Neteyes

NexusWay 800 Series

User Manual

Firmware version: 3.0

Revised Edition (June 2005)

Printed In Taiwan

RECYCLABLE

Copyright

Trademarks

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this user's guide, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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

CE Mark Warning:

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

Warnung!

Dies ist ein Produkt der Klasse A. Im Wohnbereich kann dieses Produkt Funkstoerungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Massnahmen zu ergreifen.

Precaución!

Este es un producto de Clase A. En un entorno doméstico, puede causar interferencias de radio, en cuyo case, puede requerirse al usuario para que adopte las medidas adecuadas.

Attention!

Ceci est un produit de classe A. Dans un environnement domestique, ce produit pourrait causer des interférences radio, auquel cas l`utilisateur devrait prendre les mesures adéquates.

Attenzione!

Il presente prodotto appartiene alla classe A. Se utilizzato in ambiente domestico il prodotto può causare interferenze radio, nel cui caso è possibile che l`utente debba assumere provvedimenti adeguati.

Table of Contents

CHAP 1. INTRODUCTION

1-1. Overview

Thank you for purchasing the NexusWay 800. With a simple installation process and Web interface, you can easily enjoy a better networking environment. Simply connect several ISP lines to the NexusWay 800, and the product will construct a more reliable network environment automatically by avoiding the squandering of surplus network resources and bypassing component problems. In addition, the NexusWay 800 can also integrate the bandwidth of multiple linked WAN connections to greatly improve the usage efficiency for enterprise networks. This manual provides necessary information for the NexusWay 800 hardware device, software instruction/settings and configuration parameters.

1-2. What's inside the Product

Verify the following components are included into your product package:

- **One NexusWay 800 Hardware Device**
- **One AC Power Cable**
- **One CD for NexusWay 800**
- **One Quick Installation Guide for NexusWay 800**

1-3. External Components

A. Front Panel

There is 1 console port, 2 LAN ports, and 4 WAN ports available on the front panel of the NexusWay 800.

1. ***Console Port：***

Connect a PC to this port using a cross-over cable to and communicate using terminal emulation software (such as hyper terminal on Windows).

2. LAN 1 Internal Port：

Connect a PC, a hub, or a switch to this port. Both 10BaseT and 100BaseT connections can be used.

3. LAN 2 Internal Port：

Connect a PC, a hub, or a switch to this port. Both 10BaseT and 100BaseT connections can be used.

4. WAN 1 External Port：

Connect the primary broadband modem here.

5. WAN 2 External Port：

Connect a second broadband modem here, if available.

6. WAN 3 External Port：

Connect a third broadband modem here, if available.

7. WAN 4 External Port：

Connect a fourth broadband modem here, if available.

8. Indicators：

The indicators on the front panel show the Power status for the system, and a 10/100 link indicator for: LAN1, LAN2, WAN1, WAN2, WAN3 and WAN4. The Power indicator will show an orange light when the power is on. For the 10/100 indicators, when the transmission rate reaches 10 MB, the indicator will be lightless. When 100 MB is reached, you will see a green light. Every ports indicator has two LED lights, which are "LINK" and "ACT". The green LINK light will light up to indicate a successful connection when the cable endpoint is properly plugged in. The ACT light, will flash when data is transmitted through the port.

B. Rear Panel

1. Power Input：

Plug in the supplied power cable.

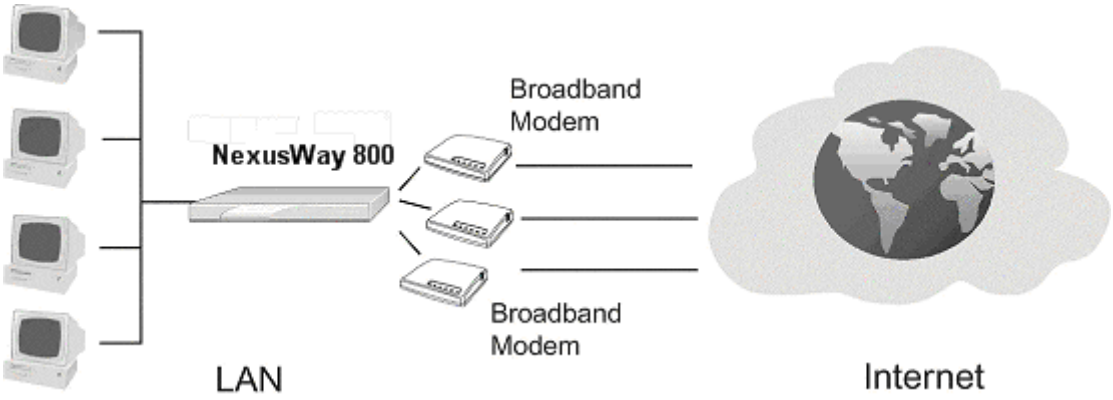
2. Power Switch：

To turn on NexusWay 800, switch to “I”; to turn off NexusWay 800, switch to “o”.

1-4. Specification

- System：Intel X86 Series
- CF：16 MB
- Chipset：Intel LAN Chip
- WAN：4 x shield RJ 45 for 10/100 MB Ethernet (Auto)
- LAN：2 x shield RJ 45 for 10/100 MB Ethernet (Auto)
- Console Port：1 COM Port (RS-232, DB-9 Connector)
- Dimensions：24x 4.5x 42.6 CM
- Certification：CE, FCC

1-5. Main Features



■ Supports Load Balancing for up to 32 XDSL/Leased Line (DHCP)

The NexusWay 800 can integrate 32 external links and integrate them into a single enterprise intranet for mutual backup, load balancing, and increasing the network's overall performance efficiency.

■ Supports Outbound/Inbound Load Balancing

The NexusWay 800 provides Load Balancing for both Outbound connections (internal users connecting to external servers) and Inbound connections (external users accessing your Web site's or servers). Administrators can setup various load balancing modes for different bandwidth usage requirements and service types to achieve optimum bandwidth and network quality by properly distributing traffic to each leased line.

■ Supports NAT and DHCP of LAN

NAT (Network Address Translation) provides an IP address translation function, efficiently separating an intranet from the external network. The DHCP Client Table can send out real-time IP address information used by PC clients on network.

■ Multiple Load Balancing Modes

Administrators can setup proper load balancing modes based on usage requirements to improve network performance efficiency by distributing traffic over multiple connections.

■ Supports PPPoE

For connections, like a XDSL, that require an account name and password, the NexusWay 800's built-in PPPoE dialup software allows you to integrate that line by simply entering the account information and password.

■ Supports SNMP

The NexusWay 800's built-in SNMP (Simple Network Management Protocol) can retrieve information on network nodes independently for the purpose of monitoring and managing network traffic.

■ Supports Multi-Link

The NexusWay 800 can maximize the external bandwidth provided by multiple ISP's by allowing multiple concurrent connections to ISP's on a single WAN Port through a Hub or Switch.

Multi-Link Feature, when used with xDSL or Cable modems, requires "Proxy ARP" features to be deactivated.

■ High Availability

The NexusWay 800 supports a backup mechanism for high availability. If one NexusWay 800 system fails unexpectedly, the backup will become active instantaneously, to continuing load balancing operations ensuring continual smooth network traffic.

■ Supports Web Management Interface

A simple and easy to use Web management interface allows you to use the NexusWay 800 easily without complex operation steps or advanced knowledge of network management. You can also change the NexusWay 800 configurations via remote connection management from any computer connected to the LAN.

■ Support VPN Trunk

Please note the VPN Trunk support is not applicable for the NexusWay 800. Only NexusWay 805, 815, 825, and 835 support this function, transmitting data accurately and rapidly to the destination with the integrated bandwidth of multiple ports.

CHAP 2. INSTALLATION

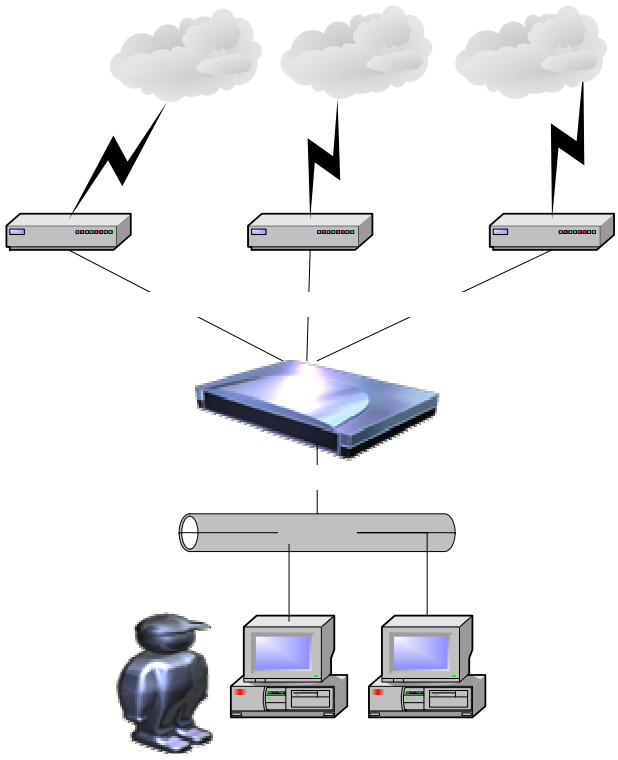
2-1. Prerequisites

- **1 - 32 DSL, Leased Lines, and an Internet Access Account provided by an internet service provider (ISP).**

  Multi-Link Feature, when used with xDSL or Cable modems, requires “Proxy ARP” features to be deactivated.

- **Standard 10/100Base T network (UTP) cable with RJ45 connectors.**
- **TCP/IP network protocol installed PC’s which connect to the NexusWay 800.**

See the following diagram for network connection example.



2-2. Procedure

1. Ensure NexusWay 800 is powered OFF.

Ensure that NexusWay 800 is turned OFF before starting the installation procedure.

2. WAN port connection

Connect a DSL Modem to the NexusWay 800's WAN port with standard Ethernet CAT5 cable or network cable supplied with the modem. If you are using only one DSL or cable modem connection, please connect it to WAN 1 port.

NOTE:

- **If your WAN Modem is connected to a firewall or a router, please locate the NexusWay 800 between the WAN and the firewall or router by connecting the NexusWay 800's LAN port to the devices.**

3. LAN port connection

Connect to a switch or hub with a 10BaseT/100BaseT cable before connecting to a PC. If you connect PC to NexusWay 800 directly, please use a cross-over cable.

NOTE:

- **Do not connect the NexusWay 800's LAN ports to an uplink port on a switch, router, or hub as the crossover function performed by this action is already integrated into the system.**

4. Startup

Power on other devices such as a DSL Modem/ Router/ or Firewall.
Connect the supplied power adapter to the NexusWay 800, and switch the power on. The power indicator should light up immediately.

5. Check LED status

The Power Indicator will light up after the NexusWay 800 is switched on. When a WAN port is connected or a LAN port is connected the corresponding indicators will light up in green.

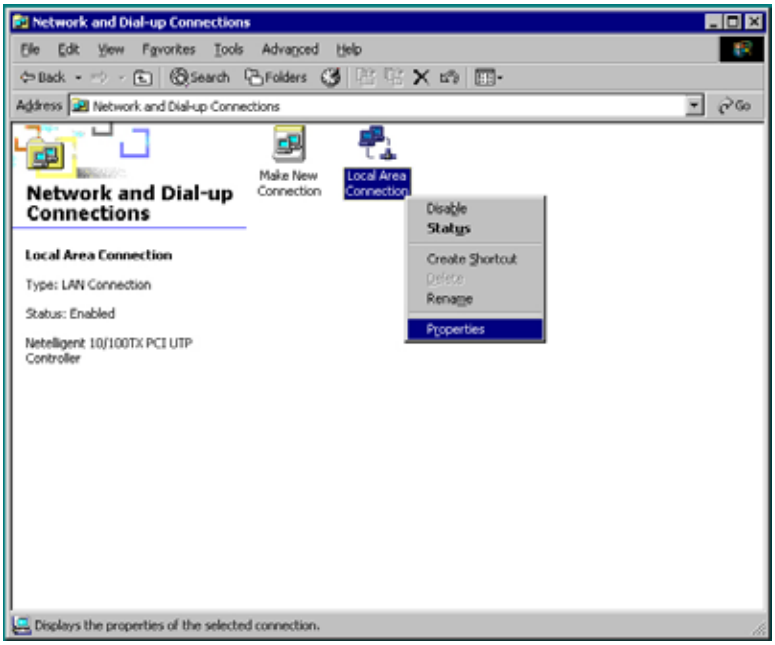
Each WAN and LAN ports has two LED indicators lights. The lower green LINK light will light up with a successful physical connection. The upper ACT light, will flash while data is transmitting through the port. For detailed information, please see Section A. in 1-3 External Components.

6. Configure administrator's IP address

After successfully connecting to the NexusWay 800, you must establish the link between an administrator's PC and the NexusWay 800 for further network configuration. Select one PC as an administrator and change its TCP/IP settings to place it in the same network segment as the NexusWay 800's default segment. To set administrator's IP to “192.168.0.X / 255.255.255.0”, please follow the steps below.

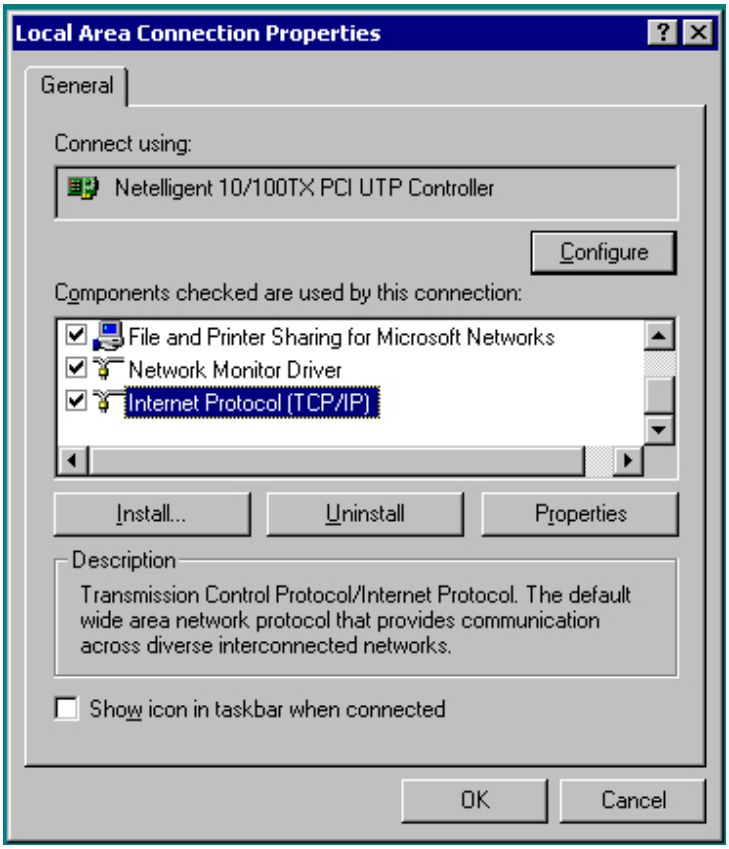
STEP 1

Select **Control Panel** - **Network and Dial-up Connections**, and click **Properties.**



STEP 2

Select the TCP/IP component of the NIC (Network Interface Card) and click **Properties**.



STEP 3

Set up IP the address as 192.168.0.X and subnet mask as 255.255.255.0, where "X" can be any number from 0~255. For example, you can enter "192.168.0.10.

Please do not use "192.168.0.1" which is the default IP address of the NexusWay 800.

Note: What is Administrator?

- **An Administrator is the user with the authority to install the NexusWay 800 in the Local Area Network environment, and to configure the NexusWay 800. Administrator can not only configure the LAN, WAN, Server and DHCP settings on the WEB management interface, but can modify the Load Balancing mode according to the requirement's of every unit, or segment, and the company's bandwidth policies.**

2-3. Configure PCs on your LAN

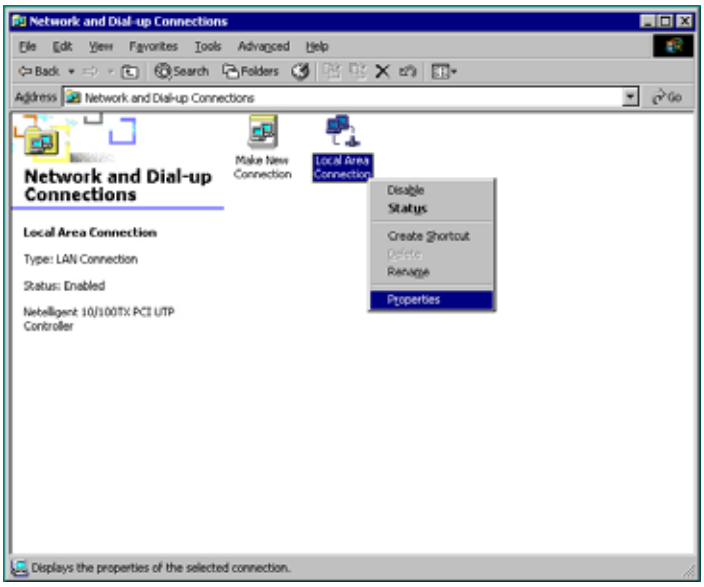
With the default Windows 95/98/ME/2000/XP configuration, no changes are required. After booting/ rebooting the PC, the NexusWay 800 will act as a DHCP Server, automatically providing a suitable dynamic IP address (and related information) to each PC. Ensure the PCs on your LAN are DHCP clients and check their TCP/IP setup according to section 2-3-1. To reserve LAN IP address for Host PC's or servers, see information about DHCP in section 4-1-4, 4-1-5 and 4-1-6 in this documentation.

2-3-1 Check TCP/IP Setup

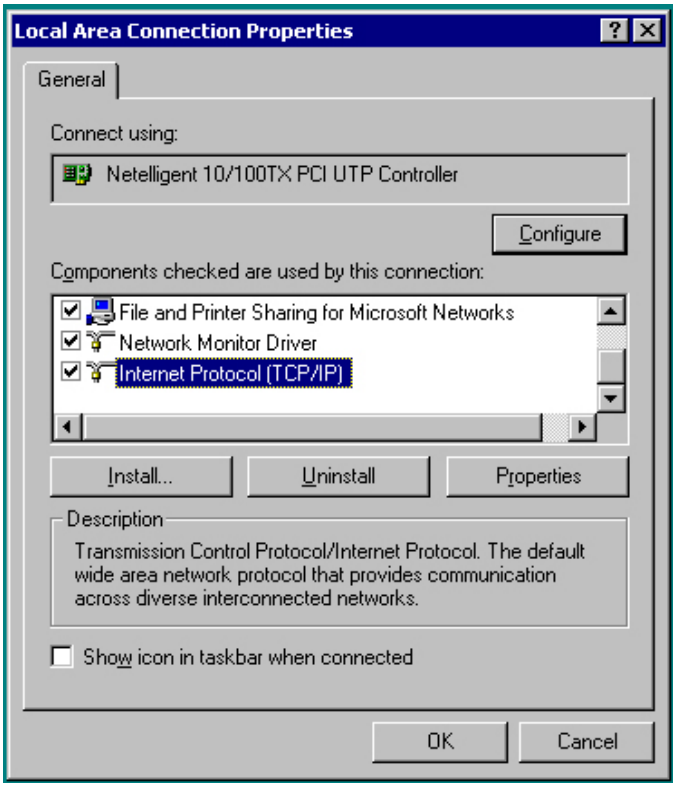
Pc's can use either Static or Dynamic IP address, however PC's requiring either type should be initially set to "Obtain an IP address automatically". If a dynamic address is acceptable (unless behaving as a server this should have no detrimental effect) follow the instructions in the following diagrams. If a static address is required follow the diagrams on the next page, then see section 4-1-4, and 4-1-6 for system settings to maintain a static address through the integrated DHCP server.

2-3-1-a. Windows 98

1. Select **Control Panel** - **Network and Dial-up Connections**, and click **Properties**.



2. Select TCP/IP protocol for your network adapter, and click **Properties**.



3. Select "**Obtain an IP address automatically**".

NOTE:

- **Windows 98 users are strongly recommended to reboot PCs after changing the TCP/IP Setup.**

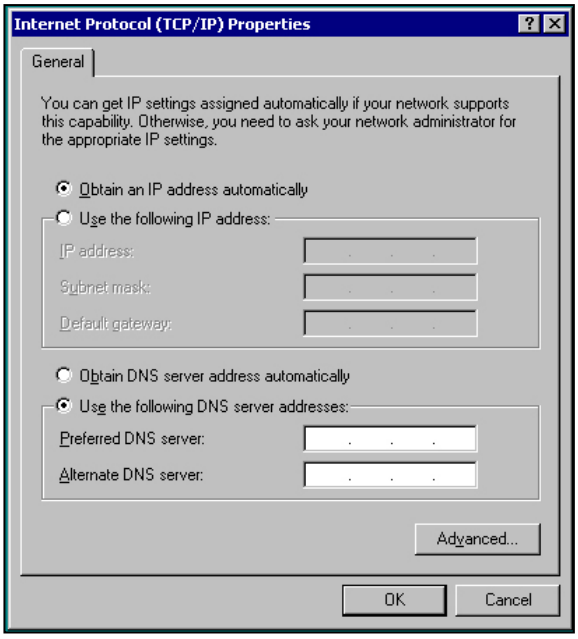
2-4-1-b. Windows 2000

1. Select **Start Menu** - **Setup** - **Control Panel** - **Network and Dial-up Connections - Local Area Connection**.

2. Select **Properties**.

3. Select TCP/IP protocol for your network adapter, click **Properties**.

4. Select "**Obtain an IP address automatically**".



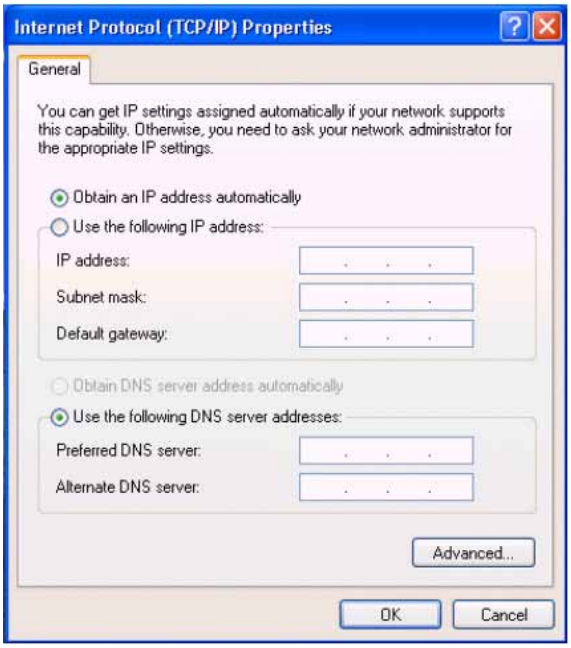
2-4-1-c. Windows XP

1. Select **Start Menu** – **Control Panel** - **Network Connections**.

2. Right click the **Local Area Connection** icon and select **Properties**.

3. Select TCP/IP protocol for your network adapter, click **Properties**.

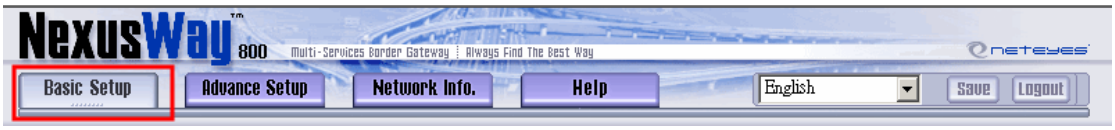
4. Select **Obtain an IP address automatically**.



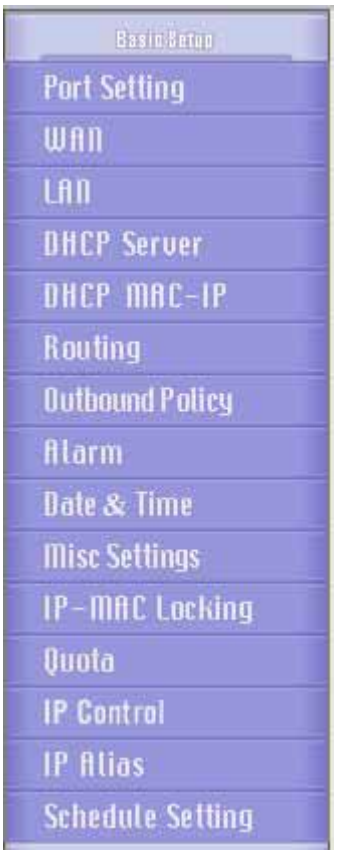
CHAP 3. FUNCTION INSTRUCTIONS

When entering the Web management interface of the NexusWay 800 (for how to login into the interface, see Chapter 4.), you'll find the following main options on top of the screen, which are Basic Setup, Advance Setup, Network Info. and Help. Please note that the instructions in this documentation are sorted according to the options in the Web interface from left to right, top to bottom.

3-1. Basic Setup



This option includes the settings for the following basic functions. Read the instructions and find solutions that best meet your requirement before starting any setup procedures for the NexusWay 800.



■ Port setting

There are 6 ports (2 for LAN and 4 for WAN) on the front panel of the NexusWay 800. This option is designed for you to configure general settings for all the ports you want to use, including media type, maximum transmission unit (MTU), and MAC address. You can modify detailed settings in WAN and LAN options after completing the basic settings in this option. For more setting information, see section 4-1-1.

■ WAN

4 WAN Ports, which provide external connections, are available in the front panel of the NexusWay 800. You can setup each for one of the different supported connection types (Static IP, PPPoE and Dynamic IP). With these settings, the NexusWay 800 will be a router with multi-WAN connection to the Internet. For more setting information, see section 4-1-2.

■ LAN

This option allows you to setup the IP address of the NexusWay 800 in your LAN, and turn the NexusWay 800 into a Gateway for other PC's external connections. For more setting information, see section 4-1-3.

■ DHCP Server

The NexusWay 800 provides a DHCP service to assign dynamic IP address to internal PCs (DHCP clients) or other devices on the network. With dynamic address, a device may have different IP addresses every time it connects to the network. You can enable or disable the DHCP service and set-up other configurations with this option. For more setting information, see section 4-1-4.

■ DHCP MAC - IP

This MAC-IP Mapping function will reserve particular IP addresses for the PCs you set so that they can dynamically receive the same IP address every time. In other words, fixed IP address will be assigned to fixed MAC address (i.e. PC). The PC user can then provide a fixed IP address to other people and applications. For more setting information, see section 4-1-6.

■ Routing

Routing is the action of moving information across a network from source to destination. You can set the route for the transmission from each IP address/Netmask, to a designated server. For more information about static/dynamic route and setup, see section 4-1-7.

■ Outbound Policy

You can set up load balancing modes provided by the NexusWay 800 according to ISP bandwidth, user's requirements for outbound traffic distribution, and to avoid overloading a single connection. For more setting information, see section 4-1-9.

■ Alarm

With this function, the system will send out the email notifications about network disconnection and reconnection to a specified email address. For more information, see section 4-1-10.

■ Date & Time

You can change the system date and time with this option. After being set, the NexusWay 800 will automatically receive the time information from a network time server and set the system clock accurately. For more information, see section 4-1-11.

■ Miscellaneous Settings

This option allows you to specify timeout values in seconds for TCP, UDP, and all other protocols. For more information, see section 4-1-12.

■ IP-MAC Locking

This function is usually used in dormitory network where Internet connection is limited. This function allows you to decide which PC(s) can or can not access the network. For more setting information, see section 4-1-13.

■ Quota

You can specify daily traffic volume limitation either download, upload, or total for any one IP address with this function. Once the machine exceeds any of the traffic quotas, all further traffic to or from the IP will be denied. For more setting information, see section 4-1-14.

■ IP Control

You can specify real time traffic volume limitations for any IP address with this function. Traffic beyond this limit will be denied or throttled. For more setting information, see section 4-1-15.

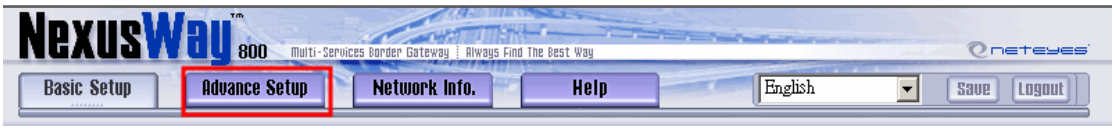
■ IP Alias

The NexusWay 800 added this function for you to designate an alias name for an IP address allowing quicker setting in other options and to simplify identification. After naming the IP address, you can select the alias name by clicking the “IP Alias” button located by columns that need to an IP Address entered. For more setting information, see section 4-1-16.

■ Schedule Setting

This function allows you to specify when you want to activate/deactivate settings. You can set multiple schedules either weekly or applied only once. For more information, see section 4-1-17.

3-2. Advance Settings



Advance Setup allows you to configure some advanced functions for more efficient usage. Read the instructions and find solutions that best meet your requirement before starting any setup procedures for the NexusWay 800.

■ IP Mapping

This function allows you to map external IP addresses to the internal virtual IP addresses of PCs inside your LAN. All service requirements for external IP or network services will be transmitted to the virtual internal IP address. It is recommended to use this function ONLY when you have the firewall activated. For more setting information, see section 4-2-1.

■ Port Mapping

You can customize the virtual server by setting an internal virtual IP and port to correspond to an external IP and port. Mapping the virtual IP address and ports with external IP address and ports accomplishes NAT (Network Address Translation) functions; if certain internal PCs serve as a server for network services. NAT functions can separate an internal network from the external network and help ensure the security of internal network. For more setting information, see section 4-2-2.

■ Server Cluster

Server cluster allows several internal servers to map to one external IP for data transmission speed enhancement. The transmission reliability can be increased since each server application can failover to other servers. Additional advantages include scalability, high availability, and easier network management. For more setting information, see section 4-2-3.

■ SNMP

SNMP (Simple Network Management Protocol) is a set of protocols for managing complex networks. SNMP is performing by sending PDUs (Protocol Data Unit) to different parts of a network. SNMP-compliant devices will store data about themselves in Management Information Bases (MIB) and return this data to SNMP requesters. You can enable or disable this SNMP function. For more setting information, see section 4-2-4.

■ Advanced Feature

This function allows you to backup all the configuration settings in the NexusWay 800. You can save and restore configuration settings, so that you do not need to reconfigure everything after restoring the hardware if some unexpected situation occurs. You can also have the system revert to the original factory settings, download an updated firmware release from the Neteyes Web site, update configurations settings from previously exported file, and enable automatic firmware updates. For more setting information, see section 4-2-5.

■ QoS (Quality of Service)

The NexusWay 800's QoS feature provides traffic shaping, and maximal bandwidth to specific services, by specifying throughput levels for applications. For more setting information, see section 4-2-6.

■ Firewall

Along with the QoS, the Firewall is also to improve Internet service quality. However, the firewall is designed to increase security by denying unexpected access. All the traffic entering or leaving the intranet will be examined by the firewall, which blocks data meeting none of the specified security criteria. For more setting information, see section 4-2-7.

■ DNS Setting

DNS (Domain Name System/Service) associates IP addresses with domain names. In addition, you can set multiple MX records for a host, allowing the mail to automatically flow to backup systems when the primary systems are unreachable. For more information, see section 4-2-8.

■ DDNS

The Dynamic DNS feature assigns a fixed hostname to your ISP-assigned dynamic IP address, making your computer accessible from any location on the Internet without knowing your current IP address. The NexusWay 800 supports 11 different Dynamic DNS services. For more setting information, see section 4-2-9.

Inbound Policy

In this option, you can setup the inbound load balancing algorithms causing the inbound traffic to be distributed across multiple Internet connections according to the algorithm you select. The NexusWay 800 will process outside users linking to your Website and load balance by active DNS and Port/IP Mapping, according to each WAN connections Line flow. For more setting information, see section 4-2-10.

NetFlow

The NexusWay 800 can export network traffic information, in flows, to an external machine that runs a NetFlow application and can collect NetFlow data for processing. For more setting information, see section 4-2-11.

Cache

You can enable a built-in Web Proxy server and a Transparent Proxy in this option. Proxy servers are used to improve performance and filter requests while a transparent proxy allows client to not change any network settings before having traffic flow through the proxy. For more information about the Web proxy server and the transparent proxy, see section 4-2-12.

URL Filter

This function allows you to prohibit internal users from viewing certain URL's for security or confidentiality considerations. For more setting information, see section 4-2-13.

High Availability

This function allows you to manage configurations for a dual device setup. Configurations can be transferred between machines, and the machines selected mode configured. For more setting information, see section 4-2-14.

3-3 VPN Setup (Not applicable in NexusWay 800)

Please note that this function is only available on the NexusWay 805, 815, 825, and 835.

VPN Setup allows you to setup the functions about the IKE Policy, VPN Policy, PPTP Server, and Certification Authority. Read the instructions and find a solution that meets your requirement best before starting to perform any setup procedures for the NexusWay 800.

■ IKE Policy

In this option, you can configure settings to exchange keys that are used when creating a VPN. Please note that Main Mode is about three times slower than Aggressive Mode, due to additional key generation steps, but is more secure. For more setting information, see section 4-3-1.

■ VPN Policy

A Virtual Private Network (VPN) is used to provide secure, encrypted communication between a network and a remote host over the public Internet. VPNs allow the establishment of an encrypted "tunnel" that protects the network traffic flow from eavesdroppers. It enables a specific group of users to access private network data and resources securely over the Internet or other networks. Please note that settings in this option must match with remote VPN settings. For more setting information, see section 4-3-2.

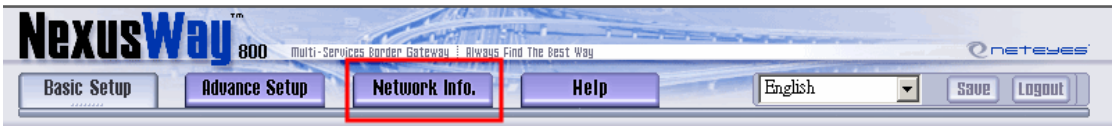
■ PPTP Server

The NexusWay 800's PPTP Server allows connections from PPTP clients. You must enter the users that can access your VPN. For more setting information, see section 4-3-3.

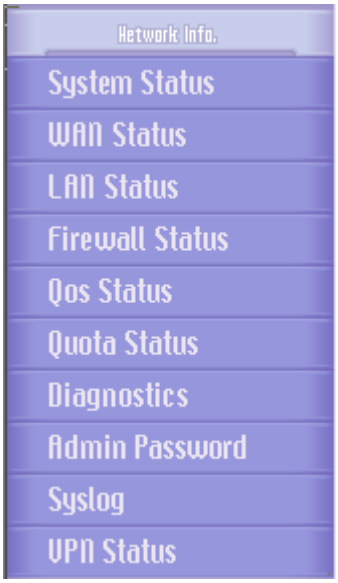
■ Certification Authority

This option is about functions related to the generation and signing of x509 certificates. These certificates are used in place of pre-shared keys while setting up IKE policies. CA (Certificate Authority) authentication is typically used in large organizations with an internal CA server. Using CA certificates reduces the amount of data entry required by each VPN endpoint. For more information, see section 4-3-4.

3-4. Network Info.



Network Info. shows all the settings you saved in previous options. You can check your NexusWay 800 configurations in this option. All the information will be updated automatically after you finish setup process.



■ System Status

This option shows the current status and settings of the system and each Internet connection in detail, including current system CPU, Memory's Utilization and Average Load status, WAN Information, LAN Information and Device Information with current loader version and firmware version information. You can also view the statistic graphics of current status for CPU, Free Memory and Loading. For more information, see section 4-4-1.

■ WAN Status

WAN Status shows Real-time information about all of the Internet connections. The Percentage data is updated every few seconds to present the ratio of current figure and specified maximum. You can also view the details information of NAT and the statistic graphics of traffic and packet analysis for each port. For more information, see section 4-4-2.

■ LAN Status

This option shows the current DHCP configuration settings you saved in previous steps. For more information, see section 4-4-3.

■ Firewall Status

This option shows the current Firewall configuration settings you saved in previous steps. For more information, see section 4-4-4.

■ QoS Status

This option displays the current QoS configuration settings you saved in previous steps. For more information, see section 4-4-5.

■ Quota Status

This option displays the Quota configuration settings you saved in previous steps. For more setting information, see section 4-4-6.

■ Diagnostics

This option allows the administrator to perform a variety of diagnostic checks. There are three diagnostic tools available, which are ping, traceroute, and nslookup, for you to check IP address' and status of connections. For more information, see section 4-4-7.

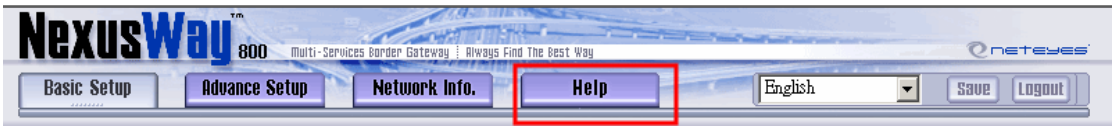
■ Admin Password

This option allows you add and remove administrators for your NexusWay 800. You can also restrict the administrator to login only from a specified IP address. Each administrator may have either both read and write access, or read only access. For more setting information, see section 4-4-8.

■ Syslog

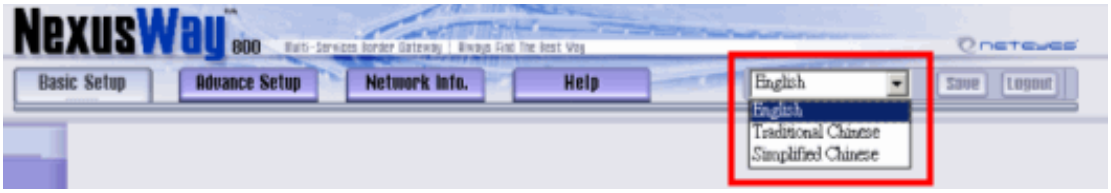
This option allows the administrator to export syslog messages to external machines, which have a syslog client installed. In the "Syslog Server List", you can see logs concerning changes and events of NexusWay 800. Administrators and internal functions of the NexusWay 800 generate Syslog events. You can see more detailed syslog messages by exporting the messages to a client machine. For more setting information, see section 4-4-9.

3-5. Help



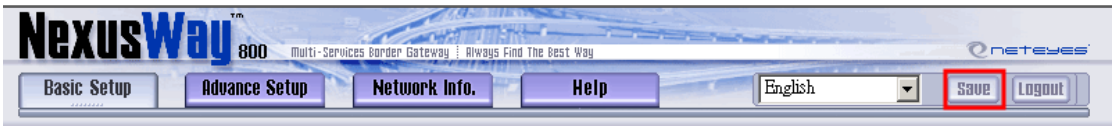
If you have any trouble, problem and need help while configuring, click Help button or the question mark  on right top of the screen for online help and detailed information.

3-6. Pull-Down Language List



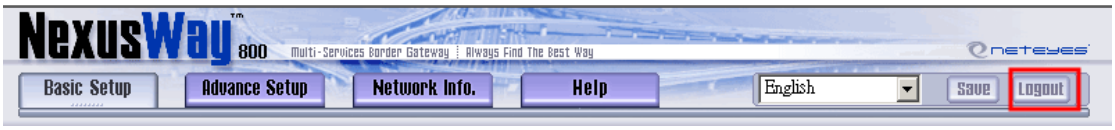
Next to Help button, you will see a pull-down language list. You can choose to view the web interface in your language. Currently, the only option available in NexusWay 800 Web interface is English.

3-7. Save



After entering all the data required on an page, please click Save button to save configurations and make your modifications effective. Please note that all the settings and information will be lost when you change the page if you have not clicked the Save button first.

3-8. Logout



Click the Logout button (next to the Save button) to logout before closing the Web interface of the NexusWay 800 to prevent others from using your account after you leave; remember to close your browser to ensure your are logged off.

CHAP 4. CONFIGURATION

Any Administrator can now configure the NexusWay 800 using a current version of any browser i.e. “Internet Explorer 6”. These configurations serve to further enhance the networking environment provided by the NexusWay 800. Once all the hardware is properly connected, and one machine is configured as detailed in section 2-2, follow the steps below to begin configuring the NexusWay800:

- **STEP 1**

Open the secure administrative Web interface by entering the NexusWay 800’s IP address (by default this is **https://192.168.0.1**) in the Address Bar on the browser to login NexusWay 800.

- **STEP 2**

The dialogue box below will be displayed. Enter “**admin**” as User Name and "**123456**" as Password, which is the default administrator user ID and password.

NOTE：

- **Recommended screen resolution: at least 800X600.**
- **You must use "https://", not "http://" when connecting to the NexusWay 800’s administrative Web interface.**
- **If you can not connect to the administrative Web interface, ping "192.168.0.1" using diagnostic commands on your computer to ensure the network is working normally.**

4-1. Basic Setup

4-1-1. Port setting

Port 1 ~ 2 represent the LAN Ports while Port 3 ~ 6 represent the WAN Ports. Complete the settings accordingly and respectively for each port:

Media Type

There are three modes for Media type: Auto Select, 100BaseTX and 10BaseT/UTP. Select the proper mode. If you are not sure about the media type, leave it as Auto Select.

MTU

This field is for you to define the Maximum Transmission Unit, the largest physical package size (in bytes) from 72 to 1500. Enter proper numeric value based on actual usage and your requirements. The default value is 1500.

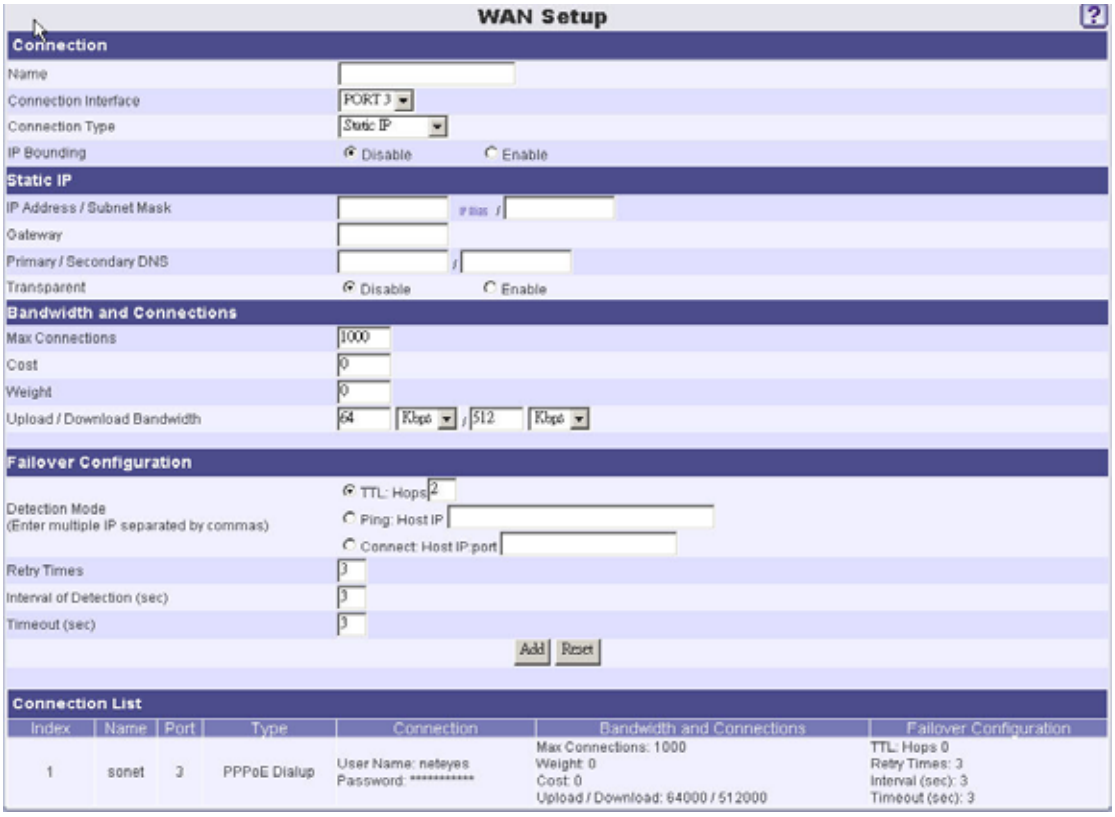
MAC Address

MAC Address (the Network Interface Card's physical Address) is not required to be setup in general, unless your ISP requires a registered MAC address to connect.

NOTE：

- **The system will detect your MAC address automatically when you click the "Clone My MAC Address" button.**

4-1-2 WAN Setup



Enter the data related to your XDSL / Leased-Line access as provided by your ISP according to the connection type being used. 4 WAN Ports, which provide external connection, are available in the NexusWay 800. **To setup one or more connections, complete all the settings in this page for one WAN connection interface whose corresponding port in the rear side of the product has external connection, and click the Add button then you can continue to input another connection.** Repeat the process until the settings for EACH connected WAN interface are completed. With these settings, the NexusWay 800 will be a router with a multi-WAN connecting to the Internet. For detailed instruction about these settings, see the following sections.

4-1-2-a. Connection

Connection	
Name	
Connection Interface	PORT 3
Connection Type	Static IP
IP Bounding	Disable Enable

Name

You can give a name to the WAN connection setting for easy management and identification.

Connection Interface

Select the WAN port (Port 3 ~ 6) you want to configure in the drop-down list before changing any settings. Verify the selected interface has an external connection in the corresponding port on the front side of the system.

Connection Type

The supported connection types for WAN include Static IP, PPPoE Dialup, Dynamic IP and PPTP. Contact your ISP provider for more information about Web connection type, IP address, DNS or other information before completing the following configurations based on various connection modes. A change applied to this field, will result in a change of the following field, to the selected connection type.

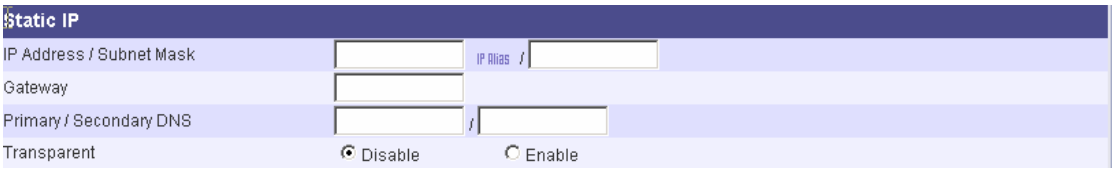
NAT

This function allows a choice of deactivating Network Address Translation for the selected wan port. When disabled the NexusWay 800 can only send packets through the configured link using it as a router, rather than a gateway.

- **Requirements for Multi-Link**

Multi-Link Feature, when used with xDSL or Cable modems, requires "Proxy ARP" features to be deactivated in each modem.

4-1-2-b. Static IP



Select this mode if you have a static connection and your ISP provides static IP(s). Fill in your IP address, subnet, gateway, and primary/secondary DNS servers. All the fields are required except the secondary DNS field. The Transparent function only applies to Static IP.

- **IP address：163.200.200.250 (as provided by ISP)**
- **Subnet Mask：255.255.255.0 (as provided by ISP)**
- **Gateway：163.200.200.254 (as provided by ISP)**
- **Primary DNS：168.95.1.1 (as provided by ISP)**
- **Secondary DNS：168.95.1.2 (as provided by ISP)**

4-1-2-c. PPPoE Dialup

PPPoE Dialup	
User Name	
Password	

A user name and password will be provided by ISP if PPPoE Dialup mode is used as the Connection Type. If this is the type of connection provided enter the User Name and the Password in the corresponding field.

4-1-2-d. Dynamic IP

Dynamic IP	
Hostname	

For Dynamic IP mode, you only need to fill in the Hostname. You can either enter a name or leave it blank.

4-1-2-e. PPTP

PPTP		
IP Address / Subnet Mask		IP Alias /
Server IP Address		
User Name		
Password		

Fill out each field with the information provided to you by your ISP. PPTP is only available from ISPs in the Europe and US region.

4-1-2-f. Bandwidth and Connections

Bandwidth and Connections					
Max Connections	1000				
Cost	0				
Weight	0				
Upload / Download Bandwidth	64	Kbps	/	512	Kbps

Complete the settings in this option for the connection type you just selected. The traffic flow is distributed based on one of these four settings to achieve a balanced traffic load.

Max Connections

The maximum number of allowed connections (default value 1000.)

Cost

The value you enter here will be a used as a basis for calculation when the balance mode "Link Cost" is activate (see 4-1-9 section). New traffic will be directed to the WAN with the lowest cost. For example, if the relative cost of WAN 1 and WAN 2 is 1:3, enter "1" in the Cost column for WAN 1 and “3” for WAN 2. When you select Link Cost in Balance Mode column, system will give priority to WAN 1 for traffic flow. If your link cost is not charged by data flow amount, you can ignore this field.

Weight

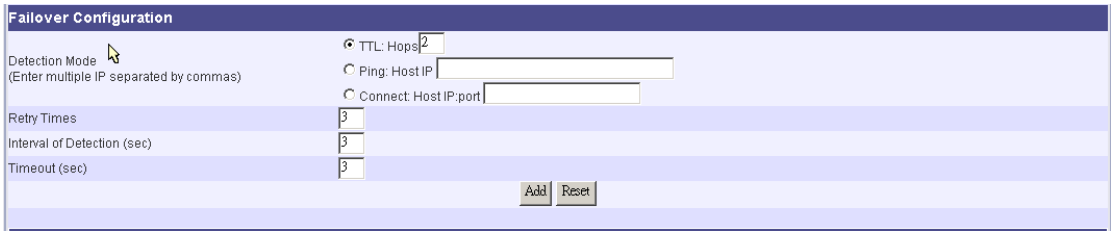
Set the load ratio of traffic in this column. For example, if the ratio of bandwidth between WAN 1 and WAN 2 is 1:3, enter "1" in the Weight column for WAN 1 and “3” for WAN 2. Traffic will then be distributed to the leased lines according to this radio.

Upload / Download Bandwidth

Enter the maximum allowed bandwidth of the line you selected. "Upload" means upload speed while "Download" means download speed. For example, for an ADSL with a two way speed of 512K, enter "512" in both "Upload" and "Download" columns in "Kbps."

You are recommended to enter the exact same maximum allowed bandwidth as it is provided by your ISP. If you set it too high, the WAN will be detected as not being fully utilized and the system will then direct more network traffic the flow to it, which may cause a WAN jam.

4-1-2-g. Failover Configuration



The automatic disconnect detection mechanism is activated when NexusWay 800 connects to a WAN. Administrators will receive the warning if the WAN is disconnected. You can set up the detection policies here to reduce the possibility of erroneous judgment. This configuration is available for every connection that is setup.

TTL: Hops

You can choose "TTL: Hops" to trace a network node (router) and to detect network disconnections by "Traceroute". Enter the number of node you want to detect, before assuming failure.

Ping: Host IP

You can also determine if the network is working normally by Pinging an IP address. Ensure the host you want to ping to test for network connection detection is open and enter its IP addresses in the Host IP column.

Connect: Host IP: port

If pinging is not supported by the remote computer system, enter IP address and port number of the host you want to connect.

Retry Times

Enter the number of continuous retry attempts when Host IP or TTL address is detected as not responding. This means, that if you set this to 3 times; when the Host IP or TTL address is detected as not responding for more than three attempts, the system will determine the line is disconnected.

Interval of Detection (sec)

Enter the interval time in seconds for contacting IP addresses or checking TTLs.

Timeout (sec)

Enter the time in seconds the IP, Host IP or TTL must response within. If the response time is over the set value, the system will determine this line is not responding.

NOTE：

- **Click the Save button on right top corner of the panel after you finish entering all the data on this page － otherwise you will immediately lose all the settings when exiting the page.**

- **Click Add to add the settings into the Connection List, or click Reset to clear the settings and enter them again.**

4-1-2-h. Connection List

Connection List

Index	Name	WAN	Type	Connection	Bandwidth and Connections	Failover Configuration
1	NetEyes Leaseline	1	Static IP	IP: 202.160.87.15 Subnet Mask: 255.255.255.192 Gateway: 202.160.87.1 Primary DNS: 168.95.1.1 Secondary DNS: 168.95.192.1	Max Connections: 10000 Weight: 9 Cost: 1 Upload / Download: 512000 / 512000	TTL: Hops 4 Retry Times: 5 Interval (sec): 5 Timeout (sec): 5
2	Backup Leaseline	2	Static IP	IP: 202.160.81.42 Subnet Mask: 255.255.255.248 Gateway: 202.160.81.46 Primary DNS: 168.95.1.1 Secondary DNS: 168.95.192.1	Max Connections: 1000 Weight: 1 Cost: 10 Upload / Download: 512000 / 512000	TTL: Hops 4 Retry Times: 5 Interval (sec): 5 Timeout (sec): 5

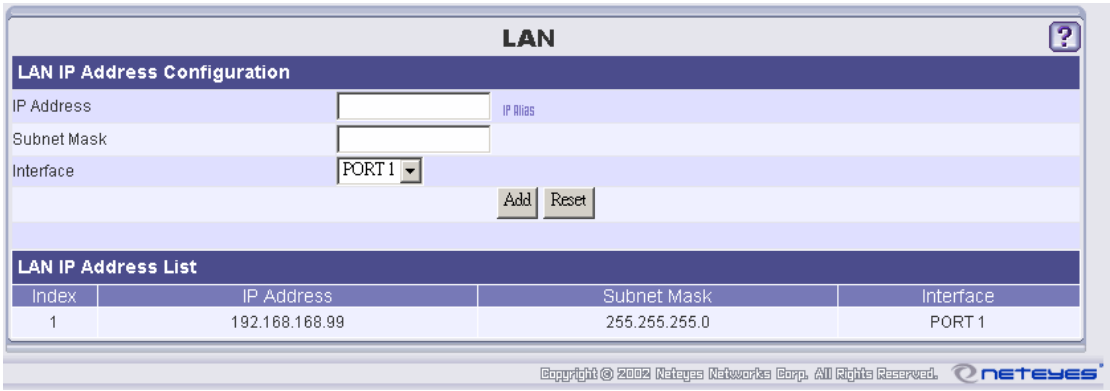
Connection List

Index	Name	WAN	Type	Connection
1	vlan5			IP: 192.168.5.1 Subnet Mask: 255.255.255.0 ay: 192.168.5.250 y DNS: 192.168.5.1
2	vlan6			2.168.6.1 t Mask: 255.255.255.0 ay: 192.168.6.250 y DNS: 192.168.6.1

Menu
Move Up
Move Down
Edit
Delete
Enable / Disable

All WAN connection settings will be listed in this. To delete a setting, right click on it and select Delete. You can also move, edit, enable or disable the setting by right clicking.

4-1-3 LAN Setup



You can setup the IP address of the NexusWay 800 in your LAN with this page, making the NexusWay 800 a Gateway for other PCs external connection's. The default value for this option is recommended. To change the settings, complete the following steps.

4-1-3-a. LAN IP Configuration

IP address

You can enter the IP address of NexusWay 800 in this column. Default IP "192.168.0.1" is recommended to be the IP address of NexusWay 800 in LAN unless it is already in use or your LAN is using a different IP address range. In this case, you can enter an unused IP address from the range used by your LAN.

Subnet Mask

The Subnet Mask is a mask used to determine what subnet an IP address belongs to. A subnet is a portion of a network that shares a common address component. For example, the address "255.255.255.0" is a standard value for small (class C) network. In other networks, use the Subnet Mask for the LAN segment to which the NexusWay 800 is attached (the same value as the PCs on that LAN segment). The subnet mask of default LAN IP "192.68.0.1" is "255.255.255.0". If you use a different subdomain you must ensure that the subnet mask used on the NexusWay 800 is the same.

Interface

Select the LAN port to be configured in the drop-down list.

NOTE：

- **Click the Save button on right top corner of the panel after you finish entering all the data on this page － otherwise you will immediately lose all the settings when exiting the page.**

- **Click Add to add the settings into the LAN IP List, or click Reset to clear the settings and enter them again.**

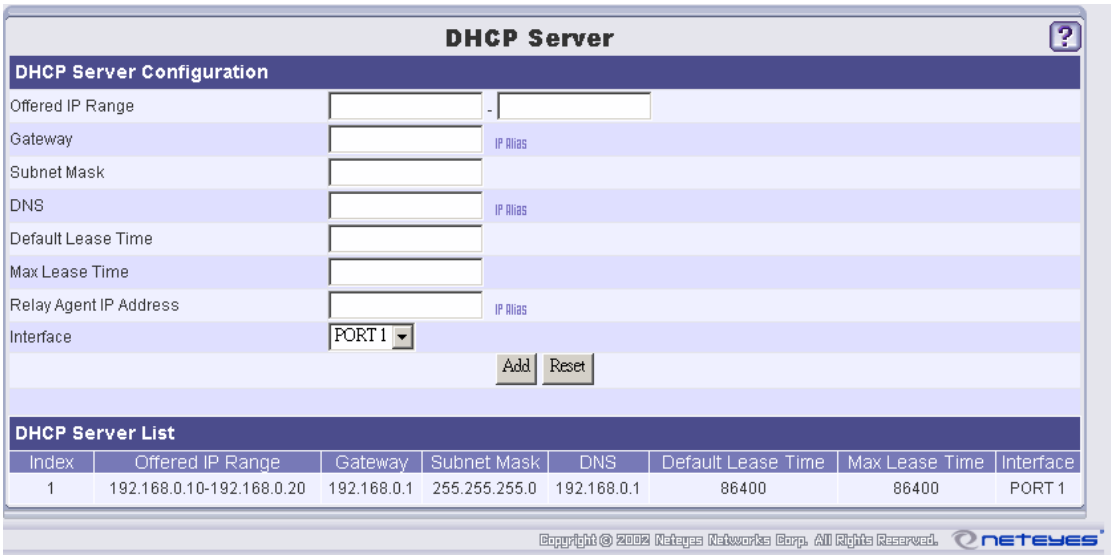
4-1-3-b. LAN IP List

LAN IP Address List

Index	IP Address	Subnet Mask	Interface
1	192.168.168.99	255.255.255.0	PORT 1

All LAN connection settings will be listed in this table. To delete a LAN connection, right click it and select Delete. You can also move, edit, enable or disable the LAN connection by right clicking.

4-1-4 DHCP Server



DHCP (Dynamic Host Configuration Protocol) is a protocol for dynamically assigning IP addresses to devices on a network. With dynamic addresses, a device may have different IP addresses every time it connects to the network.

The NexusWay 800 provides a DHCP service to assign IP address to internal PCs. You can enable or disable DHCP service and set-up other configurations with this option.

Enabling the DHCP server allows the NexusWay 800 to assign IP addresses to internal PCs (DHCP clients) or other devices on the network (by default with Windows Systems, DHCP clients can get the IP address automatically from the server). If you have already a DHCP server in your internal network, do not configure this feature for LAN Ports.

Offered IP Range

Enter an IP Address Range to be assigned by the NexusWay 800's DHCP server with the first IP in the left column and last one in the right column to activate the service. The entered IP range, which also determines the number of supported DHCP clients, must match up with your LAN's subnet.

Gateway

Enter a default gateway IP address. This IP must be one of the LAN IP's of the NexusWay 800.

Subnet Mask

The default subnet mask address of your LAN must be entered in this column.

DNS

The IP address of DNS Server to be used.

Default Lease Time

This is the Periodical IP address release time in seconds with recommended default value 86400 (24 hours.) The IP address will be released after using for the lease time you set. Please note that zero (0) is not allowed in this column.

Max Lease Time

This is the maximum IP lease time in seconds with recommended default value 86400 (24 hours). The maximum time in seconds you want the system to hold the DHCP address. Please note that zero (0) is not allowed in this column.

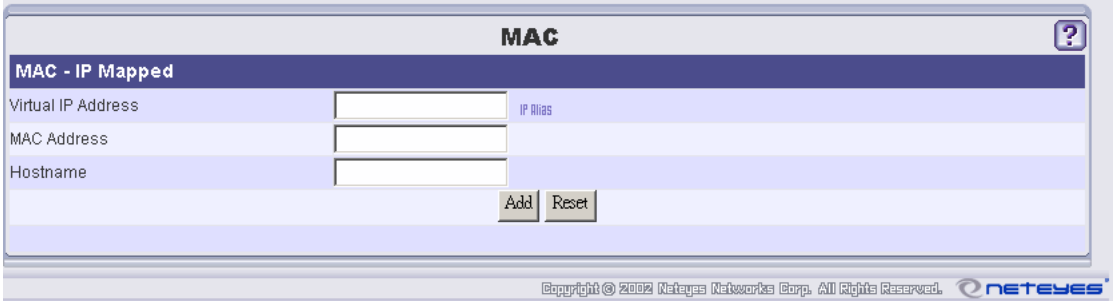
Interface

Select the LAN port you want to configure this DHCP server for.

NOTE：

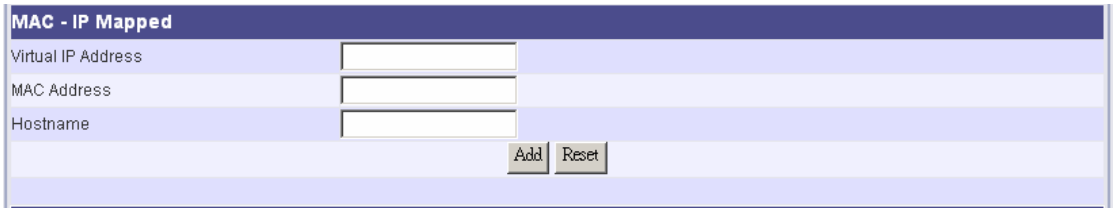
- **Click the Save button on right top corner of the panel after you finish entering all the data on this page － otherwise you will immediately lose all the settings when exiting the page.**

4-1-6 DHCP MAC-IP



The DHCP server will continuously assign IP addresses to the PCs on LAN. If you want a certain PC on LAN to use a fixed IP address, you can specify an IP address to map with a specific MAC address of particular PC. This MAC-IP Mapping function will reserve particular IP addresses for the PCs you set so that they can dynamically receive the same IP address every time. In other words, fixed IP address will be assigned to fixed MAC address (i.e. PC). The PC user can then provide a fixed IP address to other people and applications.

4-1-6-a. MAC–IP Mapped



Virtual IP Address

Enter a virtual IP address you want to assign to certain MAC address.

MAC Address

MAC Address is also called Physical Address or Network Adapter Address. Enter the MAC address of a host PC to which you want to assign above IP address.

The format of a MAC address should be "aa:bb:cc:dd:ee:ff" using the characters 0~9 and a~f.

Hostname

Give a name to the combination (MAC - virtual IP address) you just set.

NOTE：

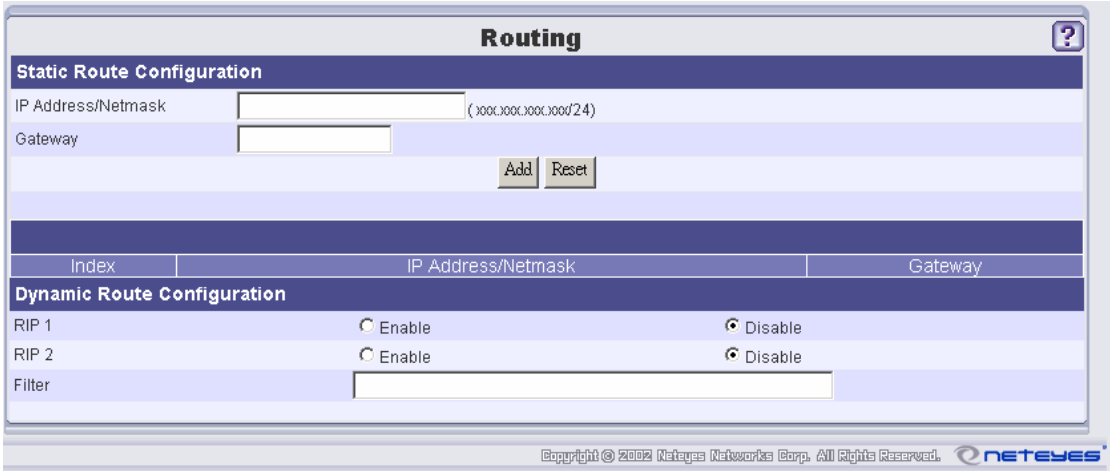
- **Click the Save button on right top corner of the panel after you finish entering all the data on this page － otherwise you will immediately lose all the settings when exiting the page.**

- **Click Add to add the settings into the following MAC – IP Mapped List, or click Reset to clear the settings and enter them again.**

4-1-6-b. MAC - IP Mapped List

All Mac-IP Mappings you set will be listed and sorted in this table. To delete a mapping, right click on it and select Delete. You can also move, edit, enable or disable the mapping by right clicking.

4-1-7 Routing



Routing is the action of directing the movement of information across a network from a source to a destination.

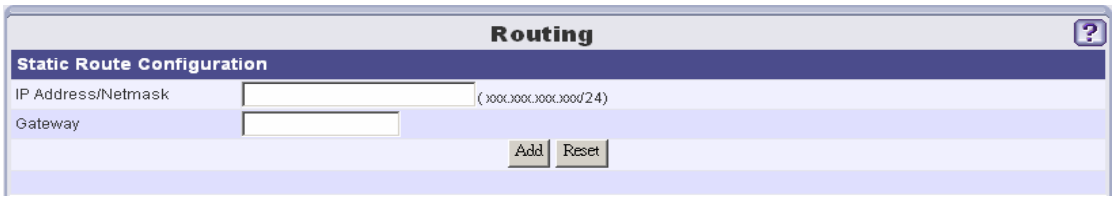
NOTE：

- **Click the Save button on right top corner of the panel after you finish entering all the data on this page － otherwise you will immediately lose all the settings when exiting the page.**

- **Click Add to add the settings into the list, or click Reset to clear the settings and enter them again.**

After adding new routes, a list will be displayed. You will see the routes in this table. To delete a route, right click on it and select Delete. You can also move, edit, enable or disable a route by right clicking.

4-1-7-a. Static Route Configuration



A Static Route can be used to integrate and utilize devices that are connected with the NexusWay 800, such as another firewall, or router.

IP Address/ Netmask

Enter the IP address and subnet mask of the static route.

Gateway

Enter the IP address of the gateway with which the NexusWay 800 needs to connect. The gateway could be any device connected with the NexusWay 800, such as a router or a firewall.

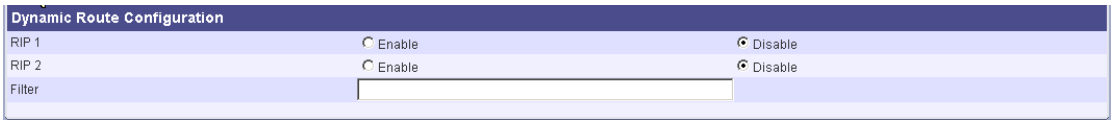
NOTE：

- **Click the Save button on right top corner of the panel after you finish entering all the data on this page － otherwise you will immediately lose all the settings when exiting the page.**

- **Click Add to add the settings into the list, or click Reset to clear the settings and enter them again.**

- **Netmask Notes:**
  10.1.1.1/32 indicates that ONLY 10.1.1.1 will match.
  10.1.1.1/32 would be identical to 10.1.1.1 and 255.255.255.255
  10.1.2.1/24 indicates that any IP From 10.1.2.0 to 10.1.2.255 will match.
  10.1.2.1/24 would be identical to 10.1.2.1 and 255.255.255.0
  10.1.3.1/16 indicates that any IP from 10.1.3.1 to 10.1.255.255 will match.
  10.1.3.1/16 would be identical to 10.1.3.1 and 255.255.0.0
  10.1.4.1/8 indicates that any IP with "10" as the first (number) will match.
  10.1.4.1/8 would be identical to 10.1.4.1 and 255.0.0.0

4-1-7-b. Dynamic Route Configuration



Most routing algorithms are Dynamic Routing algorithms, which are adjusted to change network circumstances by analyzing incoming routing update messages. If the message indicates that a network change has occurred, the routing software recalculates routes and sends out new routing update messages. RIP1 and RIP2 (Routing Information Protocol) are both protocols that allow routers to exchange routing table information between each other. You can enable these settings to allow the NexusWay 800 to receive these routing table updates. To view the routing table, click "Network Info." button on top of the main page, and click "Diagnostics".

RIP 1/RIP 2

To enable NexusWay 800's RIP function and receive routing table updates, click Enable; to disable reception of routing updates, click Disable.

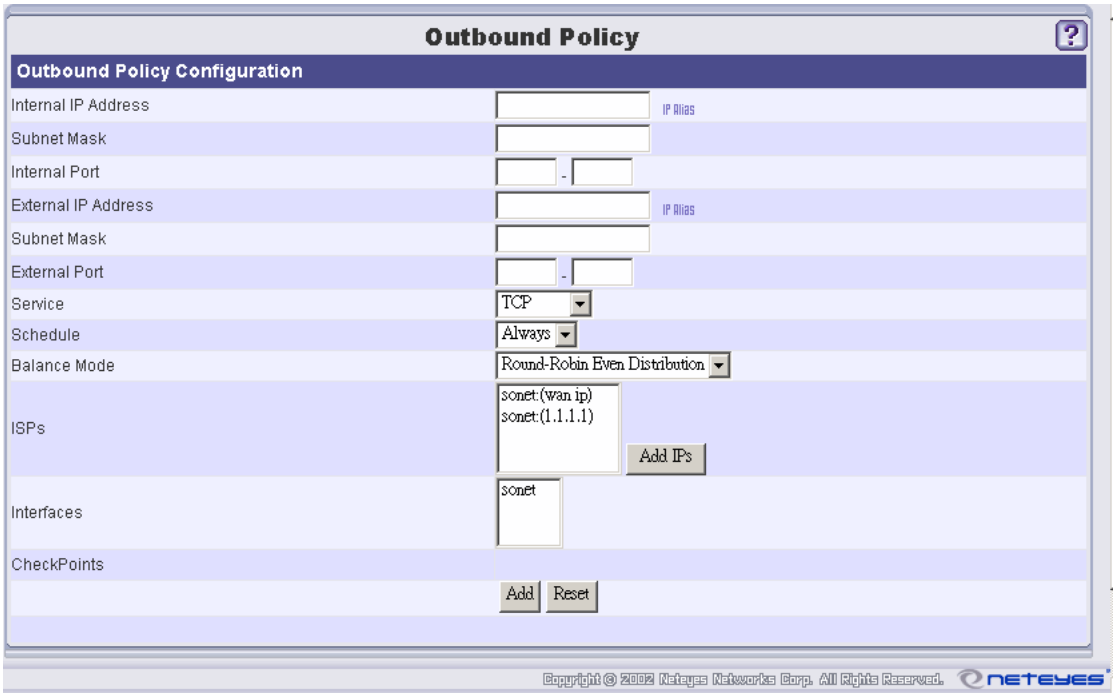
Enabled Interface

You can select which interfaces, by port number, are enabled to receive and act upon dynamic routing protocols.

NOTE：

- **Click the Save button on right top corner of the panel after you finish entering all the data on this page － otherwise you will immediately lose all the settings when exiting the page.**

4-1-9 Outbound Policy



The NexusWay 800 provides many load balancing modes (see the following table for details) for LAN users to connect external server from internal users (Outbound). You can set the load balance mode according to ISP bandwidth and user requirements to distribute network traffic and avoid overloading a single connection.

NexusWay 800 Load Balancing Modes

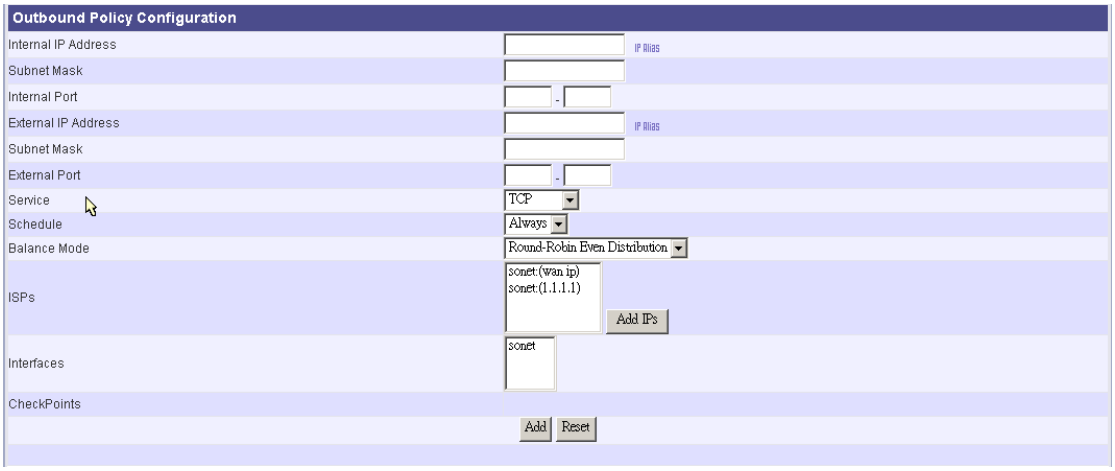
Load Balance Mode	Instruction
Round-Robin Even Distribution	Distribute network traffic evenly in turns WAN1, WAN2, WAN3… automatically.
Round-Robin by Weight	Same as above, but the lines with larger load ratings will receive more traffic (go to Weight option in section 4-1-2-f for setup).
Least Connections	Line with smallest number of connections has priority for new traffic (go to Max Connection option in section 4-1-2-f to configure).
Upload / Download / Total Traffic Based	The Line with lowest specific traffic ratio will have priority for new connections. (go to Bandwidth option in section 4-1-2-f to setup traffic options).
Session Based	Line with lowest number of Sessions gets priority for new connections. (See section 4-1-2-f to configure the maximum number of sessions).
Link Cost	Links with the lowest cost, as configured in section 4-1-2-f Wan Setup
ISP	If you don't desire any Load Balancing to be active, you can select a single configured WAN connection, or not configure any policies.

NOTE：

- **If a connection fails, other modes will be chosen automatically to complete the transfer.**

If the system is set to the Total Traffic mode mentioned above, for example, the system will detect the traffic on each of the four WAN connections and give the load to the one with lowest load ratio to ensure the Quality of Service (QoS). No overloading would occur on any single line while operating. In addition, on a connection that is usually used for a specific application, you can also limit the load balancing to specific service ports for traffic management optimization. For example, you can designate FTP connections, which require large file transmission most of the time, a specific load balancing mode for data transmission.

4-1-9-a. Outbound Policy Configuration



The Outbound Policies will be performed based on Balance Mode ONLY if each condition you select is fully matched. Policies are evaluated in a top to bottom fashion, so if a rule has a match at position two and position five position two will take precedence. Policies can be reordered or disabled after creation.

Internal IP Address

Enter the internal IP address to which you want to provide the load balancing (the start point of the outgoing traffic flow), such as **192.168.0.1.** (An asterisk "*" can be placed here to match any value)

Subnet Mask

Enter the internal IP subnet mask that you want to provide the load balancing to, such as 255.255.255.0 which represents whole Class C, or 255.255.255.255 which represents one IP.

Internal Port

Enter the internal port range to be set. The range must be numbers between 1 and 65535 (An asterisk "*" can be placed here to match any value).

External IP Address

Enter the external IP address to which you want to provide load balancing (the destination of the outgoing traffic flow). **For example: 168.95.1.1** (An asterisk "*" can be placed here to match any value)

Subnet Mask

Enter the external IP subnet mask to which you want to provide the load balancing, such as 255.255.255.0 which represents every Class C, and 255.255.255.255 which is a single IP.

External Port

Enter the external port range for the outbound policy. As with internal ports the numbers must be between 1 and 65535 (An asterisk "*" can be placed here to match any value)

Service

Select TCP, UDP, ICMP, IP or User Input in the pull-down list.

Schedule

Select a schedule to specify when you would like the policy to be active. To set the schedule, see 4-1-17. Schedule Setting.

Balance Mode

Select the load balancing mode to be used by this Policy according to your requirement or usage situation. If you do not select a specific load Balancing Mode, the system will automatically perform **Round-Robin Even Distribution** outbound load balancing for this rule.

ISP

This function allows you to select several ISPs for inclusion in this Balance Mode. You can select multiple ISPs by clicking "Add IPs", After that, a window will be displayed. Select one, and enter IP address. The options in the pull-down list are the connections set in the WAN option menu.

NOTE：

- **Please make sure to click the Save button in the upper right corner of the panel after you finish entering information on the page, or else all your changes will be lost when you change pages.**

- **Click Add to add the setting into the policy list, or click Reset to enter the data again.**

4-1-9-b. Outbound Policy List

Outbound Policy List

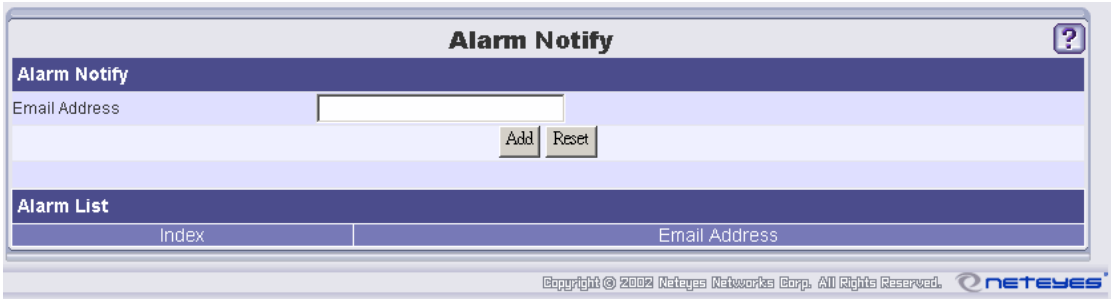
Index	Internal IP Address	Subnet Mask	Internal Port	External IP Address	Subnet Mask	External Port	Schedule	Balance Mode
Disabled	*	0.0.0.0	*	218.107.148.142	255.255.255.255	*	Always	ISP: NetEyes Leaseline
Disabled	*	0.0.0.0	*	10.0.0.160	255.255.255.240	*	Always	ISP: NetEyes Leaseline
3	*	0.0.0.0	*	*	0.0.0.0	*	Always	ISP: NetEyes Leaseline

All load balancing policies you set will be listed in this table. To delete a policy, right click on it and select Delete. You can also move, edit, enable or disable a policy by right clicking.

NOTE：

- **The asterisk (*) in this list means ALL. For example, the asterisk in Internal IP Address column means ALL internal IP addresses.**

4-1-10 Alarm Notify



This function allows the system to send out the email notifications for network disconnection and reconnection. Enter email addresses where you want to receive such notifications.

4-1-10-a. Alarm Notify

Email Address

Enter a maximum of 10 email addresses where you want the notifications to be sent.

NOTE：

- **Click Add to add the address into the following Alarm List, or click Reset to clear the address and enter it again.**

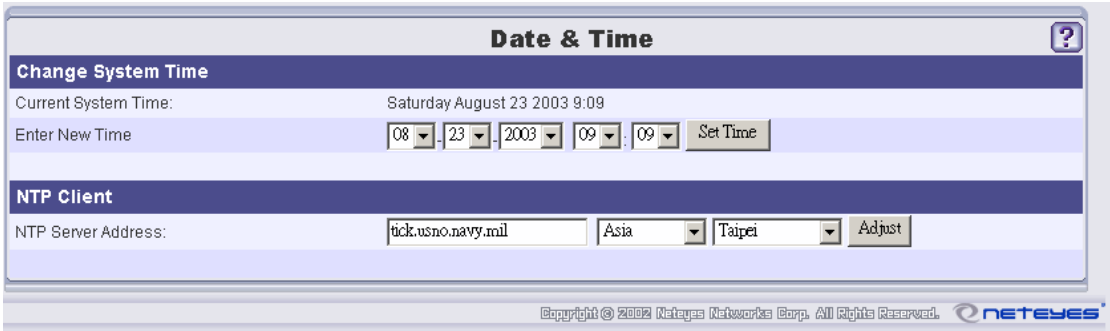
4-1-10-b Alarm List

All the email addresses you set will be listed in this table. To delete an address, right click on it and select Delete. You can also move, edit, enable or disable the address by right clicking.

NOTE：

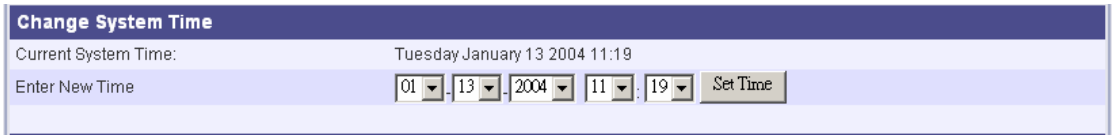
- **Click the Save button on right top corner of the panel after you finish entering all the data on this page － otherwise you will immediately lose all the settings when exiting the page.**

4-1-11 Date & Time



This option allows you to change the system date and time.

4-1-11-a. Change System Time



Current System Time

The NexusWay 800 system time at present.

Enter New Time

If the system time is incorrect, change the date and time in the format (Month-Day-Year) (Hour-Min) and click Set Time button. The new set system time will be displayed in Current System Time column.

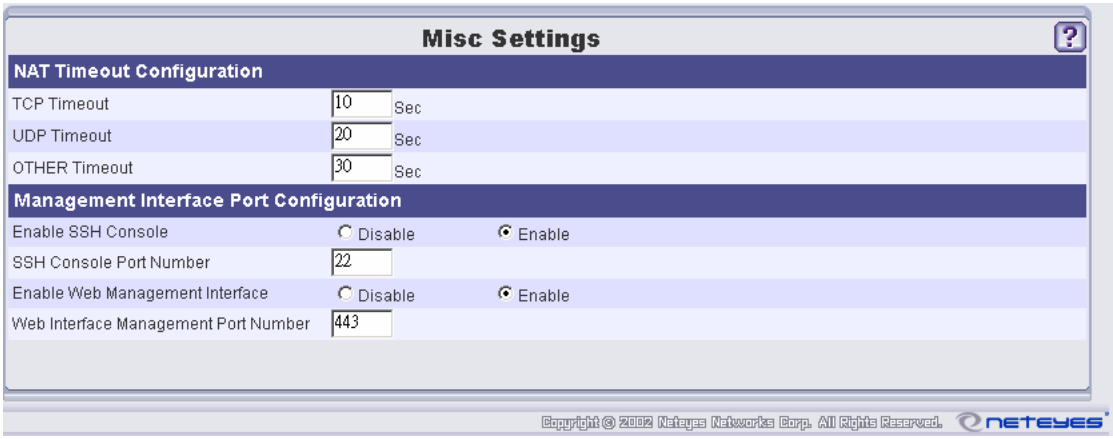
NOTE：

- **Click the Save button on right top corner of the panel after you finish entering all the data on this page － otherwise you will immediately lose all the settings when exiting the page.**

4-1-9-11 NTP Client

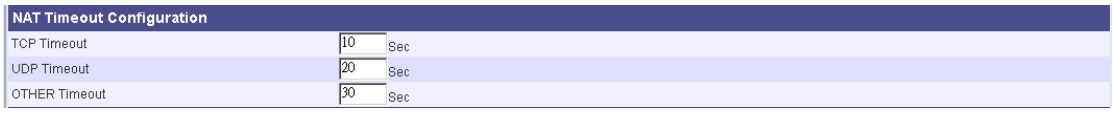
NTP (Network Time Protocol) is a client-server UDP protocol for time synchronization on IP networks. Enter a NTP server and select the region of your present location before clicking the Adjust button. The NexusWay 800 will automatically receive the time information from the server and set the system clock accurately.

4-1-12 Misc. Settings



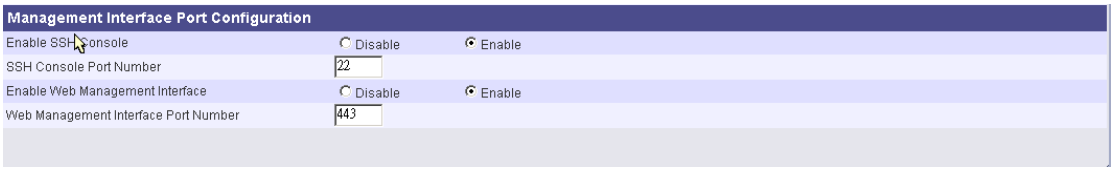
This option allows you to specify timeout values in seconds for TCP, UDP, and all other protocols.

4-1-12-a. NAT Timeout Configuration



Timeout values specify how long the NexusWay 800 will keep trying to send a packet. The maximum duration is 99999 seconds. If the timeout value is exceeded without receiving an ACK message, which indicates receipt of an uncorrupted packet, the packet will be dropped.

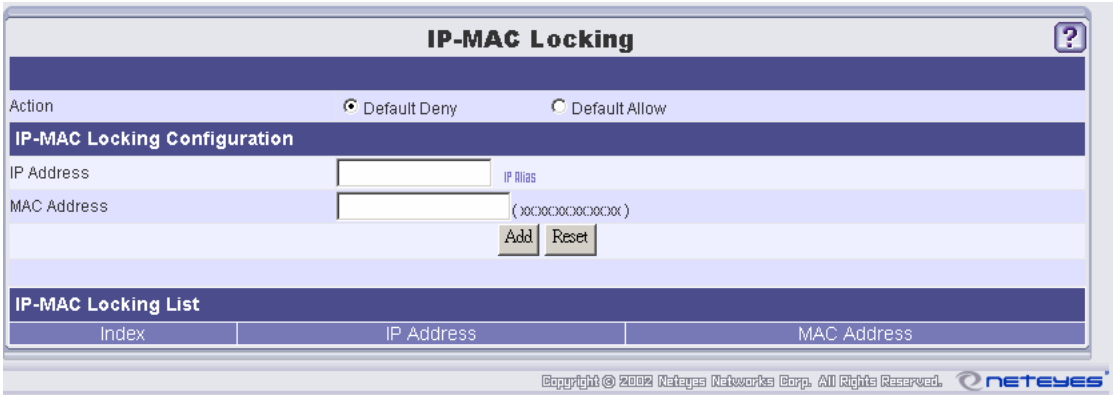
4-1-12-b. Management Interface Configuration



Enable Web Management Interface

It is are not recommended to disable the Web Management Interface unless you want to freeze the setting and let nobody, including yourself, change any settings via the web. When disabling the web or SSH interface, export the settings first. You can also modify the necessary parameters to connect to via the web. And while it is strongly discouraged you can also disable the console connection ability. For how to export the settings, see section 4-2-5.

4-1-13 IP-MAC Locking



This function is often used in dormitory network where Internet connection is limited.

When Default Deny is selected, all the connections are denied by default except the ones whose IP-MAC combinations have been setup with this option.

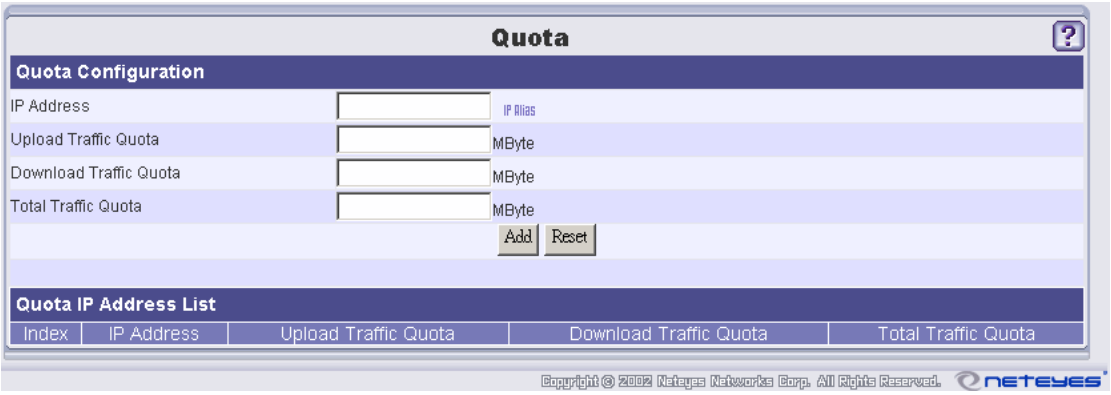
When Default Allow is selected, enter an IP and MAC address pair to lock together. If a user tries to connect using that IP from another MAC address, or uses that MAC address but a different IP, the connection will be denied. Connections will be allowed if both of the IP and MAC address match a single entry or neither match a single entry. Every connection matching exactly one condition of one rule will be dropped. You can also enter a * in the IP field and enter a MAC address. This will deny all connections using any IP from this MAC address. Any machines not matching any entries on the list will be allowed by default.

Please note that if you do not set the **IP Address** and **MAC Address**, these 2 options will be invalid.

NOTE：

- **Click Add to add the setting into the IP-MAC Locking List, or click Reset to clear the settings and enter them again.**

4-1-14 Quota



This function allows you to specify daily traffic volume limitation for any IP address and Netmask. After entering the IP Address, you can specify Upload, Download, and Total traffic limitations, in megabytes. Once any one of the 3 specified traffic quotas is exceeded all further traffic to or from the target will be denied. The traffic volume will be recalculated from 0 at midnight. If you wish to allow traffic to or from a computer that has exceeded its daily quota, you can disable the quota rule for that computer. To reset a quota, you must edit the rule to add the additional traffic allowance. Disabling and enabling a rule will not clear the daily traffic amount used by that machine.

NOTE：

- **Click Add to add the settings into the following Quota IP Address List, or click Reset to clear the settings and enter them again.**

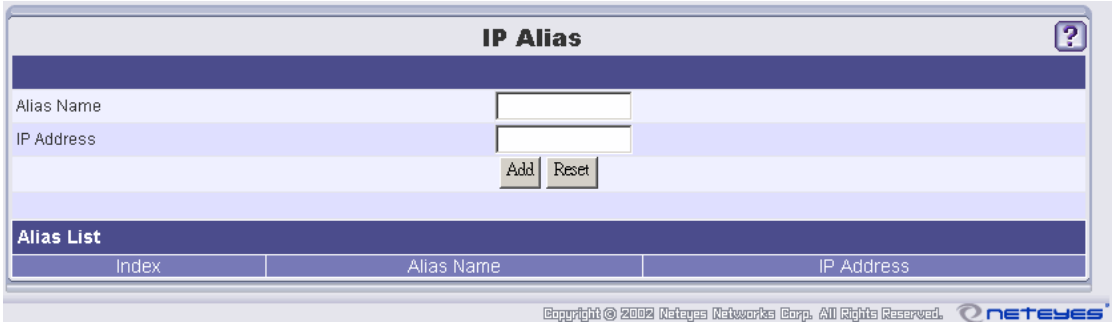
4-1-15 IP Control

This function allows you to shape traffic volume for any IP address and Netmask. After entering the IP Address information, you can specify Upload, Download, Total traffic, and connection limitations, in kilobytes per second. This is a feature designed to maintain a speed limit for the selected IP address and Netmask.

NOTE：

- **Click Add to add the settings into the following Quota IP Address List, or click Reset to clear the settings and enter them again.**

4-1-16 IP Alias



This function allows you to designate an alias name to an IP address, so that you can use the alias name for quick setting in other options and easy identification. After naming the IP address, you can select the alias name by clicking the “IP Alias” button located by the columns that need an IP Address entered.

Alias Name

Enter an alias name for an IP address.

IP Address

Enter an IP address to which you want to designate with the alias.

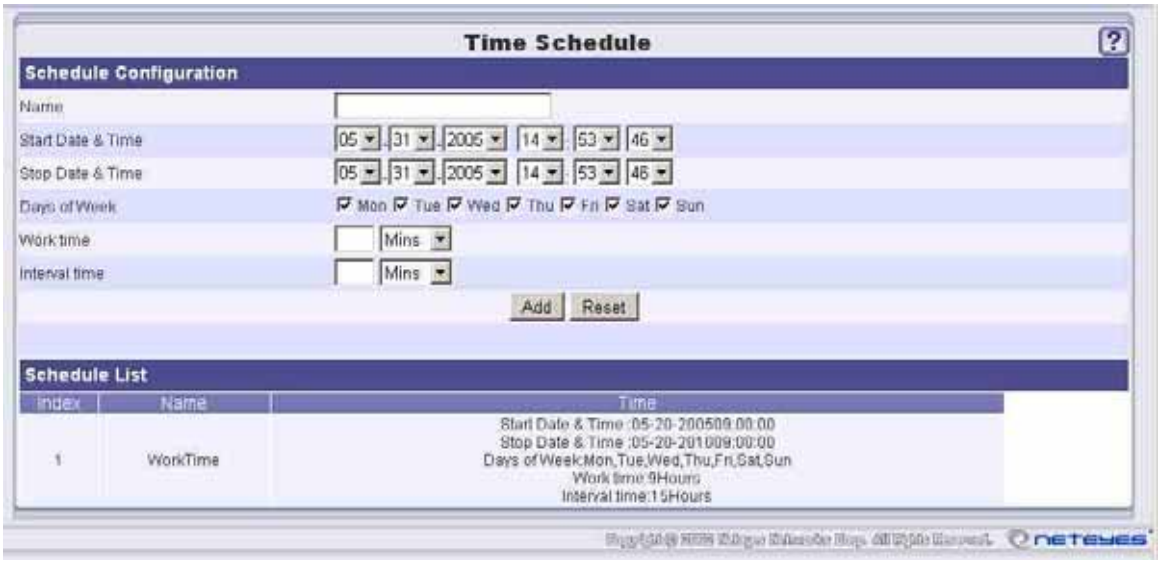
Alias List

All the alias’ will be listed in this table. To delete an alias, right click on it and select Delete. You can also move, edit, enable or disable the alias by right clicking.

NOTE：

- **Click Add to add the settings into the Alias List, or click Reset to clear the settings and enter them again.**

4-1-17 Schedule Setting



This option allows the NexusWay 800's functions to be active only for certain periods, which you specify in this page . For instance, you can define a schedule for "working hours," which are effective from 9am to 5pm on weekdays, and apply this schedule to your QoS rules to enable them only in these working hours. You can also relax your firewall rules on the weekends, or turn off the URL Filtering during off hours with this function.

Define a schedule with format "Month-Day-Year Hour-Min". The first selection is the beginning time for this schedule, and the second is the finish time. These times are intended to be large scale time frames, primarily encompassing weeks, months, or years. The check marks labeled with the days of the week allow you to choose which days are included in this schedule.

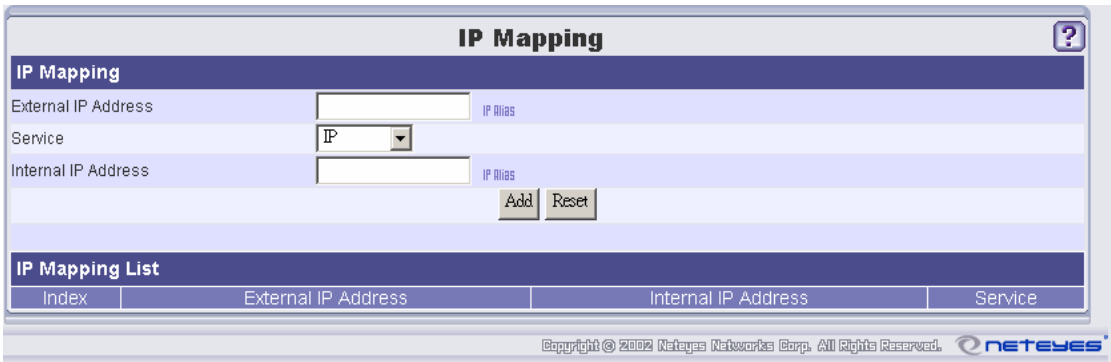
The “Work Time” field indicates how long the policy will be considered active after the start date and time. This field can be configured in minutes, hours, or days.

The “Interval Time” is a length of time that the policy will be inactive, after this time has expired the policy will become active for the “Work Time” again, completing a single cycle which will continue until Stop time and Date. This field can be configured in minutes, hours, or days.

In the example above the policy is configured to run for 5 years, and starting at 9AM, the policy becomes active for 9 hours, and inactive for 15; making 24 hours. In time zones where daylight savings time is observed, the start and end times can be configured far in advance to maintain correct policies.

4-2. Advanced Setup

4-2-1 IP Mapping

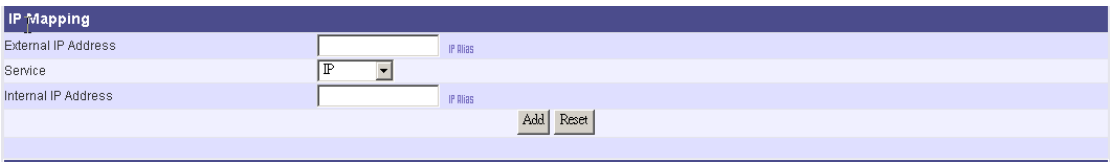


This function allows you to map external IP addresses to the internal virtual IP addresses of PCs inside your LAN. Everything required for the external IP address and network services will be transmitted to the virtual internal IP address.

NOTE：

- **It is recommended to use this function ONLY when you have the firewall enabled.**

4-2-1-a. IP Mapping



External IP Address

Enter an external real IP address in this column.

Service

Select the service type you want.

Internal IP Address

Enter a corresponding internal IP address in this column.

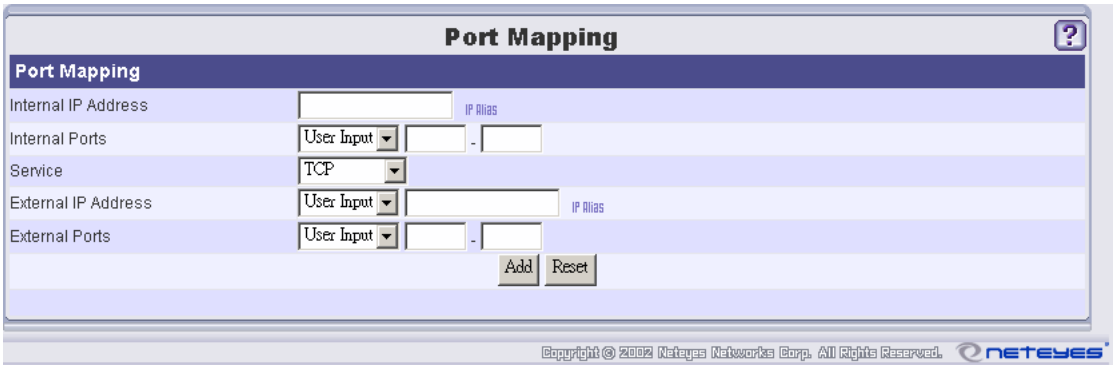
NOTE：

- **The IP address of WAN link should NEVER be used as mapped IP address, UNLESS it is Static IP address.**
- **Do not attempt to apply more than one function (outbound policies, IP mapping, or port mapping) to a single WAN IP address simultaneously, otherwise you can become confused about which function is being used.**
- **Click the Save button on right top corner of the panel after you finish entering all the data in this page. If you do not your changes will be lost when you exit the page.**
- **Click Add to add the settings into the following Connection List, or click Reset to clear the settings and enter them again.**

4-2-1-b. IP Mapping List

All Mappings you set will be listed in this table. To delete a Mapping, right click on it and select Delete. You can also move, edit, enable or disable the Mapping by right clicking.

4-2-2 Port Mapping



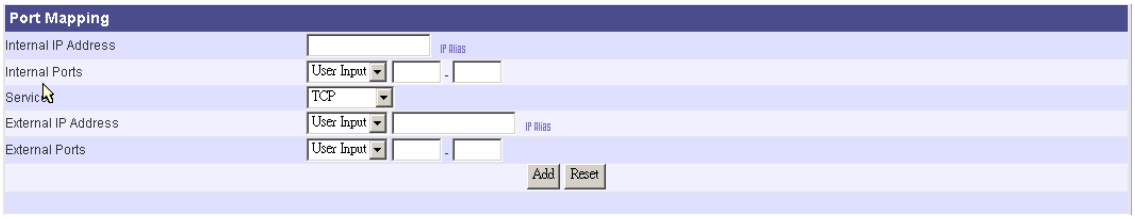
You can customize the virtual server by setting an internal IP and port to correspond to a real external IP address, and map the internal IP address and ports to the external IP address and ports by NAT (Network Address Translation) functions. When specific internal PCs provide network services, NAT functions can separate an internal network from the external network and ensure the security of the internal network.

NOTE：

- **The IP address of WAN link should NEVER be used as a mapped IP address, UNLESS it is Static IP address.**

- **Do not attempt to apply more than one function (outbound policies, IP mapping, or port mapping) to a single WAN IP address simultaneously, otherwise you can become confused about which function is being used.**

4-2-2-a. Port Mapping



Internal IP Address

Enter an internal IP address of a virtual server in this column.

Internal Ports

Enter internal Port number range, which will be used for external connection. If the network service property requested by external users matches this range, the requirements will be transmitted to the virtual internal IP address. If only one port is used for this service, enter that port number in the left column, and leave the right field blank.

Type

Select the data packet type (TCP or UDP).

External IP Address

Enter an external IP address for mapping.

External Ports

Enter an external Port number or range, which will be used for internal network services. The number of ports mapped from the external IP must match the number of ports mapped to the internal IP. If only one port is used for this service, enter that port number in the left column.

NOTE：

- **Some port number are in use, by the NexusWay 800 such as SSL (443), SSH (22) and DNS (25).**

- **Click the Save button on right top corner of the panel after you finish entering all the data on this page － otherwise you will immediately lose all the settings when exiting the page.**

4-2-2-b. Port Mapping List

Port Mapping List

Index	Internal IP Address	Internal Ports	Type	External IP Address	External Ports
1	10.88.168.128	20 - 21	TCP	202.160.87.15	20 - 21
2	10.88.168.128	5800	TCP	202.160.87.15	5800
3	10.88.168.128	5900	TCP	202.160.87.15	5900
4	10.88.168.147	80	TCP	202.160.87.15	81
5	10.88.168.25	25	TCP	202.160.87.15	25
6	10.88.168.25	110	TCP	202.160.87.15	110
7	10.88.168.25	80	TCP	202.160.87.15	80
Disabled	10.88.168.7	53	TCP	202.160.87.7	53
Disabled	10.88.168.7	53	UDP	202.160.87.7	53
Disabled	10.88.168.7	80	TCP	202.160.87.7	80
11	10.88.168.241	443	TCP	202.160.87.15	82

All Mappings you set will be listed in this table. To delete a Mapping, right click on it and select Delete. You can also move, edit, enable or disable the Mapping by right clicking.

4-2-3 Server Cluster

Server Cluster

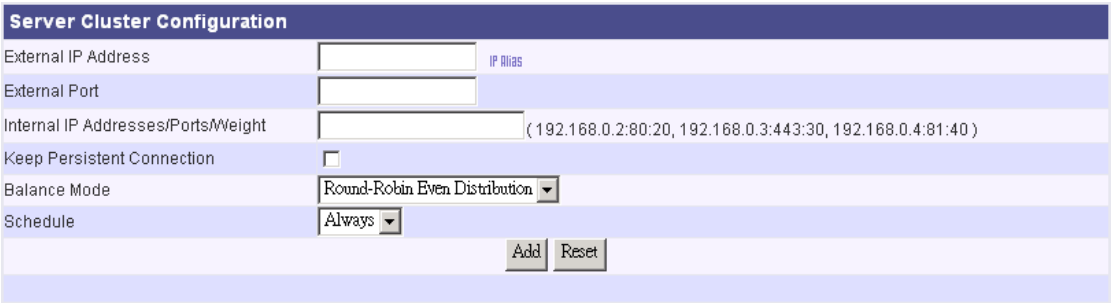
Server Cluster Configuration

External IP Address	IP Alias
External Port	
Internal IP Addresses/Ports/Weight	(192.168.0.2:80:20, 192.168.0.3:443:30, 192.168.0.4:81:40)
Keep Persistent Connection	☐
Balance Mode	Round-Robin Even Distribution
Schedule	Always

Add Reset

Server clustering allows several internal servers to map to a single external IP for data transmission speed enhancement. The transmission reliability can be increased since each server application can failover to other servers. It enables high availability, additional scalability, and easier network management.

4-2-3-a. Server Cluster Configuration



External IP Address

Enter an external IP address where the server can be accessed.

External Port

Enter the port number corresponding to the IP address that the server will be accessible from.

Internal IP Address/Port/Weight

Enter the internal IP addresses, ports and weights separated by Colons (:), such as "192.168.0.2**:**80**:**20", and use Comma (,) symbol to separate the IP addresses. To use "Round Robin by Weight" as the Balance Mode, you must specify a weight after the port, such as "192.168.0.2:80:20", otherwise it will be functionally equivalent to "Round Robin."

Keep Persistent Connection

After a connection has been established with one machine in the server cluster, this function will keep the traffic from the external source on the same machine in the cluster. For the remainder of the session, the traffic between this source and server cluster will not be handled by any other machines in the cluster. It is recommended to enable this function.

Balance Mode

Select the load Balancing Mode, which handles the load balancing for the traffic to the server cluster. For the description of different load balancing algorithms, see **NexusWay 800 Load Balance Mode** table in section **4-1-9 Outbound Policy**.

NOTE：

- **Click the Save button on right top corner of the panel after you finish entering all the data on this page － otherwise you will immediately lose all the settings when exiting the page.**

- **Click Add to add the settings into the Server Cluster List, or click Reset to clear the settings and enter them again.**

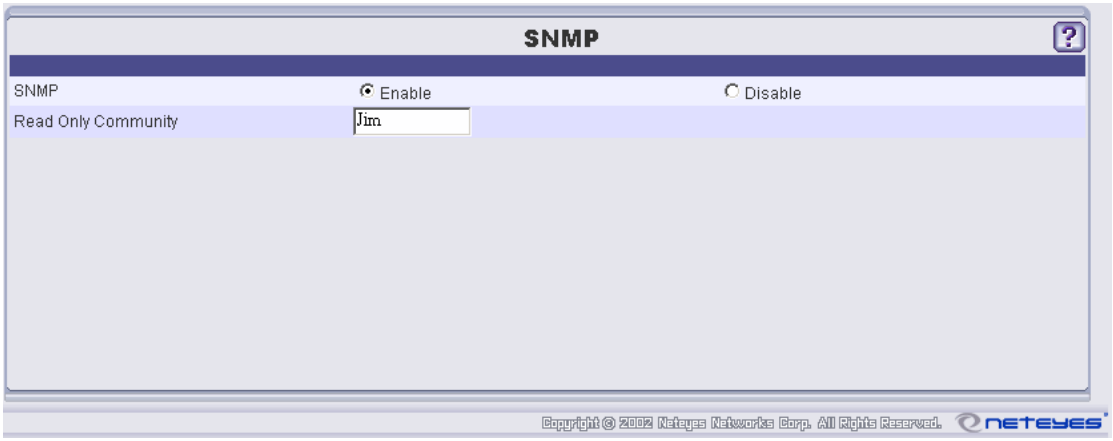
4-2-3-b. Server Cluster List

Server Cluster List

Index	External IP Address	External Port	Internal IP Addresses/Ports/Weight	Keep Persistent Connection	Balance Mode	Schedule

All server cluster settings will be listed in this table. To delete a server cluster setting, right click on it and select Delete. You can also move, edit, enable or disable a server cluster setting by right clicking.

4-2-4 SNMP



SNMP (Simple Network Management Protocol) is a set of protocols for the management of complex networks. SNMP is performed by sending PDUs (Protocol Data Units) to different portions of a network. SNMP-compliant devices can store the data about themselves in Management Information Bases (MIB) and, when requested, return the data to the SNMP requesters.

SNMP Enable/ Disable

Select Enable or Disable to start or stop the SNMP function.

Read Only Community

This option will only be displayed when you have selected the SNMP Enable option. You can Define a name for SNMP requesters to prevent unknown users from accessing the information.

NOTE：

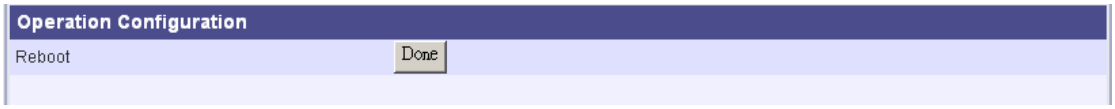
- **Click the Save button on right top corner of the panel after you finish entering all the data on this page － otherwise you will immediately lose all the settings when exiting the page.**

4-2-5 Advanced Feature

This function allows you to backup all the configuration settings in NexusWay 800 so that you can restore all your configurations after restoring the hardware if an unexpected situation occurs. The “Software Update” buttons allow you to manage saved configurations, loader versions, and firmware versions.

For more information, see **Enable Web Management Interface** option in section **4-1-12 Misc. Settings.**

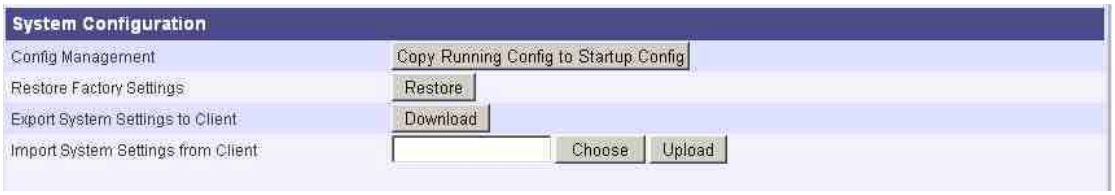
4-2-5-a. Operation Configuration



Reboot

Click the Done button to reboot the NexusWay 800 when necessary.

4-2-5-b. System Configuration



Config Management

Click the “Copy Running Config to Startup Config” button to save active configurations to the disk. If the running information is not saved to disk a reboot will result in a loss of settings.

Restore to Factory settings

Click the Restore button to reset your NexusWay 800 to its original factory configuration.

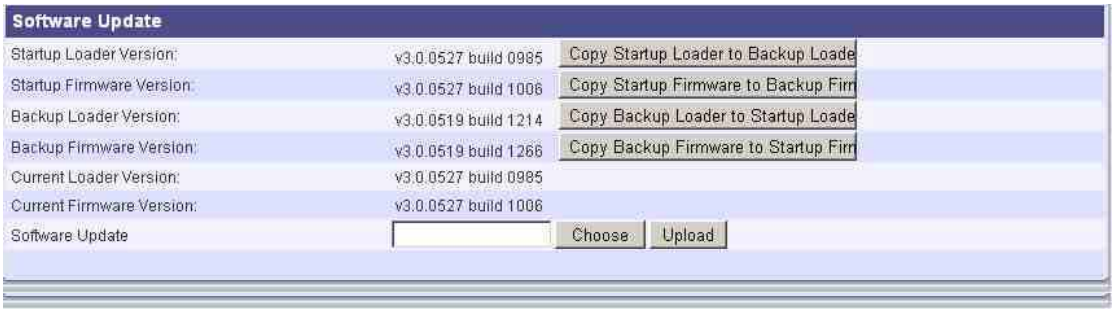
Export System Settings to Client

To backup the current system settings by saving them locally, simply click the Download button. The default file name is config.hhmmss, where “hh”, “mm” and “ss” are respectively the hour, minute and second of the time you click Download button.

Import System Settings from Client

You can restore the systems configuration settings from a previously exported file using this function. Click the Browse button to find an exported configuration file and click the Upload button to modify the configuration for the NexusWay 800 automatically.

4-2-5-c. Software Update



Startup Loader Version Number

The startup loader version is shown here, this should be the same as the current loader version. The “Copy Startup Loader to Backup Loader” button will copy the loader used when starting the NexusWay into the backup slot.

Startup Firmware Version Number

The startup firmware version is shown here, this should be the same as the current firmware version. The “Copy Startup Firmware to Backup Firmware” button will copy the firmware used when starting the NexusWay into the backup slot.

Backup Loader Version Number

The backup loader version is shown here, this may be different from the current loader version. The “Copy Backup Loader to Startup Loader” button will copy the backup loader into the slot used when starting the NexusWay.

Backup Firmware Version Number

The backup firmware version is shown here, this may be different from the current firmware version. The "Copy Backup Firmware to Startup Firmware" button will copy the backup firmware into the slot used when starting the NexusWay.

Current Loader Version Number

The current loader version is shown here.

Current Firmware Version Number

The current firmware version is shown here.

Automatic Update

The system will check with Neteyes for new firmware version once per day when Automatic Update is enabled. When a new version is detected, the system will automatically download the file(s) and prompt you with the version number and by making an Update button active when you log into this screen. The system will not automatically change the firmware in use, this action must be initiated be an administrator.

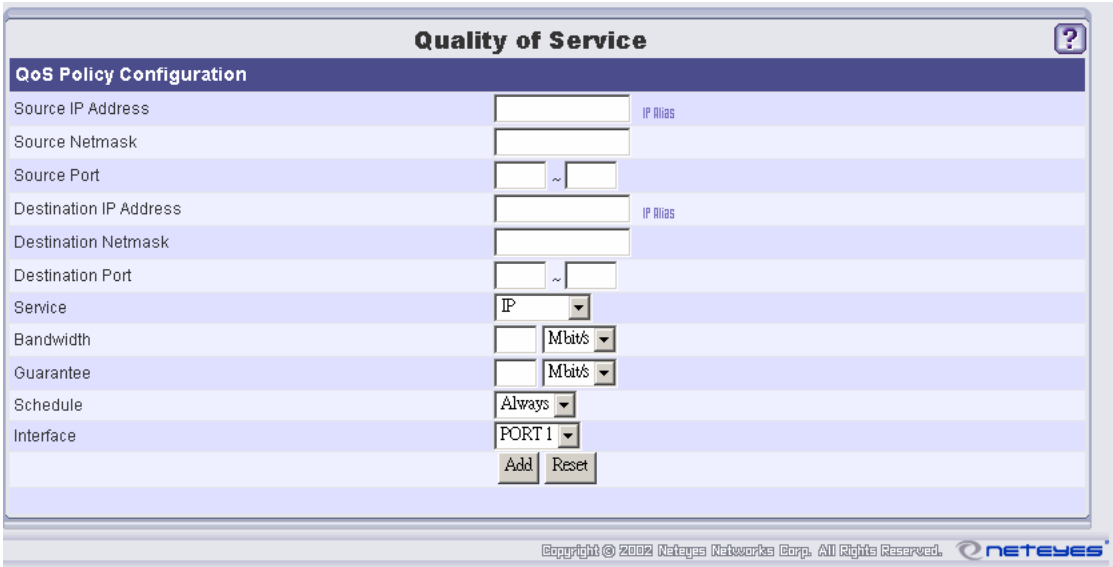
Software Update

Click the Browse button to find the latest firmware update file and click Upload button to update the software of the NexusWay 800. You can find the newest release of the NexusWay 800 firmware on the Neteyes Web site. If you don't have automatic update enabled Please go to the Web site and download the newest firmware released at http://www.neteyes.biz/firmware.asp.

NOTE：

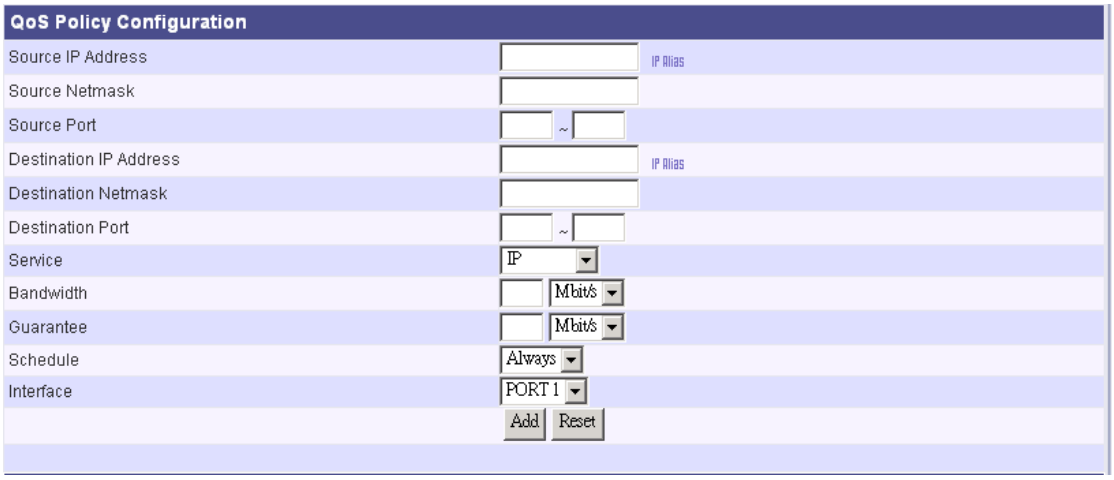
- **Click the Save button on right top corner of the panel after you finish entering all the data on this page － otherwise you will immediately lose all the settings when exiting the page.**

4-2-6 QoS (Quality of Service)



QoS (Quality of Service) specifies a maximal throughput level. The NexusWay 800's QoS feature provides managed bandwidth for specific services, guaranteeing applications don't monopolize bandwidth. To apply QoS policy to all available ports, place an asterisk (*) in the left column of Source Port for external to internal traffic or Destination Port for internal to external traffic. If you enter an asterisk in both Source and Destination Port options, then the QoS policy will apply to all the traffic in both directions.

4-2-6-a. QoS Policy Configuration



Enter the source and destination IP address, Netmask, port in the corresponding columns.

Service

Select the data-packet type such as TCP or UDP.

Direction

Select ingress for this rule to apply to inbound traffic, and egress for it to apply to outbound traffic.

Bandwidth

Enter the bandwidth you would like to maintain as a minimum (in Bytes, KB or MB).

Schedule

Select a schedule to specify when you would like the policy to be active. To set the schedule, see 4-1-17. Schedule Setting.

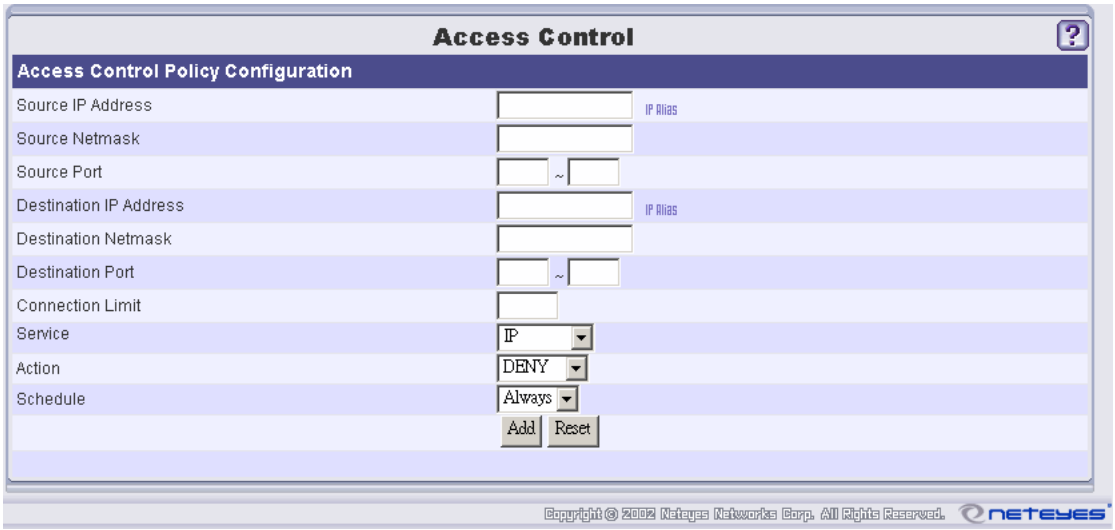
NOTE：

- **The QoS policy can only be set by IP address and Netmask, not by RANGE.**
- **Click the Save button after you finish entering all the data on this page. Click Add to add the settings into the QoS Policy List, or click Reset to reenter them.**

4-2-6-b. QoS Policy List

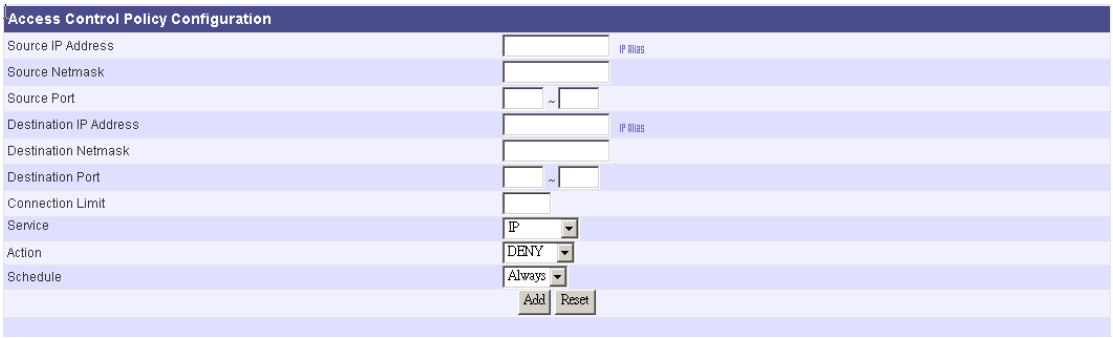
All policies you set will be listed in this table. To delete a policy, right click on it and select Delete. You can also move, edit, enable or disable a policy by right clicking.

4-2-7 Firewall



Along with the QoS policies, the Firewall can also be used to manage throughput levels based on the certain traffic flows to improve Internet service quality and increase security. However, the firewall is specifically designed to increase security, and limit access by denying unexpected access types and known undesirable connections. All the traffic entering or leaving the intranet will be examined by the firewall, which will block data meeting none of the specified security criteria

4-2-7-a. Firewall Policy Configuration



Enter the source and destination IP address, Netmask, and ports in the corresponding columns.

Connection Limit

Connection Limit is the maximum number of connections of the source IP address allowed by the firewall for this rule. If leave this column empty, no limitations will be applied to this rule.

Service

Select the data-packet type. The options are IP, TCP, UDP, ICMP and UserInput available in this pull-down list.

Action

You can DENY or ALLOW the traffic, which meets the criteria you set above, to be limited.

Schedule

Select a schedule to specify when you would like the firewall settings to activate. To set the schedule, see 4-1-17. Schedule Setting.

NOTE：

- **The Firewall policies can only be set by IP address and Netmask, not by RANGE.**

- **Click Save button on right top corner of the panel after you finish entering all the data in this page. Click Add to add the new policy into the Firewall Policy List, or click Reset to enter it again.**

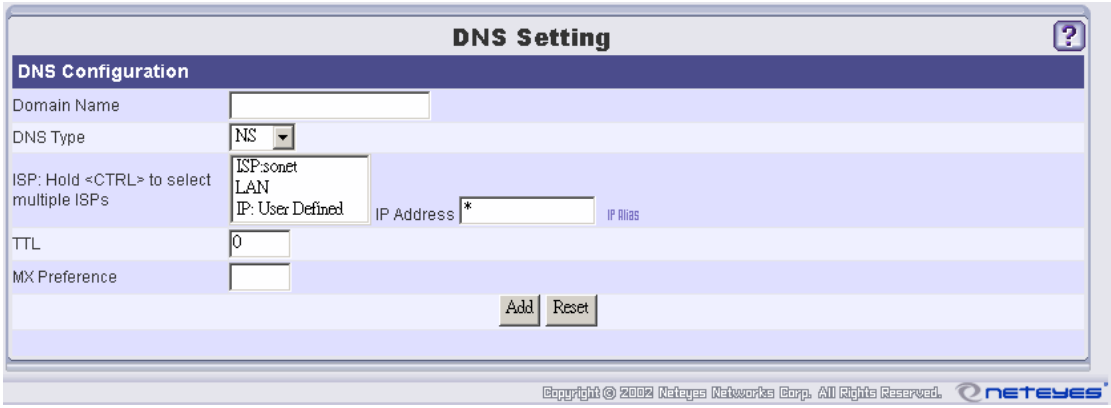
4-2-7-b. Firewall Policy List

Firewall Policy List

Index	Source IP Address	Source Netmask	Source Port Range	Destination IP Address	Destination Netmask	Destination Port Range	Limit	Service	Action	Schedule
1	*	0.0.0.0	*	10.88.168.16	255.255.255.255	80		TCP	ALLOW	Always
2	*	0.0.0.0	*	10.88.168.18	255.255.255.255	20 - 21		TCP	ALLOW	Always
37	210.10.181.3	255.255.255.255	*	*	0.0.0.0	*		TCP	DENY	Always
38	210.85.82.134	255.255.255.255	*	*	0.0.0.0	*		TCP	DENY	Always
39	146.82.220.0	255.255.255.0	*	*	0.0.0.0	*		TCP	DENY	Always
40	*	0.0.0.0	*	202.160.97.15	255.255.255.255	22		TCP	DENY	Always
41	*	0.0.0.0	*	202.160.81.42	255.255.255.255	22		TCP	DENY	Always
42	10.0.0.168	255.255.255.255	*	10.88.168.128	255.255.255.255	*		TCP	ALLOW	Always
43	10.0.0.0	255.255.255.0	*	10.88.188.0	255.255.255.0	*		TCP	DENY	Always
44	10.0.0.0	255.255.255.0	*	10.88.188.0	255.255.255.0	*		UDP	DENY	Always

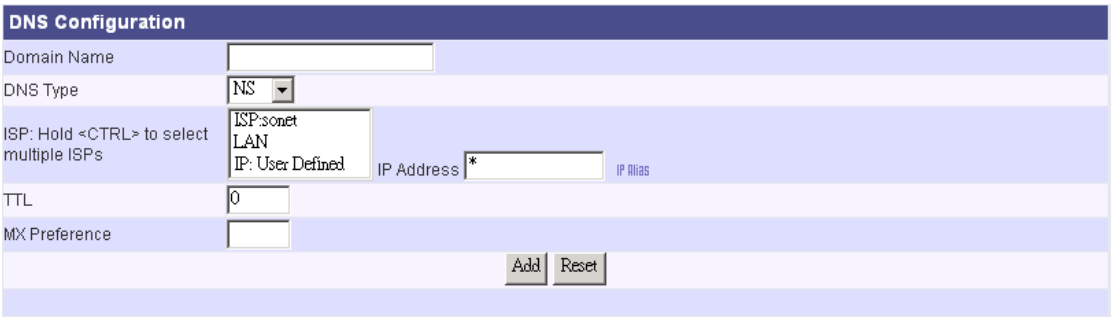
All firewall policies you set will be listed in this table. To delete a firewall policy, right click on it and select Delete. You can also move, edit, enable or disable the policy by right clicking.

4-2-8 DNS Setting



DNS (Domain Name Server/Service) translates domain names into IP addresses. This function allows you to translate between IP addresses and domain names.

4-2-8-a. DNS Configuration



Domain Name

Enter the domain name you would like to map.

DNS Type

There are NS (Name Server), Host, MX (Mail eXchanger), Alias, and SOA (Start Of Authority) modes available in this pull-down list. Where Host means any machine on the network; MX is to find servers that can deliver mail; Alias presents a host name; SOA contains some parameters about the domain itself, such as contact email addresses and collections of more technical data.

ISP: Hold <CTRL> to select multiple ISPs

This is a multiple selection list. To make a multiple selection hold the Ctrl key and select several ISPs.

IP

Enter the internal IP address for this DNS Mapping.

TTL (Time to Live)

The duration of life for LAN requests. Enter a value in seconds to specify how long the cached record is valid before being purged. It is recommended that you set this value to zero (0) for real-time load balancing.

MX Preference

MX Preference is used to determine the order of delivery when a host has multiple MX records. A host can have multiple MX records, so that the mail can automatically go to backup systems if primary systems are unreachable. The lower number you set, the higher priority the record has, and records with the same priority will equally share the workload.

NOTE：

- **DNS must be set with IP/Port Mapping. Verify the IP has been setup in the IP Mapping or the Port Mapping option and shown in the mapping list before assigning a Domain Name to a WAN IP. If the WAN IP is not available in the list, external user will never be able to access internal IP through the WAN IP.**

- **Click the Save button on right top corner of the panel after you finish entering all the data on this page － otherwise you will immediately lose all the settings when exiting the page.**

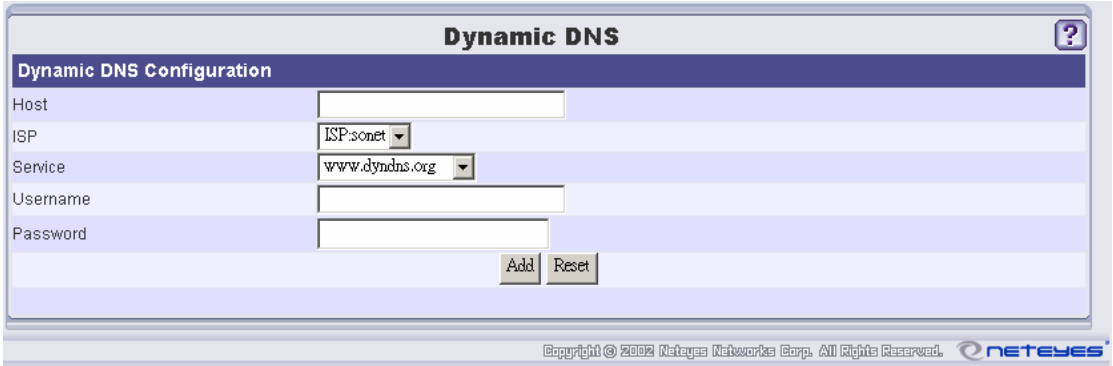
4-2-8-b. DNS Mapping List

DNS Mapping List

Index	Domain Name	DNS Type	ISP	IP	TTL	MX Preference
1	yugux.com	NS	ISP:NetEyes Leaseline	*	0	
2	yugux.com	SOA	ISP:NetEyes Leaseline	*	0	
3	yugux.com	MX	ISP:NetEyes Leaseline	*	0	10
4	yugux.com	MX	IP: User Defined	202.160.87.4	0	15
5	www.yugux.com	Host	IP: User Defined	202.160.87.16	0	
6	yugux.com	NS	LAN	10.88.168.7	0	
7	yugux.com	MX	LAN	10.88.168.4	0	15
8	yugux.com	MX	LAN	10.88.168.25	0	10
9	www.yugux.com	Host	LAN	10.88.168.16	0	

All DNS mappings you set will be listed in this table. To delete a mapping, right click on it and select Delete. You can also move, edit, enable or disable mappings by right clicking.

4-2-9 DDNS



The Dynamic DNS feature assigns a fixed hostname to your ISP-assigned dynamic IP address, making your computer accessible from any location on the Internet without knowing your current IP. The NexusWay 800 supports 11 different Dynamic DNS services. To use the Dynamic DNS feature, you must have already signed up for Dynamic DNS service from one of following organizations:

* www.dyndns.org
* www.ez-ip.net
* www.dhs.org
* www.ods.org
* gnudip.cheapnet.net
* www.dyn.ca
* www.tzo.com
* www.easydns.com
* www.dyns.cx
* www.hn.org
* www.zonenet.com

Host

Enter the host name you registered to associate with your current IP address. This is a fixed hostname you have selected or entered when signing up for whichever third party service you use.

ISP

Enter the ISP corresponding to this hostname.

Service

Select the third party Dynamic DNS service you wish to use.

Username/Password

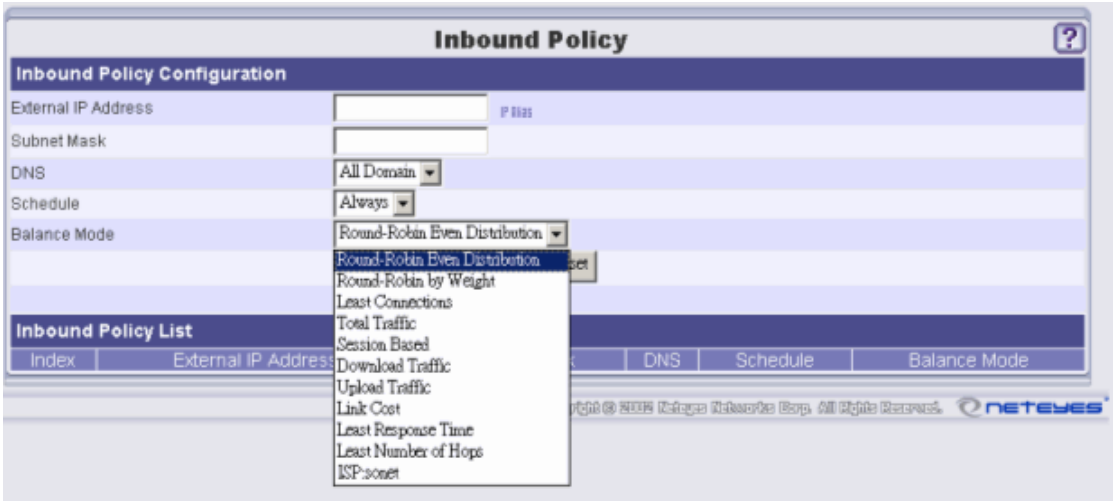
Enter the username and password which apply to your account for the service you use.

NOTE：

- **Click the Save button on right top corner of the panel after you finish entering all the data in this page. Click Add to add the settings into the Dynamic DNS List, or click Reset to enter the information again.**

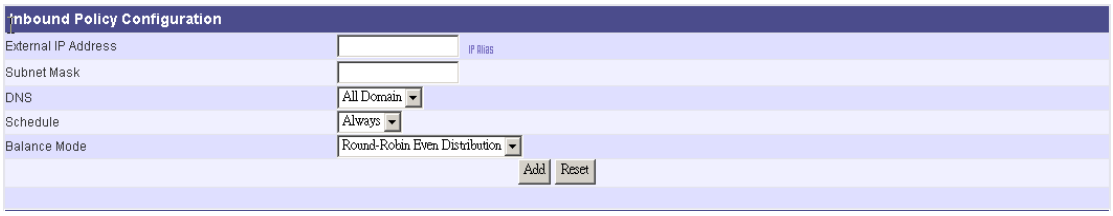
After clicking the Add button, the Dynamic DNS settings will be listed in Dynamic DNS List. To delete a setting, right click on it and select Delete. You can also move, edit, enable or disable a Dynamic DNS setting by right clicking.

4-2-10 Inbound Policy



In this option, you can setup the load balancing algorithms, to distribute the inbound traffic across the different Internet connections according to the algorithm you selected.

4-2-10-a. Inbound Policy Configuration



External IP Address

Enter an external IP address, the source of the incoming traffic that applies to the Load Balancing mode. For example, 168.95.1.1

Subnet Mask

Enter the Subnet Mask of the external IP address. For example, 255.255.255.0.

DNS

Select an internal DNS IP address. This is the destination of the incoming traffic that the Load Balancing mode applies to.

Schedule

Select a schedule to specify when you would like the Inbound Policy to be active. To set the schedule, see 4-1-17. Schedule Setting.

Balance Mode

Select a Load Balance mode for the policy according to your requirements or usage situation. For the description of different load balancing algorithms, see the **NexusWay 800 Load Balance Mode table** in 4-1-9 **Outbound Policy**. If you don't desire any load balancing select a single ISP, drawn from the list of configured ISP's.

Session Based

Select whether the load-balancing mode includes session based management. When enabled Balancing will be applied in the selected manner to separate sessions.

NOTE：

- **Click the Save button on the top right corner of the panel after you finish entering all the data to avoid data loss when exit the page.**

4-2-10-b. Inbound Policy List

Inbound Policy List

Index	External IP Address	Subnet Mask	DNS	Schedule	Balance Mode

All policies you set will be listed in this table. To delete a policy, right click on it and select Delete. You can also move, edit, enable or disable policies by right clicking.

4-2-11 NetFlow

Cisco NetFlow is a technology developed by Cisco, and is widely used for IP accounting and billing.

The NexusWay 800 can export network traffic information, in flows, to an external machine. This external machine, presumably running a NetFlow application, will then collect this NetFlow data for processing.

NetFlow

To enable NetFlow, simply click the Enable button.

IP Address

Enter an IP address with port number, where you wish the NetFlow data to be exported

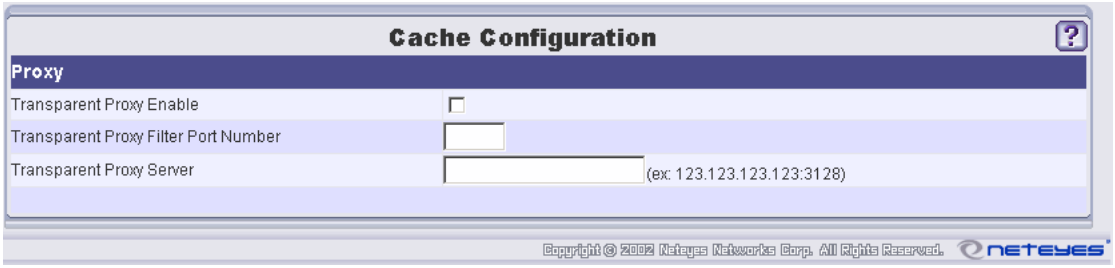
Port

Select the Port whose flow data you want to transfer via NetFlow.

Version

Select the NetFlow version to be exported.

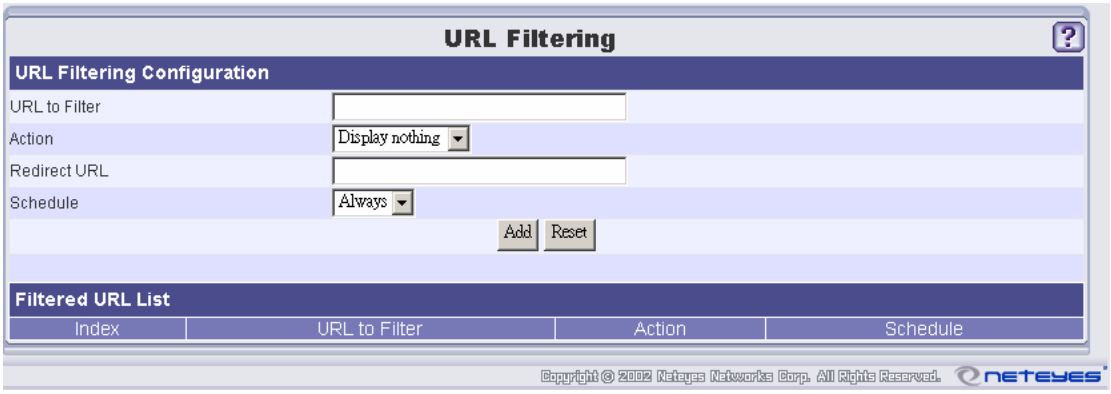
4-2-12 Cache Configuration



You can enable a built-in Web Proxy server and a Transparent Proxy with this option. A proxy server is a server that sits between a client application (such as Web browser) and a real server. The proxy server will forward the requests to the real server if it detects that the requests can not be fulfilled by itself after intercepted all the requests to the real server. Proxy servers can be used to improve performance or filter requests.

A transparent proxy functions as same as a proxy. The only difference between them is that a transparent proxy allows clients to not change any network settings before traffic starts flowing through the proxy. After enabling the Transparent Proxy, you must also fill in the port number connected to filter, as well as the IP and port number of the proxy server.

4-2-13 URL Filtering



This function allows you to prohibit internal users from viewing certain URLs.

URL to Filter

Enter the URL you wish to block. It is acceptable to enter wildcards (*).

Schedule

Select a schedule to specify when you would like the policy to be active. To set the schedule, see 4-1-17. Schedule Setting.

4-2-13 High Availability

High availability features allow for a second NexusWay device. This configuration option will allow you to manage all High Availibility options.

High Availability:

This radio button allows the activation or deactivation of the High Availability features.

Function As:

This radio button configures which role the active NexusWay will assume in a High Availability configuration.

Virtual IP Address

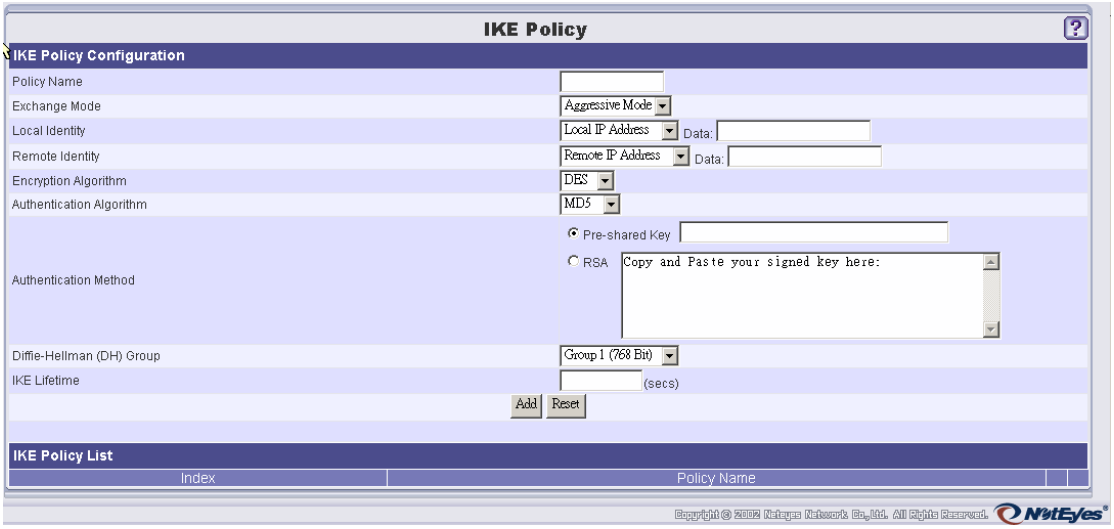
The Virtual IP Address is the shared gateway address, used by LAN machines. This virtual address ensures that if one devices physically fails, the other can effectively take over, without reconfiguring devices on the LAN.

Alternate IP Address

The Alternate IP Address is the physical address, of the other NexusWay.

4-3. VPN Setup

4-3-1 IKE Policy (Not applicable in NexusWay 800)



Please note that this function is only available in the NexusWay 805, 815, 825, and 835.

In this option, you can configure settings to exchange keys that will be used when establishing a VPN, such as host authentication, negotiation of security parameters for an encrypted connection, and key generation, as well as key exchange.

Policy Name

Enter an unique name for the IKE policy.

Exchange Mode

There are two exchange modes available, which are Main Mode and Aggressive Mode. IKE consists of two phases. The Authentication phase includes verification of the identities of the local and remote systems via pre-shared secrets or certificates, while the Key Exchange phase involves the negotiation of security parameters. If the Authentication phase exchange is in Aggressive Mode, the Key Exchange phase will not be encrypted. When set in Main Mode, the Authentication phase will generate session keys if a secure channel is required for the Key Exchange phase. Due to additional key generation steps, Main Mode is about three times slower than Aggressive Mode, however it has higher security.

Local Identity/Remote Identity

Enter your Fully Qualified Domain Name box if you select ***Local User_FQDN*** or ***Local FQDN***. For using X509 Certificates for Authentication, select ***Remote User_asn1dn*** for your Local and Remote Identities.

Encryption Algorithm

Select either DES (Data Encryption Standard) using 56 Bit Keys or 3DES (Triple DES) which uses 168 bit keys.

Authentication Algorithm

You can select MD5 (returns a 32 byte hash) or SHA-1 (returns a 160 byte hash). SHA-1 is more secure but much slower than MD5 and requires more system resources. For general application, MD5 is secure enough and much more suitable choice.

Authentication Method

To use a Pre-shared Key, select Pre-shared Key button and enter the key. To use RSA (Rivest-Shamir-Adleman), a public-key algorithm for asymmetric Encryption, copy and paste the signed public key of the desired endpoint as provided by a Certification Authority. For more information about Certificate Authorities, please see **4-3-4 Certificate Authority**

Diffie-Hellman (DH) Group

DH is an algorithm for developing a shared secret between endpoints by separately integrating endpoints' public key combination result with private key. Essentially, this is a method for authenticating and negotiating keys; allowing two hosts to create and share a secret key. A 768 bit algorithm is used by "Group 1", a 1024 bit by "Group 2" and a 1536 bit by "Group 5," which subsequently has the highest security, requires the longest time and the most resources.

IKE Lifetime

Enter a value between 60 to 86,400 seconds for how long you want an IKE Security Association to remain valid after establishment. Generally the shorter the lifetime is, the more secure your IKE negotiations will be. However, with longer lifetimes, Security Associations between two points can be set up more quickly after the first one. If you have no idea what is a good lifetime, it is suggested to enter the default value of 28,800 seconds (8 hours).

NOTE：

- **Click Save button on right top corner of the panel after you finish entering all the data on this page. Click Add to add the settings into the IKE Policy List, or click Reset to enter them again.**

After clicking the Add button, the settings will be listed in the IKE Policy List. To delete an IKE Policy, right click and select Delete. You can also move, edit, enable or disable the IKE policy by right clicking.

4-3-2 VPN Policy (Not applicable in the NexusWay 800)

Please note that this function is only available in NexusWay 805, 815, 825, and 835.

VPN Policy

A Virtual Private Network (VPN) is used to provide secure, encrypted communication across the public Internet between two remote hosts. VPNs allow the establishment of an encrypted "tunnel" that protects the network traffic flow from eavesdroppers.

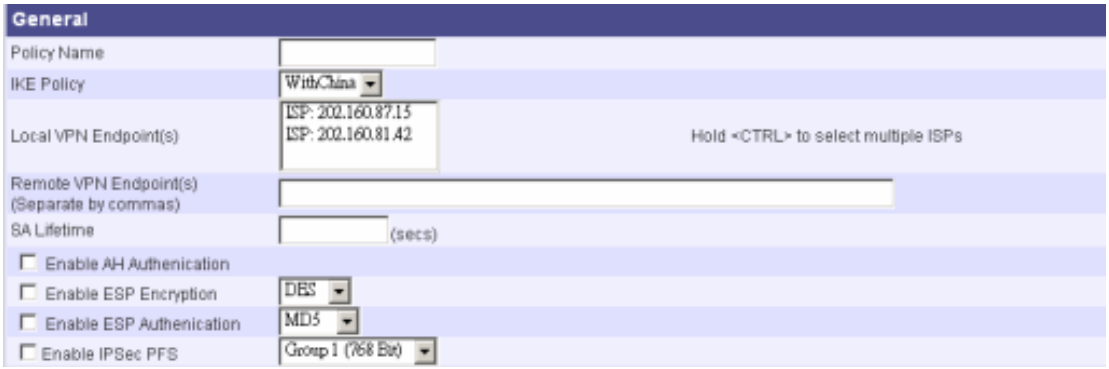
It enables users to access private network data and resources securely over the Internet or other networks. Even if using public networks, a VPN will inherit the characteristics of a private network. That's why it is called "**Virtual**" Private Network. It's used for tunneling, encryption, authentication, and access control over a public network that supports VPN.

4-3-2-a VPN Policy Configuration

Type

There are two types available, which are Manual Policy and Auto Policy. The most common configuration, Auto Policy, automatically manages the authentication and encryption keys with an IKE policy. IKE protocols perform negotiations between two VPN Endpoints to automatically generate the required parameters. For this reason, you will be required to select a configured IKE Policy if you select Auto Policy. See **4-3-1 IKE Policy** in this documentation for more information about IKE Policy configuration. On the other hand, IKE Policies will not be used with a Manual Policy. All the required key information will be entered manually.

4-3-2-b General



Policy Name

All VPN Policies must have a unique policy name. This name is not supplied to the remote VPN Endpoint. It is used only to help you identify your VPN Policy.

IKE Policy

This column is enabled when you have selected Auto Policy so you can choose a configured IKE policy. If Manual Policy is enabled this entry will be disabled.

Local VPN Endpoint(s)

Select the WAN IP address of your network. You may select with maximum of four local endpoints. Hold the <CTRL> key and right click to select multiple endpoints.

Remote VPN endpoint(s)

Enter the WAN IP address of the remote VPN that you wish to connect to. If the remote endpoint is another VPN-capable NexusWay product, you can enter up to 4 endpoints. Multiple endpoints must be valid Internet addresses separated by commas.

SA Lifetime (Security Association lifetime)

Enter a value between 60 to 86,400 seconds for how long you want an IKE Security Association to remain valid after initial establishment. As a general rule, the shorter the lifetime is, the more secure your IKE negotiations will be. However, with longer lifetimes, Security Associations can be set up more quickly afterward. If you don't know what a good lifetime length is, we suggest entering a default value of 28,800 seconds (8 hours).

Enable AH Authentication

Enable this to verify that the contents of a packet have not been changed and to validate the identity of the sender. An Authentication Header does not provide packet encryption.

NOTE: Setting here must match with remote VPN Endpoint settings.

Enable ESP Encryption (Encapsulated Security Payload Encryption)

ESP Encryption provides security for the payload (data) sent through the VPN tunnel.

NOTE: Setting here must match with remote VPN Endpoint settings.

In general cases, AH Authentication and ESP Encryption will be enabled.

Enable ESP Authentication

If you enable ESP Authentication, both the IP datagram and ESP Header will be encrypted, providing an additional layer of security.

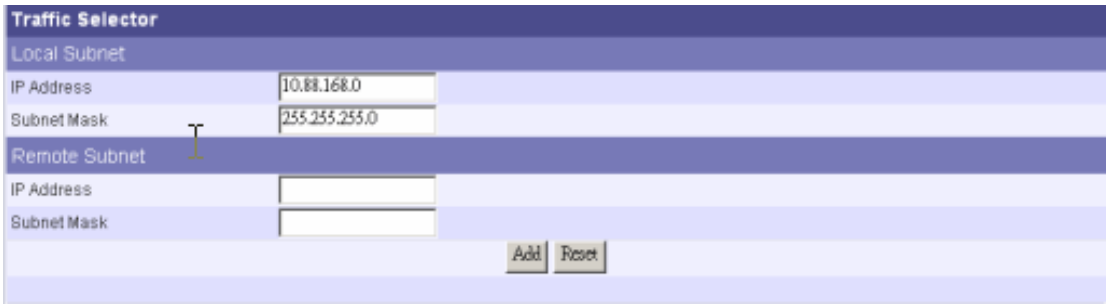
NOTE: Setting here must match with remote VPN Endpoint settings.

Enable IPSec PFS (Perfect Forward Secrecy)

To enable IPSec PFS, the keys that protect data transmission will not be used to derive additional keys, and seeds used to create data transmission keys will also not be reused. In the other words, if a key becomes compromised, no other keys can be derived using that information. Since it is very unlikely for any encryption or authentication keys to be compromised, PFS is not generally required. If you enable PFS, you will see a Diffie-Hellman group pull-down list similar to the one used for IKE, however this one is used for PFS only. You must select one of the three groups.

NOTE: Setting here must match with remote VPN Endpoint settings.

4-3-2-c Traffic Selector

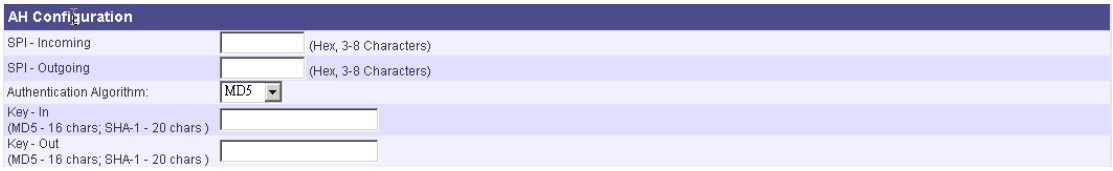


Enter the IP Address and subnet mask of your private, local subnet, which you wish to make accessible from the remote endpoint of your VPN. You must also enter remote IP and subnet mask of your remote location. These two subnets can overlap.

NOTE:

- **If you chose Manual Policy, please fill in the following columns for exchanging keys. These settings must also match the settings on the remote.**

4-3-2-d AH Configuration



SPI – Incoming/ SPI - Outgoing

Enter a Hex value (3 - 8 characters) which matches the settings of remote VPN endpoint in both SPI – Incoming and Outgoing columns.

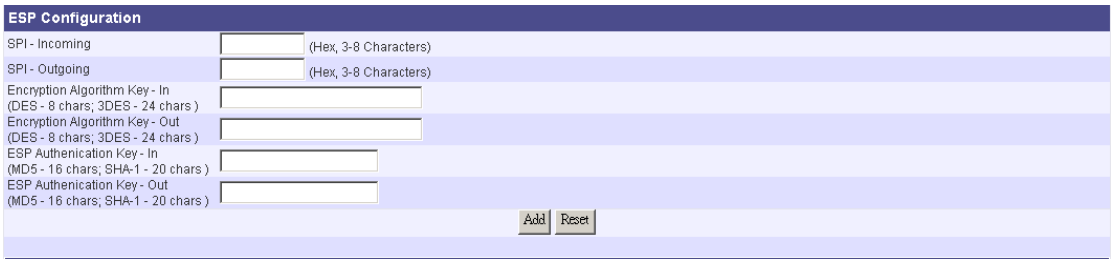
Authentication Algorithm

There are MD5 and SHA-1 available for this option, where MD5 is the default value, and SHA-1 is more secure.

Key–In / Key-Out

For MD5, the keys should be 16 characters. For SHA-1, the keys should be 20 characters.

4-3-2-e ESP Configuration



SPI – Incoming/ SPI - Outgoing

Enter a Hex value (3 - 8 characters) which matches the settings of remote VPN endpoint in both SPI – Incoming and Outgoing columns.

Encryption Algorithm Key–In / Key-Out

Enter a key with 8 characters for DES, or the one with 24 characters for 3DES.

ESP Authentication Key–In / Key-Out

Enter a key with 16 characters for MD5, or the one with 20 characters for SHA-1.

NOTE：

- **Click the Save button in top right corner of the panel after you finish entering all the data in this page. Click Add to add the settings into the IKE Policy List, or click Reset to enter them again.**

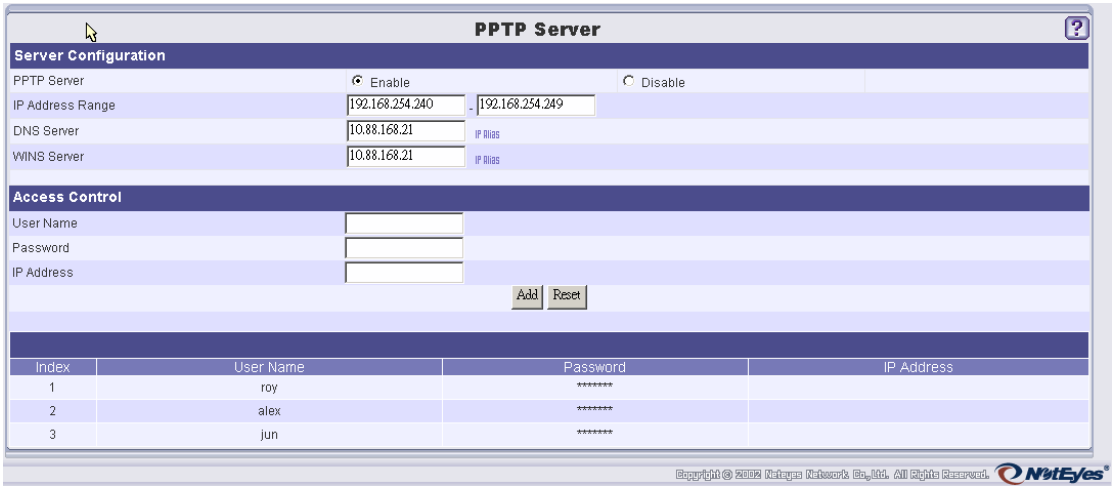
4-3-2-e VPN Policy List

VPN Policy List

Index	General	Traffic Selector	AH Configuration	ESP Configuration
Disabled	**Policy Name:** ConnectBJ **Type:** Auto Policy **IKE Policy:** treker_test **Local VPN Endpoint(s)**202.160.87.15,202.160.81.42 **Remote VPN Endpoint(s):** 218.107.148.137 **SA Lifetime**: 2800 **AH Authentication:** Disabled **ESP Encryption:** Enabled **ESP Authenication:** Enabled **Enable IPSec PFS**: No	**Local IP:** 10.88.168.0 **Local Subnet:** 255.255.255.0 **Remote IP:** 10.0.0.0 **Remote Subnet:** 255.255.255.0	Auto Policy	Auto Policy
2	**Policy Name:** treker_test **Type:** Auto Policy **IKE Policy:** treker_test **Local VPN Endpoint(s)**202.160.87.15 **Remote VPN Endpoint(s):** 202.160.81.45 **SA Lifetime**: 300 **AH Authentication:** Disabled **ESP Encryption:** Enabled **ESP Authenication:** Enabled **Enable IPSec PFS**: No	**Local IP:** 10.88.168.0 **Local Subnet:** 255.255.255.0 **Remote IP:** 192.168.10.0 **Remote Subnet:** 255.255.255.0	Auto Policy	Auto Policy
Disabled	**Policy Name:** 123 **Type:** Auto Policy **IKE Policy:** WithChina **Local VPN Endpoint(s)**202.160.87.15,202.160.81.42 **Remote VPN Endpoint(s):** 1.1.1.1 **SA Lifetime**: 300 **AH Authentication:** Disabled **ESP Encryption:** Enabled **ESP Authenication:** Enabled **Enable IPSec PFS**: No	**Local IP:** 10.88.168.0 **Local Subnet:** 255.255.255.0 **Remote IP:** 192.168.10.0 **Remote Subnet:** 255.255.255.0	Auto Policy	Auto Policy

All the VPN policies will be listed in VPN Policy List. To delete a policy, right click on it and select Delete. You can also move, edit, enable or disable a VPN policy by right clicking.

4-3-3 PPTP Server (Not applicable in NexusWay 800)



Please note that this function is only available in NexusWay 805, 815, 825, and 835.

In this option, you can enable or disable the NexusWay's PPTP Server, which will allow connections from PPTP clients.

Server Configuration

If you enable the PPTP Server, you must select an IP address range for PPTP connections. This range should be as same as your LAN subnet. The maximum number of IP addresses in this range for the NexusWay series is 15.

Access Control

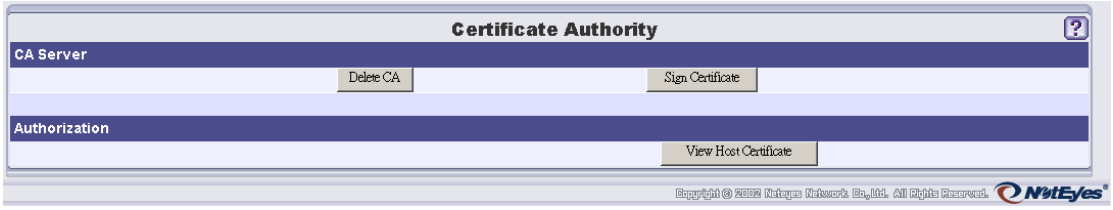
Enter the users that can access your VPN. It is necessary to provide a name, password, and IP address for each user. The NexusWay will accept users according to the IP address with optional Netmask ranges, such as 1.2.3.4 or 1.2.3.4/32. If you leave the column blank, the system will accept all the users without any restriction.

4-3-4 Certificate Authority (N/A in the NexusWay 800)

Please note that this function is only available in NexusWay 805, 815, 825, and 835.

You can generate and sign x509 certificates in this option. These certificates are used in place of pre-shared keys while setting up IKE policies. CA (Certificate Authority) authentication is typically used in large organizations with internal CA server. This requires each VPN gateway to have a certificate from the CA. Using CA certificates reduces the amount of data entry required by each VPN endpoint.

If you want the NexusWay to serve as CA Server, push the “Create CA” button and you will see the following panel displayed.



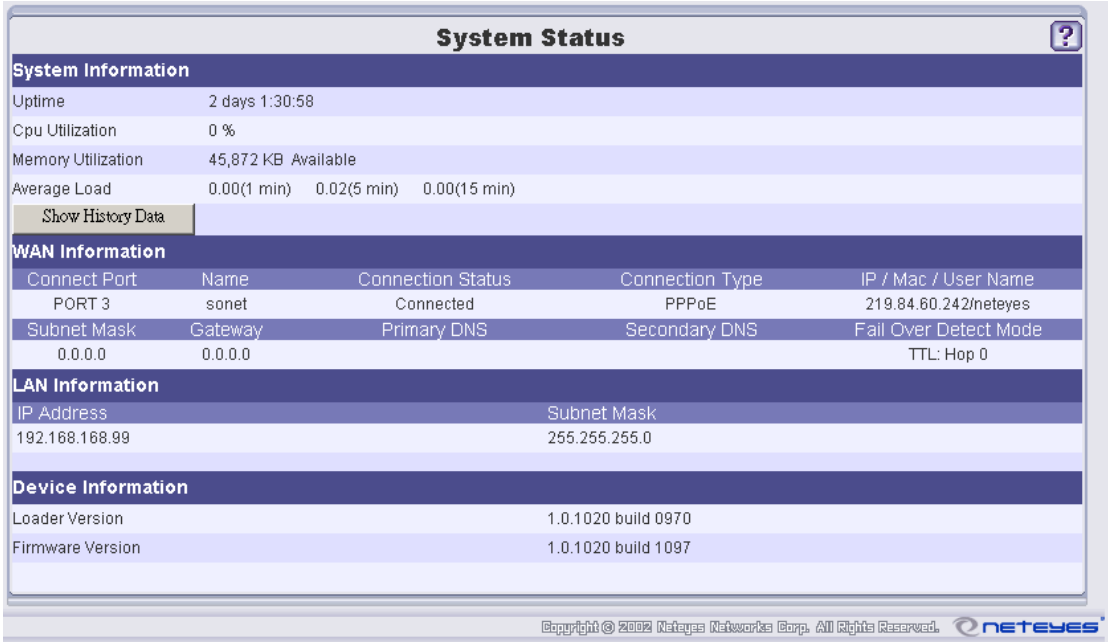
Click “Delete CA”, or “Sign Certificate” based on your requirement. If you select the Sign Certificate button, you will be requested to copy and paste your certificate into a box on the popup window.

In the Authorization section, the NexusWay no longer needs the Generate Certificate or the Load Certificate buttons and since it is serving as the CA server, these two buttons are removed. After clicking View Host Certificate a new window will be displayed with your host certificate. This encrypted text is your public key. The other endpoint of VPN and CA Clients should copy and paste this key into the IKE Policy page. In the Authentication Method option in IKE Policy page, the administrator should select "RSA" and enter the key in the text box on the right of the RSA option.

For CA Client, click Generate Certificate button to generate a certificate request. A window will then be displayed with an encrypted key request. Copy the contents in the box into your computers buffer. For a NexusWay series that is serving as CA Server, click the Sign Certificate button and paste the contents into the new window. The new, signed key it returns should also be copied into your computers buffer. This key needs to be pasted in to two places: the IKE Policy page and the window opened after clicking the Load Certificate button. On the CA Client machine, the administrator should select "RSA" as the Authentication Method section in the IKE Policy page, and enter the key in the text box on the right of the RSA option. The key generated by CA Server machine also needs to be saved onto the CA Client machine. Click Load Certificate button and paste the key into the text box in the new window. After the key is saved on the Client machine, the key can be displayed by clicking View Host Certificate button.

4-4. Network Info.

4-4-1 System Status

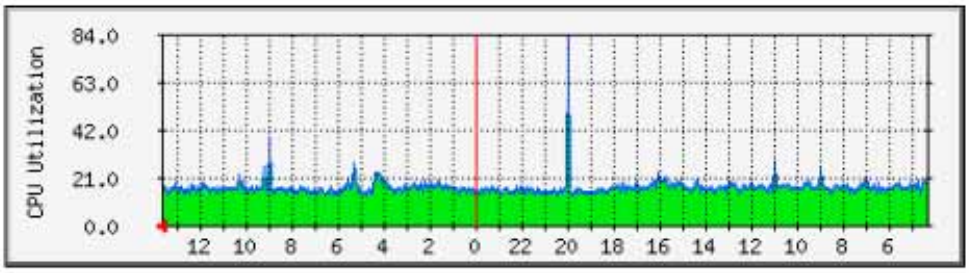


This option shows the current status and settings of the system and each Internet connection in detail, including WAN Information, LAN Information and Device Information with current loader version and firmware version information.

Click the Show History Data button for graphics of the current status relating to CPU, Free Memory, and Loading.

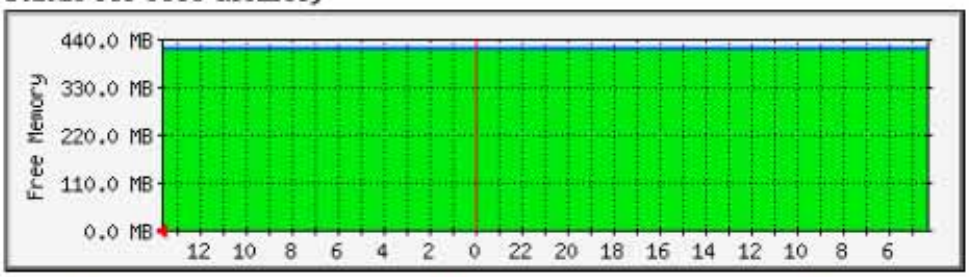
History Data Index Page for system

Status for CPU



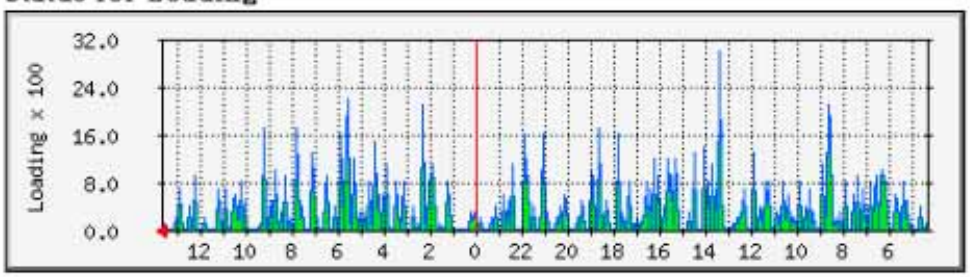
Max In:	82 %	Average In:	17 %	Current In:	15 %
Max Out:	82 %	Average Out:	17 %	Current Out:	15 %

Status for Free Memory



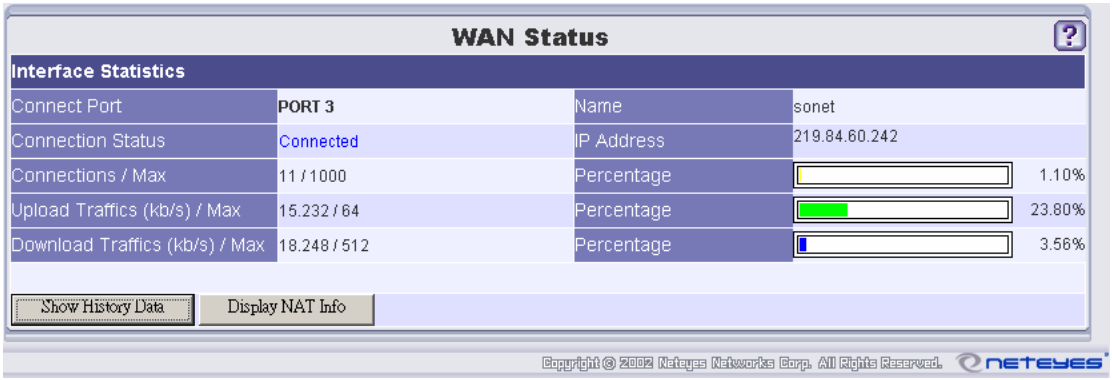
Max In:	421,788 KB	Average In:	421,256 KB	Current In:	420,932 KB
Max Out:	421,788 KB	Average Out:	421,256 KB	Current Out:	420,932 KB

Status for Loading



Max In:	0.3	Average In:	0.06	Current In:	0
Max Out:	0.3	Average Out:	0.06	Current Out:	0

4-4-2 WAN Status



WAN Status shows the current information about all of the Internet connections, including WAN interface, name, connection status, IP address, number of connections, upload traffic, and download traffic. The colored bar in the percentage column will change length every few seconds depending on the ratio of the current figures and their specified maximums.

For more detailed information about these settings, see 4-1-2 WAN section in this document.

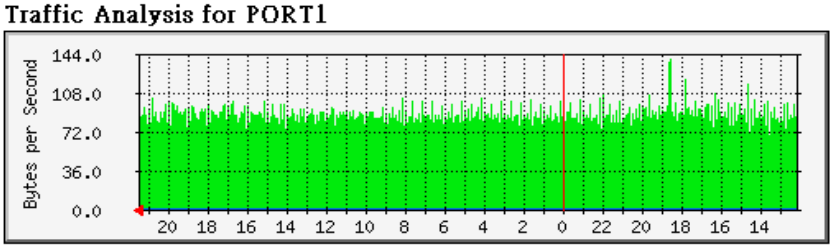
After clicking the Show History Data button, you will see graphics of traffic and packet analysis for each port. See the Figure 1 for a sample of the graphics for Port 1, Port 2, and Port 3.

If you click Display Client Info, or Display Connection Info, you will see detailed information about the current NAT functions, including protocol, ISP, alias IP, source and destination transmission amounts and protocols. See Figure. 2 for the panel displayed. The different buttons show different arrangements of the same information.

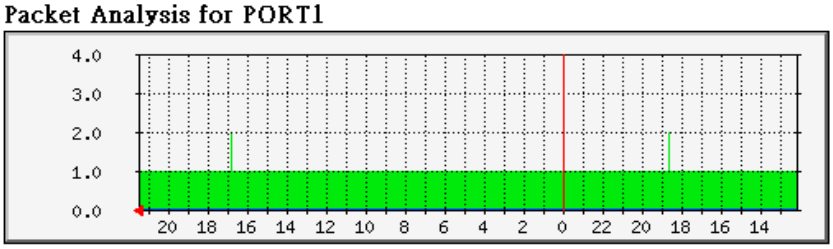
The Health Check Log Button will display information about potential network failures and failover occurrences. See figure 3 for an image of the displayed information.

History Data Index Page for Interface

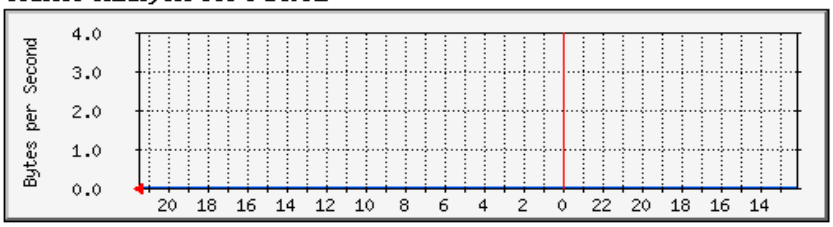
Traffic Analysis for PORT1



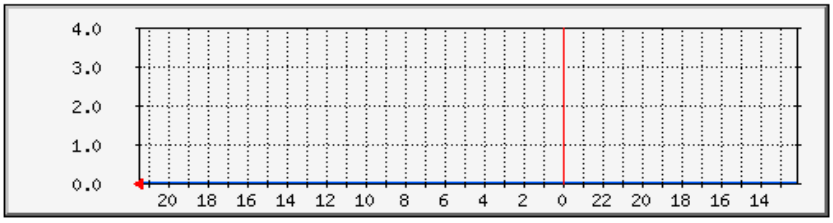
Packet Analysis for PORT1



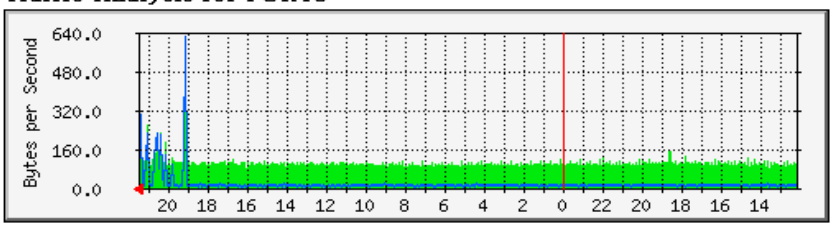
Traffic Analysis for PORT2



Packet Analysis for PORT2



Traffic Analysis for PORT3



Packet Analysis for PORT3

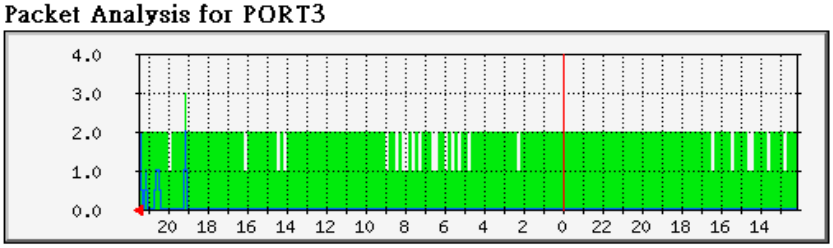


Figure 1: Graphics showed after clicking the Show History Data button.

NAT Info Fast Print Version Zoom in Zoom out

ISP	Source IP Address	Protocol	Connections	Send Bytes	Recv Bytes	Total Bytes	Send Pkts	Recv Pkts	Total Pkts
Hinet_dialup	61.230.0.232	Udp	9	360	0	360	9	0	9
Neteyes	10.88.169.86	Udp	2	2,028	4,584	6,612	30	30	60
Neteyes	10.88.168.146	Tcp	1	419,179	409,577	828,756	2,265	1,267	3,532
Adsl_leaseline	10.88.168.217	Udp	12	2,180	1,625	3,805	36	36	72
Neteyes	10.88.168.132	Tcp	13	374,231	34,605	408,836	632	361	993
Neteyes	10.88.168.217	Udp	11	2,537	1,539	4,076	32	32	64
Adsl_leaseline	10.88.168.144	Udp	4	916	631	1,547	9	6	15
Adsl_leaseline	10.88.168.132	Tcp	13	527,757	29,858	557,615	759	481	1,240
Hinet_dialup	10.88.169.60	Udp	3	1,671	610	2,281	12	12	24
	10.88.168.23	Tcp	2	1,074	0	1,074	10	0	10
Hinet_dialup	10.88.169.24	Udp	4	160	0	160	4	0	4
Neteyes	10.88.168.179	Udp	2	1,539	645	2,184	10	10	20
Neteyes	202.160.87.15	Udp	10	400	0	400	10	0	10
Hinet_dialup	10.88.168.217	Udp	14	2,586	6,440	9,026	40	40	80
Adsl_leaseline	10.88.168.170	Udp	6	2,401	1,409	3,810	22	22	44
Neteyes	10.88.168.182	Udp	3	1,820	743	2,563	13	13	26
Adsl_leaseline	10.88.169.86	Udp	2	2,177	4,919	7,096	32	32	64
Adsl_leaseline	10.88.168.217	Tcp	8	37,694	24,574	62,268	95	83	178
Hinet_dialup	10.88.168.132	Tcp	10	223,554	13,921	237,475	338	232	570
Adsl_leaseline	221.217.161.49	Udp	7	53,963,500	0	53,963,500	539,635	0	539,635
Hinet_dialup	10.88.168.160	Tcp	3	117,015	313,780	430,795	2,246	2,427	4,673
Hinet_dialup	10.88.168.182	Udp	2	1,366	508	1,874	11	11	22
Adsl_leaseline	221.217.161.75	Udp	7	24,394,700	0	24,394,700	243,947	0	243,947
Neteyes	210.71.60.125	Tcp	1	199,601	5,932,745	6,132,346	3,619	5,209	8,828
Neteyes	10.88.169.60	Udp	3	1,078	586	1,664	11	11	22
Adsl_leaseline	10.88.168.179	Udp	2	803	679	1,482	6	6	12
Neteyes	202.96.64.70	Udp	1	324	520	844	5	5	10
Adsl_leaseline	10.88.168.157	Tcp	1	39,790	103,634	143,424	850	595	1,445
Neteyes	10.88.168.169	Tcp	1	71,759	360,934	432,693	1,617	1,421	3,038
Neteyes	10.88.169.24	Udp	3	120	0	120	3	0	3

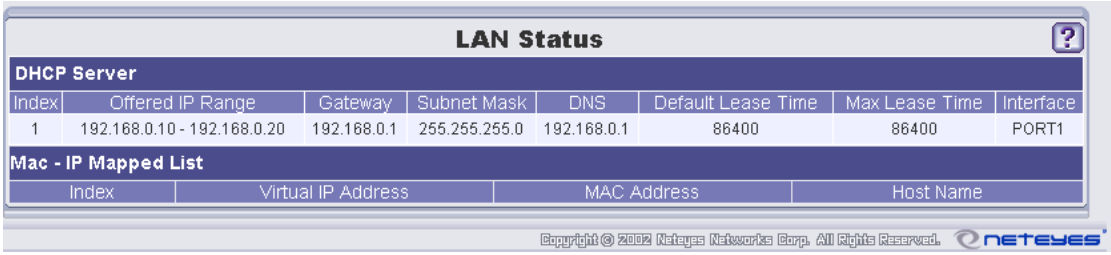
Figure 2: The graphics showed after clicking the Display Client Statistics / Connection Info.

Health Check Log Filter: Refersh

```
failover: isp_monitor 1 no time data append
failover: isp_monitor 1 received packet (56 bytes from 61.61.129.166)
failover: isp_monitor 1 attempt 1 PING 168.95.1.1 from 202.160.87.15, send 40 Bytes
failover: isp_monitor 1 timeout 3 identity 27303 retry 3, interval 3
failover: 2005-05-31 16:34:43 isp_monitor 1 link Neteyes is UDP mode
failover: isp_monitor 3 no time data append
failover: isp_monitor 3 received packet (56 bytes from 61.230.0.254)
failover: isp_monitor 3 attempt 1 PING 168.95.1.1 from 61.230.0.232, send 40 Bytes
failover: isp_monitor 3 timeout 3 identity 20679 retry 3, interval 3
failover: 2005-05-31 16:34:42 isp_monitor 3 link HiNet_Dialup is UDP mode
failover: isp_monitor 2 no time data append
failover: isp_monitor 2 received packet (56 bytes from 211.78.0.253)
failover: isp_monitor 2 attempt 1 PING 168.95.1.1 from 202.160.81.45, send 40 Bytes
failover: isp_monitor 2 timeout 3 identity 53806 retry 3, interval 3
failover: 2005-05-31 16:34:40 isp_monitor 2 link ADSL_Leaseline is UDP mode
failover: isp_monitor 1 no time data append
failover: isp_monitor 1 received packet (56 bytes from 61.61.129.166)
failover: isp_monitor 1 attempt 1 PING 168.95.1.1 from 202.160.87.15, send 40 Bytes
failover: isp_monitor 1 timeout 3 identity 27302 retry 3, interval 3
failover: 2005-05-31 16:34:40 isp_monitor 1 link Neteyes is UDP mode
failover: isp_monitor 3 no time data append
failover: isp_monitor 3 received packet (56 bytes from 61.230.0.254)
```

Figure 3: The graphics shown after clicking the Display Health Check button.

4-4-3 LAN Status



LAN Status

DHCP Server

Index	Offered IP Range	Gateway	Subnet Mask	DNS	Default Lease Time	Max Lease Time	Interface
1	192.168.0.10 - 192.168.0.20	192.168.0.1	255.255.255.0	192.168.0.1	86400	86400	PORT1

Mac - IP Mapped List

Index	Virtual IP Address	MAC Address	Host Name

This option shows information on the current LAN configuration.

The DHCP Server section lists settings related to the DHCP addresses offered to clients: the DHCP address range, gateway, subnet mask, DNS, default lease time, max lease time and interface.

The Mac – IP Mapped List shows the reserved IP addresses and the MAC addresses they correspond with.

For more detailed information of these settings, see 4-1-4 DHCP Server, and 4-1-6 DHCP Mac-IP in this documentation.

4-4-4 Firewall Status

This option shows the current Firewall customizations.

For more detailed information of these settings, see 4-2-7 Firewall in this documentation.

4-4-5 QoS Status

This option shows the current QoS settings.

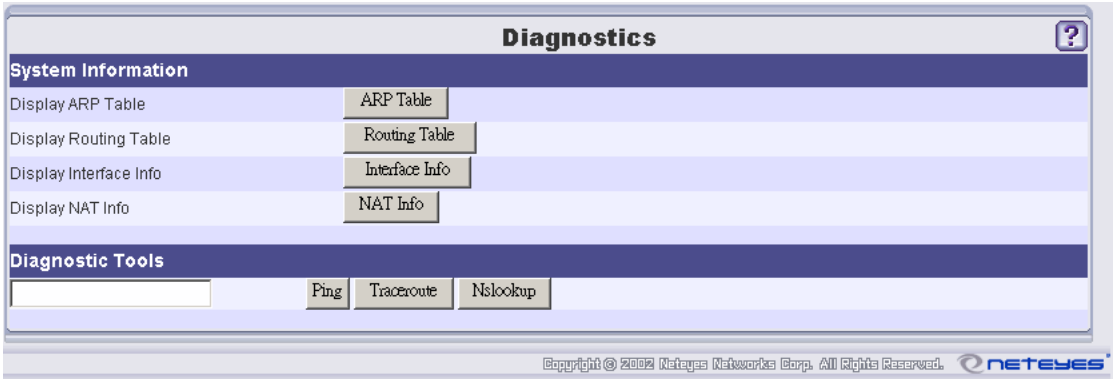
For more detailed information of these settings, see 4-2-6 QoS in this documentation.

4-4-6 Quota Status

This option shows the current Quota settings.

For more detailed information of these settings, see 4-1-14 Quota in this documentation.

4-4-7 Diagnostics



This option allows the administrator to perform a variety of diagnostic checks.

Display ARP Table

ARP (Address Resolution Protocol) is a TCP/IP protocol used to convert an IP address into a physical address, such as a MAC address. A host wishing to obtain a physical address will broadcast an ARP request onto the TCP/IP network. The host on the network with IP address within the request will then reply with its physical hardware address. This feature allows you to view the table of these known IP/MAC Address mappings.

Display Routing Table

This will show the table which the NexusWay 800 uses when determining which gateway to use while forwarding data.

Display Interface Info

This option shows the information relating to all the interfaces of NexusWay 800 (4 WAN and 2 LAN).

Display NAT Info

This shows the information about the current NAT connections and their protocols.

Diagnostic Tools

The diagnostic tools (ping, traceroute, and nslookup) are used as diagnostic tools to check IP addresses and the connection status.
Enter an IP address or Domain Name and select one of the 3 tools you want to use.

Ping is used to determine whether a specific IP address is accessible by sending several data packets to the specified address and waiting for a reply. Ping is primarily used to troubleshoot Internet connectivity.

Traceroute is used to trace the path a packet from your computer travels along to reach a remote host, the tool shows how many hops the packet requires to reach the host and the time each hop takes. Traceroute can help determining where the longest delays are occurring. And traceroute works by sending packets with low time-to-live (TTL) fields. The TTL value specifies how many hops the packet is allowed before it is returned. When a packet can't reach its destination due to an excessively low TTL value, the last host returns the packet and identifies itself. By sending a series of packets and incrementing the TTL value with each successive packet, traceroute finds out which are the intermediary hosts.

Nslookup is a tool to query a DNS server and look up the IP address information of computers in the Internet.

4-4-8 Admin Password

This option allows you add and remove administrators for your NexusWay 800.

After entering a username and password, you can also enter an IP in the Allow IP Address column to restrict the administrator so that they may only login from this specific IP address. Each administrator can have either read and write access, or read only access.

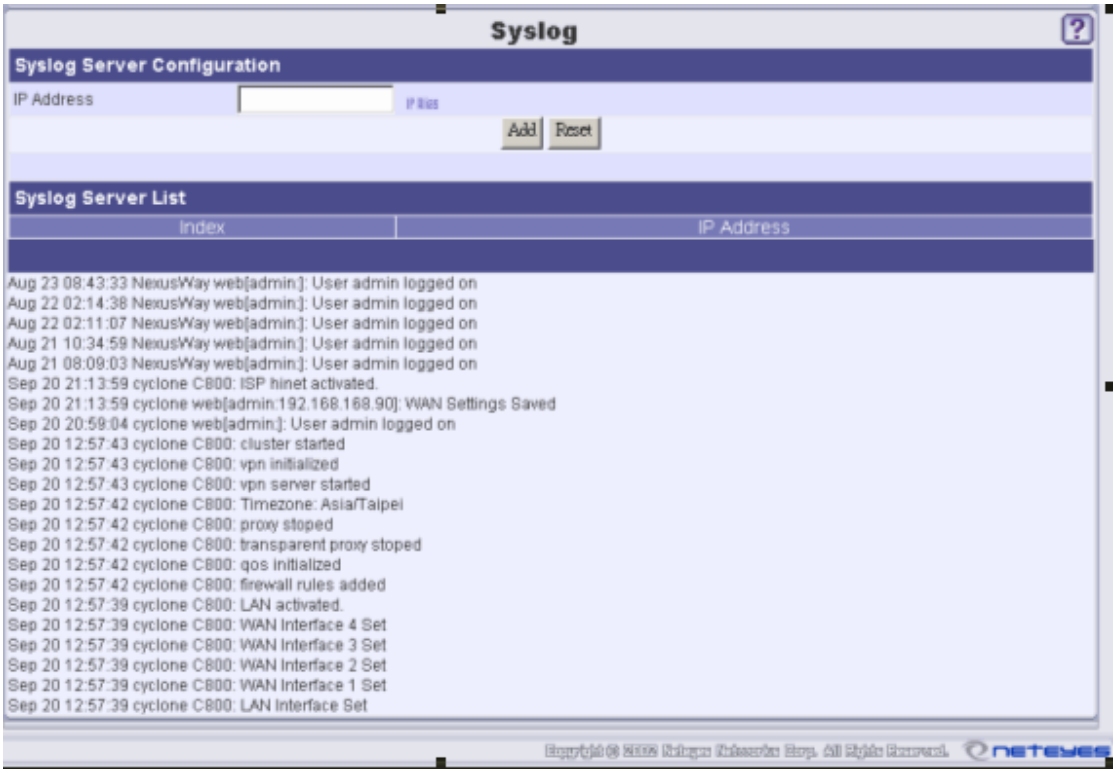
All the administrators you configure will be listed in the Administrator List.
The default administrator with user name as "admin" and password as "123456" is available in the list when you first login to a the NexusWay 800. You can right click the default setting to delete it, and then add new administrators.

NOTE:

- **When using the allow IP Address column, if you were to enter "192.168.0.140", only this IP could login into the NexusWay 800 with that username and password. However, if you enter "192.168.0", IPs from 192.168.0.1 to 192.168.0.255 are allowed to login. By keeping this column empty, EVERY IP is allowed to login.**

- **Click the Save button on right top corner of the panel after you finish entering all the data on this page – otherwise you will immediately lose all the settings when exiting the page.**

4-4-9 Syslog

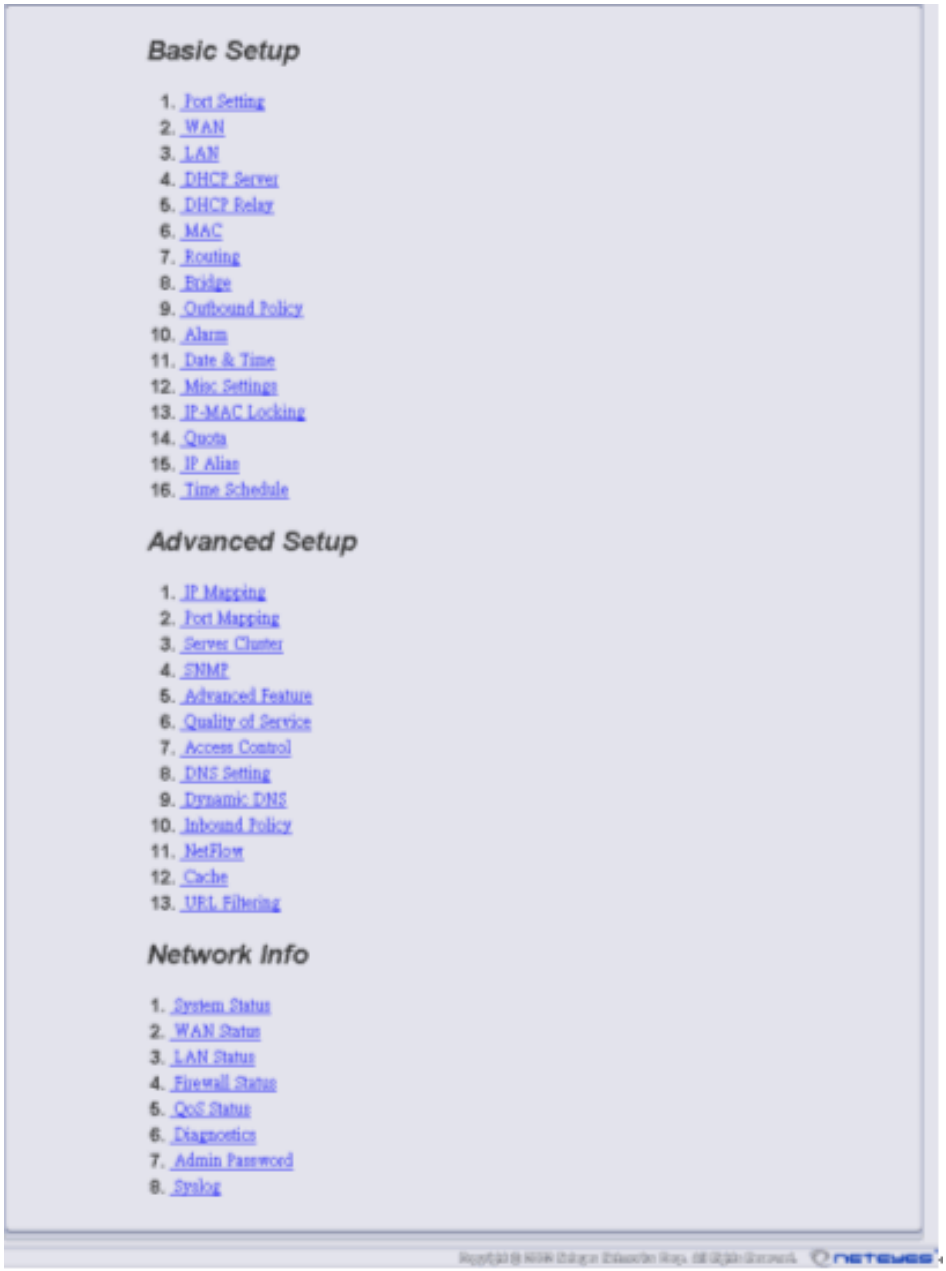


This option allows the administrator to export syslog messages to external machines and view some critical messages. Enter the IP address of the machine where you want to export the syslog messages to (UDP packets on port 514). The client machine must have a syslog client installed to properly receive the syslog messages (RFC 3164 describes the protocol used).

There is a “Show syslog in a New Window” button, which will display an extended syslog in a new window.

In the "Syslog Server List", you can see some logs concerning changes and events in the NexusWay 800. These syslog events are generated by administrators and some internal functions of NexusWay 800. You can see more detailed syslog messages by exporting the messages to a client machine. Only several recent events will be listed and most current one will located at the top.

CHAP 5. HELP



Click the subject, which you have problems with while operating or configuring for more online instruction or information.

CHAP 6. APPENDIX

6-1. Appendix 1 - Trouble Shooting

This chapter covers some common problems you may encounter while operating the NexusWay 800 and possible solutions. If the NexusWay 800 still does not function properly after performing the following steps, please contact your dealer for further advice.

6-1-1 General Problems

Problem 1: I cant connect to my NexusWay for initial configuration.

Solution 1: Check the following steps:

1. Is the NexusWay is properly installed with successful LAN connections, and powered ON?

2. Ensure that your PC and the NexusWay are on the same network segment. (If you don't have a router, this is required; when using a router it must be on the same network segment.)

3. Is your PC is set to "Obtain an IP address automatically" (DHCP client)? Did you restart it?

4. If your PC uses a Static (Fixed) IP address, ensure it is using an IP address inside the range of 192.168.0.2 to 192.168.0.254 and is compatible with the NexusWay's default IP address (192.168.0.1). In addition, the Network Mask should be set as 255.255.255.0 to match the NexusWay. In a Windows environment, you can check these settings using the Control Panel-Network then checking the Properties of TCP/IP protocol. See section 2-1 part 6 “”configuring administrator's IP address”

6-1-2 Internet Access

Problem 1: I had a “time out error” occur when I entered a URL or IP address.

Solution 1: This error has several possible reasons. Try the following troubleshooting steps.

1. Check if other PCs work correctly. If so, ensure the IP settings of your PCs are correct. To use a Static IP address, check the Network Mask, Default gateway and DNS as well as the IP address you have configured. Ensure these settings fall within the correct settings for the NexusWay’s current configuration.

2. If other PCs fail to operate properly with the correct configurations, check the NexusWay’s connections: power, WAN, and LAN. If you also cant connect to the NexusWay check the power and LAN connections.

3. If you can connect to the NexusWay and it is configured correctly, check your Internet connections (DSL/Cable modem etc) to ensure they are working properly.

6-2. Neteyes Customer Service Information

UK

Address: The Barracks Wakefield road, Pontefract West Yorkshire wf8 4hh
Telephone: +44-845-6443-226
FAX: +44-845-6443-227
Web: http://www.neteyes.eu.com
E-mail: Sales: sales@neteyes.eu.com
Support: support@neteyes.eu.com
General: info@neteyes.eu.com

Southern Asia

Address:
Menara Maxis, 36th Floor, Kuala Lumpur City Centre,
Kuala Lumpur, 50088, Malaysia
Telephone: +603-2615-7213
FAX: +603-2164-5157
Web: http://www.neteyes.biz
E-mail: Sales: sales@my.neteyes.biz
Support: support@my.neteyes.biz
General: info@my.neteyes.biz

台灣 - 全球總部 (Headquarters)

地址：台北市內湖區內湖路一段 120 巷 13 號 6 樓之一
電話： +886-2-2657-2813
傳真： +886-2-2657-2814
網址：http://tw.neteyes.biz
電子郵件： 業務方面：sales@tw.neteyes.com
技術支援：support@tw.neteyes.com
一般資訊：info@tw.neteyes.com

中国大陆

地址：北京市朝阳区光华路丙 **12** 号数码 **01** 大厦 **22** 层 **04A**
电话：+86-10-6500-7618
传真：+86-10-6500-7617
网址：http://cn.neteyes.biz
电子邮件： 业务方面：sales@cn.neteyes.com
技术支持：support@cn.neteyes.com
一般信息：info@cn.neteyes.com