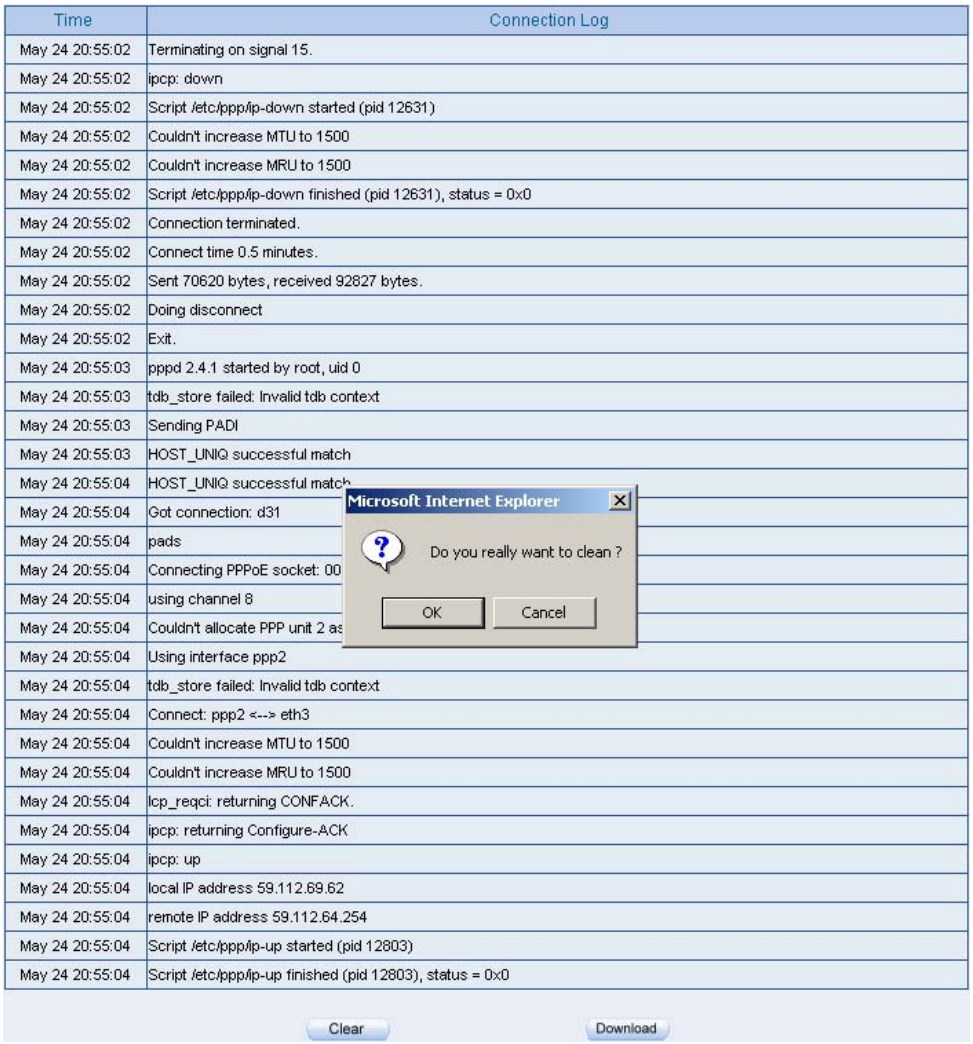
Connection records

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



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.

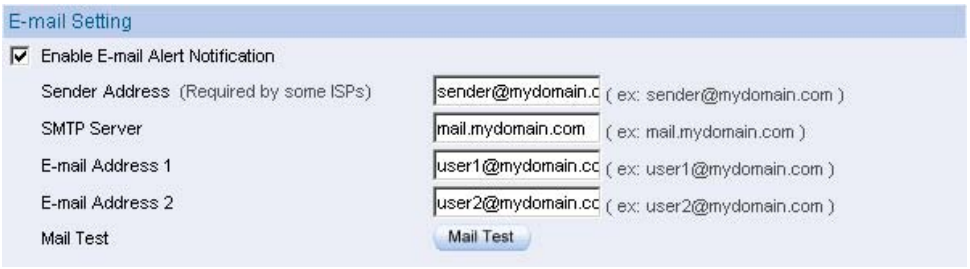


Delete all the connection log files

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



E-mail setting

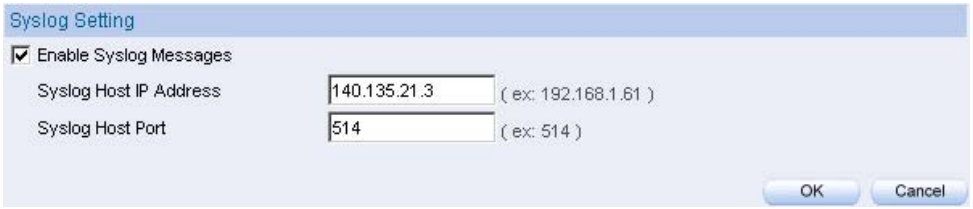
Step2. **Monitor → Backup → enable log mail support.** Click **OK.**

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 Prt number in **Syslog host Port.**
- Click OK.
- Complete the setting.



Syslog setting

Chapter 16

Accounting Report

MIS engineer can use **Accounting Report** to view all the internal and external user's network accssing 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

- Display LAN and DMZ user ‘s accounting report.

Site

- Display external server accounting report.

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

- 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  .
- **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.

Outbound accounting report

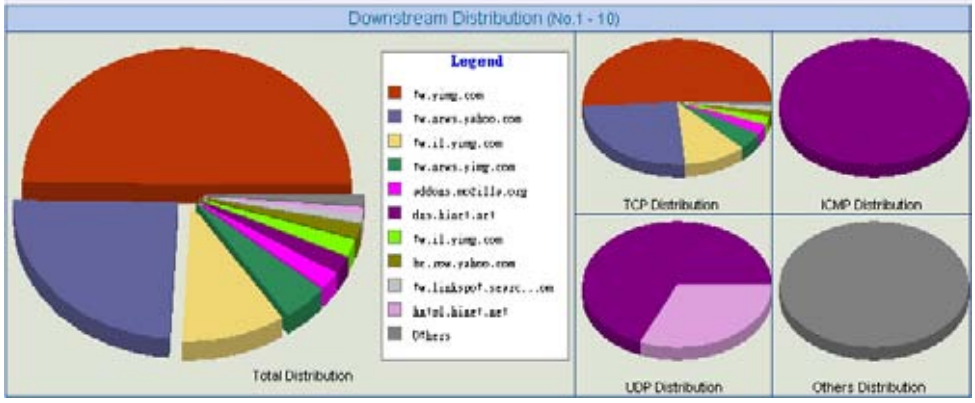
192.168.139.71 Information

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 (UNKNOWN)
Total Data Downstream / Upstream	813.3 KBytes / 151.1 KBytes

1 / 2 Next

Top Sites: 1 - 10

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.rl.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	18.9 KB	2.3%	18.9 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	68.6%	420.0 B	100.0%	0.0 B	0.0%
7	tw.rl.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.ruw.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.searc...om	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	hntpt.hinet.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	



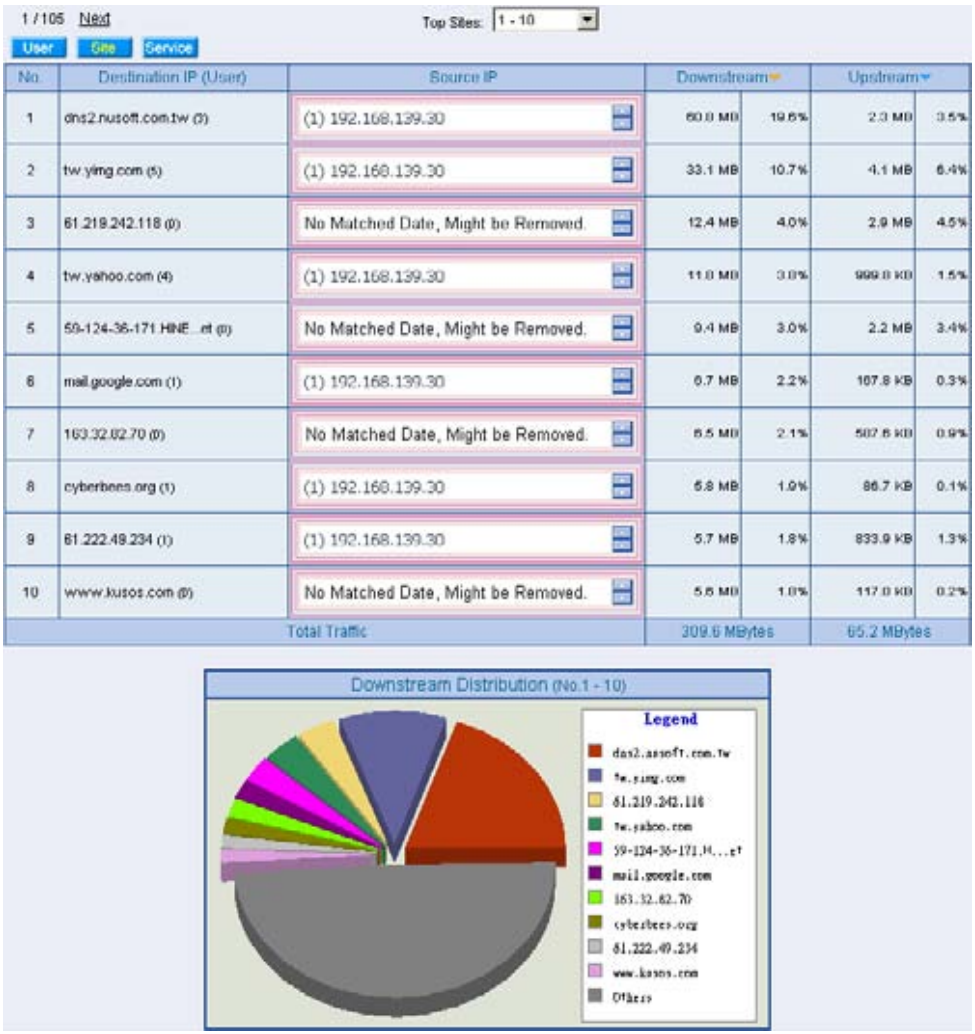
Outbound use information

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.

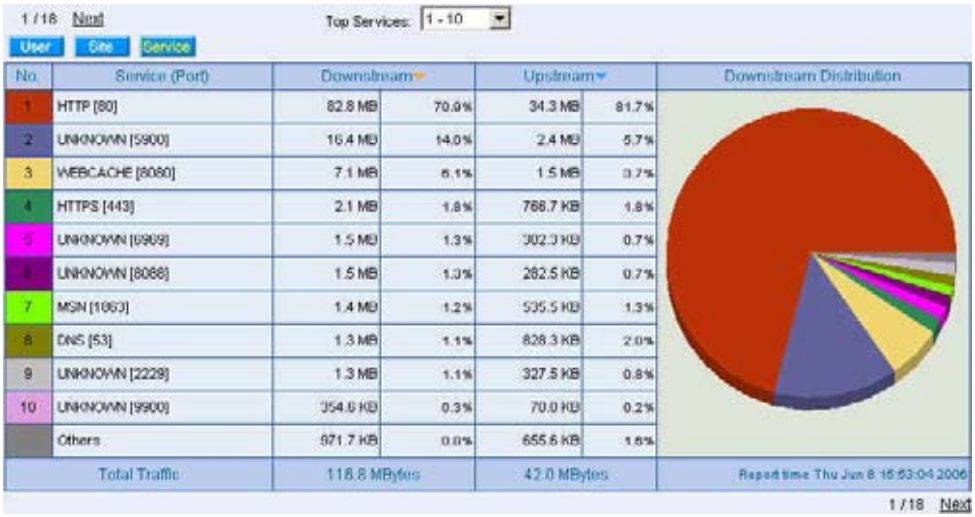
- **Downstream Distribution**：Display the distribution charts depends on the real downstream traffic.



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.



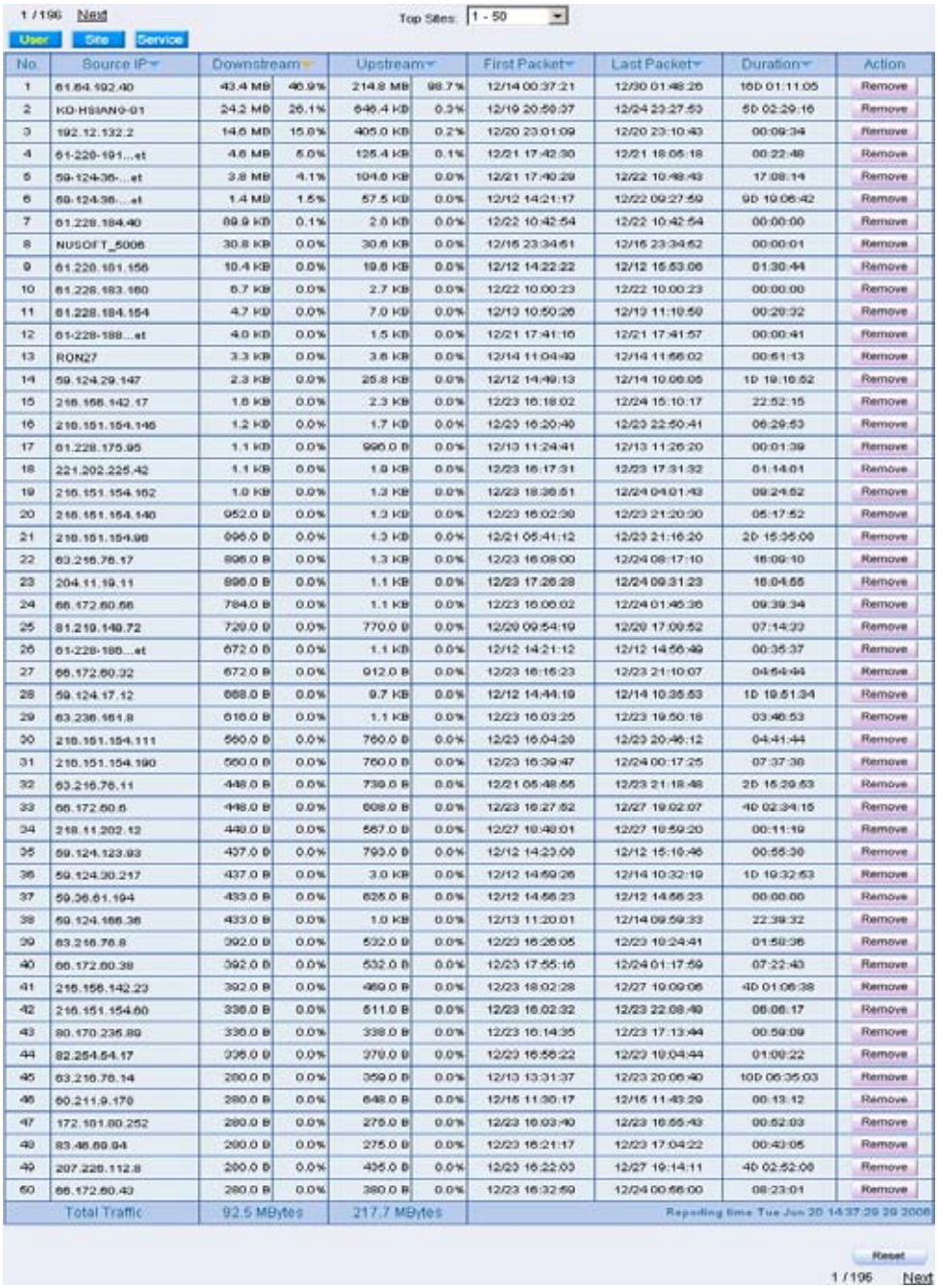
Outbound service accounting report

16.2 Inbound

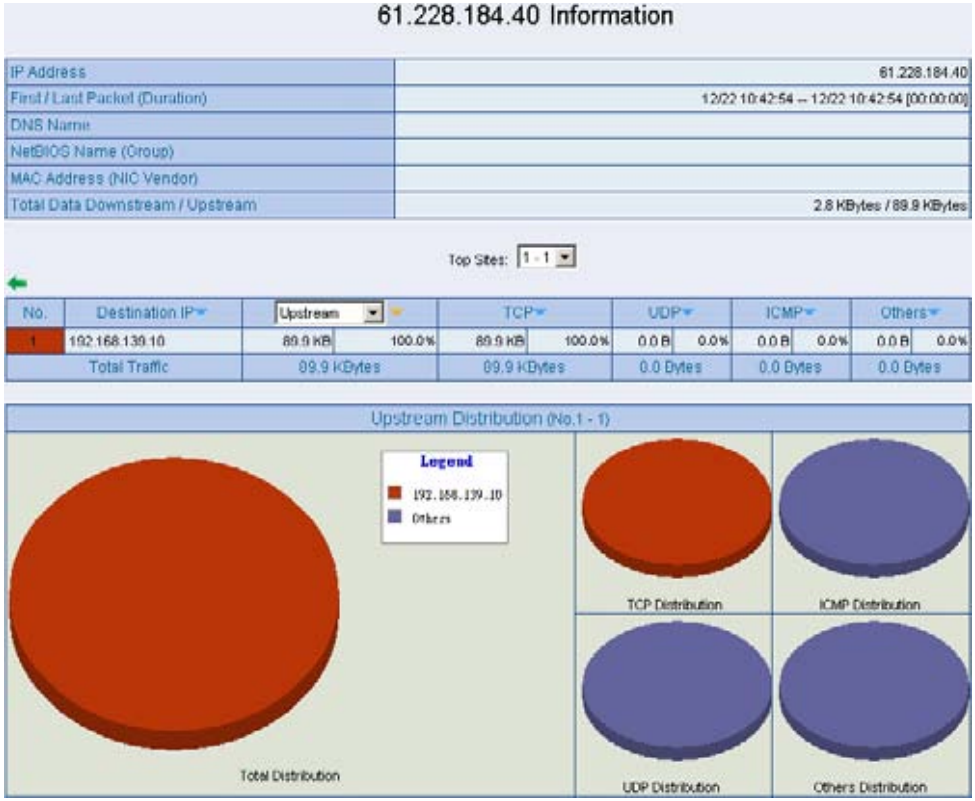
Step1 **Accounting Report → Inbound** , click **User** , it shows the accounting report of send/retrieve packets in downstream , upstream, first packet , last packet duration from external server to access the user IP address in BM-2101.

- **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.



Inbound user accounting report

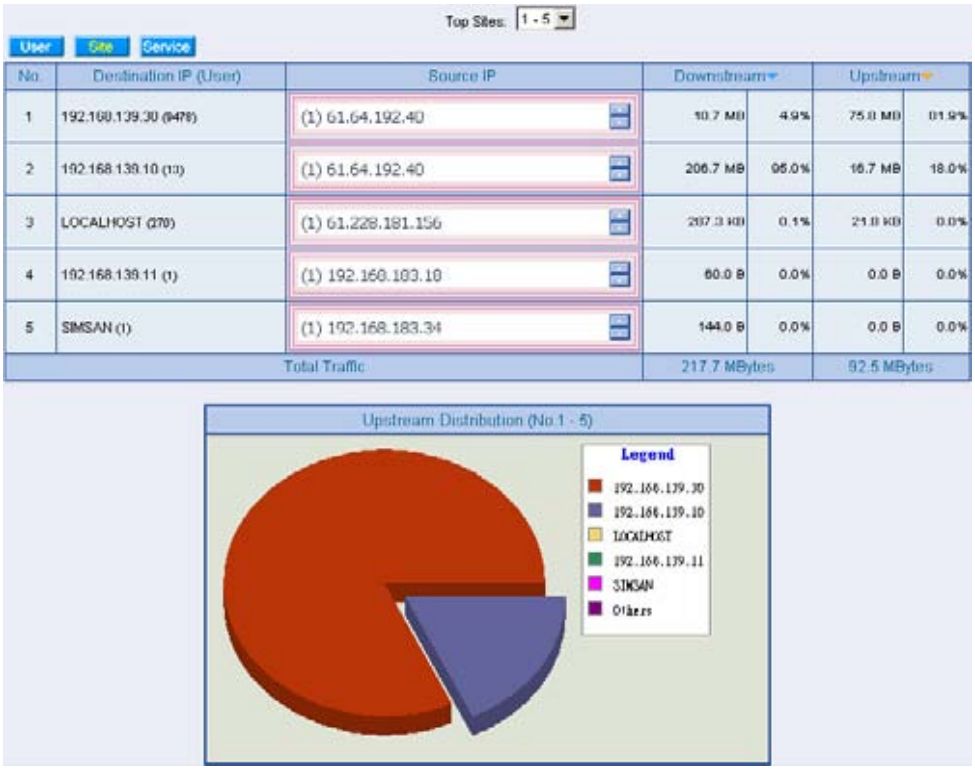


Inbound user information

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 

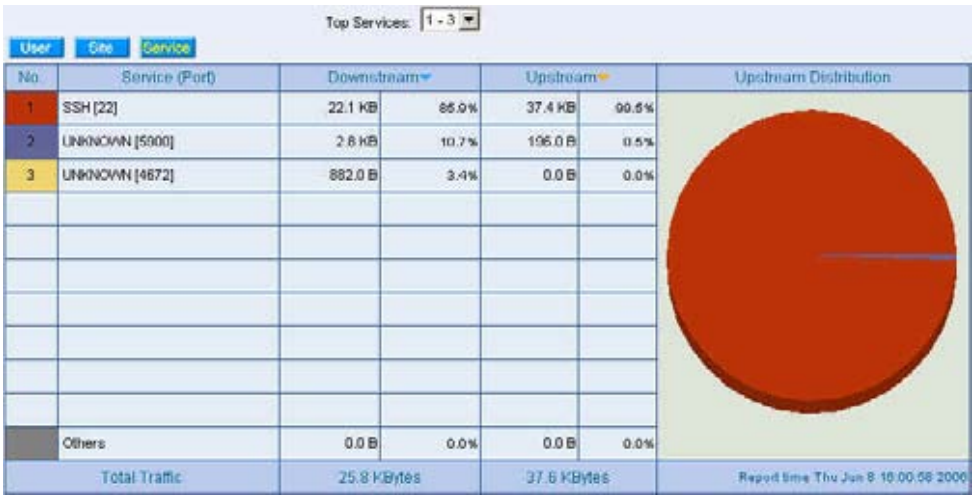
- **Destination IP (User)**：It means the LAN or DMZ server IP or represents the external user numbers to access the LAN or DMZ server.
- **Source IP**：It means the external user's IP address , to access the LAN or DMZ server.
- **Downstream**：The percentage of traffic and total downstream traffic from 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.



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	Minute Hour Day Week Month Year
WAN 2	Minute Hour Day Week Month Year
All WAN Interface	Minute Hour Day Week Month Year

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

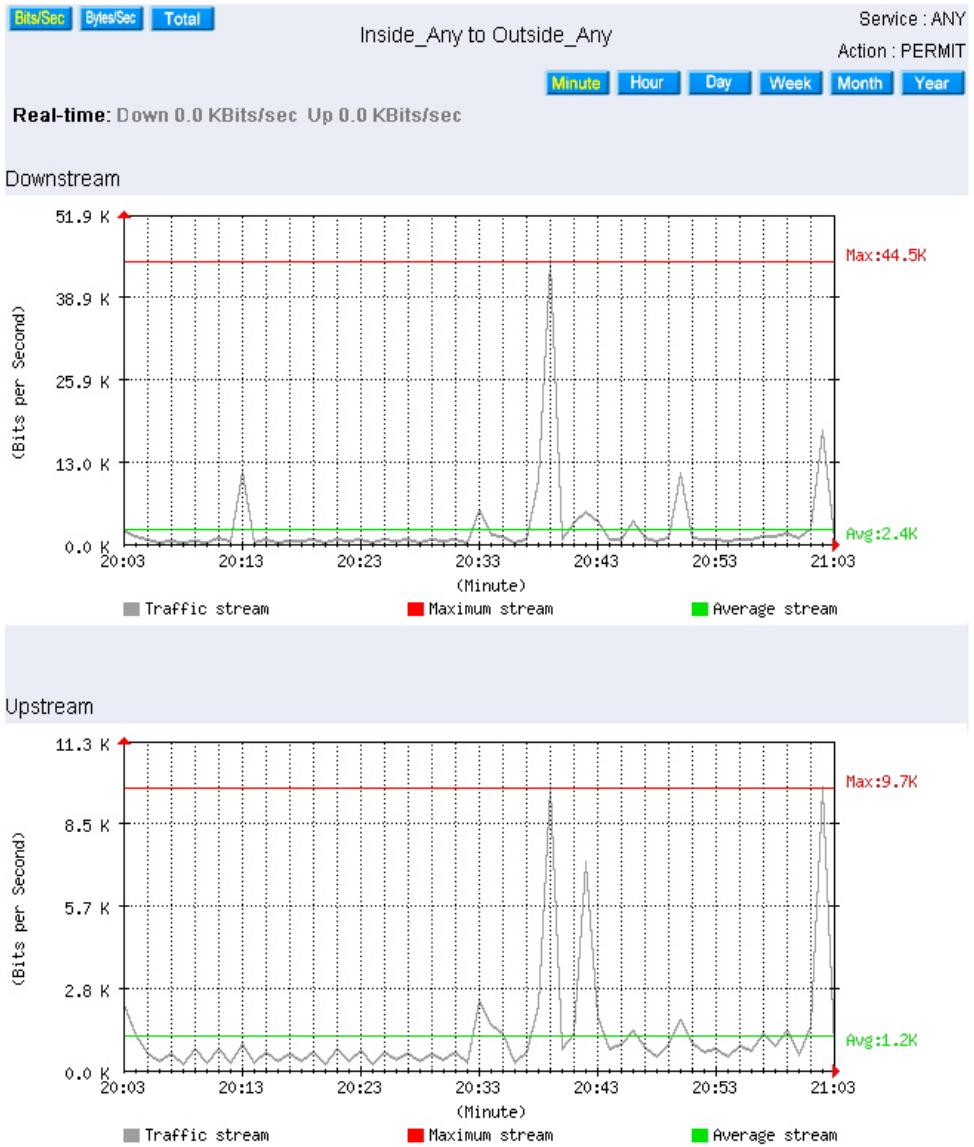
The policy statistics

 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）.



View the policy statistics charts

Chapter 18

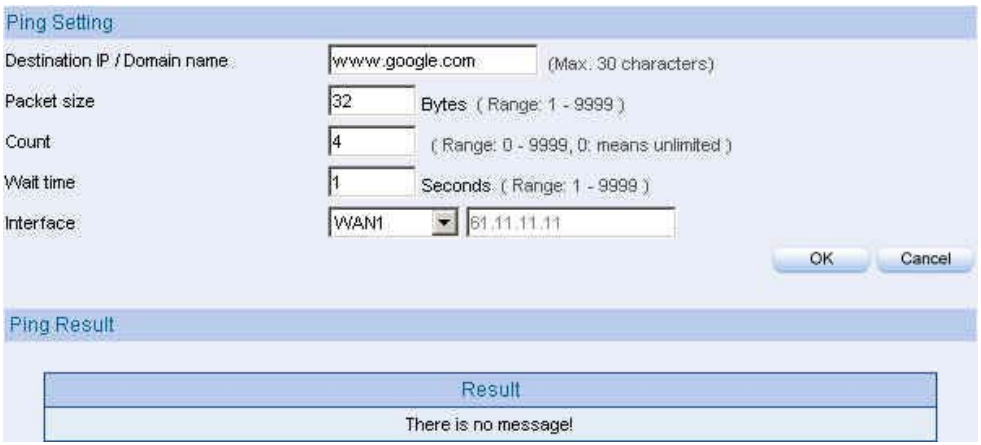
Diagnostic

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

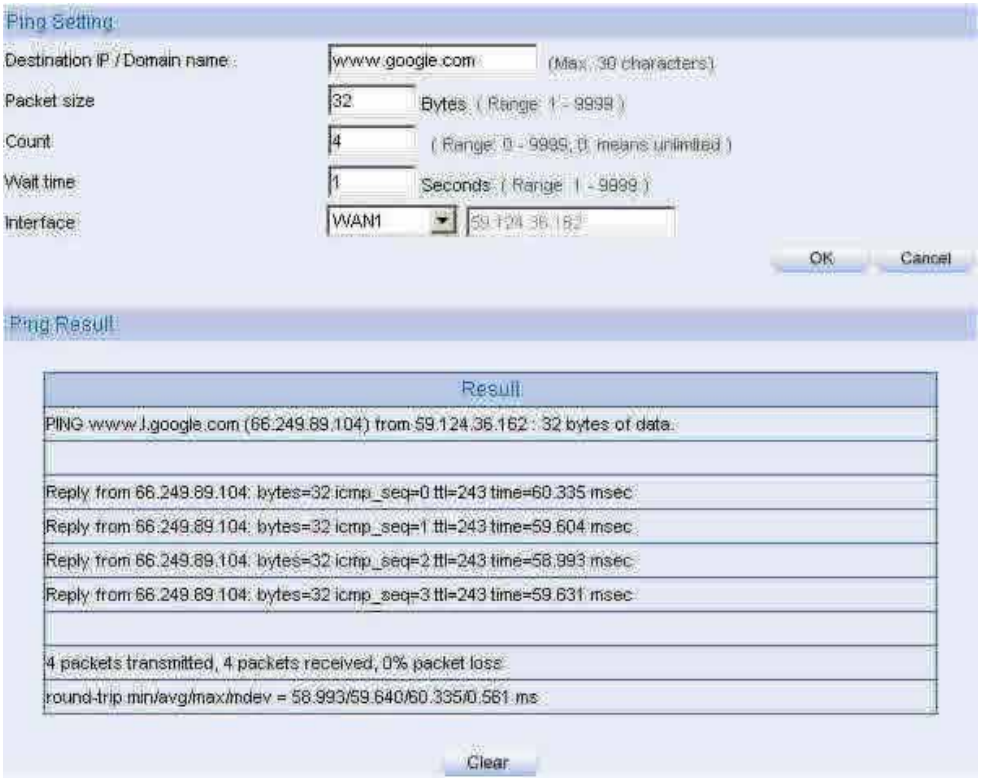
18.1 Ping

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**.



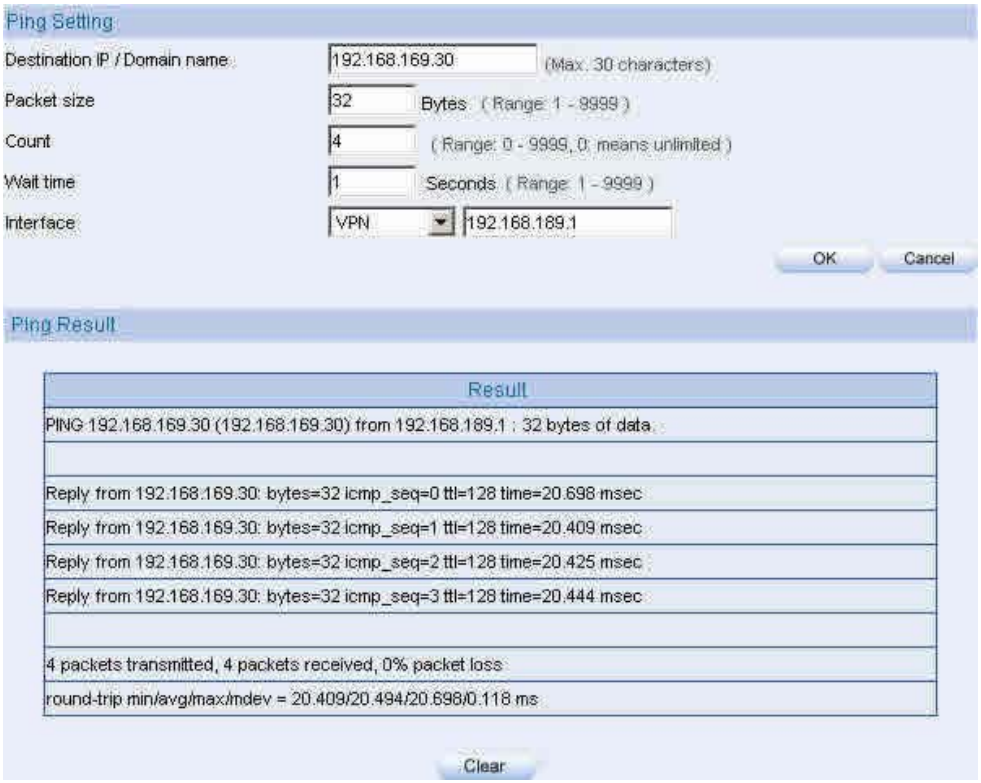
Ping setting



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 coulumn.**

- 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.

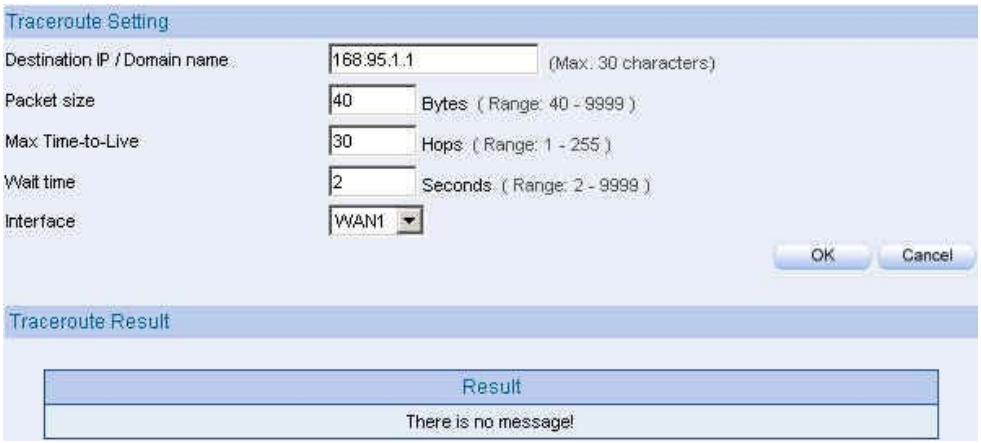


The Ping results of VPN

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

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.**

Set the internal PC to be monitored

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

Start up the PC

Chapter 20

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.

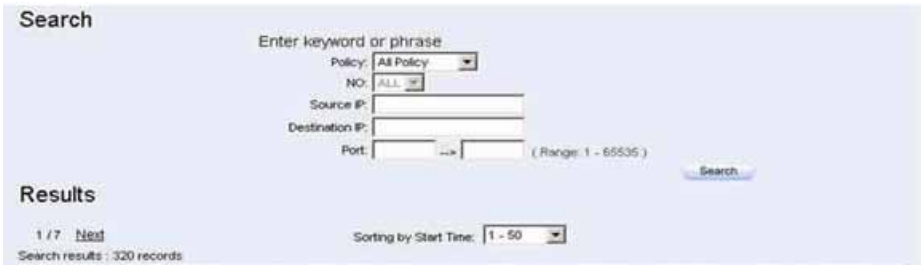
5. **Sessions Info**：It records all the session packets pass through BM-2101.

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**.

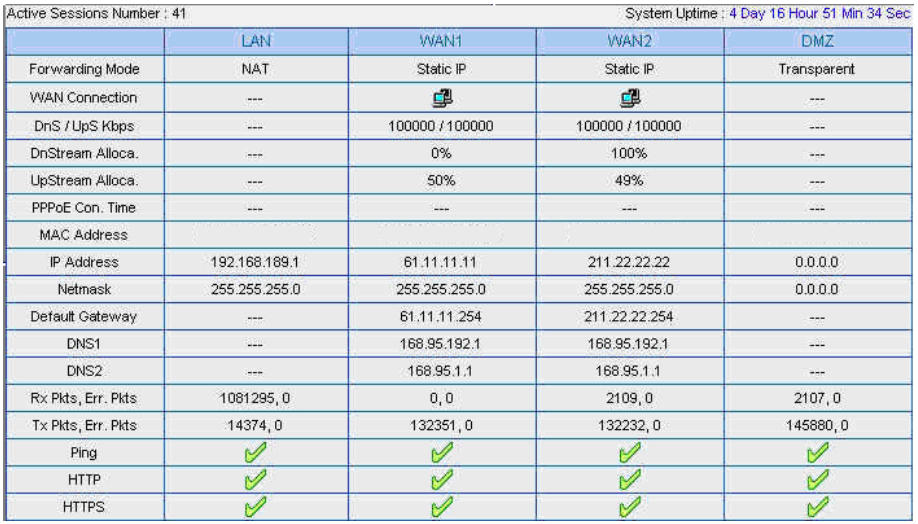


Search the specific record

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 maximium 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

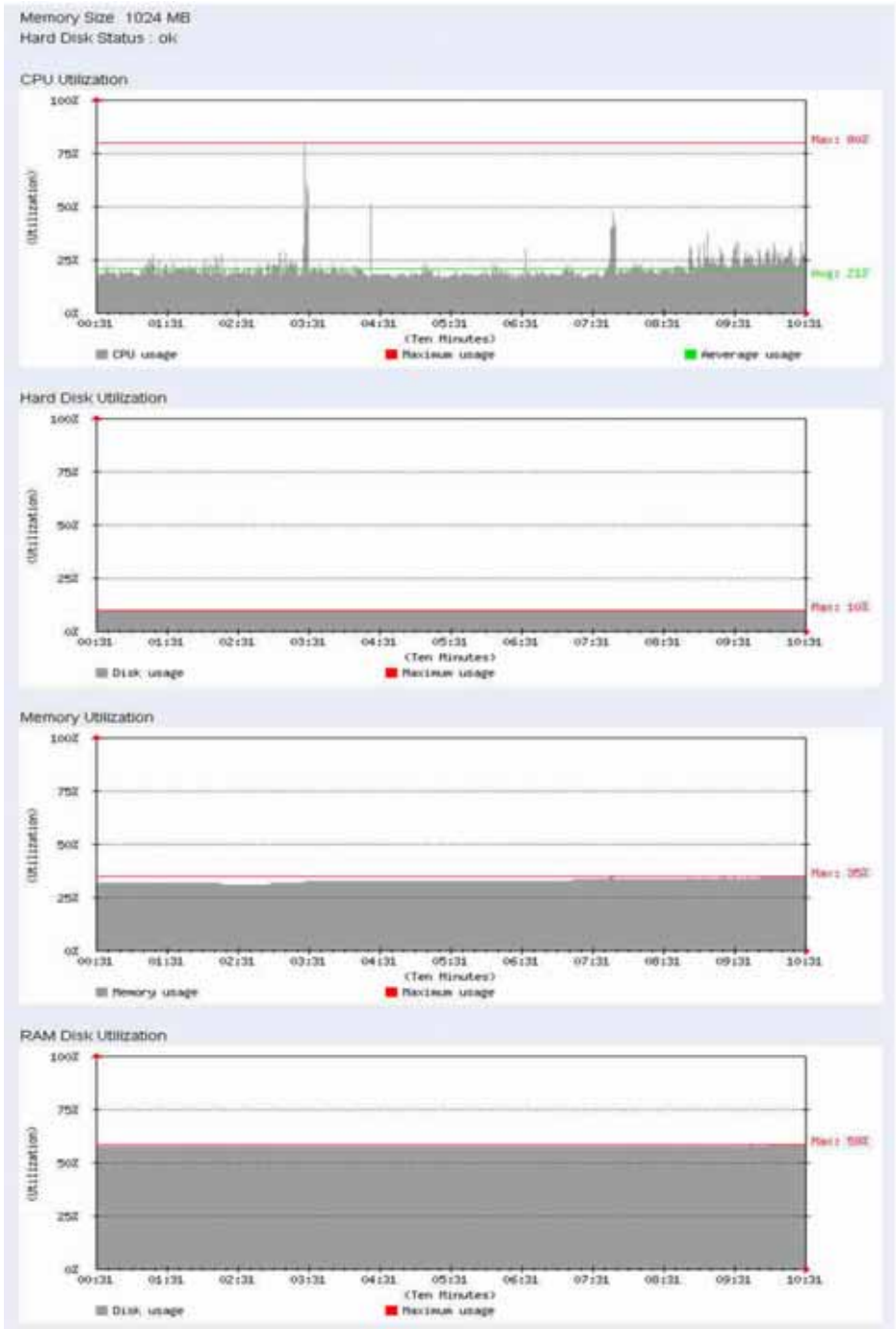
	LAN	WAN1	WAN2	DMZ
Forwarding Mode	NAT	Static IP	Static IP	Transparent
WAN Connection	---			---
DnS / UpS Kbps	---	100000 / 100000	100000 / 100000	---
DnStream Alloca.	---	0%	100%	---
UpStream Alloca.	---	50%	49%	---
PPPoE Con. Time	---	---	---	---
MAC Address				
IP Address	192.168.189.1	61.11.11.11	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 .



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
192.168.139.30	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

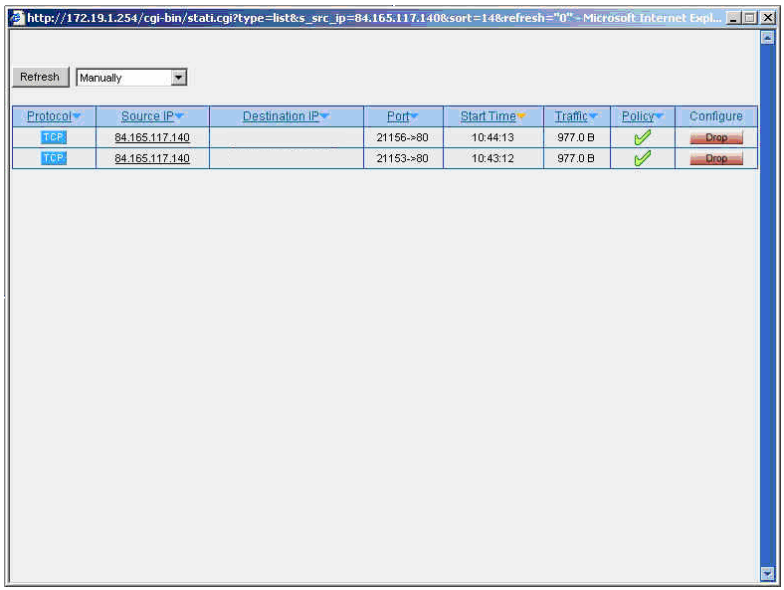
Step1 **Status → ARP Table** , it shows the information of Net BIOS name , IP address , MAC address and interface .

- **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 staistics by user's IP , host name or domain name to access the network resources of pop up window.



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