CE Mark Warning

This equipment complies with the requirements relating to electromagnetic compatibility, EN55022 class B for ITE, the essential protection requirement of Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility.

FCC Certifications

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

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

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.

Company has an on-going policy of upgrading its products and it may be possible that information in this document is not up-to-date. Please check with your local distributors for the latest information. No part of this document can be copied or reproduced in any form without written consent from the company.

Trademarks:
All trade names and trademarks are the properties of their respective companies.

Copyright © 2003, All Rights Reserved.

Document Version: 2.0

Table of Contents

WELCOME TO MULTI HOMING 1

SETTING UP THE HARDWARE..... 2

NETWORKING WITH THE WIZARD 3

UNDERSTANDING THE USER INTERFACE 4

BASIC CONFIGURATION..... 6

- Connection Type Set-up 8
- Configuring a static IP address..... 8
- Configuring a (Dynamic) DHCP Account 9
- Configuring Multi Homing to use a PPPoE account..... 10
- Configuring Multi Homing to use a PPTP connection..... 12
- NAT configuration 13
- Configuring the DNS Service 14
- Load Balance Configuration 15
- Cloning a MAC address..... 17
- Dynamic DNS Configuration..... 18
- LAN interface Configuration 21
- Router Service Configuration 23

SECURITY..... 24

- Disabling ICMP replies 25
- Blocking individual (or service port) of IP addresses on the Internet..... 27
- Modifying an IP address or removing an policy from the incoming policy list..... 28
- Blocking individual (or service port) of LAN clients from accessing the Internet..... 28
- Mapping Internal Ports to the Outside 30
- Configuring a Virtual Server 32

PORT TRIGGERING CONFIGURATION 33
URL BLOCKING 34

INTRANET 35

ACTIVATING/DEACTIVATING THE DHCP SERVICE 36
IP ADDRESS POOL ASSIGNMENT 36
AUTOMATIC MAC-IP ASSOCIATION 39

ADMINISTRATION 40

CHANGING THE VALID USER AND PASSWORD 42
CONTROLLING WEB ACCESS CONFIGURATION BY IP ADDRESS 43
DISPLAY SYSTEM STATUS 45
SETUP SYSTEM TIME 45
SETUP ROUTER SERVICES TIME 47
RESTARTING YOUR SYSTEM 48
SET FACTORY DEFAULT 48
UPDATE YOUR SYSTEM SOFTWARE 47
PRESERVING YOUR SYSTEM CONFIGURATION 49
LOADING YOUR SYSTEM CONFIGURATION 49
VIEW SYSTEM LOG 49

APPENDIX A
SPECIFICATIONS & ACCESSORIES

SYSTEM LED 52
PORT LED 52
PORTS' LED SUMMARY TABLE 53
FACTORY SETTING BUTTON 54
KEY FEATURE 55

APPENDIX B
SPECIFYING INTERNET ADDRESSES 57

APPENDIX C
COMMON PORT NUMBERS 59

Welcome to Multi Homing

Chapter 1

The safest and most convenient way to the Info Superhighway

Welcome to Multi Homing! This powerful network tool will enable you to securely connect multiple computers to the Internet through a single DSL/Cable modem or T1/E1/ISDN CSU/DSU.

Through this simple comprehensive appliance, you can connect multiple computers in your home or office using standard Ethernet networking.

Its highly configurable built-in network firewall provides you with the power to choose specific services allowed through your network, while keeping all malicious Internet attackers out. Multi Homing also provides super advanced features like transparent proxy caching, remote utilization monitoring, virtual private networking, printer sharing and sophisticated bandwidth control.

The simple Web-based interface will help you configure your Multi Homing with true point-and-click ease.

This document will provide you with the guidance needed to tailor-fit Multi Homing to your own networking needs.

Thank you for choosing Multi Homing to be part of your networking solution.

Setting up the Hardware

Chapter 2

Network cabling made easy.

Multi Homing is a turnkey solution to connect your home or office to the Internet through a high speed or 'always on' connection. The following easy steps will get you hooked up and ready to go onto the Internet.

1. Behind the Multi Homing unit, locate 6 Ethernet network ports (RJ-45). These look like standard phone jacks, but wider.
2. Connect the wide area network (WAN) uplink port to the equipment provided by your Internet service provider (ISP) (e.g. Cable/DSL modem or T1/E1/ISDN CSU/DSU)
3. Connect the local area network (LAN) port to your office network hub or switch
4. Set up a computer on your LAN[1] to obtain a dynamic IP address (please refer to your operating system manual or reference guide for details)
5. Obtain an IP address from Multi Homing
6. Start up a Internet browser on your configuration computer and point it to http://192.168.1.1. You should see the graphical user interface (GUI) screen.

Congratulations! You have completed the hardware configuration requirements for Multi Homing. Incidentally, you can now add to your title *"Network Administrator"*

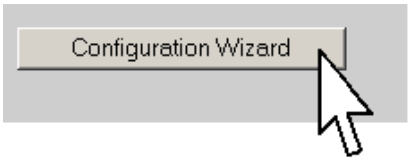
1 This computer will be referred to as the "configuration computer" or "Administrator computer" in other parts of this document

Networking with the Wizard

Chapter 3

Using the Multi Homing Networking Wizard is the fastest way to get started!

SecureSOHO comes with a web-based wizard that breezes you through configuration. The wizard presents you with each necessary configuration step and each possible option. Upon completion of a wizard based set up, Multi Homing will be ready for use. When set to factory defaults, the wizard starts up automatically -- It can also be invoked by clicking on the Configuration Wizard button on the home tab. At the end of the initial configuration, the appliance will ask the user for a username and password. This is a standard authentication mechanism used to ensure that subsequent configuration changes are done by the proper individuals. Do not give the username/password to people who are not authorized to change your network configuration.



Understanding the User Interface

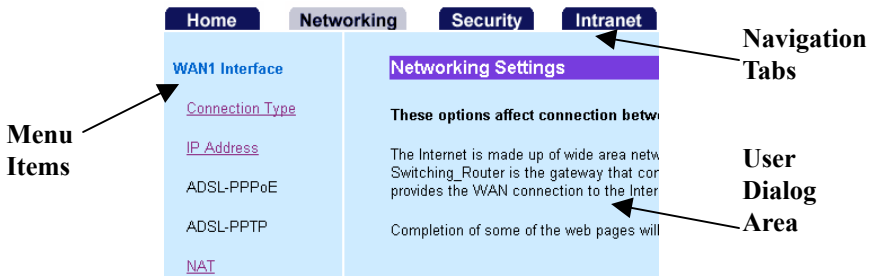
Chapter 4

Navigation Rules

Multi Homing has a web-based graphical user interface (GUI) that can be accessed using a standard HTML (HTTP v1.0) compliant browser. Once the LAN is properly connected a network administrator can connect to it through the URL http://192.168.1.1

The GUI has two main navigational components: Tabs and Menus.

Each Tab represents a major group of functions that a user can configure and are located on the top part of the screen.



The Home tab presents version information as well as a brief feature list. The Networking tab includes all the essential configuration items required to get a LAN up and running.

The Security tab provides configuration items that control firewall behavior. By default, Multi Homing comes configured to lock out unsolicited network connections. To allow specific services to be allowed through Multi Homing, some modifications under this tab is required.

The Intranet tab accommodates changes that are LAN specific. Under this tab, a network administrator can specify rules for the assignment of IP addresses as well as manipulate tools that improve local area network performance and resource availability, such as the transparent proxy cache.

The Administration Tab provides control, monitoring and troubleshooting tools.

The Help Tab provide additional context sensitive information.

Menus are located at the left side of the screen provides additional navigation for tab components.

After each session involving configuration modifications, the changes should be saved and the system should be restarted to activate the changes.

Basic Configuration

Chapter 5

First things first

This chapter covers the use of all the configuration items under the Networking Tab. Once configured, you should be able to securely access the Internet through your Multi Homing.

Wide Area Network (WAN1)

The Internet is made up of wide area networks (WAN) and local area networks (LAN). Each local area network connects to the Internet through a wide area network.

The Multi Homing is the gateway used by your LAN to connect to your WAN. Your WAN is provided by your Internet service provider (ISP) using a WAN medium (Cable/DSL modem or T1/E1/ISDN CSU/DSU).

You will need information provided by your ISP to complete this step.

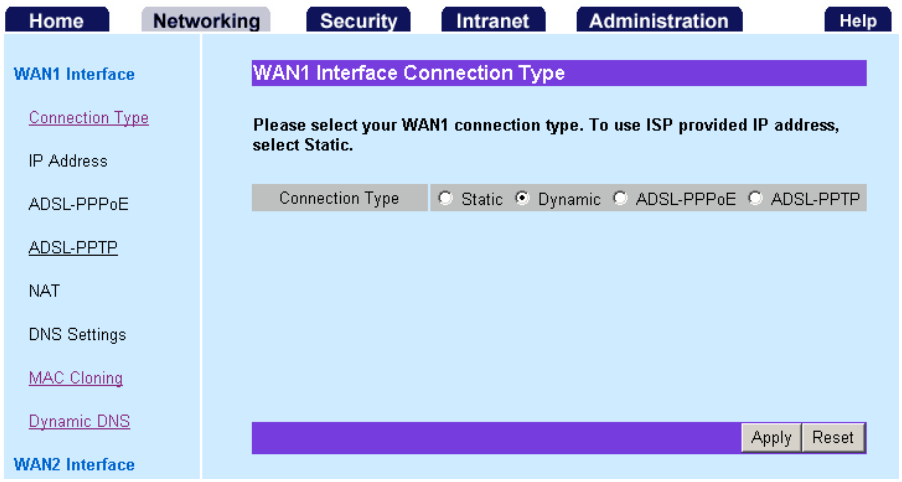
Depending on your WAN medium, your ISP may provide you with either a static or dynamic (DHCP/BootP) connection. This information should be included in the package that came from your ISP. Generally, if your ISP has provided you with a fixed IP address, you have a static IP address. If your ISP has provided a username and password, you have a PPPoE[2] link. If your ISP provided neither an IP address or username/password pair, you most likely have a DHCP based connection. If unsure, contact your Internet provider's customer support.

2 Point to Point Protocol over Ethernet (PPPoE) is a common authentication/billing mechanism used by ISPs.

Dynamic Host Configuration Protocol (DHCP) based configurations do not require further set-up since IP address, gateway and DNS information are automatically set by the ISP.

Secondary Wide Area Network (WAN 2)

Multi Homing has a second WAN port for a secondary WAN connection to the Internet. Having two WAN ports, Multi Homing can share the Internet traffics thru load balancing. The setup of secondary WAN interface (WAN 2) is the same as the primary WAN interface. You can choose a second ISP to provide your WAN 2 connection. Like primary WAN connection, you have the choice of Static, Dynamic, PPPoE connection type to suit your ISP supporting package. Otherwise, you may simple disable it if this does not apply to you.



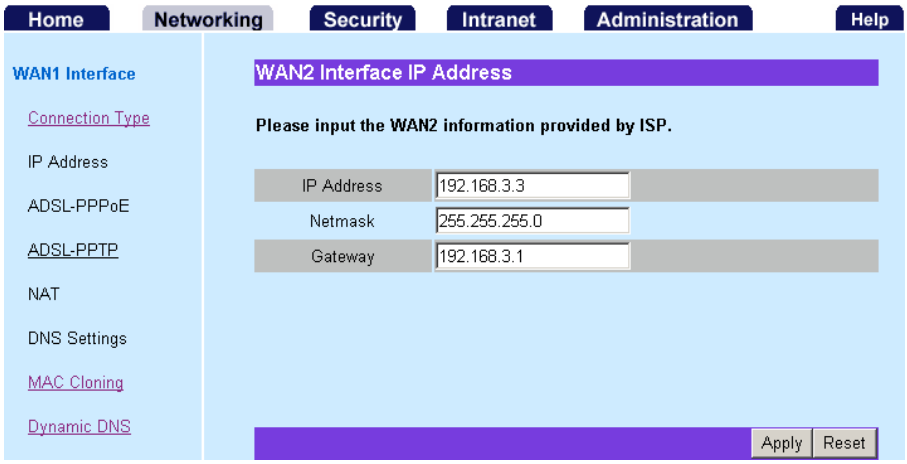
CONNECTION TYPE SET-UP

1. Determine which connection type is assigned by ISP (check documentation provided by ISP)
2. Click on **Networking** tab
3. Under the WAN1 Interface menu item, click on **Connection Type**
4. Click on the appropriate radio button
5. Click on **Apply**
6. Do the rest of setting according to prompt window

CONFIGURING A STATIC IP ADDRESS

1. Determine the fixed IP address assigned by the ISP
2. Click on the **Networking** tab
3. Under the WAN2 Interface menu item, click on **IP Address**[3]
4. Enter the IP address provided by the ISP in the appropriate text box
5. Enter the netmask of the IP address provided by the ISP in the appropriate text box
6. Enter the default router (or gateway) information provided by the ISP in the appropriate text box.
7. Click on **Update**
8. Do the rest of setting according to prompt window

3 This option is only available if the connection type is configured to be **static**

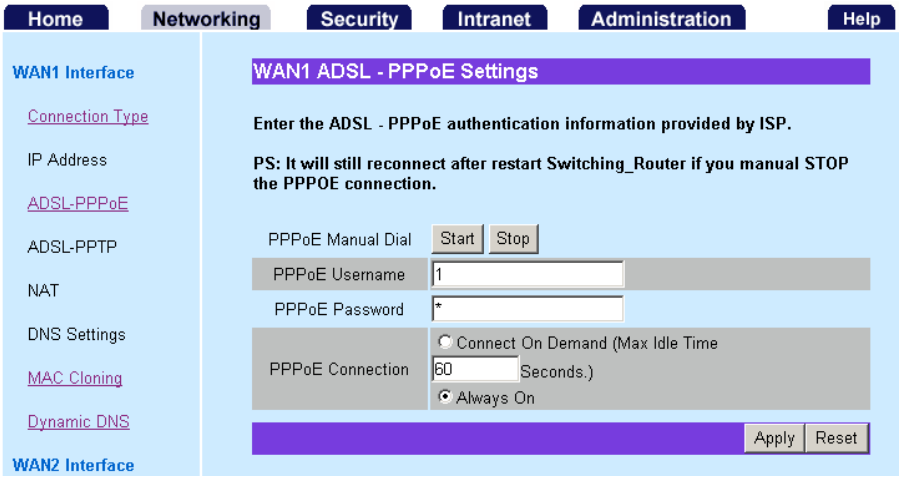


CONFIGURING A (DYNAMIC) DHCP ACCOUNT

DHCP accounts do not need further configuration. However, for DHCP accounts with ISPs that restrict IP addresses to specific MAC addresses, see the subsection on MAC Cloning in the Advanced Networking Tools section of this chapter.

CONFIGURING MULTI HOMING TO USE A ADSL PPPOE ACCOUNT

1. Determine the username and password information provided by the ISP
2. Click on the **Networking** tab
3. Under the WAN1 Interface menu item, click on **ADSL-PPPoE**
4. Enter the username and password provided by the ISP into the appropriate fields.
5. Select the appropriate connection mode for your ADSL-PPPoE link[4]
6. Click on **Apply**
7. Do the rest setting according to prompt window



4 ADSL-PPPoE allows your ISP to monitor the amount of time you are using the Internet for billing purposes. If your ISP or network provider bills you for the amount of time that you are connected, you should set the 'Connect on Demand' option and set the 'Maximum Idle Time'. This feature automatically connects your system when needed, and disconnects it if you are not using the Internet. This feature is both convenient and practical.

STARTING WAN1 ADSL-PPPOE MANUALLY

1. Click on **ADSL-PPPoE** under WAN1 Interface in the **Networking** tab.
2. Click on **Start**

STOPPING WAN1 ADSL-PPPOE MANUALLY

1. Click on **ADSL-PPPoE** under WAN1 Interface in the Networking tab.
2. Click on **Stop**.

CONFIGURING MULTI HOMING TO USE A PPTP CONNECTION

1. Click on **Connection Type** under WAN1 Interface in the **Networking** tab.
2. Click on **ADSL-PPTP** and press **Apply**.
3. Enter My IP Address (ex: 192.168.100.100), My Subnet Mask (ex: 255.255.255.0), Server IP Address (ex: 192.168.100.1), PPTP Account (ex: 123456) , PPTP Password (ex: 123456) and press **Apply**.

NAT CONFIGURATION

SET UP ONE-TO-MANY NAT WITH WAN1 INTERFACE

1. Click on **NAT** under WAN1 Interface in the **Networking** tab.
2. Click on **One-to-Many NAT** and press **Apply**.

SET UP MANY-TO-MANY NAT WITH WAN1 INTERFACE

1. Click on **NAT** under WAN1 Interface in the **Networking** tab.
2. Click on **Advanced** Setting.
3. Enter Public IP Range (ex: 61.220.168.202-61.220.168.206).
4. Press **Apply**.

SET UP ONE-TO-ONE NAT WITH WAN1 INTERFACE

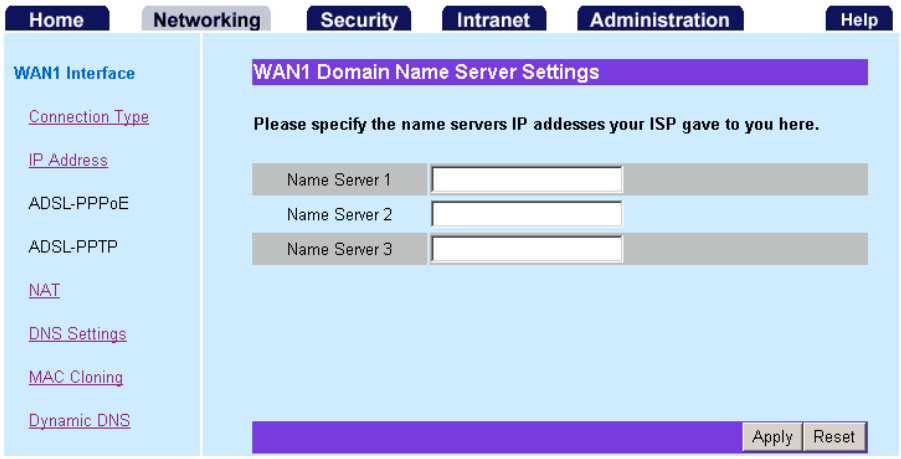
1. Click on **NAT** under WAN1 Interface in the **Networking** tab.
2. Click on **Advanced Setting**.
3. Enter Public IP in WAN (ex: 61.220.168.204), Private IP in LAN (ex: 192.168.1.50).
4. Click on **Apply**

Domain Name Service (DNS)

Domain name service helps you to work with IP addresses by mapping them out to simple 'human readable' names. Multi Homing needs the correct values for certain LAN side client services (like web-browsing) to work properly. The DNS server IP addresses should be provided to you by your ISP.[5]

CONFIGURING THE DNS SERVICE

1. Click on the **Networking** tab
2. Under the WAN1 interface menu item, select **DNS Settings**
3. Enter up to 3 DNS IP addresses into their corresponding fields
4. Click on **Apply**



Load Balance

SETTING LOAD BALANCE BY BANDWIDTH

1. Click on **Load Balance** under WAN2 Interface in the

5 DHCP and PPPoE configurations may not require this step.

Networking tab.

2. Choose **Bandwidth** in **Load Balance** by combo box.
3. Choose Rate in **WAN1:WAN2** combo box (ex: 50%: 50%).
4. Press **Apply** button.

SETTING LOAD BALANCE BY IP

1. Click on **Load Balance** under WAN2 Interface in the **Networking** tab.
2. Enter some IP addresses (ex: 140.131.50.20) in the text box under Hosts which use WAN#1.
3. Enter some IP addresses (ex: 211.72.254.6) in the text box under Hosts which use WAN#2.
4. Press **Apply**.

SETTING LOAD BALANCE BY PORT

1. Click on **Load Balance** under WAN2 Interface in the **Networking** tab.
2. Click some items under Ports which use **WAN#1**.
3. Click some items under Ports which use **WAN#2**.
4. Press **Apply**.

ADDING LOAD BALANCE PREDEFINED PORT

1. Click on **Load Balance** under WAN2 Interface in the **Networking** tab.
2. Click on **Predefined**.
3. Enter Port Number (ex: 23), Description (ex: Telnet), and press **Apply**.

DELETING LOAD BALANCE PREDEFINED PORT

1. Click on **Load Balance** under WAN2 Interface in the **Networking** tab.
2. Click on **Predefined**.
3. Choose one pair of item and leave them blank.

Advanced Networking Tools

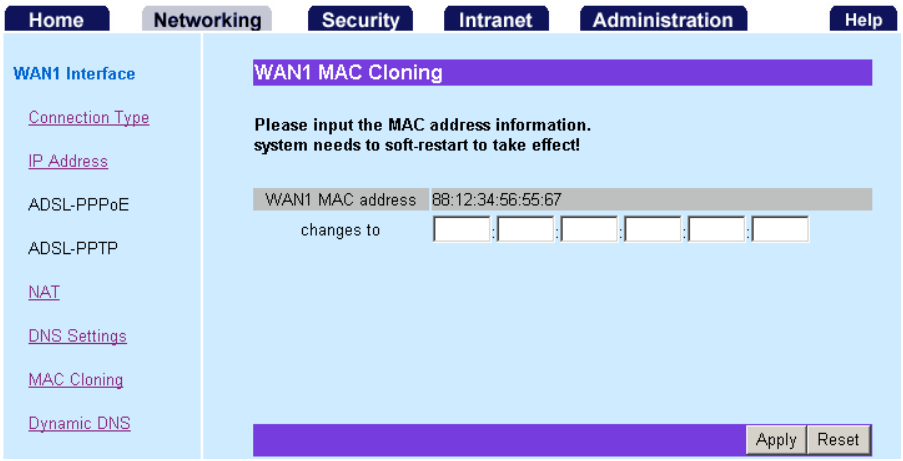
Multi Homing provides advanced networking features that aid in deploying the network. The crafty Network Administrator can find various applications for these tools.

MAC Cloning

Some ISPs audit connections using the MAC addresses[6]. These systems only allow 'registered' MAC address to connect to the Internet. To circumvent this obstacle, Multi Homing provides a 'MAC Cloning' feature which allows the Network Administrator to modify the MAC address that is reported to the ISP. This feature facilitates the use of Multi Homing in such environments.

CLONING A MAC ADDRESS

1. Obtain a registered MAC address (to determine the MAC address on a desktop computer, refer to the operating system manual)
2. Click on the **Networking** tab
3. Under the WAN1 Interface menu item, click on **MAC Cloning**
4. Enter the MAC address obtained in step 1 (separate each hex-byte by a colon, e.g. AA:BB:CC:DD:EE:FF)
5. Click on **Apply**



6 Machine Access Control Layer Address (MAC Address) is a 6-byte (48-bit) number used to uniquely identify networking equipment. Each network interface card should have a unique MAC address assigned to it by its manufacturer. MAC addresses are commonly represented in hexadecimal values.

Dynamic DNS

Conventional DNS information associates a static IP address with a human readable machine name, for use on the World Wide Web. When a DNS server receives a name lookup request, it compares it against a list of published IP-host name associations. Once a match is found, the server replies with either the IP address or host name. Since the published lists are static, conventional DNS servers are unable to map DHCP or PPPoE configured hosts as the configuration protocols do not guarantee that the host computer will always have the same IP address. (thus, the IP address-hostname mapping will not always be correct).

Dynamic DNS overcomes the fixed IP requirement of conventional DNS by running a daemon that automatically updates DNS server information. To avail of this service, you will have to register with one of several dynamic DNS service providers and configure Multi Homing to forward IP address changes to the dynamic DNS server.

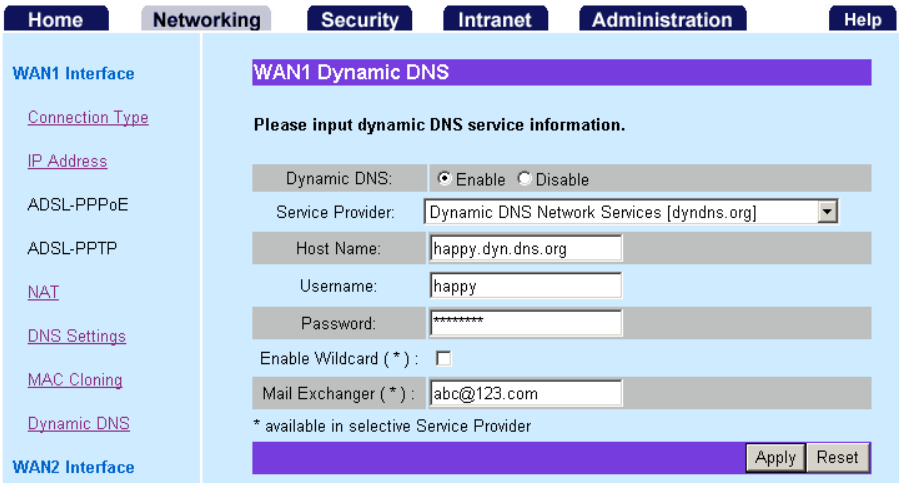
This feature is particularly useful for providing WAN side services (e.g. HTTP or FTP).

DYNAMIC DNS CONFIGURATION

1. Click on the **Network** tab
2. Under the WAN1 Interface menu item, click on **Dynamic DNS**
3. Click on **enable/disable** to **activate/deactivate** the feature
4. Select the **Service Provider** that you signed up on the drop down box[7]
5. Enter the registered hostname in the appropriate text box
6. Enter the username/password in the appropriate text boxes

7 Multi Homing does not have direct affiliations with the listed service providers an guarantees on the level of service provided by them

7. For some service providers, Enable Wildcard and Mail Exchanger can be specified.
8. Click on **Apply** to save changes



LAN (Local Area Network) Interface

In this section, you specify the IP address that the Multi Homing will use.

Multi Homing uses 192.168.1.1 as its default address, with a netmask of 255.255.255.0 (Class C netmask)[8]. This IP is used as the **default router**[9] for the LAN as well as the Web server address for the Multi Homing configuration interface.

Multi Homing allows a single Internet account to be shared by several computers. This is done through a principle called **Network Address Translation** (or NAT). Connection requests from LAN side computers are translated into the single IP address provided through the ISP account. Multi Homing tracks each individual LAN client connection in a way that the process is transparent to the LAN side computers. The NAT mechanism also provides part of the firewall features of Multi Homing since only LAN side initiated connections are translated. WAN side connection attempts are ignored unless specifically configured to be accepted (see chapter on **Security**).

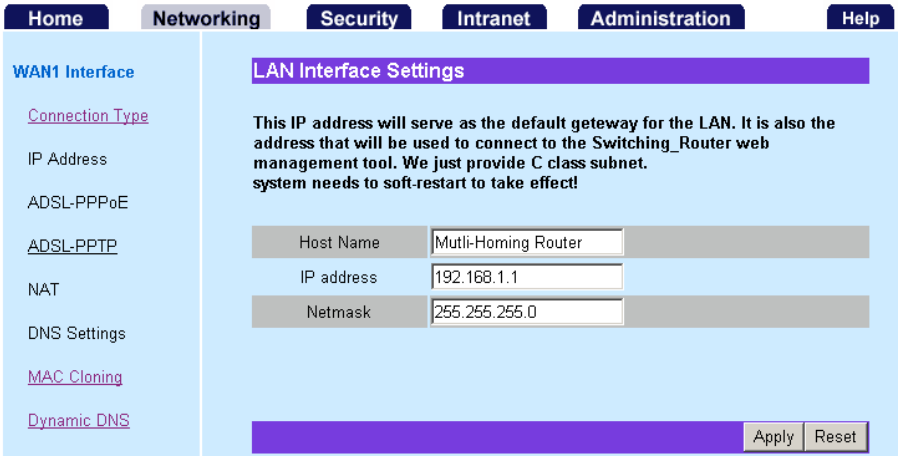
---

8 192.168.1.0-255 is a special range of Class C addresses set aside by the Internet Engineering Task Force (IETF) for use by private networks (see RFC 1918 for more details). RFCs (Refer for Comments) are documents published through the Internet Engineering Task Force (IETF) to solicit comments and present guidelines for proposed (as well as endorsed) Internet standards. Newer RFCs may be proposed which supersede the RFCs identified in this document.

9 Also called the default gateway. Changing this value on an already running LAN will require computers on the LAN with dynamically allocated IP addresses to renew their leases (see DHCP section) while computers on the LAN with statically allocated IP addresses will need to be reconfigured

CHANGING THE LAN IP ADDRESS

1. Click on the **Networking** tab
2. Under the LAN Interface menu item, click on **IP address**
3. Enter the **Host Name**
4. Enter the desired IP address in the appropriate field
5. You may enter **MAC address** to change LAN MAC address.
6. Click on **Apply** to save your changes



DYNAMIC ROUTING

SETTING DYNAMIC ROUTING PROTOCOL

1. Click on **Dynamic Routing** under Router Services in the **Networking** tab.
2. Click on **Yes** to enable **RIP support**.
3. Choose on **Version 1** of Send and Receive Protocol.
4. Choose on **Version 2** of Send and Receive Protocol.
5. Press **Apply**.

STATIC ROUTE

SETTING STATIC ROUTE (NET-TO-HOST)

1. Click on **Static Route** under Router Services in the **Networking** tab.
2. Choose host from **Type** combo box.
3. Enter **Destination**.
4. Choose WAN1 from **Dev** combo box.
5. Press **Apply**.

SETTING STATIC ROUTE (NET-TO-NET)

1. Click on **Static Route** under Router Services in the **Networking** tab.
2. Choose net from **Type** combo box.
3. Enter Destination, Netmask and Gateway.
4. Choose WAN1 from Dev combo box.
5. Press **Apply**.

Security

Chapter 6

Multi Homing is the key to controlling the flow of information

A real world firewall is built between buildings to slow down the progress of a disaster, and preserve valuable life and property. Network firewalls are put between networks to control the amount of information that flows through them. One of the fundamental goals of a firewall is to prevent unwanted connections from the outside of the network from entering the LAN. On the other hand, a firewall can also block connection from LAN to the Internet. A common practice of this feature is the URL (Uniform Resource Locator) blocking used by parents to limit access to certain Internet sites for their children. The Security tab enables the network administrator to fine-tune or customize various features of the Multi Homing firewall.

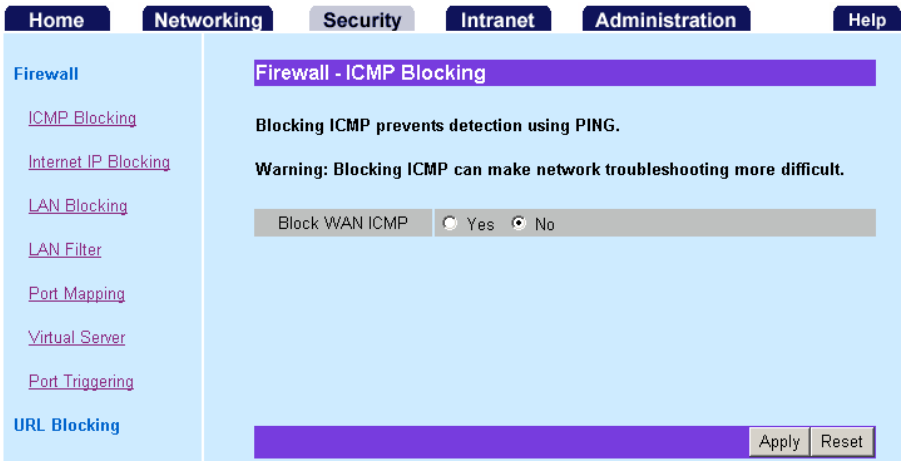
Packet Internet Groper (PING)

Packet Internet Groper (or 'ping') is a very useful utility used by network administrators to determine if a computer is up and running. The ping program sends a small packet to an address, if there is a computer assigned to the address, it sends a reply. Ping uses the Internet Control Messaging Protocol (ICMP). Multi Homing can be configured not to reply to PING requests.[10]

10 There are advantages as well as disadvantages to disabling PING replies. The crafty Network Administrator should determine if ICMP replies should be turned off.

DISABLING ICMP REPLIES

1. Click on the **Security** tab
2. Under the **Firewall** menu option, click on **ICMP Blocking**
3. Click on the appropriate radio button to enable/disable ICMP replies
4. Press **Apply**

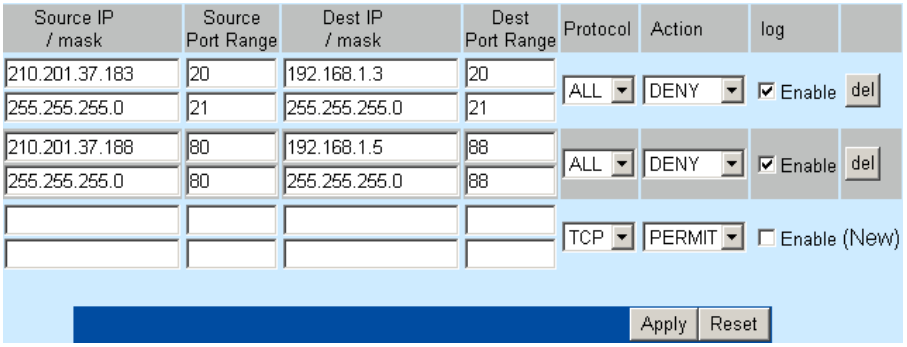


Keeping Stuff out

Multi Homing blocks all traffic from WAN side computers from getting into your LAN by default. On the other hand, LAN clients can connect to any computer that is on the Internet. This behavior can be modified to prevent particular (or all) LAN clients from accessing certain WAN side IP addresses. These features are useful for network administrators of offices or households that have policies or guidelines about the proper use of the Internet.

BLOCKING INDIVIDUAL (OR SERVICE PORT) OF IP ADDRESSES ON THE INTERNET

1. Click on the **Security** tab
2. Under the Firewall menu item, click on **Incoming Policy**
3. Enter the IP address and port number (or range) to be blocked onto the corresponding text box at the bottom of the list (marked New) according the following figure
4. Click combo box and select **protocol**
5. Click combo box and select **PERMIT/DENY** action
6. Check **Enable** box to log the event
7. Click on **Apply**



This figure describes all the IP address coming from **WAN** port will be **allowed** to access your LAN clients, but:

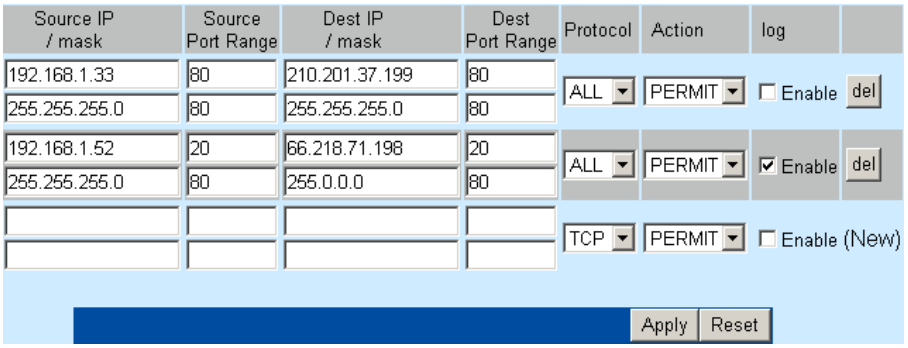
- Accessing to the port 20, 21 of IP 192.168.1.3 from IP 210.201.37.183 (with port 20, 21) will be **denied**
- Accessing to the port 88 of IP 192.168.1.5 from IP 210.201.37.188 (with port 80) will be **denied**

MODIFYING AN IP ADDRESS OR REMOVING AN POLICY FROM THE INCOMING POLICY LIST

1. Click on the **Security** tab
2. Under the Firewall menu item, click on **Incoming Policy**
3. To modify an IP address, enter new parameters
4. To remove an **Policy**, click the **del** key
5. Click on **Apply**

BLOCKING INDIVIDUAL (OR SERVICE PORT) OF LAN CLIENTS FROM ACCESSING THE INTERNET

1. Click on the **Security** tab
2. Under the Firewall menu item, click on **Outgoing Policy**
3. Enter the IP address and port number (or range) to be blocked onto the corresponding text box at the bottom of the list (marked New) according the following figure
4. Click combo box and select **protocol**
5. Click combo box and select **PERMIT/DENY** action
6. Check **Enable** box to log the event
7. Click on **Apply**



This figure describes all the IP address coming from **LAN** port will be **denied** to access WAN services, but:

- Accessing to the port 80 (HTTP service) of WAN IP 210.201.37.199 from LAN IP 192.168.1.33 (with port 80) will be **allowed**
- Accessing to the port 20~80 of WAN IP 66.218.71.198 from LAN IP 192.168.1.52 (with port 20~80) will be **allowed**

Letting Stuff in

By default, Multi Homing is deployed in firewall mode and will not allow outside computers to reach the LAN unless the connection is initiated by a LAN client. Multi Homing empowers network administrators to allow WAN clients to access certain services provided by LAN clients. In other words, it is possible for WAN side computers to initiate connections provided the Network Administrator allows it.

This is done through a technique called **Port Mapping**[11]. When computers on the Internet communicate, they do so through IP addresses and special numbers called port addresses (or simply ports). The port determines which service is trying to connect to (e.g. port 80=HTTP/Web services). Each service also has what is known as a transmission protocol (either TCP or UDP). To properly use this feature, you would need the connection details for the service you wish to open to the Internet. Each WAN port/LAN IP/port group is called a **rule**. In addition, Multi Homing rules can be further defined to allow or deny connections according to IP address using **filters**.

Port Mapping allows Multi Homing to "pretend" to offer the service that an outside computer (WAN side) wishes to reach. Once the connection is made, all the requests between the outside and local (LAN side) computers are redirected by Multi Homing to the proper destination. This process is completely transparent to the outside computers.

11 Port Mapping is also called Port Address Translation in some contexts

1. Determine the port number and transmission protocol of the service[12]
2. Click on the **Security** tab
3. Under the Firewall menu item, click on **Port Mapping**
4. Click on **Add**
5. Enter **Service Name** (ex: FTP), **External Port** (ex: 21).
6. Click on **TCP**
7. Enter the IP address into **Internal Host** (ex: 192.168.1.22), port (ex:21).
8. Click on **Enable**.
9. Press **Apply**.

Any request from Internet for port 21 (FTP service port) to the Multi Homing will be forwarded to LAN client 192.168.1.22

12 See Appendix B for a list of common ports

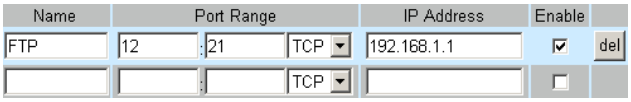
DELETING A RECORD OF PORT MAPPING

1. Determine the port number and transmission protocol of the service[13]
2. Click on the **Security** tab
3. Under the Firewall menu item, click on **Port Mapping**
4. Click on **Delete?** beside record you want to delete
5. Press **Apply**.

Virtual Server

ADDING A RECORD ABOUT VIRTUAL SERVER

1. Click on **Virtual Server** under Firewall in the **Security tab**.
2. Enter **Name** (ex: FTP)
3. Enter **Port Range** (ex: 12, 21).
4. Select **TCP / UDP / ALL**. (ex: TCP)
5. Enter **IP address** (ex: 192.168.1.1).
6. Click on **Enable**.
7. Press **Apply**.



13 See Appendix C for a list of common ports

DELETING A RECORD ABOUT VIRTUAL SERVER

1. Click on **Virtual Server** under Firewall in the **Security** tab.
2. Select the rule you want to delete
3. Press "**del**" button in the right of the rule
4. Press **Apply**.

PORT TRIGGERING

Port trigger is a set of rules which is used to open port forwarding dynamically. Each rule is composed of a trigger condition and a port forwarding rule.

Add One Port Trigger For Realplayer

1. Click on **Port trigger** under Firewall in Networking tab.
2. Add the following items in the port trigger page and press Apply.

   A. The name. RealOne

   B. The triggered port: 554-554

   C. The triggered protocol: TCP

   D. The incoming port: 7070-7071

   E. The incoming protocol: UDP

   F. The Server check: No

Add one PORT Trigger for mIRC

1. Click on **Port trigger** under **Firewall** in **Networking** tab.
2. Add the following items in the port trigger page and press **Apply**.

   A. The name. mIRC

   B. The triggered port: 6660:6670

   C. The triggered protocol: TCP

   D. The opened port: 113-113

   E. The opened protocol: TCP

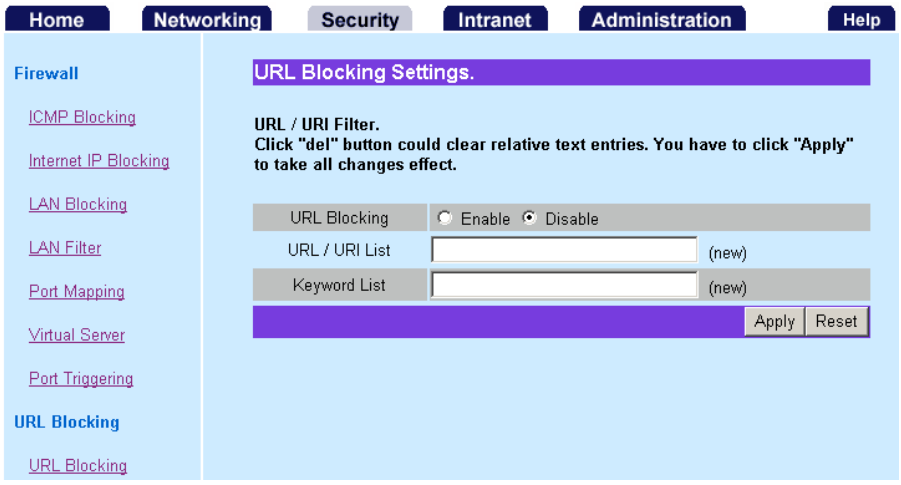
   F. The Server check: No

URL Blocking

Uniform Resource Locator (URL) blocking can be used by parent to limit access to certain Internet sites for their children. This feature is more effective than **Internet IP Blocking** as Internet sites might have multiple IP addresses and the user does not required to know the IP address to set a blocking rule. In addition, the user can set a keyword list that would block any URL that comprises the keyword. This way, the user can make the list short, making it easier to manage.

URL BLOCKING

1. Click on the **Security** tab
2. Under the URL Blocking menu item, click on **URL Blocking**
3. Select **Enable** on URL Blocking
4. Enter the **URL/URI List** you wish to block
5. You may also enter a **Keyword List** to block access by keyword
6. Click on **Apply** to start blocking



Intranet

Chapter 7

Local Area Network Computing Internet style

The technology developed for the Internet has revolutionized so many aspects of modern day society. Application of the Internet technology within a corporate environment present the same benefits and synergy at a much more personal scale.

Dubbed Intranets, local area networks that leverage technology developed for the World Wide Web provide a wealth of resources to the office. Like its global counter-part intranets offer the user with fast, reliable on-line services. Unlike its global counter-parts, intranets that are run behind properly configured firewalls are safe from malicious or unintentional intrusions that cause serious interruptions or intellectual property loss or damage.

Dynamic LAN Client Configuration

LAN side client computers can automatically obtain new IP addresses from Multi Homing, through its built-in DHCP daemon[14]. To achieve this each client computer should be set to acquire IP addresses via dynamic host configuration protocol (DHCP) or its predecessor the Bootstrap Protocol (BootP)[15].

By default, Multi Homing will assign up to 99 IP addresses within the range starting from 192.168.1.2 up to 192.168.1.100[16]. Once assigned, a client

14 Daemons are also sometimes referred to as servers. The term daemon is used to denote the program that provides the services. The term server can denote either the program that provides the service, but is also used to refer to the physical device that executes the program. The origin of the daemon concept stems from its applications in Unix. The original designers viewed the operating system as a great sorcerer with little 'daemons' or minions (or servants) to do various menial tasks for him. Although the sorcerer concept did not catch on, the term daemon became the accepted term.

15 Please refer to your operating system manual or reference guide for the proper configuration procedure.

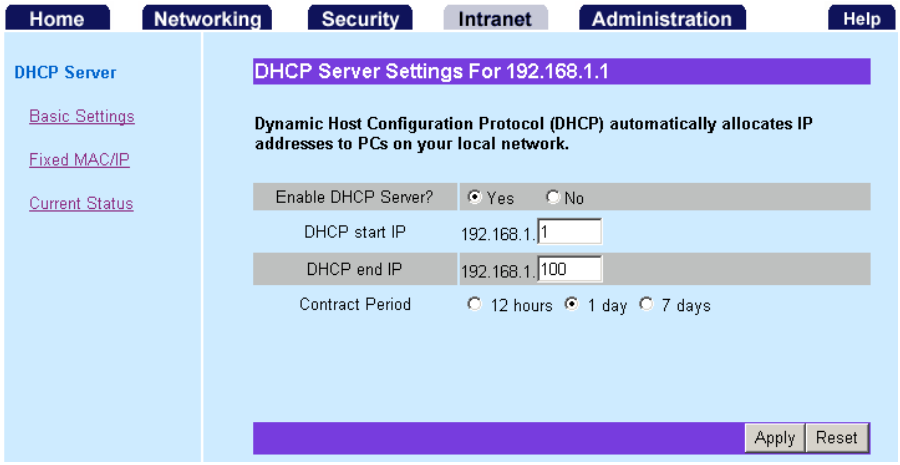
16 The range of available DHCP IP addresses is called the DHCP pool.

computer would retain or lease the IP address for as long as 1 day (7 day max). Once the lease expires, the client computer can re-apply for a new IP address. It is possible that the DHCP daemon may assign a different IP address from what was just released. In order to guarantee that a LAN side computer gets the same IP address every time, see the section on permanent IP address assignment below.

Caution: There should be only one (1) DHCP daemon on your LAN. If you are already running another DHCP daemon or server, you should disable it before activating Multi Homing DHCP daemon. Running more than one DHCP daemon on a LAN can have unpredictable (and sometimes difficult to fix) consequences.

ACTIVATING/DEACTIVATING THE DHCP SERVICE

1. Click on the **Intranet** tab
2. Under the DHCP menu item, select **Basic Settings**
3. Click on the appropriate enable or disable (yes or no) button[17]
4. Click on **Apply**



17 DHCP daemon is enabled by default.

1. Click on the **Intranet** tab
2. Under the DHCP menu item, select **Basic Settings**
3. Enter the **start of the range** onto the DHCP start IP text box (value must be between 1 and 254)
4. Enter the **end of the range** onto the DHCP end IP text box (value must be between 1 and 254)
5. Click on **Apply** to save the setting

Permanent IP Address Assignment

Typically, DHCP daemons assign the next available IP address from the DHCP pool. A client computer can therefore be assigned a different IP address every time a lease is renewed. If a client machine is a web server, FTP[18] server or electronic mail server, users will find it difficult to access the services since the machine could change its address on a daily basis. Machines that provide Intranet (and even port mapped Internet services) should have fixed IP addresses.

Multi Homing provides 2 methods to work with LAN clients which have permanent IP addresses: permanent IP address assignments using MAC layer addresses; and automatic MAC-IP associations from the leased list.

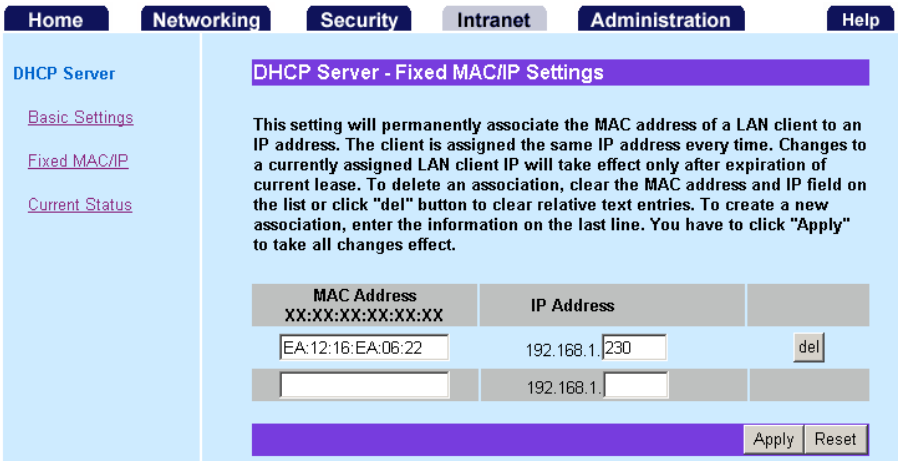
Assigning a Permanent Address based on the MAC layer address

The Machine Access Control Layer (MAC layer) address is a unique 6-byte number assigned to each network interface card (NIC). This number is a unique world wide serial number that is stamped onto NICs when they are manufactured. Low level network protocols such as DHCP and BOOTP use the MAC layer address to keep track of assigned IP addresses and ensure that assignments do not overlap[19]. Multi Homing can use the MAC layer address to ensure that a LAN client always gets the same IP address every time it requests for one.

18 File Transfer Protocol

19 Overlapped IP addresses can cause unpredictable results, are difficult to trouble shoot and may cause service interruptions

1. Determine the MAC address of the target machine[20]
2. Click on the **Intranet** tab
3. Under the DHCPD menu item, click on **Fixed MAC/IP**
4. Enter the **MAC address** in the appropriate text box (separate each hex-byte by a colon, e.g. AA:BB:CC:DD:EE:FF)[21]
5. Enter the desired IP address into the appropriate text box
6. Click on **Apply**



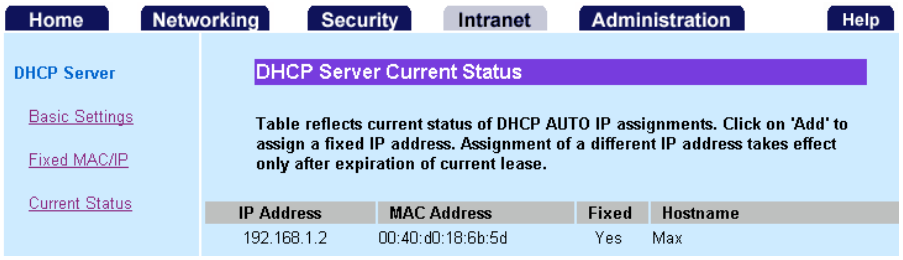
Assigning a Permanent Address to a currently running LAN Client

Since Multi Homing has a list of currently assigned IP addresses and their corresponding MAC layer addresses, it is possible to associate the IP to the MAC address directly.

20 Refer to the operating system or network interface card manual or reference guide for details

21 If the IP address entered is different from the IP address currently assigned to the LAN client, the LAN client must renew its DHCP lease. Refer to the operating system manual or reference guide for details

1. Determine the IP address currently assigned to the LAN client[22]
2. Click on the **Intranet** tab
3. Under the DHCP Server menu item, click on **Current Status**
4. Find the IP address on the table and click on the corresponding **Add** button
5. Enter the desired IP address onto the IP address text box marked New[23]
6. Click on **Apply**



Administration

Chapter 8

Access Control and Troubleshooting tools

Multi Homing provides an extensive set of system tools that equip the novice network administrator to do advanced network trouble shooting. Multi Homing also provides sophisticated control structures which can restrict access to its configuration.

22 Refer to the operating system manual or reference guide for details

23 If the IP address entered is different from the IP address currently assigned to the LAN client, the LAN client must renew its DHCP lease. Refer to the operating system manual or reference guide for details

Authentication

By now you have familiarized yourself with username/password authentication mechanism used by Multi Homing. This is an industry standard method for authenticating the identity of the user who intends to use the system. Only authorized users should be entrusted with the valid username and password.

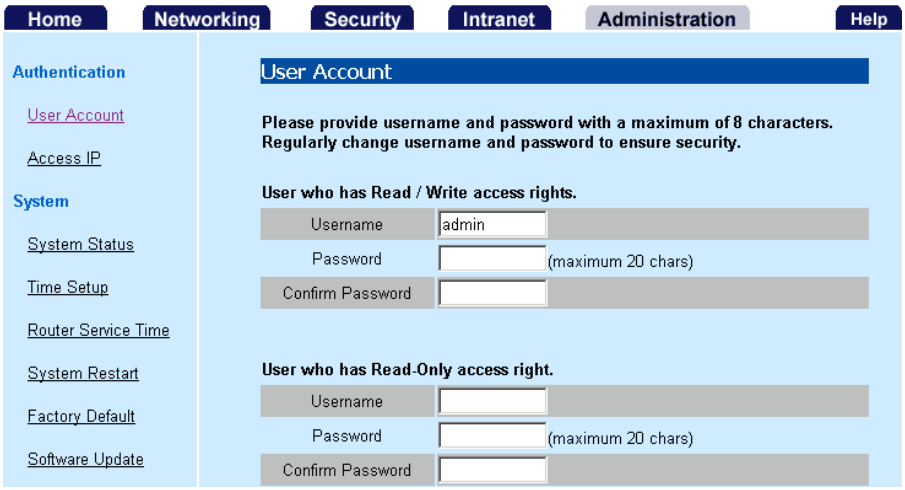
This feature allows the network administrator to manage the users who can change the Multi Homing configuration or use the tools for trouble shooting.

Users are also authenticated through the LAN clients they access Multi Homing through. Users who attempt to access Multi Homing through restricted workstations are denied access.

Besides, you can also choose a language setting. Multi Homing currently supports English and Chinese (Big 5).

CHANGING THE VALID USER AND PASSWORD

1. Click on the **Administration** tab
2. Under the Authentication menu item, click on **User Account**
3. To change the valid username, enter a new username in the appropriate text box.
4. To change the password, enter new password in both password fields[24].
5. Click on **Apply**[25]

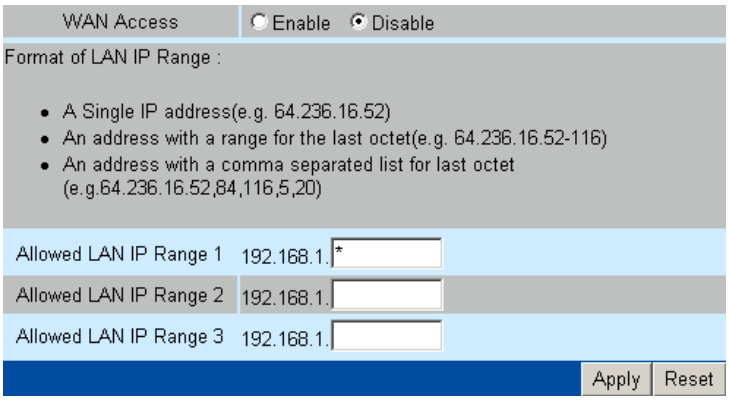


24 It is important to choose a good password. Several systems are broken into through accounts with weak passwords. It is advisable to mix in numbers into the password.

25 This change takes effect immediately

CONTROLLING WEB ACCESS CONFIGURATION BY IP ADDRESS[26]

1. Determine the IP addresses of the workstations through which the administrator is allowed to log in
2. Click on the **Administration** tab
3. Under the Authentication menu item, click on **Access IP**
4. Click **Enable/ Disable** to activate/deactivate WAN access
5. Enter up to three sets of IP addresses (or ranges) into the appropriate text box[27]
6. Click on **Apply**[28]



System Tools

Multi Homing provides the following tools which aid in administration of the network.

- **System Status.** This utility displays the current system status. It

26 By default, all LAN clients can configure the Multi Homing

27 Make sure that the new IP addresses (or range) have fixed IP addresses and includes an accessible workstation (e.g. the one you are currently using). You might lock yourself out of the system!

28 This change takes effect immediately

displays the current Network Status, Current Routing Table, and DHCP clients information. The feature shows read-only system status and it will not allow you to modify the information. It provides a method of inspecting the health of your system.

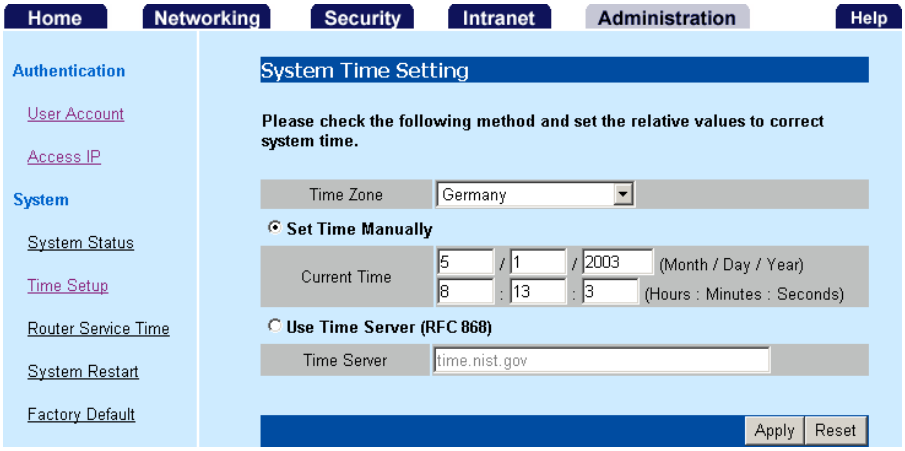
- **Time Setup.** This utility will setup your system time. You can either setup your system time manually or use Network Time Server to synchronize your system clock over the network.
- **Router Service Time.** This utility allows user to access Internet based on a predefined time frame.
- **System Restart.** This utility is used for restarting Multi Homing. System restarts is needed in events of modified important system settings. Any saved changes of the system activities will be applied after the system rebooted.
- **Factory Default.** This utility is used for clearing the configuration and resetting it back to original values (as it came out of the box)
- **Software Update.** This utility allows the Network Administrator to connect to a server which provides software which can be used to upgrade Multi Homing. he software update can also be done on local machine. Please check separate information sheet or vendor web site for more details.
- **Config Setting** This utility is used for backup your current Multi Homing configurations in your PC. In the case you need to reset Multi Homing back to factory default value, you can load the configuration you backup before.

DISPLAY SYSTEM STATUS

1. Click on the **Administration** tab
2. Under the System menu item, click on **System Status**
3. It shows the **Network Status** and DHCP clients information.

SETUP SYSTEM TIME

1. Click on the **Administration** tab
2. Under the System menu item, click on **Time Setup**
3. Select your time zone in the Time Zone selecting box
4. Choose either **Set Time Manually** or **Use NTP (Network Time Server)**
5. If you choose the setup time manually, enter current time by specifying Month, Day, Year, Hours, Minutes, and Seconds in the appropriate fields
6. If you choose to use network time server, specifying the NTP Server
7. Click on **Apply**



SETUP ROUTER SERVICES TIME

1. Click on the **Administration** tab

2. Under the **Router Services Time** menu item, select **Yes** to enable NAT Router
3. Select **Yes** to enable **Time Based Access Control**
4. Enter **Open Time** and **Close Time** in military time format (00:00 – 24:00)
5. Click on **Apply** to save changes

RESTARTING YOUR SYSTEM

1. Click on the **Administration** tab
2. Under the System menu item, click on **System Restart**
3. Click on **Yes**

SET FACTORY DEFAULT

1. Click on the **Administration** tab
2. Under the System menu item, click on **Factory Default**
3. Click on **Yes**

UPDATE YOUR SYSTEM SOFTWARE

1. Click on the **Administration** tab
2. Under the System menu item, click on **Software Update**
3. Choose either the software update file is in the **Internet** or on the **local host**
4. If the file is in the Internet, type in the URL
5. If the file is on local host, type in the name file with full path or click on Browse button to search the file on local host.
6. Click on **Apply**

PRESERVING YOUR SYSTEM CONFIGURATION

1. Click on the **Administration** tab
2. Under the System menu item, click on **Config Setting**
3. Press **Save** button
4. Do the rest of setting according to prompt window

LOADING YOUR SYSTEM CONFIGURATION

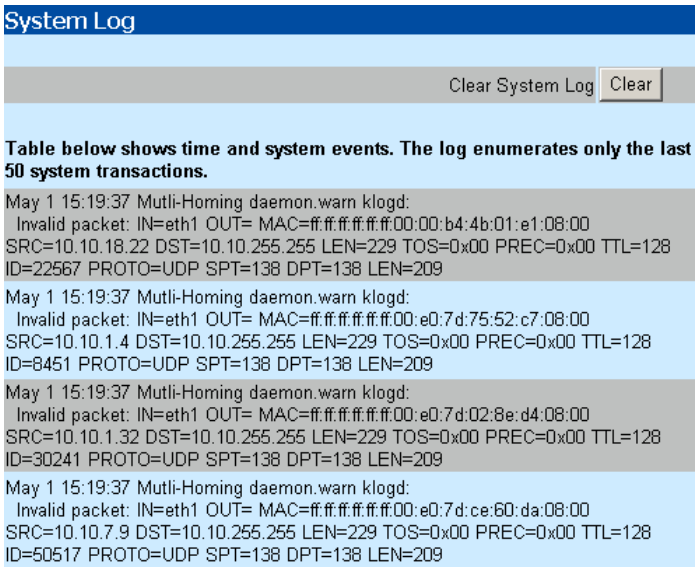
1. Click on the **Administration** tab
2. Under the System menu item, click on **Config Setting**
3. Press **Browse** button to specify the file path
4. Press **Load** button
5. Do the rest of setting according to prompt window

System Log

Multi Homing provides a system log of all system activities up to 50 entries. Old entries will be purged automatically to ensure a healthy system. However, if you want to keep a full system log, you can setup a remote system log daemon (remote syslogd) to record all system events remotely. This feature can also be very helpful to monitor the system activities at distant.

VIEW SYSTEM LOG

1. Click on the **Administration** tab
2. Under the System menu item, click on **System Log**
3. The system log shows time and system events of the last 50 system activities.



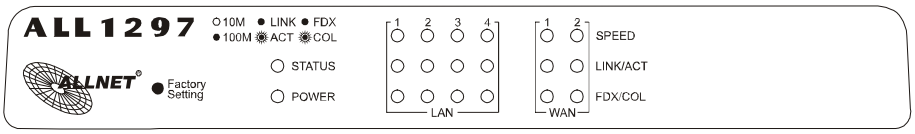
Appendix
A

Specifications & Accessories

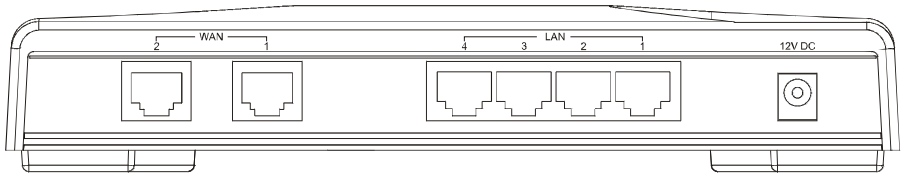
Packing List

- One Multi Homing broadband gateway
- One power adapter
- Wall mount kit
- User's Manual

Front Panel



Rear Panel



LEDs Definition

SYSTEM LED

- ***Power LED***

  This indicator lights green when the ADSL Router is receiving power; otherwise, it is off.

- ***Status LED***

  The LED will be dark for 10 seconds when the system is started. After that, the LED will **blink blue** periodically to show the ADSL Router is working normally. If the LED stays **blue/dark** that means the system is fail, you need to contact your agent or try to reboot the system.

PORT LED

- ***SPEED LED***

  The SPEED LED indicates the link speed of each port. If the LED lights **green** then the connection speed is 100Mbps, off for 10Mbps.

- ***LINK/ACT LED***

  Every port has a LINK/ACT LED. **Steady blue** (link state) indicates that the port has good linkage to its associated devices. **Flashing blue** indicates that the port is receiving or transmitting data between its associated devices.

Speed LED	Link/Activity LED	Status
Off	Off	No Connection
Off	Blue	Connect as 10Mbps

Green	Blue	Connect as 100Mbps

- ***FDX/COL LED***

  A collision occurs when two stations within a collision domain attempt to transmit data at the same time. **Intermittent flashing amber** of the collision LED is normal; the contending adapters resolve each collision by means of a wait-then-retransmit algorithm. Frequency of collisions is an indicator of heavy traffic on the network.

  If the FDX/COL **lights amber** it means the port is under full-duplex operation or dark for half-duplex mode. The following table is a summary of Port LEDs.

PORTS' LED SUMMARY TABLE

LED	Operation
SPEED	*100Mbps (Green), 10Mbps (Off)*
LINK/ACT	*Link is present (Blue), Activity (Blinking Blue)*
FDX/COL	*Full-Duplex (Amber), Half-Duplex (Off), Collision (Blinking Amber)*

FACTORY SETTING BUTTON

Push the button for 5 seconds, the system will return to factory default setting. In the meantime, system rewrites flash to default value and Status LED halts for a while. Approximately 60 seconds later, the Status LED blinks green periodically, now the whole system parameters have returned to factory default value.

Warning Incomplete factory setting recovery procedure will cause the ADSL Router malfunction.
If you are unfortunately in this situation, do not try to repair it by yourself. Consult your local distributor for help.

Standard	IEEE802.3, 10BASE-T IEEE802.3u, 100BASE-TX IEEE802.3x full duplex operation and flow control
Interface	2 * 10/100 RJ-45 WAN port 4 * 10/100 RJ-45 Fast Ethernet switching LAN ports
Cable Connections	RJ-45 (10BASE-T): Category 3,4,5 UTP/STP RJ-45 (100BASE-TX): Category 5 UTP/STP
Network Data Rate	Ethernet: Auto-negotiation (10Mbps, 100Mbps)
Transmission Mode	Auto-negotiation (Full-duplex, Half-duplex)
LED indicators	System Power Status Port (LAN/WAN) SPEED LINK/ACT FDX/COL
Buffer Memory / MAC address	1Mbit / 2K MAC address entries
System Memory	8MB Flash 16MB RAM
Emission	FCC Class B, CE
Operating Temperature	$0^0 \sim 50^0$C ($32^0 \sim 122^0$F)
Operating Humidity	10% - 90%
Power Supply	External Power Adapter, 12VDC/1000mA

Specifying Internet Addresses

Appendix B

Writing Internet Addresses the Multi Homing way

An Internet protocol address or IP address is used by the Internet to uniquely identify your computer (much like the way a postman would use your home address to uniquely identify where to deliver your mail.)

IP addresses are 32-bit numbers expressed in 4 numbers, each between 0 and 255, separated by **dots**. Each number is called a **quad**. This form of representing an IP address is called **dot-quad**.

A continuous group of addresses is called an IP address range (or simply just a range). IP address ranges make it easier for network administrators to control the behavior of sophisticated network appliances (such as the Multi Homing) when dealing with large groups of computers. A range that spans all 256 addresses of the last quad (i.e. 0 up to 255) is called a 'Class C subnet' or simply 'Class C'. An IP block is a range of IP addresses with a matching (sub)netmask.

There are several items within Multi Homing that use IP Address ranges. These items can operate on more than a single IP Address simultaneously. For example, a user may choose to configure Multi Homing's firewall to block several IP Addresses, say, every address from **10.0.0.1** to **20.0.0.255**.

Wherever an IP Address Range can be specified, the user can utilize IP Range Syntax.

There are two possibilities for the input of IP Address expressions in the controls on the GUI using IP Range Syntax:

- One requires all 4 dot-quads address format (e.g. **192.168.1.10, 10.0.0.1, 255.255.0.255**)

- The other is a field that has the first three quads of the address provided as a label, and you are required to enter an expression for the last quad in the address. For example, 192.168.1.**10** (you only specify the **10** part).

Notice that the above examples specify a single, specific address.

Operators

To provide a succinct notation wherever more than one address is desired, three operators are defined for the syntax:

Operator	Purpose
,	**Comma**: Specify multiple non-sequential addresses
–	**Dash**: Specify a range of sequential addresses
*	**Asterisk**: Wildcard for every address within the Class C [0 to 255]

Expression Examples

Comma Operator:
To specify the first three odd addresses: **192.168.1.1,3,5**
Dash Operator:
To specify the first five addresses: **192.168.1.0-4**
Asterisk Operator:
To specify all addresses when the full IP Address range is required: **192.168.1.***
Multiple Operators:
The operators can also be combined. To specify every address between 100 and 200, plus addresses 50 and 250: **192.168.1.100-200,250,50**
Note that the order in which the ranges or the individual addresses are specified is irrelevant.
Notice also that a range specified as **192.168.1.1,3,5-10,*** will specify every address from 0 to 255. This is because the Asterisk Operator supersedes all other operators; the prior operators are simply ignored.

The following the white paper on IP address assignment is recommended reading for the industrious Network Administrator. It presents guidelines for

the designation of IP Addresses within your LAN. This document is widely available on the WWW. **RFC1918 "Address Allocation for Private Internets"**[29]

29 RFCs (Refer for Comments) are documents published through the Internet Engineering Task Force (IETF) to solicit comments and present guidelines for proposed (as well as endorsed) Internet standards. Newer RFCs may be proposed which supersede the RFCs identified in this document.

Common Port Numbers

Appendix C

This is a list of commonly used port numbers and the services they are associated with.

Port numbers are generally divided into 3 categories. Well known port numbers are defined from 0 through 1023. Registered port numbers range from 1024 through 49151. While dynamic or private port number range from 49152 through 65535.

Well known port numbers normally involve daemons[30] with special system privileges, as such exposing them may present a higher security risk than opening dynamic or private ports.

The official list of well known port numbers is maintained by the Internet Assigned Numbers Authority (IANA).[31] The full list is published under RFC1700.[32]

Port Number	Protocol	Keyword	Description/Recommendation

30 Daemons are also sometimes referred to as servers. The term daemon is used to denote the program that provides the services. The term server can denote either the program that provides the service, but is also used to refer to the physical device that executes the program. The origin of the daemon concept stems from its applications in Unix. The original designers viewed the operating system as a great sorcerer with little 'daemons' or minions (or servants) to do various menial tasks for him. Although the sorcerer concept did not catch on, the term daemon became the accepted term.

31 At the time this manual was prepared

32 Newer RFCs may be proposed which supersede the RFCs identified in this document.

7	TCP/UDP	Echo	This service sends automatic replies to established connections. Although this feature is useful, it has been used for denial of service attacks. This should be kept closed.
11	TCP/UDP	Systat	This service sends automatic replies with detailed information about system status. Although this feature is useful, it can provide malicious users with information to attack a site. It is advised to keep this port closed.
19	TCP/UDP	Chargen	This service sends automatic replies to established connections. Although this feature is useful, it has been used for denial of service attacks. This should be kept closed.
20 (21)	TCP/UDP	FTP DATA (CONTROL)	These two ports are required to provide File Transfer Protocol (FTP) service. Open these ports only if mapping to an FTP server.
22	TCP/UDP	SSH	This port provides connection for Secure Shell (Secure Telnet). SSH provides encrypted connection to SSH servers. Open this port only if mapping to a system running an SSH server
23	TCP/UDP	Telnet	This port provides connection for Telnet. Before opening this port, consider using SSH. Open this port only if mapping to a system running Telnet.
25	TCP/UDP	SMTP	This port provides connection for the Simple Mail Transport Protocol (SMTP). This protocol is used for transmission of electronic mail (e-mail). Open this port only if mapping to an SMTP server.
37	TCP/UDP	Time	This port sends automatic replies indicating the time. Open this port only if mapping to a server with a time daemon.
49	TCP/UDP	TACACS	This port provides network authentication for TACACS servers. Open this port only if mapping to a TACACS server.
53	TCP/UDP	DNS	This port provides connection for Domain Name Services (DNS). Open this port only if mapping to a DNS server (not a DNS client).
67 (68)	TCP/UDP	BOOTP	These two ports are required for dynamic host configuration. Open this port only if mapping to a DHCP or BOOTP relay server (ordinary DHCP/BOOTP servers cannot transmit through the WAN port)
69	TCP/UDP	TFTP	This port provides connection for the Trivial File Transfer Protocol. Since TFTP is an unauthenticated protocol, exercise caution when mapping this port.
70	TCP/UDP	Gopher	This port provides connection for Gopher clients. (Forerunner of HTTP).
79	TCP/UDP	Finger	This port provides the Finger service. This is used to identify users currently using a system. Since this in an unauthenticated service which provides system information, exercise caution when using this port.
80	TCP/UDP	HTTP	This port provides HTTP service connection. Open this port only when mapping to HTTP servers.
88	TCP/UDP	Kerberos	This port provides connection services for the Kerberos authentication system. Open this port when mapping to a Kerberos system.

109	TCP/UDP	POP2	This port provides connection services for version 2 of the Post Office Protocol. Open this port only if mapping to a POP2 compliant server.
110	TCP/UDP	POP3	This port provides connection services for version 3 of the Post Office Protocol. Open this port only if mapping to a POP3 compliant server.
118	TCP/UDP	SQLServ	This port provides connection to SQL services. Open this port only if mapping to a SQL server using these ports.
119	TCP/UDP	News/NNTP	This port provides connections services for the Network News Transport Protocol. Open this port only if mapping to a NNTP server.
123	TCP/UDP	NTP	This port provides connection to the network time protocol. Open this port only if mapping to a NTP server.
137 (138) [139]	TCP/UDP	NetBIOS-ns NetBIOS-dgm NetBIOS-ssn	These ports are required to provide NetBIOS services. Some NetBIOS services expose important network resources. Exercise caution when mapping this port to a NetBIOS enabled relay server.
143	TCP/UDP	IMAP2	This port provides connection services for version 2 of the Interim Mail Access Protocol. Open this port only if mapping to a IMAP2 compliant server.
161 (162)	TCP/UDP	SNMP (SNMPTRAP)	These ports provide connection services for the Simple Network Management Protocol (SNMP). Open this port only if mapping to an SNMP agent.
220	TCP/UDP	IMAP3	This port provides connection services for version 3 of the Interim Mail Access Protocol. Open this port only if mapping to a IMAP3 compliant server.
389	TCP/UDP	LDAP	This port provides connection services for Lightweight Directory Access Protocol (LDAP). Open this port only if mapping to a LDAP server.
443	TCP/UDP	HTTPS	This port provides Secure HTTP service connection. Open this port only when mapping to HTTPS servers.
514	TCP/UDP	SYSLOG	This port provides connection to the SYSLOG daemon. Open this port only when mapping to a server running syslogd.
546 (547)	TCP/UDP	DHCP Client (DHCP Server)	These two ports are required for dynamic host configuration. Open this port only if mapping to a DHCP or BOOTP relay server (ordinary DHCP/BOOTP servers cannot transmit through the WAN port)