Neobit 1012VA II

ADSL Ethernet Router

User's Manual

Revision 1.2.
June. 13, 2003

FCC COMPLIANCE STATEMENT

- **NOTE :**

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.

Modifications not expressly approved by the manufacturer could void the user's authority to operated the equipment under FCC rules.

Table of Contents

Features 7
System Requirement 7
Using this Document.....8
Notational conventions 8
Typographical conventions.....8
Getting Support.....8
Parts Check.....9
Front Panel.....10
Rear Panel 11
Part 1 — Connecting the Hardware 13
Step 1. Connect the ADSL cable and optional telephone. 14
Step 2. Connect the Ethernet cable. 15
Step 3. Attach the power connector 15
Step 4. Turn on the Neobit 1012VAand power up your systems. 15
Part 2 — Configuring Your Computers 16
Before you begin.....16
Windows® XP PCs:.....16
Windows 2000 PCs: 17
Windows Me PCs 18
Windows 95, 98 PCs: 19
Windows NT 4.0 workstations.....20
Assigning static Internet information to your PCs 21
Part 3 — Configuring the Neobit 1012VA 22
Logging in to the Neobit 1012VAQuick Configuration Page.....22
Default Router Settings.....24
Testing Your Setup 25
Accessing the Configuration Manager 27
Functional Layout.....29
Commonly used buttons.....29
The Home Tab and System View Table.....30
Changing Your Login Password.....32

Changing Your Login Password.....32
Committing Your Changes and Rebooting the Device.....33
Committing your changes.....33
Rebooting the device using Configuration Manager.....34
Configuring the LAN IP Address.....35
Viewing the Neobit 1012VA's IP addresses.....39
Overview of DHCP.....41
What is DHCP?.....41
Why use DHCP?.....41
Neobit 1012VADHCP modes.....42
Configuring DHCP Server.....43
Viewing, modifying, and deleting address pools, and excluding IP addresses from a pool.....46
Viewing current DHCP address assignments.....47
Configuring DHCP Relay.....48
Setting the DHCP Mode.....49
Overview of NAT.....51
Viewing NAT Global Settings and Statistics.....52
Viewing NAT Rules and Rule Statistics.....55
Viewing Current NAT Translations.....56
Adding NAT Rules.....58
The napt rule: Translating between private and public IP addresses.....58
The rdr rule: Allowing external access to a LAN computer.....60
The basic rule: Performing 1:1 translations.....63
The filter rule: Configuring a basic rule with additional criteria.....64
The bimap rule: Performing two-way translations.....66
The pass rule: Allowing specific addresses to pass through untranslated.....67
About DNS.....69
Assigning DNS Addresses.....69
Configuring DNS Relay.....70
Overview of IP Routes.....73
Comparing IP routing to telephone switching.....73

Hops and gateways 74
Using IP routes to define default gateways.....74
Do I need to define IP routes?.....74
Viewing the IP Routing Table 75
Adding IP Routes 77
RIP Overview 79
When should you configure RIP?.....79
Configuring the Neobit 1012VA's Interfaces with RIP 80
Viewing RIP Statistics 82
Viewing Your ATM VC Setup 83
Adding ATM VCCs 84
Modifying ATM VCCs 86
Viewing Your Current PPP Configuration 87
Viewing PPP Interface Details.....89
Adding a PPP Interface Definition 91
Modifying and Deleting PPP Interfaces 92
Overview of EOA 93
Viewing Your EOA Setup 94
Adding EOA Interfaces 95
Viewing Your IPoA Interface Setup.....97
Adding IPoA Interfaces 98
Overview of Bridges.....101
Using the Bridging Feature.....102
Defining Bridge Interfaces 103
Deleting a Bridge Interface 104
Configuring Global Firewall Settings 105
Managing the Black List 108
Configuring IP Filters 110
Viewing Your IP Filter Configuration 110
Configuring IP Filter Global Settings 111
Creating IP Filter Rules.....112
IP filter rule examples 117
Viewing IP Filter Statistics.....119
Managing Current IP Filter Sessions 119
Blocking Protocols 121
Viewing System Alarms.....127

Viewing the Alarm Table....127
Displaying the Alarm Monitor in a Separate Window....128
Upgrading the Software....129
Using Diagnostics....130
Modifying Port Settings....132
Overview of IP port numbers....132
Modifying the ADSL/Ethernet routers' port numbers....132

A IP Addresses, Network Masks, and Subnets....135
IP Addresses....135
Structure of an IP address....135
Network classes....136
Subnet masks....136

B Binary Numbers....139
Binary Numbers....139
Bits and bytes....139

C Troubleshooting....141
Diagnosing Problem using IP Utilities....143
ping....143
nslookup....144

D Glossary....145

E Quick Configuration Guide....159

10 Configuring IP Routes

You can use Configuration Manager to define specific routes for your Internet and network data. This chapter describes basic routing concepts and provides instructions for creating routes.

Note that most users do not need to define IP routes.

Overview of IP Routes

The essential challenge of a router is: when it receives data intended for a particular destination, which next device should it send that data to?. When you define IP routes, you provide the rules that a computer uses to make these decisions.

Comparing IP routing to telephone switching

IP routing decisions are similar to those made by switchboards that handle telephone calls.

When you dial a long distance telephone number, you are first connected to a switchboard operated by your local phone service carrier. All calls you initiate go first to this main switchboard.

If the phone number you dialed is outside your calling area, the switchboard opens a connection to a higher-level switchboard for long distance calls. That switchboard looks at the area code you dialed and connects you with another switchboard that serves that area. This new switchboard, in turn, may look at the prefix in the number you dialed (the middle set of three numbers) and connect to a more localized switchboard that handles numbers with that prefix. This final switchboard can then look at the last four digits of the phone number to open a connection with the person or company you dialed.

In comparison, when your computer initiates communication over the Internet, such as viewing a web page connecting to an web server, the data it sends out includes the IP address of the destination computer (the “phone number”). All your outgoing requests first go to the same router at your ISP (the first “switchboard”). That router looks at the network ID portion of the destination address (the “area code”) and determines which next router to send the request to. After several such passes, the request arrives at a router for the destination network, which then uses the host ID portion of the destination IP address (the local “phone number”) to route the request to the appropriate computer. (The network ID and host ID portions of IP addresses are explained in Appendix A.)

With both the telephone and the computer, all transactions are initially sent to the same switchboard or router, which serves as a gateway to other higher- or lower-level devices. No single device knows at the outset the eventual path the data will take, but each uses a specific part of the destination address/phone number to make a decision about which device to connect to next.

Hops and gateways

Each time Internet data is passed from one Internet address to another, it is said to take a *hop*. A hop can be a handoff to a different port on the same device, to a different device on the same network, or to a device on an entirely different network.

When a hop passes data from one type of network to another, it uses a *gateway*. A gateway is an IP address that provides initial access to a network, just as a switchboard serves as a gateway to a specific set of phone numbers. For example, when a computer on your LAN requests access to a company's web site, your ISP serves as a gateway to the Internet. As your request reaches its destination, another gateway provides access to the company's web servers.

Using IP routes to define default gateways

IP routes are defined on computers, routers, and other IP-enabled devices to instruct them which hop to take, or which gateway to use, to help forward data along to its specified destination.

If no IP route is defined for a destination, then IP data is passed to a predetermined *default gateway*. The default gateway serves like a higher-level telephone switchboard; it may not be able to connect directly to the destination, but it will know a set of other devices that can help pass the data intelligently. If it cannot determine which of these devices provides a good next hop (because no such route has been defined), then that device will forward the data to *its* default gateway. Eventually, a high level device, using a predefined IP route, will be able to forward the data along a path to its destination.

Do I need to define IP routes?

Most users do not need to define IP routes. On a typical small home or office LAN, the existing routes that set up the default gateways for your LAN computers and for the Neobit 1012VAprovide the most appropriate path for all your Internet traffic.

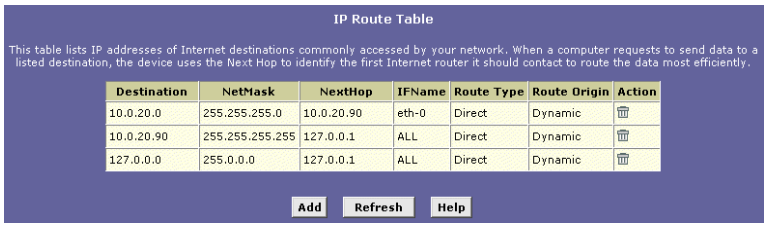
- On your LAN computers, a default gateway directs all Internet traffic to the LAN port on the Neobit 1012VA. Your LAN computers know their default gateway either because you assigned it to them when you modified their TCP/IP properties, or because you configured them to receive the information dynamically from a server whenever they access the Internet. (Each of these processes is described in the Quick Start instructions, Part 2.)
- On the Neobit 1012VAitself, a default gateway is defined to direct all outbound Internet traffic to a router at your ISP. This default gateway is assigned automatically by your ISP whenever the device negotiates an Internet connection. (The process for adding a default route is described on page 77.)

You may need to define routes if your home setup includes two or more networks or subnets, if you connect to two or more ISP services, or if you connect to a remote corporate LAN.

Viewing the IP Routing Table

All IP-enabled computers and routers maintain a table of IP addresses that are commonly accessed by their users. For each of these *destination IP addresses*, the table lists the IP address of the first hop the data should take. This table is known as the device's *routing table*.

To view the Neobit 1012VA's routing table, click the Routing tab. The IP Route page displays by default, as shown in Figure 29:



Destination	NetMask	NextHop	IFName	Route Type	Route Origin	Action
10.0.20.0	255.255.255.0	10.0.20.90	eth-0	Direct	Dynamic	
10.0.20.90	255.255.255.255	127.0.0.1	ALL	Direct	Dynamic	
127.0.0.0	255.0.0.0	127.0.0.1	ALL	Direct	Dynamic	

Figure 29. IP Route Table Page

The IP Route Table displays a row for each existing route. These include routes that were predefined on the device, routes you may have added, and routes that the device has identified automatically through communication with other devices.

The routing table should reflect a default gateway, which directs outbound Internet traffic to your ISP. This default gateway is shown in the row containing destination address 0.0.0.0.

The following table defines the fields in the IP Routing Table.

Field	Description
Destination	Specifies the IP address of the destination computer. The destination can specified as the IP address of a specific computer or an entire network. It can also be specified as all zeros to indicate that this route should be used for all destinations for which no other route is defined (this is the route that creates the default gateway).
Netmask	Indicates which parts of the destination address refer to the network and which parts refer to a computer on the network. Refer to Appendix A, for an explanation of network masks. The default gateway uses a netmask of 0.0.0.0.
NextHop	Specifies the *next* IP address to send data to when its final destination is that shown in the destination column.
IFName	Displays the name of the interface on the device through which data is forwarded to the specified next hop.
Route Type	Displays whether the route is direct or indirect. In a *direct* route, the source and destination computers are on the same network, and the router attempts to directly deliver the data to the computer. In an *indirect* route, the source and destination computers are on different networks, and the router forwards data to a device on another network for further handling.
Route Origin	Displays how the route was defined. *Dynamic* indicates that the route was created automatically or predefined by your ISP or the manufacturer. Routes you create are labeled *Local*. Other routes can be created automatically (using RIP, as described in Chapter 9), or defined remotely through various network management protocols (LCL or ICMP).
Action	Displays an icon ( ) you can click on to delete a route.

Adding IP Routes

Follow these instructions to add an IP route to the routing table.

1. From the IP Route Table page, click Add.

   The IP Route – Add page displays, as shown in Figure 30.

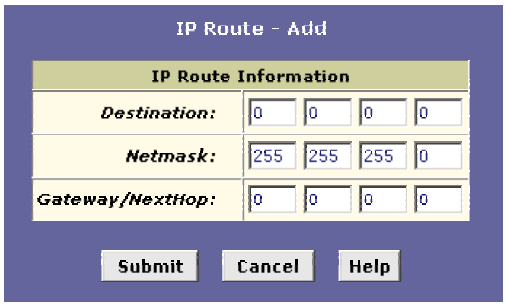


   Figure 30. IP Route – Add Page

2. Specify the destination, network mask, and gateway or next hop for this route.

   For a description of these fields, refer to the table on page 76.

   To create a route that defines the default gateway for your LAN, enter 0.0.0.0 in both the Destination and Net Mask fields. Enter your ISP's IP address in the Gateway/NextHop field.

   Note that you cannot specify the interface name, route type or route origin. These parameters are used only for routes that are identified automatically as the device communicates with other routing devices. For routes you create, the routing table displays system default values in these fields.

3. Click Submit.

4. On the confirmation page, click Close to return to the IP Route table page.

The IP Routing Table will now display the new route.

5. Click the Admin tab, and then click **Commit & Reboot** in the task bar.

6. Click Commit to save your changes to permanent memory.

11 Configuring the Routing Information Protocol

The Neobit 1012VAcan be configured to communicate with other routing devices to determine the best path for sending data to its intended destination. Routing devices communicate this information using a variety of IP protocols. This chapter describes how to configure the Neobit 1012VAto use one of these, called the Routing Information Protocol (RIP).

RIP Overview

RIP is an Internet protocol you can set up to share routing table information with other routing devices on your LAN, at your ISP's location, or on remote networks connected to your network via the ADSL line. Generally, RIP is used to enable communication on *autonomous* networks. An autonomous network is one in which all of the computers are administered by the same entity. An autonomous network may be a single network, or a grouping of several networks under the same administration. An example of an autonomous network is a corporate LAN, including devices that can access it from remote locations, such as the computers telecommuters use.

Using RIP, each device sends its routing table to its closest neighbor every 30 seconds. The neighboring device in turn passes the information on to its next neighbor and so on until all devices in the autonomous network have the same set of routes.

When should you configure RIP?

Most small home or office networks do not need to use RIP; they have only one router, such as the Neobit 1012VA, and one path to an ISP. In these cases, there is no need to share routes, because all Internet data from the network is sent to the same ISP gateway.

You may want to configure RIP if any of the following circumstances apply to your network:

- Your home network setup includes an additional router or RIP-enabled PC (other than the Neobit 1012VA). The Neobit 1012VAand the router will need to communicate via RIP to share their routing tables.
- Your network connects via the ADSL line to a remote network, such as a corporate network. In order for your LAN to learn the routes used within your corporate network, they should *both* be configured with RIP.
- Your ISP requests that you run RIP for communication with devices on their network.

Configuring the Neobit 1012VA's Interfaces with RIP

The following instructions describe how to enable RIP on the Neobit 1012VA

Note

In order for the Neobit 1012VAto communicate with other devices using RIP, you must also enable the other devices to use the protocol. See the product documentation for those devices.

1. Log into the Configuration Manager, click the Services tab, and then click **RIP** in the task bar.

   The RIP Configuration page displays, as shown in Figure 31.

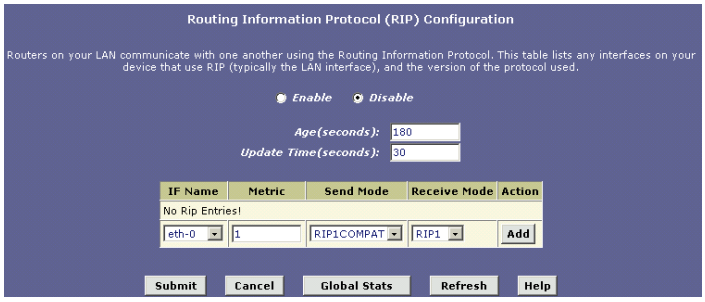


   Figure 31. RIP Configuration Page

   The page contains radio buttons for enabling or disabling the RIP feature and a table listing interfaces on which the protocol is currently running. The first time you open this page, the table may be empty.

2. If necessary, change the Age and Update Time.

   These are global settings for all interfaces that use RIP.

   - *Age* is the amount of time in seconds that the device's RIP table will retain each route that it learns from adjacent computers.
   - *Update Time* specifies how frequently the Neobit 1012VAwill send out its routing table its neighbors.

3. In the IFName column, select the name of the interface on which you want to enable RIP.

   For communication with RIP-enabled devices on your LAN, select eth-0 or the name of the appropriate virtual Ethernet interface.

   For communication with your ISP or a remote LAN, select the corresponding ppp, eoa, or other WAN interface.

4. Select a metric value for the interface.

   RIP uses a "hop count" as a way to determine the best path to a given destination in the network. The hop count is the sum of the metric values assigned to each port through which data is passed before reaching the destination. Among several

alternative routes, the one with the lowest hop count is considered the fastest path.

For example, if you assign this port a metric of 1, then RIP will add 1 to the hop count when calculating a route that passes through this port. If you know that communication via this interface is slower than through other interfaces on your network, you can assign it a higher metric value than the others.

You can select any integer from 1 to 15.

5. Select a Send Mode and a Receive Mode.

   The Send Mode setting indicates the RIP version this interface will use when it sends its route information to other devices.

   The Receive Mode setting indicates the RIP version(s) in which information must be passed to the Neobit 1012VAin order for it to be accepted into its routing table.

   RIP version 1 is the original RIP protocol. Select RIP1 if you have devices that communicate with this interface that understand RIP version 1 only.

   RIP version 2 is the preferred selection because it supports "classless" IP addresses (which are used to create subnets) and other features. Select RIP2 if all other routing devices on the autonomous network support this version of the protocol.

6. Click Add.

   The new RIP entry will display in the table.

7. Click the **Enable** radio button to enable the RIP feature.

Note

If you disable the RIP feature, the interface settings you have configured will remain available for future activation.

8. When you are finished defining RIP interfaces, click Submit.

   A page displays to confirm your changes.

9. Click the Admin tab, and then click **Commit & Reboot** in the task bar.

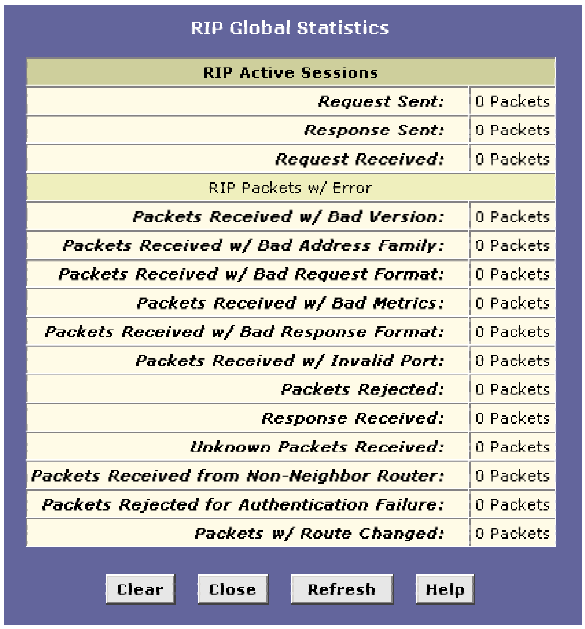
10. Click Commit to save your changes to permanent memory.

Note

You can delete an existing RIP entry by clicking in the Action column.

Viewing RIP Statistics

From the RIP Configuration page, you can click Global Stats to view statistics on attempts to send and receive route table data over RIP-enabled interfaces on the Neobit 1012VA.



RIP Global Statistics

RIP Active Sessions	
Request Sent:	0 Packets
Response Sent:	0 Packets
Request Received:	0 Packets
RIP Packets w/ Error	
Packets Received w/ Bad Version:	0 Packets
Packets Received w/ Bad Address Family:	0 Packets
Packets Received w/ Bad Request Format:	0 Packets
Packets Received w/ Bad Metrics:	0 Packets
Packets Received w/ Bad Response Format:	0 Packets
Packets Received w/ Invalid Port:	0 Packets
Packets Rejected:	0 Packets
Response Received:	0 Packets
Unknown Packets Received:	0 Packets
Packets Received from Non-Neighbor Router:	0 Packets
Packets Rejected for Authentication Failure:	0 Packets
Packets w/ Route Changed:	0 Packets

Clear Close Refresh Help

Figure 32. RIP Global Statistics Page

You can click Clear to reset all statistics to zero and Refresh to display any newly accumulated data.

12 Configuring the ATM VCC

As your LAN computers access the Internet via the Neobit 1012VA, data is exchanged with your ISP through a complex network of telephone switches, Internet routers, servers, and other specialized hardware. These various devices communicate using a common language, or protocol, called *Asynchronous Transfer Mode* (ATM). On the Wide Area Network (WAN) that connects you to your ISP, the ATM protocol performs functions like those that the Ethernet protocol performs on your LAN.

This chapter describes how to configure the ATM *virtual channel connection* (VCC). The VCC properties define the path the Neobit 1012VAuses to communicate with your ISP over the ATM network.

Viewing Your ATM VC Setup

To view your current configuration, log into Configuration Manager, click the WAN tab, and then click **ATM VCC** in the task bar. The ATM VCC Configuration page displays, as shown in Figure 33.

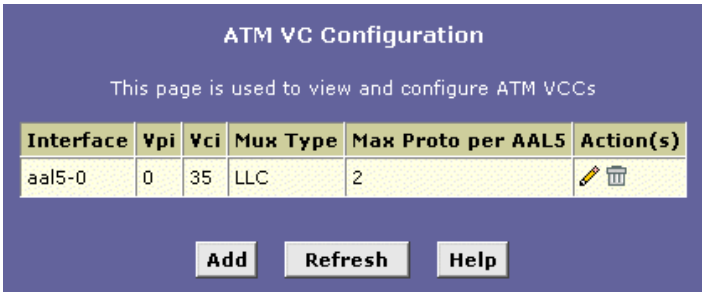


Figure 33. ATM VCC Configuration Page

The ATM VCC Configuration table displays the following fields (contact your ISP to determine these settings):

Field	Description
Interface	The name of the lower-level interface on which this VC operates. The low-level interface names are preconfigured in the software and identify the type of traffic that can be supported, such as data or voice. Internet data services typically use an AAL5-type interface.
Vpi, Vci, and Mux Type	These settings identify a unique ATM data path for communication between your ADSL/Ethernet router and your ISP.
Max Proto per AAL5	If you are using an AAL5-type of interface, this setting indicates the number of higher-level interfaces that the VC can support (the higher level interfaces can be PPP, EoA, or IPoA interfaces). Contact your ISP to determine which connection protocol(s) they require.
Actions	Displays an icon ( ) you can click on to delete the associated interface.

Adding ATM VCCs

You may need to create a VCC if none has been predefined on your system or if you use multiple services with your ISP. Each service may require its own VCC. Follow these instructions to add a VCC:

1. From the ATM VCC Configuration page, click **Add**.

   The ATM VCC – Add page displays, as shown in Figure 34.

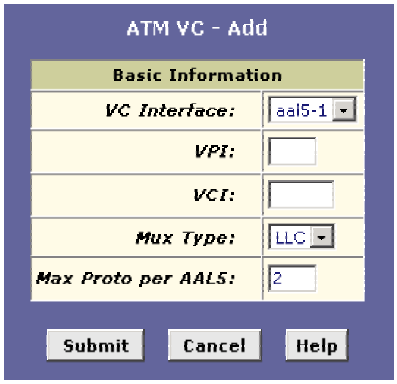


Figure 34. ATM VCC – Add Page

2. Select an interface name from the VCC Interface drop-down list.
3. Enter the VPI and VCI values assigned by your ISP, and select the mux type from the drop-down list.
4. Click Submit.
5. On the confirmation page, click Close to return to the ATM VCC Configuration page.
6. Click the Admin tab, and then click **Commit & Reboot** in the task bar.
7. Click Commit to save your changes to permanent memory.

   The new interface should now display in the ATM VCC Configuration table.

You may need to create a new WAN interface, or modify an existing interface, so that it uses the new VCC. See the instructions for configuring a PPP (Chapter 12), EoA (Chapter 14), or IPoA (Chapter 10) interfaces, depending on the type you use to communicate with your ISP.

You can verify that the new settings work by attempting to access the Internet from a LAN computer. Contact your ISP for troubleshooting assistance.

Modifying ATM VCCs

Your device may already be preconfigured with the necessary ATM VCC properties, or the table may contain placeholder values that you must change before using the device. Contact your ISP to determine your ATM VCC values. Follow these instructions to modify a preconfigured VCC:

1. From the ATM VCC Configuration page, click in the Actions column for the interface you want to modify.

   The ATM VCC Interface – Modify page displays, as shown in Figure 34.

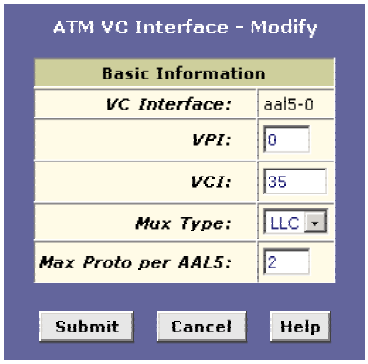


Figure 35. ATM VCC Interface – Modify Page

2. Enter the new VPI and VCI values, select the MUX type, or change the maximum number of protocols that the VCC can carry, as directed by your ISP.

   You cannot modify the interface type over which an existing VCC operates (aal5-0, for example). If you want to change the interface type, you must delete the existing interface, create a new one, and select the desired interface type.

3. Click **Submit**.

4. On the confirmation page, click **Close** to return to the ATM VCC Configuration page.

5. Click the Admin tab, and then click **Commit & Reboot** in the task bar.

6. Click **Commit** to save your changes to permanent memory.

You can verify that the new settings work by attempting to access the Internet from a LAN computer. Contact your ISP for troubleshooting assistance.

13 Configuring PPP Interfaces

When powered on, the Neobit 1012VAinitiates a connection through your DSL line to your ISP.

The point-to-point (PPP) protocol is commonly used between ISPs and their customers to identify and control various communication properties, including:

- Identifying the type of service the ISP provides to a given customer
- Identifying the customer to the ISP through a username and password login
- Enabling the ISP to assign Internet information to the customer's computers

Your ISP may or may not use the PPP protocol. Contact your ISP to determine if you will need to change the default settings in order to connect to their server.

Viewing Your Current PPP Configuration

To view your current PPP setup, log into Configuration Manager, click the WAN tab, and then click **PPP** in the task bar. The PPP Configuration page displays, as shown in Figure 36.

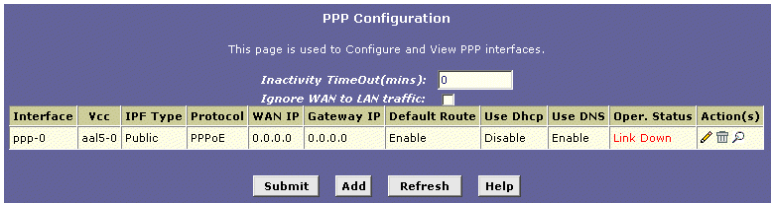


Figure 36. PPP Configuration Page

PPP is configured as a group of software settings associated with the ADSL port. Although the device has only one physical ADSL port, the Neobit 1012VAcan be defined with more than one group of PPP settings. Each group of settings is called a *PPP interface* and is given a name, such as *ppp-0*, *ppp-1*, etc.

You can configure the following settings on the PPP Configuration page:

- **Inactivity TimeOut (mins)**: The time in minutes that must elapse before a PPP connection times-out due to inactivity.
- **Ignore WAN to LAN traffic**: When enabled, data traffic traveling in the incoming direction—from the WAN port to the LAN port—will not count as activity on the WAN port; i.e., it will not prevent the connection from being terminated if inactive for the specified time.

The PPP Configuration Table displays the following fields:

Field	Description
Interface	The predefined name of the PPP interface.
VCC	The Virtual Channel Connection over which this PPP data is sent. The VCC identifies the physical path the data takes to reach your ISP. See Chapter 12 for more information.
IPF Type	The type of IP Firewall protections that are in effect on the interface (public, private, or DMZ): ○ A public interface connects to the Internet (PPP interfaces are typically public). Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software. ○ A private interface connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network. ○ The term DMZ (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public Web server). Packets incoming on a DMZ interface -- whether from a LAN or external source -- are subject to a set of protections that is in between public and private interfaces in terms of restrictiveness.
Protocol	The type of PPP protocol used. Your ISP may use PPP-over-Ethernet (PPPoE) or PPP-over-ATM (PPPoA).
WAN IP	The IP address currently assigned to your WAN (DSL) port by your ISP.
Gateway IP	The IP address of the server at your ISP that provides you access to the Internet. See "Hops and gateways" on page 74 for a description of gateway addresses.
Default Route	Indicates whether the ADSL/Ethernet router should use the IP address assigned to this connection as its default route. Can be Enabled or Disabled. See Chapter 10 for an explanation of default routes.

Field	Description
Use DHCP	When set to *Enable*, the device will acquire additional IP information from the ISP's DHCP server. The PPP connection itself acquires the device's IP address, mask, DNS address, and default gateway address. With Use DHCP enabled, the device will acquire IP addresses for various other server types (WINS, SMTP, POP3, etc. -- these server types are listed on the DHCP Server Configuration page).
User DNS	When set to *Enable*, the DNS address learned through the PPP connection will be distributed to clients of the device's DHCP server. This option is useful only when the ADSL/Ethernet Router is configured to act as a DHCP Server for your LAN. When set to *Disable*, LAN hosts will use the DNS address(es) preconfigured in the DHCP pool (see "Configuring DHCP Server" on page 43) and in the DNS feature (see Chapter 9, "Configuring DNS Server Addresses").
Oper. Status	Indicates whether the link is currently up or down or if a specific type of data exchange is under way (e.g., password authorization or DHCP).
Actions	You can use these icons to modify ( ), delete ( ), and view additional details on ( ) the PPP interface.

Viewing PPP Interface Details

When you click to view additional details, the PPP Interface - Detail page displays, as shown in Figure 37.

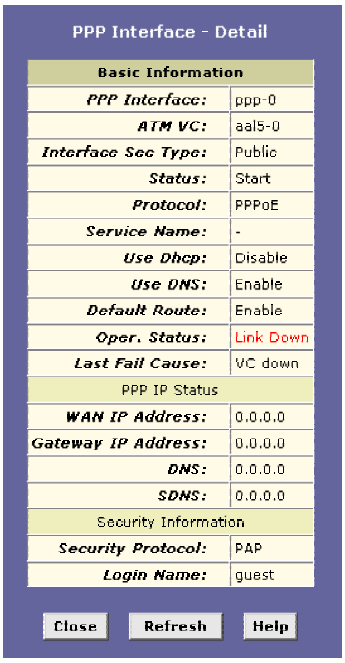


Figure 37. PPP – Detail Page

In addition to the properties defined on page 88, the Detail page displays these fields:

Field	Description
Status	Indicates whether the interface has been specified in the system as: o Enabled: A connection will be established for use when the device is turned on or rebooted. o Disabled: The PPP interface cannot currently be used. o Start On Data: The PPP connection will be made only when data is sent to the interface (e.g., when a LAN user attempts to use the Internet).
Service Name	The name of the ISP service you are using with this PPP connection. ISPs may offer different types of services (for example, for online gaming or business communications), each requiring a different login and other connection properties.
Last Fail Cause	Indicates the action that ended the previous PPP session: o No Valid PADO Recvd: The unit initiated a PPPoE handshake but did not receive a packet in reply from the ISP. o No Valid PADS Recvd: After the initial handshake, the unit did not receive a confirmation packet from the ISP. o Stopped by User: The user stopped the connection (for example, by changing the Configuration Manager settings for the PPP interface.) o No Activity: The PPP communication timed out, in accordance with the timeout period specified on the PPP Configuration page. o Auth Failure: The ISP could not authorize the connection based on the user name and/or password provided. o PADT recvd: The ISP issued a special packet type to terminate the PPP connection. o VC down: The Virtual Circuit between the unit and the ISP is down. o Internal failure: A system software failure occurred.
DNS	The IP address of the DNS server (located with your ISP) used on this PPP connection.
SDNS	The IP address of the secondary DNS server (located with your ISP) used on this PPP connection.
Security Protocol	The type of PPP security your ISP uses: *PAP* (Password Authentication Protocol) or *CHAP* (Challenge Handshake Authentication Protocol).
Login Name	The name you use to log in to your ISP each time this PPP connection is established.

Adding a PPP Interface Definition

If you intend to use more than one type of service from your ISP, the device may be configured with multiple PPP interfaces, each with unique logon and other properties. Follow this procedure to define properties for a PPP interface:

1. From the PPP Configuration Page, click **Add**.

   The PPP Interface – Add page displays, as shown in Figure 38.

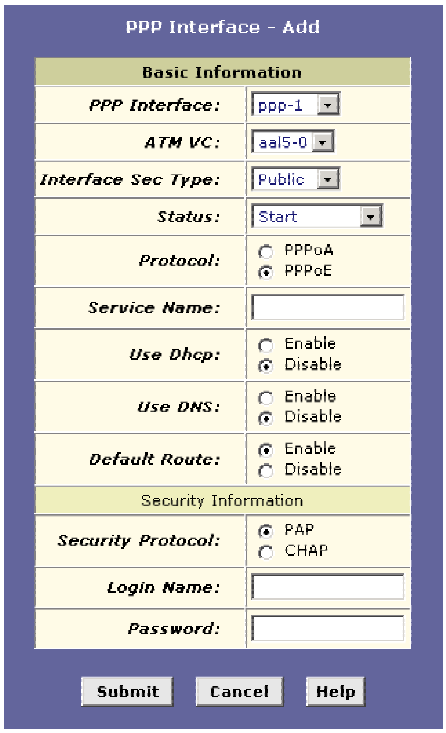


Figure 38. PPP Interface – Add Page

2. Select a PPP interface name from the drop-down list, and then enter or select data for each field.

Note

You can create multiple PPP interfaces only if you are using the PPPoA protocol; only one PPP interface can be define if you are using PPPoE. Check with your ISP which version of the protocol they require.

   The fields are defined in the tables on page 88 and 90.

3. Click **Submit**.

   A page displays to confirm your changes.

4. Click **Close** to return to the PPP page and view the new interface in the table.

5. Click the Admin tab, and then click **Commit & Reboot** in the task bar.

6. Click Commit to save your changes to permanent memory.

Modifying and Deleting PPP Interfaces

To modify a PPP interface, display the PPP Configuration page and click in the Action(s) column for the interface you want to modify. The PPP Interface – Modify page displays, as shown in Figure 39.

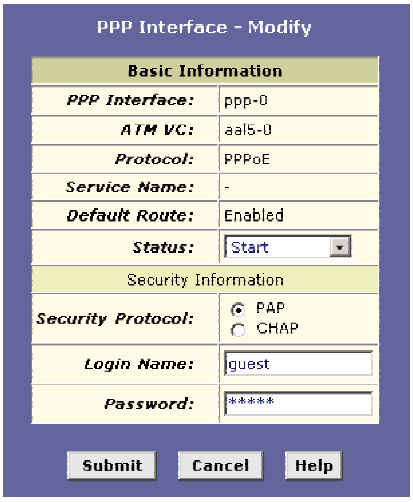


Figure 39. PPP Interface – Modify

You can change only the status of the PPP connection, the security protocol, your login name, and your password. To modify the other settings, you must delete the interface and create a new one.

To delete a PPP interface, display the PPP Configuration page and click in the Action(s) column for the interface you want to delete. You should not delete a PPP interface unless you have received instructions to do so from your ISP. Without an appropriately defined PPP interface, you will not be able to connect to your ISP. You can recreate the PPP interface with the same name at a later time.

After modifying or deleting a PPP interface, click Submit. Then, Click the Admin tab, click **Commit & Reboot** in the task bar, and click Commit to save your changes to permanent memory.

14 Configuring EOA Interfaces

This chapter describes how to configure an Ethernet-over-ATM interface on the Neobit 1012VA, if one is needed to communicate with your ISP.

Overview of EOA

The Ethernet-over-ATM (EOA) protocol is commonly used to carry data between local area networks that use the Ethernet protocol and wide-area networks that use the ATM protocol. Many telecommunications industry networks use the ATM protocol. ISPs who provide DSL services often use the EOA protocol for data transfer with their customers' DSL modems.

EOA can be implemented to provide a bridged connection between a DSL modem and the ISP. In a bridged connection, data is shared between the ISP's network and their customer's as if the networks were on the same physical LAN. Bridged connections do not use the IP protocol. EOA can also be configured to provide a routed connection with the ISP, which uses the IP protocol to exchange data.

Before creating an EOA interface or modifying the default settings, contact your ISP to determine which type of protocol they use.

Note

PPP vs. EOA: *Your ISP may use a protocol other than EOA for communication with the Neobit 1012VA, such as the point-to-point protocol (PPP). One type of PPP, named PPP over Ethernet (PPPoE), actually works "on top" of the EOA protocol. The other type, PP over ATM (PPPoA), does not. However, if your ISP uses either type of PPP, you* ***do not*** *need to separately create an EOA interface. See Chapter 12 for instructions on creating or configuring a PPP interface.*

Viewing Your EOA Setup

To view your current EOA configuration, log into Configuration Manager, click **Advanced** in the task bar, and then click **EOA**. Figure 40 shows the EOA Configuration page.

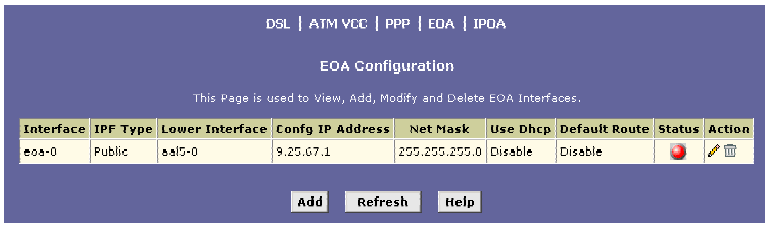


Figure 40. EOA Configuration Page

The EOA table contains a row for each EOA interface currently defined on the device. The table may contain no entries if your ISP does not use the EOA protocol.

The following table describes the fields on this page:

Field	Description
Interface	The name the software uses to identify the EOA interface.
IPF Type	The type of IP Firewall protections in effect on the interface (public, private, or DMZ): ○ A *public* interface connects to the Internet (IPoA interfaces are typically public). Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software. ○ A *private* interface connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network. ○ The term *DMZ* (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public Web server). Packets incoming on a DMZ interface—whether from a LAN or external source—are subject to a level of protection that is in between those for public and private interfaces.
Lower interface	EOA interfaces are defined in software, and then associated with lower-level software and hardware structures (at the lowest level, they are associated with a physical port —the WAN port). This field should reflect an interface name defined in the next lower level of software over which the EOA interface will operate. This will be an ATM VCC interface, such as *aal5-0*, as described in Chapter 12.

Field	Description
Config IP Address and Net Mask	The IP address and network mask you want to assign to the interface. If the interface will be used for bridging with your ISP and you will not be using the Neobit 1012VAas a router on your LAN, then you do not need to specify IP information. If you enable DHCP for this interface, then the Configured IP address will serve only as a request to the DHCP server. The actual address that is assigned by the ISP may differ if this address is not available.
Use DHCP	When checked, this setting instructs the device to accept IP information assigned dynamically by your ISP's DHCP server. If the interface will be used for bridging with your ISP and you will not be routing data through it, leave this checkbox unselected.
Default Route	Indicates whether the Neobit 1012VAuses the IP address assigned to this interface, if any, as its default route for your LAN. Your system can have only one default route. See Chapter 9 for an explanation of default routes.
Status	A green or red ball will display to indicate that the interface is currently up or down, respectively. You cannot manually enable or disable the interface; a red ball may indicate a problem with the DSL connection.
Action	Icons you can click on to edit ( ) or delete ( ) the associated EOA interface.

Adding EOA Interfaces

Follow these instructions to add an EOA interface:

1. Click the WAN tab, and then click **EOA** in the task bar.
2. Click **Add**.

   The EOA Interface – Add page displays, as shown in Figure 41.

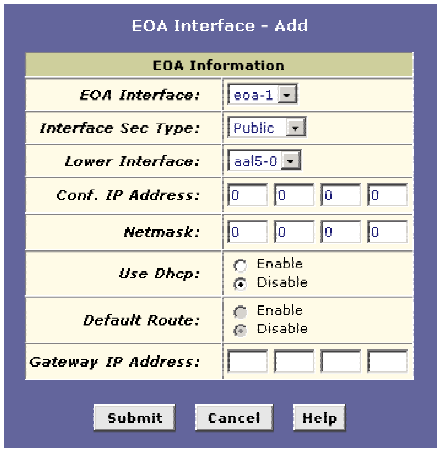


Figure 41. EOA Interface – Add Page

3. Select one of the predefined interface names from the EOA Interface drop down list.

4. From the IPF Type drop-down list, select the level of IP Firewall to be used on this interface, as defined above.
5. In the Lower Interface field, select the lower-level interface name over which this protocol is being configured. Typically, an EOA interface is configured to operate over an aal5 interface, such as *aal5-0*.

   If you are using the Neobit 1012VAas a bridge only, skip to step 7.
6. If you are using the Neobit 1012VAas a router on your LAN, enter the IP address and network mask you want to assign to the interface. This address serves as the public IP address for your entire LAN and is usually assigned by your ISP.

   Or, if your ISP will assign this information, click the Enable radio button to set up the DHCP service.

   Also, specify whether this interface should serve as the default route for your LAN for accessing the Internet.
7. Click Submit.

   A confirmation page display to confirm your changes.
8. Click Close to return to the EOA page and view the new interface in the table.
9. Click the Admin tab, and then click **Commit & Reboot** in the task bar.
10. Click Commit to save your changes to permanent memory.

15 Configuring IPoA Interfaces

This chapter describes how to configure an IPoA (Internet Protocol-over-ATM) interface on the Neobit 1012VA.

An IPoA interface can be used to exchange IP packets over the ATM network, without using an underlying Ethernet over ATM (EOA) connection. Typically, this type of interface is used only in product development and test environments, to eliminate unneeded variables when evaluating IP layer processing.

Viewing Your IPoA Interface Setup

To configure an IPoA interface, log into Configuration Manager, click the WAN tab, and then click **IPoA** in the task bar. The IPoA page displays, as shown in Figure 42.

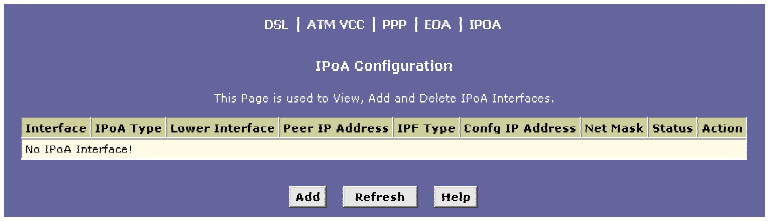


Figure 42. IPoA Configuration Page

The IPoA table contains a row for each EOA interface currently defined on the device. The table may initially contain no entries.

The following table describes the fields on this page:

Field	Description
Interface	The name the software uses to identify the IPoA interface
IPoA Type	Specifies whether the IPoA protocol to be used complies with the IEFT RFC 1577 "Classical IP and ARP over ATM" (contact your ISP if unsure).
Lower interface	IPoA interfaces are defined in software, and then associated with lower-level software and hardware structures (at the lowest level, they are associated with a physical port – the WAN port). This field should reflect an interface name defined in the next lower level of software over which the IPoA interface will operate. This will be an ATM VCC interface, such as *aal5-0*, as described in Chapter 12.
Peer IP Address	The IP address of the remote computer you will be connecting to via the WAN interface.

Field	Description
IPF Type	The type of IP Firewall protections that are in effect on the interface (public, private, or DMZ): ○ A *public* interface connects to the Internet (IPoA interfaces are typically public). Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software. ○ A *private* interface connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network. ○ The term *DMZ* (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public Web server). Packets incoming on a DMZ interface—whether from a LAN or external source—are subject to a level of protection that is in between those for public and private interfaces.
Config IP Address and Net Mask	The IP address and network mask you want to assign to the interface.
Status	A green or red ball will display to indicate that the interface is currently up or down, respectively. You cannot manually enable or disable the interface; a down interface may indicate a problem with the DSL connection.
Action	Icons you can click on to edit ( ) or delete ( ) the associated EOA interface.

Adding IPoA Interfaces

Follow these instructions to add an IPoA interface:

1. Display the IPoA page and click **Add**.

   The IPoA Interface – Add page displays, as shown in Figure 43.

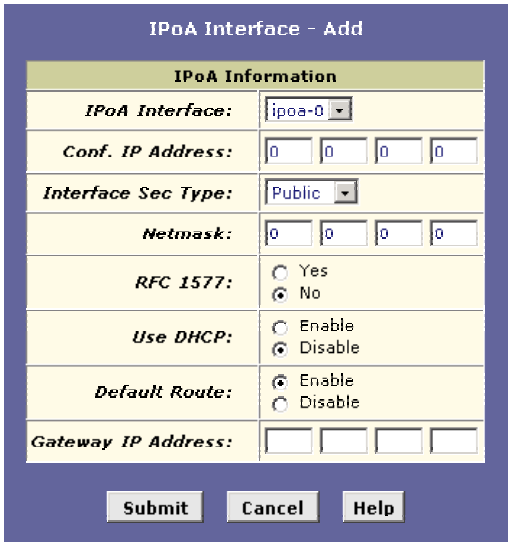


Figure 43. IPoA Interface – Add Page

2. Select the next available interface name from the IPoA Interface drop-down list.
3. In the Configured IP Address and Net Mask boxes, type the address and mask that you want to assign to the IPoA interface.

   If you enable the DHCP option (in step 6 below), then the IP address you enter here will serve as a requested address; the remote computer may assign another address if necessary.
4. From the Interface Sec Type drop-down list, select the level of firewall security for the interface: *Public*, *Private*, or *DMZ* (see page 오류! 책갈피가 정의되어 있지 않습니다. for definitions).
5. In the RFC 1577 Click the Yes radio button if the interface complies with the IETF specification RFC 1577 and click **Add**.
6. If the remote IPoA computer provides a DHCP server, you can click the Enable radio button in the Use DHCP field to have the IP address dynamically assigned from the server.
7. If you want the IPoA interface to serve as the default route for your LAN, click the Enable radio button in the Default Route field.
8. In the Gateway IP Address field, enter the address of the Internet computer to contact to gain initial access to the Internet.
9. Click **Submit**.

   A confirmation page will display to confirm your changes.
10. Click **Close** to return to the IPoA page and view the new interface in the table.

11. Click the Admin tab, and then click **Commit & Reboot** in the task bar.
12. Click Commit to save your changes to permanent memory.

16 Configuring Bridging

The Neobit 1012VAcan be configured to act as a bridging device between your LAN and your ISP. Bridges are devices that enable two or more networks to communicate as if they are two segments of the same physical LAN. This chapter describes how to configure the Neobit 1012VAto operate as a bridge.

Note

Before changing your bridge configuration, check with your ISP to determine the type of connection they use to exchange data with their customer's DSL modems (such as Ethernet bridging or IP routing).

Overview of Bridges

A bridge is a device used to connect two or more networks so they can exchange data. A bridge learns the unique manufacturer-assigned hardware IDs of each computer or device on both (or all) networks it is attached to. It learns that some of the IDs represent computers attached via one of the device's interfaces and others represent computers connected via other interfaces. For example, the hardware IDs of your home computers are attached via the Ethernet port, and the hardware IDs of your ISP's computers are attached via the WAN (DSL) port. It stores the ID list and the interface associated with each ID in its *bridge forwarding table*.

When the bridge receives a data packet, it compares its destination hardware ID to the entries in the bridge forwarding table. When the packet's ID matches one of the entries, it forwards the packet through the interface that connects to the corresponding network. Note that the bridge does not send the data directly to the receiving computer, but broadcasts it to the receiving network, making it available to any node on that network. On the receiving network, a LAN protocol such as Ethernet takes over, helping the packet reaches its destination.

When the bridge does not recognize a packet's destination hardware ID, it broadcasts the packet through all of its interfaces – to each network it is attached to.

Note

Bridges vs. Routers : *The essential difference between a bridge and a router is that a router uses a higher-level protocol (such as IP) to determine how to pass data. IP data packets contain IP addresses that specifically identify the destination computer. Routers can read this information and pass the data to the destination computer, or determine which next router to send the data to if the destination is not on a connected network.*

Bridges cannot read IP information, but instead refer to the hardware ID of the destination computer, which is also included in data packets. The hardware ID is a unique number that the manufacturer assigns to each piece of hardware it sells. A bridge learns to recognize the hardware IDs accessible through each of its ports. When it receives a packet, the bridge simply forwards the packet through the port it associates with the given hardware ID, or through all its ports if it does not recognize the ID. The hardware ID is often referred to as the Media Access Control *(MAC) address.*

Routers are considered more intelligent and flexible devices than bridges, and often provide a variety of security and network administration services based on the IP protocols.

Using the Bridging Feature

Although the Neobit 1012VAis pre-configured to serve as a router for providing Internet connectivity to you LAN, there are several instances in which you may also want to configure bridging:

- Your ISP may use protocols that require bridging with your LAN. The device can be configured to appear as a bridge when communicating with your ISP, while continuing to provide router functionality for your LAN.
- Your LAN may include computers that communicate using "layer-3" protocols other than the Internet Protocol. These include IPX® and AppleTalk®. In this case, the device can be configured to act as a bridge for packets that use these protocols while continuing to serve as a router for IP data.

In both cases, you need to specify the device's interfaces as bridge interfaces.

Defining Bridge Interfaces

To enable bridging, you simply specify the device interfaces on which you want to bridge data, and then enable bridging mode:

1. Log into Configuration Manager and click the Bridging tab.

   The Bridge Configuration page displays, as shown in Figure 44.

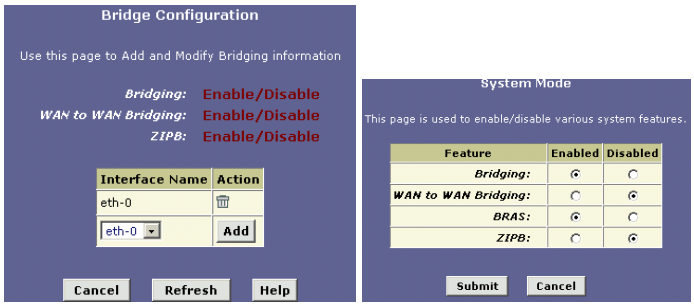


Figure 44. Bridge Configuration page

   The table may be empty if bridging has not yet been configured.

2. Select the interface names on which you want to perform bridging and click **Add**.

   For example, select *eth-0* (LAN) and *eoa-0* (WAN) interfaces. If you use a USB-connected computer, you can also select *usb-0*.

Note

If you do not have an eoa-0 interface, but instead have an interface named ppp-0 *or* ipoa-0*, your device is not currently configured with a WAN interface that allows bridging with your ISP. Check with your ISP to determine whether they use the eoa protocol before changing this setting. See Chapter 14 for instructions on creating an eoa interface.*

If you enable bridging on an interface that has already been assigned an IP address, then it is considered IP-enabled and will route (rather than bridge) IP packets received on the interface. The interface will bridge non-IP data it receives, however.

You can determine whether the Ethernet (eth-0) and USB (usb-0) interfaces have been assigned IP addresses by displaying the IP Address Table (display the Routing tab, and then click **IP Address***). These interfaces will display in the table only if they have been assigned IP addresses.*

You can check whether the eoa-0 interface has been assigned an IP address by displaying the EOA configuration table (click the WAN tab, and then click **EOA***). If the Config IP Address field is empty and the Use DHCP field contains the word Disable, then no IP address has been assigned.*

3. Click **Enable/Disable**

4. Click the **Bridging: Enable** radio button to turn on bridging. Do not click the ZIPB: Enable button unless you want to

configure this mode, as described on page 오류! 책갈피가 정의되어 있지 않습니다..

5. Click Submit.

   A page will briefly display to confirm your changes, and will return you to the Bridge Configuration page.

6. Click the Admin tab, and then click **Commit & Reboot** in the task bar.

7. Click Commit to save your changes to permanent memory.

Deleting a Bridge Interface

To make an interface non-bridgeable, display the Bridge Configuration page and click 🗑 next to the interface you want to delete. Click OK to confirm the deletion. The interface remains defined in the system, but is no longer capable of performing bridging.

17 Configuring Firewall Settings

Configuration Manager provides built-in firewall functions, enabling you to protect the system against denial of service (DoS) attacks and other types of malicious accesses to your LAN. You can also specify how to monitor attempted attacks, and who should be automatically notified.

Configuring Global Firewall Settings

Follow these instructions to configure global firewall settings:

1. Log into Configuration Manager, click the Services tab, and then click **Firewall** in the task bar.

   The Firewall Configuration page displays, as shown in Figure 45.

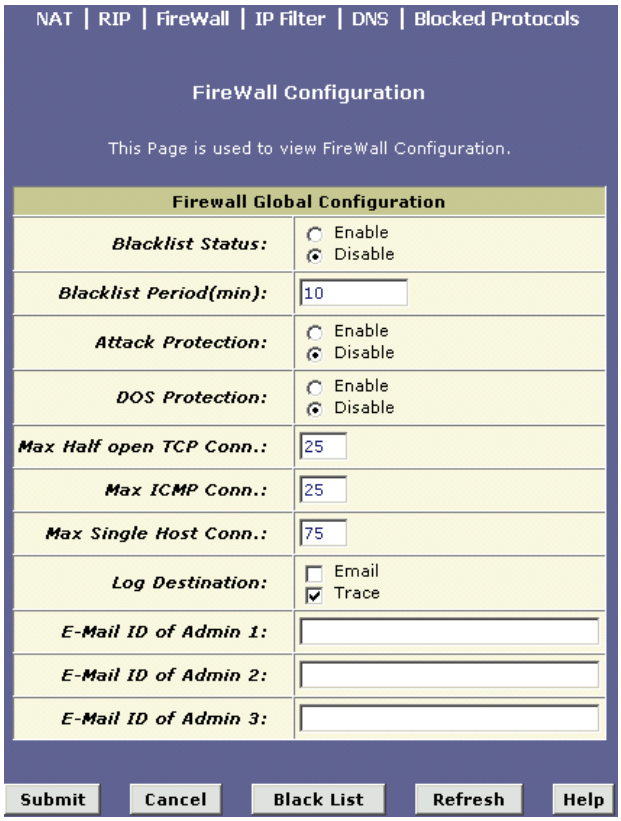


Figure 45. Firewall Configuration Page

Note that the Firewall Configuration page contains a drop-down list on the right side of the page that enables you to view firewall settings, as discussed in this chapter, or configure IP filters, as discussed in Chapter 18.

2. Configure any of the following settings that display in the Firewall Global Information table

Field	Description
Black List Status	If you want the device to maintain and use a black list, click *Enable*. Click *Disable* if you do not want to maintain a list.
Black List Period(min)	Specifies the number of minutes that a computer's IP address will remain on the black list (i.e., all traffic originating from that computer will be blocked from passing through any interface on the ADSL/Ethernet router). For more information, see "Managing the Black List" on page 108.
Attack Protection	Click the *Enable* radio button to use the built-in firewall protections that prevent the following common types of attacks: ○ IP Spoofing: Sending packets over the WAN interface using an internal LAN IP address as the source address. ○ Tear Drop: Sending packets that contain overlapping fragments. ○ Smurf and Fragile: Sending packets that use the WAN or LAN IP broadcast address as the source address. ○ Land Attack: Sending packets that use the same address as the source and destination address. ○ Ping of Death: Illegal IP packet length.
DoS Protection	Click the Enable radio button to use the following denial of service protections: ○ SYN DoS ○ ICMP DoS ○ Per-host DoS protection
Max Half open TCP Connection	Sets the percentage of concurrent IP sessions that can be in the half-open state. In ordinary TCP communication, packets are in the half-open state only briefly as a connection is being initiated; the state changes to active when packets are being exchanged, or closed when the exchange is complete. TCP connections in the half-open state can use up the available IP sessions. If the percentage is exceeded, then the half-open sessions will be closed and replaced with new sessions as they are initiated.
Max ICMP Connection	Sets the percentage of concurrent IP sessions that can be used for ICMP messages. If the percentage is exceeded, then older ICMP IP sessions will be replaced by new sessions as the are initiated.
Max Single Host Connection	Sets the percentage of concurrent IP session that can originate from a single computer. This percentage should take into account the number of hosts on the LAN.

Field	Description
Log Destination	Specifies how attempted violations of the firewall settings will be tracked. Records of such events can be sent via Ethernet to be handled by a system utility Ethernet to (*Trace*) or can e-mailed to specified administrators.
E-mail ID of Admin 1/2/3	Specifies the e-mail addresses of the administrators who should receive notices of any attempted firewall violations. Type the addresses in standard internet e-mail address format, e.g., *jxsmith@onecompany.com*. The e-mail message will contain the time of the violation, the source address of the computer responsible for the violation, the destination IP address, the protocol being used, the source and destination ports, and the number violations occurring the previous 30 minutes. If the ICMP protocol were being used, then instead of the source and destination ports, the e-mail will report the ICMP code and type.

3. Click Submit.
4. Click the Admin tab, and then click **Commit & Reboot** in the task bar.
5. Click Commit to save your changes to permanent memory.

Managing the Black List

If data packets are received that violate the firewall settings or any of the IP Filter rules, then the source IP address of the offending packets can be blocked from such accesses for a specified period of time. You can enable or disable use of the black list using the settings described above. The source computer remains on the black list for the period of time that you specify.

To view the list of currently blacklisted computers, click **Black List** at the bottom of the Firewall Configuration page. The Firewall Blacklisted Hosts page displays, as shown in Figure 46.

Figure 46. Firewall Blacklisted Hosts Page

The table displays the following information for each entry:

Field	Description
Host IP Address	The IP address of the computer that sent the packet(s) that caused the violation
Reason	A short description of the type of violation. If the packet violated an IP Filter rule, the custom text from the Log Tag field will display. (See "Creating IP Filter Rules" on page 112.)
IPF Rule ID	If the packet violated an IP Filter rule, this field will display the ID assigned to the rule.
Action(s)	Displays an icon (🗑) you can click on to delete the entry from the list, if you want it to be removed prior to its automatic timed expiration.

18 Configuring IP Filters and Blocking Protocols

This chapter describes two Configuration Manager features that enable you to control the data passing through your network:

- The IP filter feature enables you to create rules to block attempts by certain computers on your LAN to access certain types of data or Internet locations. You can also block incoming access to computers on your LAN. Although IP filter rules provide a very flexible and powerful tool to enhance network security and control user activity, they can also be complex and generally require an advanced understanding of IP protocols.
- The blocked protocols feature enables you to simply select from a predefined list the protocol that you want to block. All data passed to the ADSL/Ethernet router using a blocked protocol will be discarded, without consideration of the source computer, destination computer, or the device interface on which it was received.

Configuring IP Filters

When you define an IP filter rule and enable the feature, you instruct the Neobit 1012VAto examine each data packet it receives to determine whether it meets criteria set forth in the rule. The criteria can include the size of the packet, the network or internet protocol it is carrying, the direction in which it is traveling (for example, from the LAN to the Internet or vice versa), the IP address of the sending computer, the destination IP address, and other characteristics of the packet data.

If the packet matches the criteria established in a rule, the packet can either be accepted (forwarded towards its destination), or denied (discarded), depending on the action specified in the rule.

Viewing Your IP Filter Configuration

To view your current IP filter configuration, log into Configuration Manager, click the Services tab, and then click **IP Filter** in the task bar. The IP Filter page displays, as shown in Figure 47.

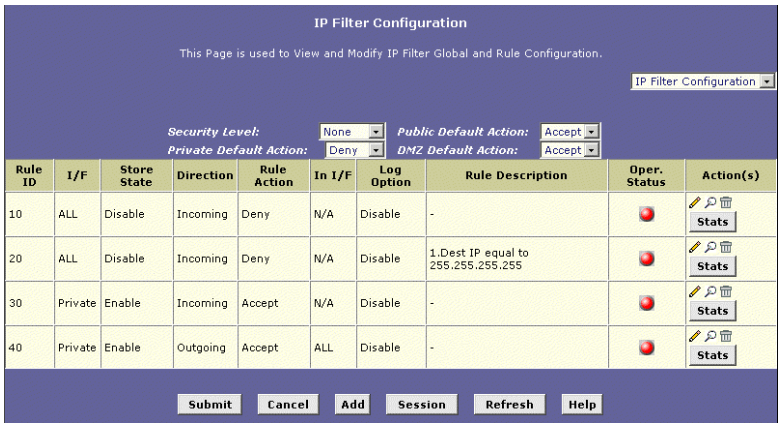


Figure 47. IP Filter Page

The IP Filter Configuration page displays global settings that you can modify, and the IP Filter rule table, which shows all currently established rules. See "Creating IP Filter Rules" on page 112 for a description of the items that make up a rule. When rules are defined, you can use the icons that display in the Actions column to edit ( ), delete ( ), and view details on ( ) the corresponding rule.

Configuring IP Filter Global Settings

The IP Filter Configuration page enables you to configure several global IP Filter settings, and displays a table showing all existing IP Filter rules. The global settings that you can configure are:

- **Security Level:** This setting determines which IP Filter rules take effect, based on the security level specified in each rule. For example, when *High* is selected, only those rules that are assigned a security value of *High* will be in effect. The same is true for the *Medium* and *Low* settings. When *None* is selected, IP Filtering is disabled.
- **Private/Public/DMZ Default Action:** This setting specifies a default action to be taken (Accept or Deny) on private, public, or DMZ-type device interfaces when they receive packets that *do not* match any of the filtering rules. You can specify a different default action for each interface type. (You specify an interface's type when you create the interface; see the PPP configuration page, for example.)
  - A *public* interface typically connects to the Internet. PPP, EoA, and IPoA interfaces are typically public. Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software. Typically, the global setting for public interfaces is *Deny*, so that all accesses to your LAN initiated from external computers are denied (discarded at the public interface), except for those allowed by a specific IP Filter rule.
  - A *private* interface connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network. Typically, the global setting for private interfaces is *Accept*, so that LAN computers have access to the ADSL/Ethernet routers' Internet connection.
  - The term *DMZ* (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public Web server). Packets received on a DMZ interface—a whether from a LAN or external source—are subject to a set of protections that is in between public and private interfaces in terms of restrictiveness. The global setting for DMZ-type interfaces may be set to *Deny* so that all attempts to access these servers are denied by default; the administrator may then configure IP Filter rules to allow accesses of certain types.

Creating IP Filter Rules

To create an IP filter rule, you set various criteria that must be met in order for the rule to be invoked. Use these instructions to add a new IP filter rule, and refer to the examples on page 117 for assistance:

1. On the main IP Filter page, click **Add**.

   The IP Filter Rule – Add page displays, as shown in Figure 48.

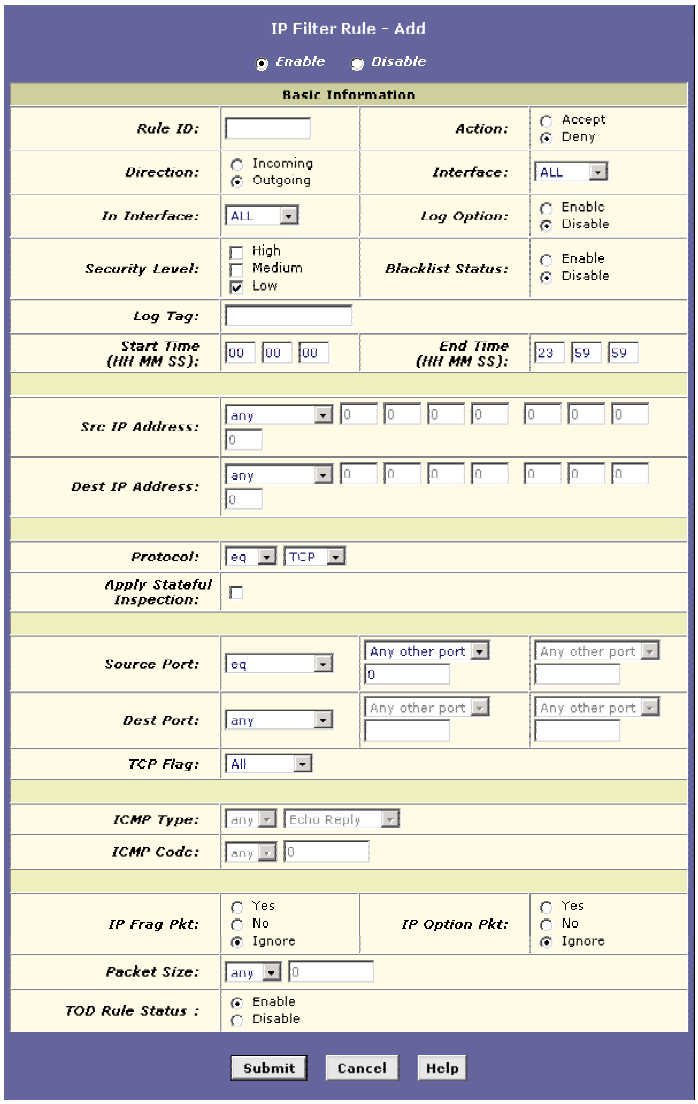


Figure 48. IP Filter Rule – Add Page

2. Enter or select data for each field that applies to your rule. The following table describes the fields:

Field	Description
Rule ID	Each rule must be assigned a sequential ID number. Rules are processed from lowest to highest on each data packet, until a match is found. It is recommended that you assign rule IDs in multiples of 5 or 10 (e.g., *10*, *20*, *30*) so that you leave enough room between them for inserting a new rule if necessary.
Action	The action that will be taken when a packet matches the rule criteria. The action can be *Accept* (forward to destination) or *Deny* (discard the packet).
Direction	Specifies whether the rule should apply to data packets that are incoming or outgoing on the selected interface. *Incoming* refers to packets coming from the LAN, and *outgoing* refers to packets going to the Internet. You can use rules that specify the incoming direction to restrict external computers from accessing your LAN.
Interface	The interface on the Neobit 1012VAon which the rule will take effect. See the examples on page 117 for suggestions on choosing the appropriate interface for various rule types.
In Interface	The interface from which packets must have been forwarded to the interface specified in the previous selection. This option is valid only for the outgoing direction.
Log Option	When *Enabled* is selected, a log entry will be created on the system each time this rule is invoked. The log entry will include the time of the violation, the source address of the computer responsible for the violation, the destination IP address, the protocol being used, the source and destination ports, and the number violations occurring in the previous x minutes. (Logging may be helpful when troubleshooting.) This information can also be e-mailed to designated administrators. See Chapter 17, "Configuring Firewall Settings" for instructions.
Security Level	The security level that must be enabled globally for this rule to take affect. A rule will be active only if its security level is the same as the globally configured setting (shown on the main IP Filter page). For example, if the rule is set to Medium and the global firewall level is set to Medium, then the rule will be active; but if the global firewall level is set to High or Low, then the rule will be inactive.

Field	Description
Black List Status	Specifies whether or not a violation of this rule will result in the offending computer's IP address being added to the Black List, which blocks the ADSL/Ethernet router from forwarding packets from that source for a specified period of time. See Chapter 17, "Configuring Firewall Settings" for instructions.
Log Tag	A description of up to 16 characters to be recorded in the log in the event that a packet violates this rule. Be sure to set the Log Option to *Enable* if you configure a Log Tag.
Start/End Time	The time range during which this rule is to be in effect, specified in military units.
Src IP Address/Dest IP Address	IP address criteria for the source computer(s) (from which the packet originates) and the destination computer. In the drop-down list, you can configure the rule to be invoked on packets containing: **any**: any source IP address. **lt**: *any* source IP address that is numerically *less than* the specified address. **lteq**: any source IP address that is numerically *less than or equal to* the specified address. **gt**: any source IP address that is numerically *greater than* the specified address. **eq**: any source IP address that is numerically *equal to* the specified address. **neq**: any source IP address that is *not equal to* the specified address. **range**: any source IP address that is within the specified range, inclusive. **out of range**: any source IP address that is outside the specified range. **self**: the IP address of the ADSL/Ethernet router interface on which this rule takes effect. **bcast**: (destination address only) Specifies that the rule will be invoked for any packets sent to the broadcast address for the receiving interface. (The broadcast address is used to send packets to all hosts on the LAN or subnet connected to the specified interface.) When you select this option, you do not need to specify the address, so the address fields are dimmed.

Field	Description
Protocol	The basic IP protocol criteria that must be met for rule to be invoked. Using the options in the drop-down list, you can specify that packets must contain the selected protocol (*eq*), that they must not contain the specified protocol (*neq*), or that the rule can be invoked regardless of the protocol (*any*). TCP, UDP, and ICMP are commonly IP protocols; others can be identified by number from 0-255, as defined by the Internet Assigned Numbers Authority (IANA).
Apply Stateful Inspection	When this option is enabled, packets are monitored for their state (i.e., whether they are the initiating packet or a subsequent packet in an ongoing communication, etc). This option provides a degree of security by blocking/dropping packets that are not received in the anticipated state. Such packets can signify unwelcome attempt to gain access to a network.
Source/Destination Port	Port number criteria for the source computer(s) (from which the packet originates) and destination computers. Port numbers identify the type of traffic that the computer or server can handle and are specified by the Internet Assigned Numbers Authority (IANA). For example, port number 80 indicates a Web server, 21 indicates an FTP server. You can choose a port type by name from the drop-down lists or, if not available in the list, specify the IANA port number in the text boxes. Select *Any other port* if this criteria will not be used. These fields will be dimmed (unavailable for entry) unless you have selected TCP or UDP as the protocol. See the description of Src IP Address for the statement options (any, eq, gt, etc.)
TCP Flag	Specifies whether the rule should apply only to TCP packets that contain the synchronous (*SYN*) flag, only to those that contain the non-synchronous (*NOT-SYN*) flag, or to all TCP packets. This field will be dimmed (unavailable for entry) unless you selected TCP as the protocol.
ICMP Type	Specifies whether the value in the type field in ICMP packet headers will be used as criteria. The code value can be any decimal value from 0-255. You can specify that the value must equal (*eq*) or not equal (*neq*) the specified value, or you can select *any* to enable the rule to be invoked on all ICMP packets. This field will be dimmed (unavailable for entry) unless you specify ICMP as the protocol.

Field	Description
ICMP Code	Specifies whether the value in the code field in ICMP packet headers will be used as criteria. The code value can be any decimal value from 0-255. You can specify that the value must equal (*eq*) or not equal (*neq*) the specified value, or you can select *any* to enable the rule to be invoked on all ICMP packets. This field will be dimmed (unavailable for entry) unless you specify ICMP as the protocol.
IP Frag Pkt	Determines how the rule applies to IP packets that contain fragments. You can choose from the following options: ○ **Yes**: The rule will be applied only to packets that contain fragments. ○ **No**: The rule will be applied only to packets that do not contain fragments. ○ **Ignore**: (Default) The rule will be applied to packets whether or not they contain fragments, assuming that they match the other criteria.
IP Option Pkt	Determines whether the rule should apply to IP packets that have options specified in their packet headers. ○ **Yes:** The rule will be applied only to packets that contain header options. ○ **No:** The rule will be applied only to packets that do not contain header options. ○ **Ignore:** (Default) The rule will be applied to packets whether or not they contain header options, assuming that they match the other criteria.
Packet Size	Specifies that the IP filter rule will take affect only on packets whose size in bytes matches this criterion. (*lt* = less than, *gt* = greater than, *lteq* = less than or equal to, etc.)
TOD Rule Status	The Time of Day Rule Status determines how the Start Time/End Time settings are used. ○ **Enable:** (Default) The rule is in effect for the specified time period. ○ **Disable:** The rule is not in effect for the specified time period, but is effective at all other times.

3. When you are done selecting criteria, ensure that the Enable radio button is selected at the top of the page, and then click Submit.

   After a confirmation page displays, the IP Filter Configuration page will redisplay with the new rule showing in the table.

   If the security level of the rule matches the globally configured setting, a green ball in the Status column for that rule, indicating that the rule is now in effect. A red ball will display when the rule is disabled or if its security level is different from the globally configured level.

4. Ensure that the Security Level and Private/Public/DMZ Default Action settings on the IP Filter Configuration page are configured as needed, then click Submit

   A page displays to confirm your changes.

5. Click the Admin tab, and then click **Commit & Reboot** in the task bar.

6. Click Commit to save your changes to permanent memory.

IP filter rule examples

Example 1. Blocking a specific computer on your LAN from using accessing web servers on the Internet:

1. Add a new rule for outgoing packets on the ppp-0 interface from any incoming interface (this would include the eth-0 and usb-0 interfaces, for example).
2. Specify a source IP address of the computer you want to block.
3. Specify the Protocol = *TCP* and enable the Store State setting.
4. Select the TCP Protocol, and then specify a destination port = *80*, which is the well-known port number for web servers.
5. Enable the rule by clicking the radio button at the top of the page.
6. Click Submit to create the rule.
7. On the IP Filter Configuration page, set the Security Level to the same level you chose for the rule, and set both the Private Default Action and the Public Default Action to *Accept*.
8. Click Submit, and commit your changes.

Figure 48 on page 112 shows the configuration for this rule. The specified computer will not be able to access the Web, but will be able to access FTP Internet sites (and any others that use destination port numbers other than 80).

Example 2. Blocking Telnet accesses to the Neobit 1012VA:

1. Add a new rule for packets incoming on the ppp-0 interface.
2. Specify that the packet must contain the TCP protocol, and must be destined for port 23, the well-known port number used for the Telnet protocol.
3. Enable the rule by clicking the radio button at the top of the page.
4. Click **Submit** to create the rule, and commit your changes.

Figure 49 shows how this rule could be configured:

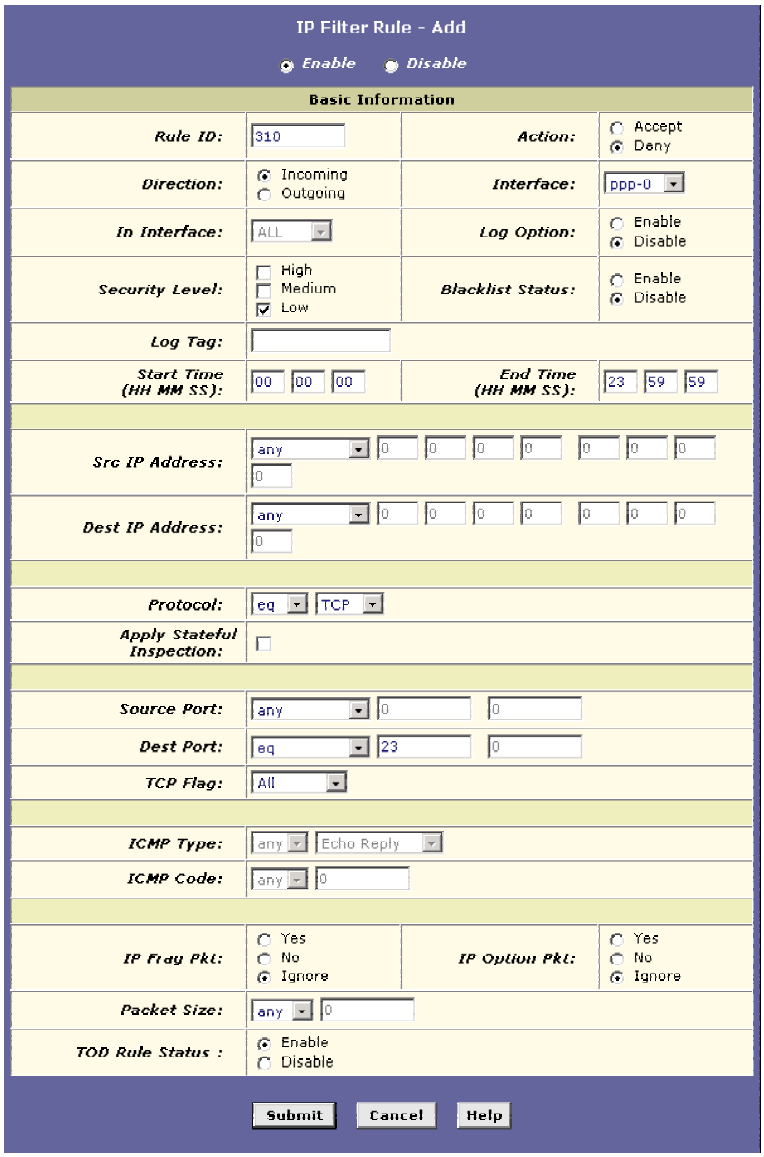


Figure 49. IP Filter Rule Example 2

Viewing IP Filter Statistics

For each rule, you can view statistics on how many packets were accepted or denied. Display the IP Filter Configuration page, and then click Stats in the row corresponding to the rule. The IP Filter Rule – Statistics page displays, as shown in Figure 50.

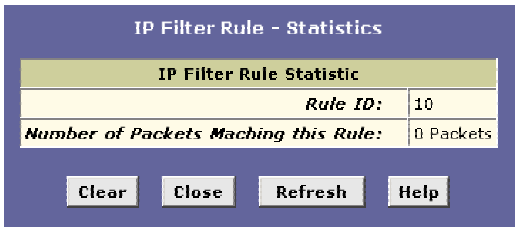


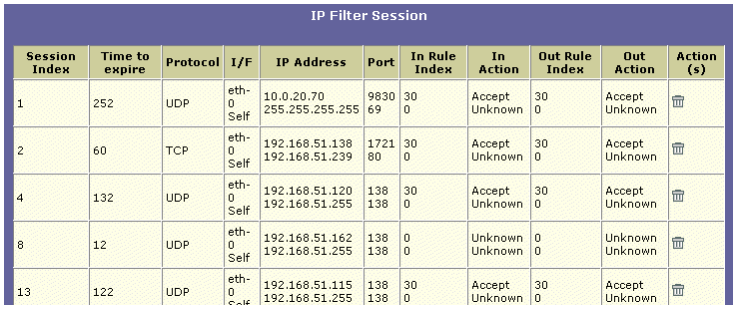
Figure 50. IP Filter Rule – Statistics Page

You can click Clear to reset the count to zero and Refresh to display newly accumulated data.

Managing Current IP Filter Sessions

When two computers communicate using the IP protocol, an IP session is created for the duration of the communication. The Neobit 1012VAallows a fixed number of concurrent IP sessions. You can view information about each current IP session and delete sessions (for security reasons, for example).

To view all current IP sessions, display the IP Filters Configuration page, and then click Session. Figure 119 shows an example of an IP Filter Sessions page.



Session Index	Time to expire	Protocol	I/F	IP Address	Port	In Rule Index	In Action	Out Rule Index	Out Action	Action (s)
1	252	UDP	eth-0 Self	10.0.20.70 255.255.255.255	9830 69	30 0	Accept Unknown	30 0	Accept Unknown	
2	60	TCP	eth-0 Self	192.168.51.138 192.168.51.239	1721 80	30 0	Accept Unknown	30 0	Accept Unknown	
4	132	UDP	eth-0 Self	192.168.51.120 192.168.51.255	138 138	30 0	Accept Unknown	30 0	Accept Unknown	
8	12	UDP	eth-0 Self	192.168.51.162 192.168.51.255	138 138	0 0	Unknown Unknown	0 0	Unknown Unknown	
13	122	UDP	eth-0	192.168.51.115 192.168.51.255	138 138	30 0	Accept Unknown	30 0	Accept Unknown	

Figure 51. IP Filter Sessions Page

The IP Filter Session table displays the following fields for each current IP session:

Field	Description
Session Index	The ID assigned by the system to the IP session (all sessions, whether or not they are affected by an IP filter rule, are assigned a session index).
Time to expire	The number of seconds in which the connection will automatically expire
Protocol	The underlying IP protocol used on the connection, such as TCP, UDP, IGMP, etc.)
I/F	The interface on which the IP Filter rule is effective
IP Address	The IP addresses involved in the communication. The first one shown is the initiator of the communication.
Port	The hardware addresses of the ports involved in the communication
In/Out Rule Index	The number of the IP Filter rule that is applies to this session (assigned when the rule was created)
In/Out Action	The action (accept, deny, or unknown), being taken on data coming into or going out on the interface. This action is specified in the rule definition.
Actions	Provides a icon you can click on ( ) to delete the IP session. When you delete a session, the communication between is discontinued.

You can click Refresh to display newly accumulated data.

Blocking Protocols

The Blocked Protocols feature enables you to prevent the ADSL/Ethernet router from passing any data that uses a particular protocol. Unlike the IP Filter feature, you cannot specify additional criteria for blocked protocols, such as particular users or destinations. However, when you are certain that a particular protocol is not needed or wanted on your network, this feature provides a convenient way to discard such data before it is passed.

To display the Blocked Protocols page, click the Services tab, and then click **Blocked Protocols** in the task bar. The Blocked Protocols page displays, as shown in Figure 52.

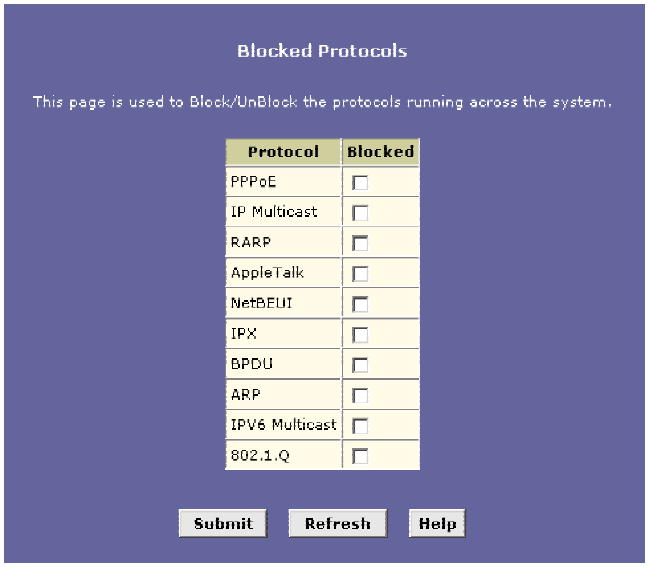


Figure 52. Blocked Protocols Page

WARNING

Blocking certain protocols may disrupt or disable your network communication or Internet access. If you are unfamiliar with how your network or Internet connection uses these protocols, contact your ISP before disabling.

The following list describes each of the available protocols.

Protocol	Description
PPoE	Point-to-Point Protocol over Ethernet. Many DSL modems use PPoE to establish and maintain a connection with a service provider. PPoE provides a means of logging in to the ISPs servers so that they can authenticate you as a customer and provide you access to the Internet. Check with your ISP before blocking this protocol.

Protocol	Description
IP Multicast	IP Multicast is an extension to the IP protocol. It enables individual packets to be sent to multiple hosts on the Internet, and is often used for handling e-mail mailing lists and teleconferencing/videoconferencing.
RARP	Reverse Address Resolution Protocol. This IP protocol provides a way for computers to determine their own IP addresses when they only know their hardware address (i.e., MAC addresses). Certain types of computers, such as diskless workstations, must use RARP to determine their IP address before communicating with other network devices.
AppleTalk®	A networking protocol used in for Apple Macintosh® networks.
NetBEUI	NetBIOS Enhanced User Interface. On many LAN operating systems, the NetBEUI protocol provides the method by which computers identify themselves to and communicate with each other.
IPX	Internet work Packet Exchange. A networking protocol used on Novell Netware ®-based LANs.
BPDU	Bridge Protocol Data Unit. BPDUs are data messages that are exchanged across the switches between LANs that are connected by a bridge. BPDU packets contain information on ports, addresses, priorities, and costs, and are exchanged across bridges to detect and eliminate loops in a network.
ARP	Address Resolution Protocol. Computers on a LAN use ARP to learn the hardware addresses (i.e., MAC addresses) of other computers when they know only their IP addresses.
IPV6 Multicast	IP Multicasting under IP Protocol version 6. See *IP Multicast* above.
802.1.Q	This IEEE specification defines a protocol for *virtual LANs* on Ethernet networks. A virtual LAN is a group of PCs that function as a local area network, even though the PCs may not be physically connected. They are commonly used to facilitate administration of large networks.

To block a protocol, click the appropriate check box, and click Submit. After you have verified that the device continues to function as expected, click the Admin tab, click **Commit & Reboot** in the task bar, and then click Commit to save your changes to permanent memory.

19 Viewing DSL Parameters

To view configuration parameters and performance statistics for the Neobit 1012VA's DSL line, log into Configuration Manager, and then click the WAN tab. The DSL Status page displays by default, as shown in Figure 53.

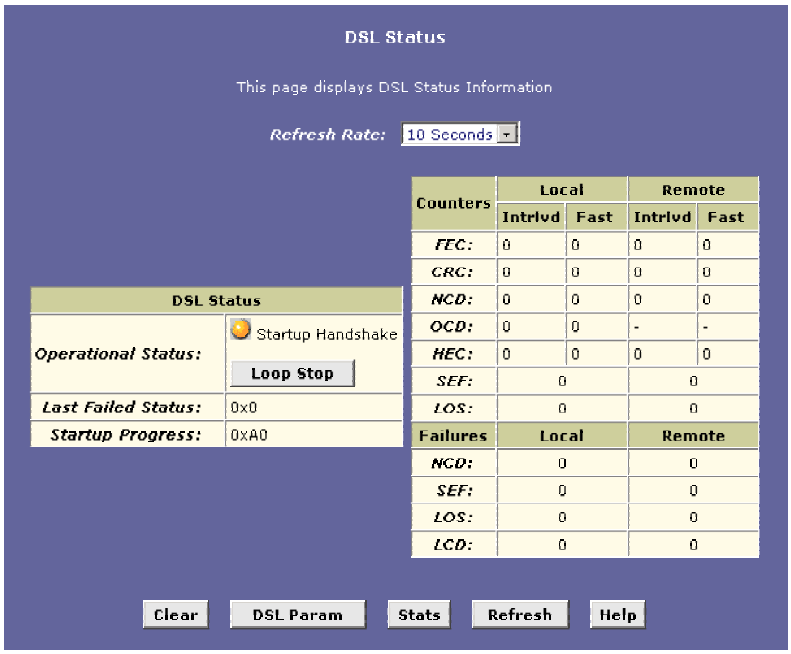


Figure 53. DSL Status Page

The DSL Status page displays current information on the DSL line performance. The page refreshes according to the setting in the Refresh drop-down list, which you can configure.

In the DSL Status table, the Operational Status setting displays a red, orange, or green ball to indicate that the DSL line is idle, starting up, or up-and-running, respectively. You can click **Loop Stop** to end the DSL connection. To restart the connection, you can click **Loop Start**.

Although you generally will not need to view the remaining data, it may be helpful when troubleshooting connection or performance problems with your ISP.

You can click **Clear** to reset all counters to zero, and **Refresh** to redisplay the page with newly accumulated values.

You can click **DSL Param** to display data about the configuration of the DSL line, as shown in Fig 55

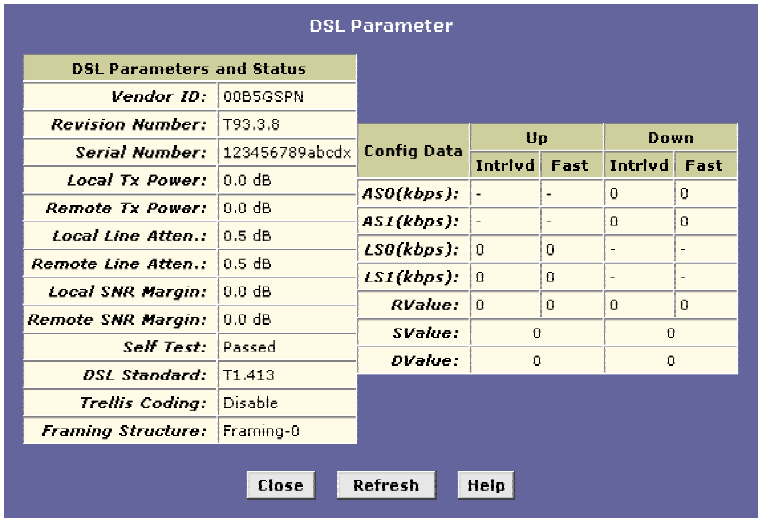


Figure 54. DSL Parameters Page

- The DSL Parameters and Status table displays settings preconfigured by the product manufacturer or your ISP.
- The Config Data table lists various types of error and defects measurements found on the DSL line.

You cannot modify this data.

From the DSL Status page, you can click **Stats** to display DSL line performance statistics, as shown in Figure 55.

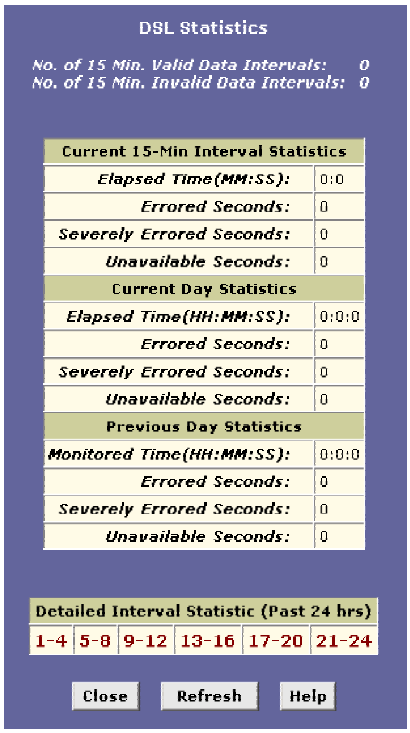


Figure 55. DSL Statistics Page

The DSL Statistics page reports error data relating to the last 15-minute interval, the current day, and the previous day.

At the bottom of the page, the Detailed Interval Statistic table displays links you can click on to display detailed data for each 15-minute interval in the past 24 hours. For example, when you click on 1-4, data displays for the 16 intervals (15-minutes each) that make up the previous 4 hours. Figure 56 shows an example.

DSL Interval Statistics

15-Min Interval No.	Errored Seconds	Severely Errored Seconds	Unavailable Seconds	Valid Data
1	0	0	0	No
2	0	0	0	No
3	0	0	0	No
4	0	0	0	No
5	0	0	0	No
6	0	0	0	No
7	0	0	0	No
8	0	0	0	No
9	0	0	0	No
10	0	0	0	No
11	0	0	0	No
12	0	0	0	No
13	0	0	0	No
14	0	0	0	No
15	0	0	0	No
16	0	0	0	No

Detailed Interval Statistic (Past 24 hrs)

1-4 | 5-8 | 9-12 | 13-16 | 17-20 | 21-24

Close Refresh Help

Figure 56. DSL Interval Statistics Page

20 Administrative Tasks

This chapter describes the following administrative tasks that you can perform using Configuration Manager:

- Viewing System Alarms
- Upgrading the Software
- Using Diagnostics
- Modifying Port Settings

You can access these tasks from the Admin tab task bar. The other Admin tasks listed in the Admin tab—Configuring User Logon and Committing and Rebooting—are described in Chapter 4, “Getting Started with the Configuration Manager.”

Viewing System Alarms

You can use the Configuration Manager to view information about alarms that occur in the system. Alarms, also called traps, are caused by a variety of system events, including connection attempts, resets, and configuration changes.

Although you will not typically need to view this information, it may be helpful in working with your ISP to troubleshoot problems you encounter with the device. (Despite their name, not all alarms indicate problems in the functioning of the system.)

Viewing the Alarm Table

To display the Alarm page, log into the Configuration Manager, click the Admin tab, and then click **Alarm** in the task bar.

The Alarm page is shown in Figure 57.

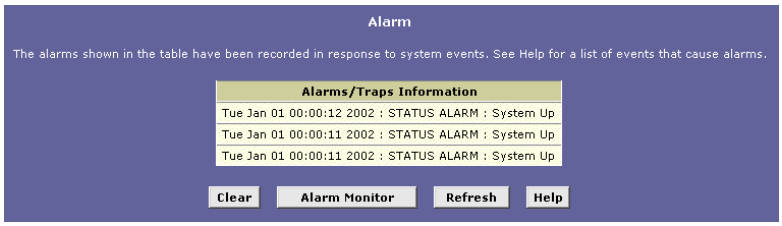


Figure 57. Alarm Page

Each row in the table displays the time and date that an alarm occurred, the type of alarm, and a brief statement indicating its cause.

To remove all entries from the list, click Clear. New entries will begin accumulating and will display when you click Refresh.

Displaying the Alarm Monitor in a Separate Window

If you want to display an automatically updating Alarm table, you can click Alarm Monitor to display a separate Alarm Monitor window, as shown in Figure 58.

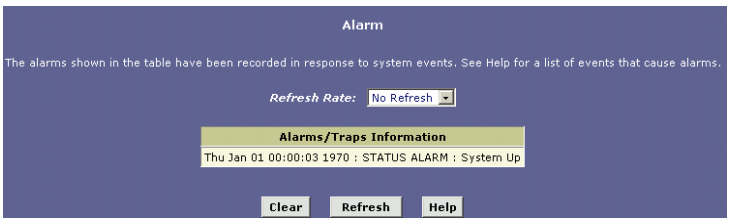


Figure 58. Alarm Monitor Window

You can click on the Refresh Rate drop-down list to select a recurring time interval after which the page will redisplay with new data.

You can leave the Alarm Monitor window open and active even after closing the Configuration Manager.

Upgrading the Software

Your ISP may from time to time provide you with an upgrade to the software running on the ADSL/Ethernet router. All system software is contained in a single file, called an *image*. The image is composed of several distinct parts, each of which implements a different set of functions.

Configuration Manager provides an easy way to upload the new software image, or a specific part of the image) to the memory on the ADSL/Ethernet router. To upgrade the image, follow this procedure:

1. Log into Configuration Manager, click the Admin tab, and then click **Local Image Upgrade** in the task bar.

   The Image Upgrade window is shown in Figure 59.

   Figure 59. Image Upgrade Page

2. In the Target Filename text box, type the name of the file as it must be stored in system memory.

   In most cases, the Target filename is the same as the source filename; your ISP should advise you if otherwise.

3. In the Source Filename text box, type the path and file name of the file as provided by your ISP. You can click Browse... to search for it on your hard drive.

4. Click Upload.

   After a few seconds, a message like the following should display (the file name may differ):

   File: TEDsl.gsz successfully saved to flash. Please reboot for the new image to take effect.

5. Turn power to the unit off, wait a few seconds, and turn it on again.

The new software will now be in effect. If the system is not working properly or fails to boot, contact your ISP for troubleshooting assistance.

Using Diagnostics

The diagnostics feature executes a series of test of your system software and hardware connections. Use this feature when working with your ISP to troubleshoot problems.

Follow these instructions to begin the diagnostics program:

1. Log into Configuration Manager, click the Admin tab, and then click **Diagnostics** in the task bar.

   Figure 60 shows the Diagnostics page.

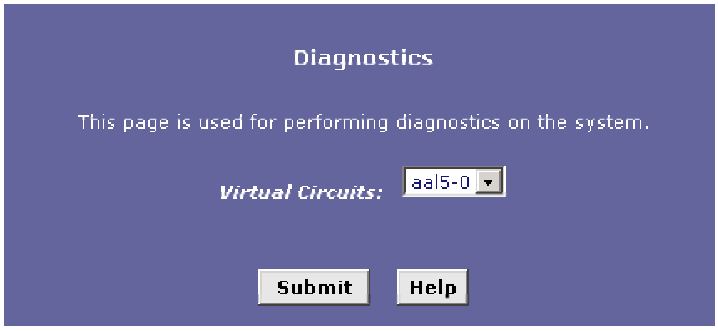


   Figure 60. Diagnostics Page

2. From the Virtual Circuits drop-down list, select the name of your ATM interface (see Configuring the ATM VCC for a explanation of ATM interfaces). Usually, this will be *atm-0*.

3. Click Submit.

The diagnostics utility will run a series of test to check whether the device's connections are up and working. This takes only a few seconds. The program reports whether the test passed or failed, as shown in Figure 61. A test may be skipped if the program determines that no suitable interface is configured on which to run the test.

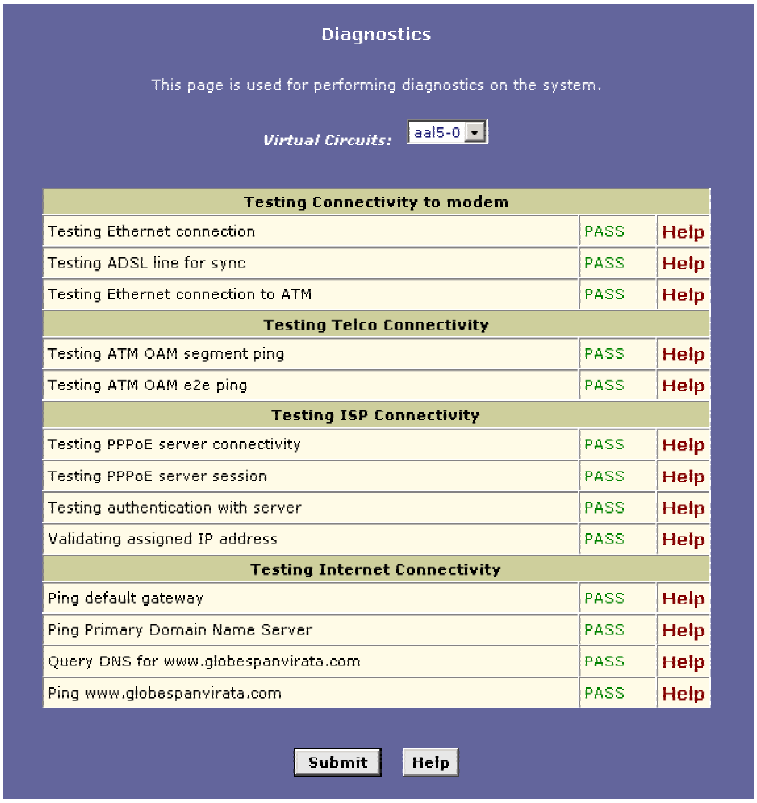


Figure 61. Diagnostics Page—After Execution

You can click **Help** to display an explanation of each test. Work with your ISP to interpret the results of the diagnostic tests.

Modifying Port Settings

Overview of IP port numbers

The header information in an IP data packet specifies a destination port number. Routers use the port number along with the specified IP addresses to forward the packet to its intended recipient.

For example, all IP data packets that the ADSL/Ethernet router receives from the Internet specify the same IP address (your public IP address) as the destination. However, depending on the port number contained in a data packets, the ADSL/Ethernet router may pass the packet on to its embedded Web or Telnet servers, or to another computer on the network.

The Internet community has developed a list of common server types such as HTTP, Telnet, e-mail, and many others, and assigned a unique port number to each. These are not mandatory, but are useful in promoting communication between separately administered LANs.

Modifying the ADSL/Ethernet routers' port numbers

In some cases, you may want to assign non-standard port numbers to the HTTP and Telnet servers that are embedded on the Neobit 1012VA. The following scenario is one example of why changing the HTTP port number may be necessary:

> You have an externally visible Web server on your LAN, with a NAT rule (rdr flavor) that redirects incoming HTTP packets to that Web server. When incoming packets contain a destination IP address of your public IP address (which is assigned to the ADSL/Ethernet router's WAN port) and the standard Web server port number of 80, the NAT rule recognizes the port number and redirects the packets to your Web server's local IP address.
>
> Assume in this scenario that you also want to enable external access to the [Productname's] Configuration Manager, so that your ISP can log in and manager your system, for example. Accessing Configuration Manager requires accessing the [Productname's] own Web server (also called its HTTP server). In this case, you would want to use the Port Settings feature to assign a non-standard port number to the Neobit 1012VA's HTTP server. Without a non-standard port number, the NAT rule would redirect your ISP's log in attempt to your LAN HTTP server rather than to the HTTP server on the Neobit 1012VA.
>
> Thereafter, when your ISP wants to log on to your Configuration Manager, they would type your IP address in their browser, followed by a colon and the non-standard port number, as shown in this example:
>
> **http://192.168.1.1:61000**

Your ISP may also have special circumstances that require changing the HTTP or Telnet port numbers; contact them before making any changes here.

Follow these steps to modify port settings:

1. Log into Configuration Manager, click the Admin tab, and then click **Port Settings** in the task bar.

   The Port Settings page is shown in Figure 62.

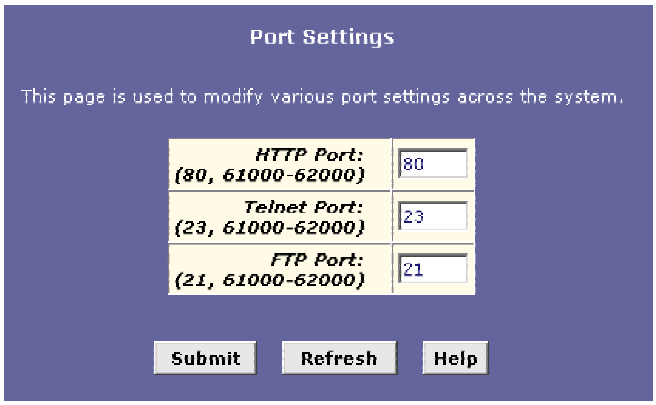


Figure 62. Port Settings Page

2. Type the new port number(s) in the appropriate text box(es) and click Submit.

   The default port numbers are shown in Figure 62. You can enter non-standard port numbers in the range 61000-62000.

3. Click **Commit & Reboot** in the task bar, and click Commit to save your changes to permanent memory.

4. On the Commit & Reboot page, click Reboot.

   Note that the new settings will not be effective until you reboot the system.

A IP Addresses, Network Masks, and Subnets

IP Addresses

Note

This section pertains only to IP addresses for IPv4 (version 4 of the Internet Protocol). IPv6 addresses are not covered.

This section assumes basic knowledge of binary numbers, bits, and bytes. For details on this subject, see Appendix A.

IP addresses, the Internet's version of telephone numbers, are used to identify individual nodes (computers or devices) on the Internet. Every IP address contains four numbers, each from 0 to 255 and separated by dots (periods), e.g. 20.56.0.211. These numbers are called, from left to right, field1, field2, field3, and field4.

This style of writing IP addresses as decimal numbers separated by dots is called *dotted decimal notation*. The IP address 20.56.0.211 is read "twenty dot fifty-six dot zero dot two-eleven."

Structure of an IP address

IP addresses have a hierarchical design similar to that of telephone numbers. For example, a 7-digit telephone number starts with a 3-digit prefix that identifies a group of thousands of telephone lines, and ends with four digits that identify one specific line in that group.

Similarly, IP addresses contain two kinds of information.

- *Network ID*
  Identifies a particular network within the Internet or intranet
- *Host ID*
  Identifies a particular computer or device on the network

The first part of every IP address contains the network ID, and the rest of the address contains the host ID. The length of the network ID depends on the network's *class* (see following section). Table 3 shows the structure of an IP address.

Table 3. IP Address structure

	Field1	Field2	Field3	Field4
Class A	Network ID	Host ID		
Class B	Network ID		Host ID	
Class C	Network ID			Host ID

Here are some examples of valid IP addresses:

Class A: 10.30.6.125 (network = 10, host = 30.6.125)
Class B: 129.88.16.49 (network = 129.88, host = 16.49)
Class C: 192.60.201.11 (network = 192.60.201, host = 11)

Network classes

The three commonly used network classes are A, B, and C. (There is also a class D but it has a special use beyond the scope of this discussion.) These classes have different uses and characteristics.

Class A networks are the Internet's largest networks, each with room for over 16 million hosts. Up to 126 of these huge networks can exist, for a total of over 2 billion hosts. Because of their huge size, these networks are used for WANs and by organizations at the infrastructure level of the Internet, such as your ISP.

Class B networks are smaller but still quite large, each able to hold over 65,000 hosts. There can be up to 16,384 class B networks in existence. A class B network might be appropriate for a large organization such as a business or government agency.

Class C networks are the smallest, only able to hold 254 hosts at most, but the total possible number of class C networks exceeds 2 million (2,097,152 to be exact). LANs connected to the Internet are usually class C networks.

Some important notes regarding IP addresses:

- The class can be determined easily from field1:
  field1 = 1-126: Class A
  field1 = 128-191: Class B
  field1 = 192-223: Class C
  (field1 values not shown are reserved for special uses)
- A host ID can have any value except all fields set to 0 or all fields set to 255, as those values are reserved for special uses.

Subnet masks

Definition
mask

A mask *looks like a regular IP address, but contains a pattern of bits that tells what parts of an IP address are the network ID and what parts are the host ID: bits set to 1 mean "this bit is part of the network ID" and bits set to 0 mean "this bit is part of the host ID."*

Subnet masks are used to define *subnets* (what you get after dividing a network into smaller pieces). A subnet's network ID is created by "borrowing" one or more bits from the host ID portion of the address. The subnet mask identifies these host ID bits.

For example, consider a class C network 192.168.1. To split this into two subnets, you would use the subnet mask:

255.255.255.128

It's easier to see what's happening if we write this in binary:

11111111. 11111111. 11111111.10000000

As with any class C address, all of the bits in field1 through field 3 are part of the network ID, but note how the mask specifies that the first bit in field 4 is also included. Since this extra bit has only two values (0 and 1), this means there are two subnets. Each subnet

uses the remaining 7 bits in field4 for its host IDs, which range from 0 to 127 (instead of the usual 0 to 255 for a class C address).

Similarly, to split a class C network into four subnets, the mask is:

255.255.255.192 or 11111111. 11111111. 11111111.11000000

The two extra bits in field4 can have four values (00, 01, 10, 11), so there are four subnets. Each subnet uses the remaining six bits in field4 for its host IDs, ranging from 0 to 63.

Note

Sometimes a subnet mask does not specify any additional network ID bits, and thus no subnets. Such a mask is called a default subnet mask*. These masks are:*

Class A: 255.0.0.0
Class B: 255.255.0.0
Class C: 255.255.255.0

These are called default *because they are used when a network is initially configured, at which time it has no subnets.*

B Binary Numbers

Binary Numbers

In everyday life, we use the decimal system of numbers. In decimal, numbers are written using the ten digits 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9. Computers, however, do not use decimal. Instead, they use *binary*.

Definition
binary numbers

Binary numbers are numbers written using only the two digits 0 and 1, e.g., 110100.

Hint

Does "base ten" sound familiar? (Think grade school.) Base ten is just another name for decimal. Similarly, base two is binary.

Just as each digit in a decimal number represents a multiple of 10 (1, 10, 100, 1000, 10,000, etc.), each digit in a binary number represents a multiple of 2 (1, 2, 4, 8, 16, etc.). For example:

Decimal					Binary			
1,000's	100's	10's	1's		8's	4's	2's	1's
-	-	**1**	**3**	=	**1**	**1**	**0**	**1**

Also, since binary uses only two digits to represent all numbers, a binary number has more digits than the same number in decimal. In the example above, you can see that the decimal number 13 is the same as the binary number 1101 (8 + 4 + 1 = 13).

Bits and bytes

Computers handle binary numbers by grouping them into units of distinct sizes. The smallest unit is called a *bit*, and the most commonly used unit is called a *byte*.

Definition
bit and byte

A bit *is a single binary digit, i.e., 0 or 1.*

A byte *is a group of eight consecutive bits (the number of bits can vary with computers, but is almost always eight), e.g., 11011001. The value of a byte ranges from 0 (00000000) to 255 (11111111).*

The following shows the values of the eight digits in a byte along with a sample value:

128's	64's	32's	16's	8's	4's	2's	1's
1	**0**	**1**	**0**	**1**	**1**	**0**	**1**

The decimal value of this byte is 173 (128 + 32 + 8 + 4 + 1 = 173).

Index

100BASE-T, 157
10BASE-T, 157
ADSL, 157
ADSL cable, 16
ADSL port, 16
Alarm Monitor window, 140
Alarm page, 139
Alarms, 139
Analog, 157
Asynchronous Transfer Mode. *See* ATM
ATM, 157
  defined, 93
  viewing configuration, 93
ATM VCC – Add page, 94, 96
ATM VCC Configuration page, 93
Attacks, 118
BASIC NAT flavor, 73
BIMAP NAT flavor, 76
Binary numbers, 151, 157
Bits, 151, 157
Black List, 118
  managing, 120
Blocked Protocols page, 133
Bridge Configuration page, 115
Bridge forwarding table, 113
Bridges vs routers, 114
Bridging, 157
  defined, 113
  defining interfaces, 115
  with IP-enabled interfaces, 115
Broadband, 157
Broadcast, 157
Bytes, 151
Commit & Reboot page, 40
Computers
  configuring IP information, 18
Configuration Manager
  overview, 33
  troubleshooting, 154
Connectors
  rear panel, 13
Data packet, 61
Date and time, changing, 38
Default configuration, 31
Default gateway, 84
De-militarized zones, 123
Denial of Service, 118
DHCP
  defined, 51, 157
  device modes, 52
  setting operating mode, 59
DHCP Address Table page, 57
DHCP client
  configuring device as, 45
  defined, 51
DHCP Configuration page, 53, 59
DHCP relay, 158
  configuring device as, 52, 58
DHCP Relay Configuration page, 58
DHCP server, 158
  configuring the device as, 53
  defined, 51
  modifying, viewing pools, 56
  pools, 51
  using a LAN device as, 52
  using existing on LAN, 44, 45

using ISP
as, 52
using the device as, 52
viewing assigned addresses, 57
DHCP Server Pool—Add page, 54
Diagnosing problems
after installation, 32
Diagnostics, 143
Diagnostics page, 143
Digital, 158
DNS, 55, 79, 158
defined, 79
relay, 80
DNS Configuration page, 81
Domain name, 55, 158
Domain Name System. *See* DNS
download, 158
DSL
defined, 158
DSL interface
IP address, 49
DSL Interval Statistics page, 137
DSL Modem Installer dialog box, 27
DSL Parameters page, 136
DSL Statistics page, 136
DSL Status page, 135
Dynamically assigned IP addresses, 51
EOA
defined, 104
settings, 105
EOA interface, 49
EOA Interface – Add page, 106
EOA page, 105
Eth-0 interface
defined, 31
Ethernet
defined, 158
Ethernet cable, 17
straight-through vs crossover, 153
Features, 9
FILTER NAT flavor, 74
Filtering rule, 158
Firewall, 158
settings, 118
Firewall Blacklisted Hosts page, 120
Firewall Configuration page, 117
Front panel, 12
FTP, 159
Gatewas
in DHCP pools, 55
Gateway
defined, 84
Gigabit, 159
Hardware connections, 15, 16
Home Tab, 36
Hop, 159
defined, 84
Hop count, 90, 159
Host, 159
Host ID, 147
HTTP, 159
HTTP port, modifying address, 144
Image Upgrade page, 141
In-line filter. *See* Microfilter
Internet, 159
troubleshooting access to, 153
Intranet, 159
IP address
in device's routing table, 85
IP address pools
excluding addresses, 57
modifying, 57
IP Address Table page, 49
IP addresses, 159

explained, 147
viewing device's, 49
IP configuration
static, 23
static IP addresses, 23
Windows 2000, 19
Windows 95/98, 21
Windows Me, 20
Windows NT 4.0, 22
IP Configuration
Windows XP, 18
IP data packet, 61
IP Filter Configuration page, 122
IP Filter Rule – Statistics page, 131
IP Filter Rule – Add Page, 124
IP filter rules
adding, 124
examples, 129
settings, 125
IP filter sessions, 131
IP Filter Sessions page, 131
IP filters
viewing statistics, 131
IP Global Statistics page, 50
IP information
configuring on LAN computers, 18
IP Route – Add page, 87
IP Route Table page, 85
IP routes
adding, 87
manually configuring, 84
type, 86
IP Routes
defined, 83
IPOA
defined, 109
IPoA Interface – Add page, 111
IPoA page, 109
ISP, 160
LAN, 160
LAN Configuration page, 44
LAN interface, 58
configuring multiple, 49
LAN IP address, 43, 45
configuring, 44
specifying, 44
viewing, 49
LAN network mask, 45
LAN port
default IP information, 23
LEDs, 12, 160
troubleshooting, 153
Login
to Configuration Manager, 33
Loopback IP address, 49
MAC addresses, 160
in DHCP Address Table, 57
in DHCP pools, 55
Mask. *See* Network mask
Mbps, 160
Microfilter, 160
NAPT (NAT flavor), 68
NAT, 160
adding rules, 68
BASIC flavor, 73
BIMAP flavor, 76
default configuration, 62
defined, 61
FILTER flavor, 74
global settings, 62
napt flavor, 68
PASS flavor, 77
RDR flavor, 70
viewing performance statistics, 65

NAT Configuration page, 62
NAT Rule Configuration page, 65
NAT Rule Global Statistics page, 64
NAT Rule Statistics page, 65
NAT Rule—Add page - basic, 73
NAT Rule—Add page - bimap, 76
NAT Rule—Add page - filter, 74
NAT Rule—Add page - napt, 68
NAT Rule—Add page - pass, 77
NAT Rule—Add page - rdr, 71
NAT Translation – Details page, 67
NAT Translations page, 66
Navigating, 35
Netmask. *See Network mask*
Network. *See* LAN
Network Address Translation. *See* NAT
Network classes, 148
Network ID, 147
Network interface card, 9
Network mask, 160
  in DHCP address table, 57
Network mask, 148
NIC, 160
Node on network
  defined, 44
Notational conventions, 10
nslookup, 156
Packet, 160
Packets
  filtering, 122
Pages
  Alarm, 139
  Alarm Monitor window, 140
  ATM VCC - Add, 94, 96
  ATM VCC Configuration, 93
  Blocked Protocols, 133
  Bridge Configuration, 115
Commit & Reboot, 40
DHCP Address Table, 57
DHCP Configuration, 53, 59
DHCP Relay Configuration, 58
DHCP Server Pool - Add, 54
Diagnostics, 143
DNS Configuration, 81
DSL Interval Statistics, 137
DSL Parameters, 136
DSL Statistics, 136
DSL Status, 135
EOA, 105
EOA Interface - Add, 106
Firewall Blacklisted Hosts, 120
Firewall Configuration, 117
Image Upgrade, 141
IP Address Table, 49
IP Filter Configuration, 122
IP Filter Rule - Add, 124
IP Filter Rule - Statistics, 131
IP Filter Sessions, 131
IP Global Statistics, 50
IP Route - Add, 87
IP Route Table, 85
IPoA, 109
IPoA Interface, 111
LAN Configuration, 44
NAT Configuration, 62
NAT Rule Add - basic, 73
NAT Rule Add - bimap, 76
NAT Rule Add - filter, 74
NAT Rule Add - napt, 68
NAT Rule Add - pass, 77
NAT Rule Add - rdr, 71
NAT Rule Configuration, 65
NAT Rule Global Statistics, 64
NAT Rule Statistics, 65

NAT Translations, 66
NAT Translations - Details, 67
Port Settings, 145
PPP - Detail, 100
PPP Configuration, 97
PPP Interface - Add, 102
PPP Interface - Modify, 103
Quick Configuration, 29
RIP Configuration, 90
RIP Global Statistics, 92
System View, 36
System—Modify, 38
User Password Configuration, 39
Parts
checking for, 11
PASS - NAT flavor, 77
Password
changing, 39
default, 34
recovering, 154
PC configuration, 18
PC Configuration
static IP addresses, 23
Performance statistics, 50
Ping, 155, 161
Port, 161
Port numbers
using non-standard, 72
Port settings, 144
Port Settings page, 145
POTS, 161
Power connector, 17
PPP, 161
settings, 98, 100
PPP – Detail page, 100
PPP Configuration page, 97
PPP interface, 49
PPP Interface – Add page, 102
PPP Interface – Modify page, 103
PPPoA, 161
PPPoE, 161
Protocol, 161
Quick Configuration
logging in, 29
Quick Configuration page, 29
RDR (NAT flavor), 70
Rear Panel, 13
Rebooting, 41
Remote, 161
Reset button, 41
RIP, 161
configuring on device, 90
overview, 89
viewing statistics, 92
RIP Configuration page, 90
RIP Global Statistics page, 92
RJ-11, 161
RJ-45, 161
Routing, 161
Routing Information Protocol. *See* RIP
Security levels
setting, 123
Software upgrades, 141
Splitter, 162
Splitterless, 162
Static IP addresses, 23
Statically assigned IP addresses, 51
Submitting vs committing, 40
Subnet, 162
defined, 55
Subnet mask. See Network mask
Subnet masks, 148
System requirements
for Configuration Manager, 33

System requirements:, 9
System View page, 36
System--Modify page, 38
TCP/IP, 162
Telephone, 16
Telnet port, modifying address, 144
Testing setup, 32
Time and date, changing, 38
Traps. *See* Alarms
Troubleshooting, 153
TTL, 162
Twisted pair, 162
Typographical conventions, 10
Upgrading software, 141
Upstream, 163
USB, 163
  configuring IP on PC, 28
  Configuring PC, 24
  installing, 17
  installing driver, 24
  configuring IP information, 43, 47
User Password Configuration page, 39
Username
  default, 34
VC, 163
VCI, 163
VPI, 163
WAN, 163
WAN interface
  configuring multiple, 49
  IP address, 49
Web browser, 163
  requirements, 9
  version requirements, 33
Web browsers
  compatible versions, 33
Web page, 163
Web site, 163
Windows NT
  configuring IP information, 22
World Wide Web, 163

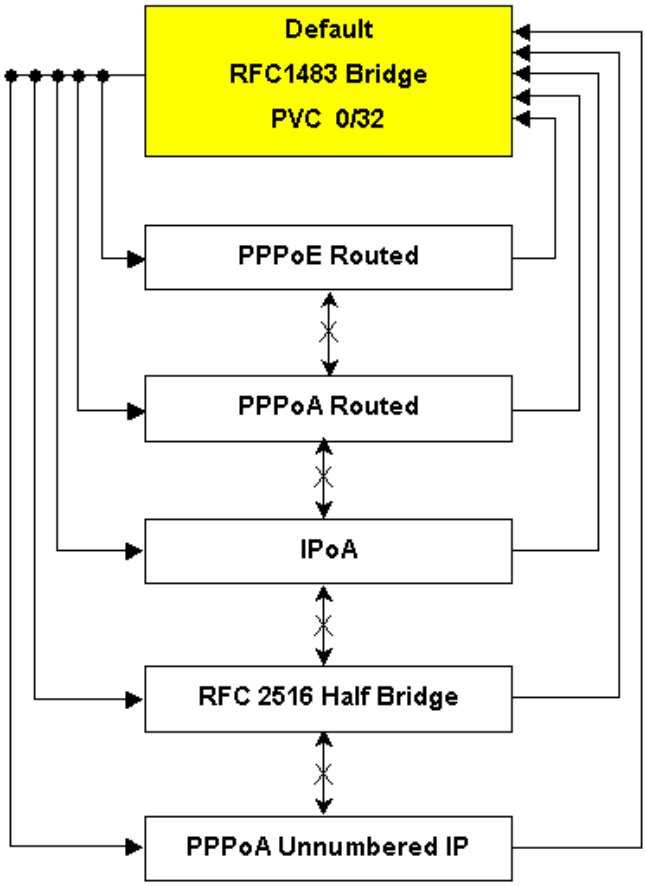
E Quick Configuration Guide

Neobit1012VA Modem basic setting is RFC1483_Bridge.

If you need to change the configuration of modem, first confirm following method to change configuration and then change to proper protocol.

The changing of configuration starts with deleting an existing RFC1483_Bridge interface. So if you want to change the configuration not in RFC1483_Bridge condition, first change to default setting (Bridge) through TELNET and then change to the configuration which you need.

Protocol Configuration Change might be different according to each ISP. Please contact ISP for further information with changing Default Configuration.



▪PPPoE routed Mode

Deleting EoA

1."Bridging" tap > "Bridging"

①Click to delete Eoa-0 in the Bridge configuration.

②Click Enable/Disable and configure the system mode below and then click Submit.

Feature	Enabled	Disabled
Bridging:	○	◉
WAN to WAN Bridging:	○	◉
BRAS:	○	◉
ZIPB:	○	◉

2."Bridging" tap > "RFC1483 Interface (EoA)"

Click to delete interface EoA-0 in the action column.

Adding PPP

"WAN" tap > "PPP"

Click Add and change "protocol→ PPPoE, status→ StartOndata, use DNS→ enable" in the PPP interface – add page. Enter the value assigned by ISP in the Login screen, and click Submit.

Running NAT

"Services" tap > "NAT"

1. Select 'Nat Rule Entry' in the NAT option box column on configuring NAT page.

① Click Add in the NAT rule configuration.

② Select "NAPT" in the rule Flavor of NAT rule add page and enter "1" as Rule ID, and then click Submit.

2. After changing disable to enable, click Submit.

Saving configuration

"Admin" tap > "Commit & Reboot"

Select "Reboot from last configuration" in the reboot mode and then click Submit.

Click reboot after page has been changed automatically.

▪PPPoA routed Mode

Deleting EoA

1."Bridging" tap > "Bridging"

① Click to delete EoA in the bridge configuration.

② Click Enable/Disable and configure system mode below, and then click Submit.

Feature	Enabled	Disabled
Bridging:	○	◉
WAN to WAN Bridging:	○	◉
BRAS:	○	◉
ZIPB:	○	◉

2."Bridging" tap > "RFC1483 Interface (EoA)"

Click to delete interface eoa-0 in the Action column.

Adding PPP

"WAN" tap > "PPP"

Click Add and then change protocol→ PPPoA, Poppas→ StartOndata, use DNS→ enable in the "PPP interface – add" page. Enter the values assigned by ISP in the Login page and then click Submit.

Changing ATM VC

"WAN" tap > "ATM VC"

From the ATM VC configuration page click in the Action column and change MUX type to VC, and then click Submit.

Running NAT

"Services" tap > "NAT"

1. Select NAT Rule Entry in the NAT option column of NAT configuration page.

① Click Add in the NAT rule configuration page.

② Select NAPT in the NAT rule add of Rule Flavor page and enter "1" as Rule ID, and then Submit.

2. After changing disable to enable in the NAT configuration, click Submit.

Committing Configuration

"Admin" tap > "Commit & Reboot"

Select Reboot from last configuration in reboot mode and then click Submit.

Click reboot after page has been changed automatically.

▪IPoA routed Mode

Deleting EoA

1."Bridging" tap > "Bridging"

① Click to delete Eoa-0 in the bridge configuration page.

② Click Enable/Disable and configure system mode below, and then click Submit.

Feature	Enabled	Disabled
Bridging:	○	◉
WAN to WAN Bridging:	○	◉
BRAS:	○	◉
ZIPB:	○	◉

2."Bridging" tap > "RFC1483 Interface (EoA)"

Click to delete interface eoa-0 in the Action column.

Adding IpoA

1. Click Add in the "WAN" tap > "IPoA."

In the IPoA interface – add page,

① Enter IP and Subnet mask assigned by ISP to Configure IP Address, Netmask box. (Modem WAN IP)

② Enter WAN gateway(BRAS IP) in the Gateway IP Address box.

2. Click Map in the Action column of IpoA-0 Interface item and then click lower interface Add in the IPoA Interface – MAP page.

Changing LAN IP

"LAN" tap > "LAN config"

Enter LAN IP, Subnet mask assigned by ISP in the LAN IP Address, LAN Network Mask box.

☞ After changing LAN configuration of modem, Connectivity between existing modem and PC would be disconnected.

Modem cannot be rebooted.

Configuring PC Network

Changes configuration to network provided by ISP. In this case, the gateway is as LAN IP in PC view.

Re-connection to modem

Open your web browser, type LAN IP in the web address box. And then connect with modem again.

Saving configuration

"Admin" tap > "Commit & Reboot"

After selecting "reboot from last configuration" in the reboot mode, click Submit.

Click reboot after page has been changed automatically.

▪RFC2516 Half Bridge(PPPOE) Mode

Deleting EoA

1."Bridging" tap > "Bridging"

① Click to delete Eoa-0 in the Bridge configuration page.

② Click Enable/Disable and configure system mode below, and then click Submit.

Feature	Enabled	Disabled
Bridging:	○	●
WAN to WAN Bridging:	●	○
BRAS:	○	●
ZIPB:	●	○

2."Bridging" tap > "RFC1483 Interface (EoA)"

Click to delete interface eoa-0 in the Action column.

Adding PPP

"WAN" tap > "PPP"

. Click Add, change protocol→ PPPoE, status→ StartOndata, use DNS→ enable in "the PPP interface – add" page. And then enter the value assigned by ISP in the Login screen and click Submit.

Changing DHCP Mode

"LAN" tap > "DHCP Mode"

After selecting DHCP Server in the DHCP Mode, click Submit.

Saving configuration

"Admin" tap > "Commit & Reboot"

Select "Reboot from last configuration" in the reboot mode and then click Submit.

Click reboot after page has been changed automatically.

▪ PPPoA (Unnumbered IP)

Deleting EoA

1."Bridging" tap > "Bridging"

① Click to delete Eoa-0 in the Bridge configuration page.

② Click Enable/Disable and configure system mode below, and then click Submit.

Feature	Enabled	Disabled
Bridging:	○	◉
WAN to WAN Bridging:	○	◉
BRAS:	○	◉
ZIPB:	○	◉

2."Bridging" tap > "RFC1483 Interface (EoA)"

Click to delete interface eoa-0 in the Action column.

Changing LAN IP

"LAN" tap > "LAN config"

Enter LAN IP, Subnet mask assigned by ISP in the LAN IP Address, LAN Network Mask box. E.g. IP-219.73.94.9/29

☞ After changing LAN configuration of modem, Connectivity between existing modem and PC would be disconnected.

Modem cannot be rebooted.

Configuring PC Network

Changes configuration to network provided by ISP.

E.g. IP-219.73.94.10 Net Mask-255.255.255.248 G/W-219.73.94.9

Re-connection to modem

Open your web browser, type LAN IP (E.g. 219.73.49.9) in the web address box. And then connect with modem again.

Adding PPP

Enter telnet *Modem IP Address (*E.g. telnet 219.73.94.9) in the run of Start of Windows. And then enter root/root in ID and Password box of Login screen.

If symbol "$" appears,

$create PPP intf ifname ppp-0 lowif aal5-0 numif eth-0 droute true

$create PPP security ifname ppp-0 pap login **ID** passwd **password**

Saving configuration

"Admin" tap> "Commit & Reboot"

Select "Reboot from last configuration" in the reboot mode and then click Submit.

Click reboot after page has been changed automatically.

Initialization

- Return to factory default configuration

1. If you use PPPoA Routed, PPPoE Routed, Half Bridge

PC Network Condition Composition

PC IP – 192.168.1.3, Subnet mask – 255.255.255.0 , G/W – 192.168.1.1

TELNET

Enter telnet 192.168.1.1 in the Run of Start. And then enter root/root in ID and Password box of Login screen.

If symbol "$" appears, **run $reboot default**

2. If you use IPoA, PPPoA (Unnumbered IP)

For default setting of modem, you should know the information about LAN configuration such as modem IP, Subnet Mask.

If you have had modem LAN IP changed, you should configure PC Network Condition to Subnet such as Modem LAN.

Running TELNET

Enter telnet 192.168.1.1 in the run of Start. And then enter root/root in ID and Password box of Login screen.

If symbol "$" appears, **run $reboot default**

exam> Modem LAN IP – 219.73.94.9 Subnet mask – 255.255.255.248

PC Network Condition

IP – 219.73.94.10 Net mask – 255.255.255.248 G/W – 219.73.94.9

Enter telnet 219.73.94.9 in the run of Start. And then enter root/root in ID and Password box of Login screen.

If symbol "$" appears, run **$reboot default**