

NETCOMM VELOCITY™ SERIES

NetComm®

Gigabit Wireless Router

NP805N



USER GUIDE

Copyright

Copyright©2011 NetComm Wireless Limited. All rights reserved.

The information contained herein is proprietary to NetComm Wireless Limited. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of NetComm Wireless Limited.



Please note: This document is subject to change without notice.

Save Our Environment

When this equipment has reached the end of its useful life, it must be taken to a recycling centre and processed separately from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this device can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with your household waste. You may be subject to penalties or sanctions under the law. Instead, ask for disposal instructions from your municipal government.

Please be responsible and protect our environment.

This manual covers the following products:

NetComm NP805N

DOCUMENT VERSION	DATE
1.0 - Initial document release	03/12/2011

Table of Contents

Overview	4
Introduction	4
Target Users.....	4
Prerequisites.....	4
Notation	4
Product Introduction	5
Product Overview	5
Package Contents.....	5
Product Features.....	5
Physical Dimensions and Indicators	6
LED Indicators.....	6
Physical Dimensions	7
NP805N Default Settings	7
Integrated Interfaces	8
Safety and Product Care	9
Transport and Handling	9
Installation and Configuration of the NP805N	10
Placement of your NP805N.....	10
Hardware installation.....	11
Connecting via a cable.....	11
Connecting wirelessly	11
Web Based Configuration Interface	12
First-time Setup Wizard.....	12
Advanced Configuration.....	18
Status	19
Network Setup	20
Forwarding Rules.....	30
Security Settings.....	32
Advanced Settings.....	39
NAS Settings.....	50
Toolbox.....	55
Additional Product Information	57
Establishing a wireless connection.....	57
Troubleshooting.....	58
Technical Data	59
Electrical Specifications.....	59
Environmental Specifications / Tolerances	59
Legal & Regulatory Information	60
Contact	62

Overview

Introduction

This manual provides information related to the installation, operation, and utilisation of the NP805N.

Target Users

The individual reading this manual is presumed to have a basic understanding of telecommunications terminology and concepts.

Prerequisites

Before continuing with the installation of your NP805N, please confirm that you comply with the minimum system requirements below.

- An activated ADSL, activated 3G, or configured WAN connection.
- Computer with Windows, Macintosh, or Linux-based operating systems with a working Ethernet adapter with TCP/IP Protocol installed.
- A Web Browser such as Internet Explorer, Netscape Navigator, Mozilla Firefox, Opera, Safari etc.
- Wireless Computer System Requirements:
 - Computer with a working 802.11b, 802.11g or 802.11n wireless adapter.

Notation

The following symbols are utilised in this user manual:



-

The following note requires attention



-

The following note provides a warning



-

The following note provides relevant information

Product Introduction

Product Overview

- Supports Wireless N standard with data speeds up to 300Mbps
- One WAN port for alternate wired Internet connection (DSL/Cable/Satellite via Ethernet)
- Four LAN ports to connect wired devices like PCs or gaming consoles
- Easy Wi-Fi Protected Setup (WPS) by the single touch of a button to establish a secure wireless connection
- Full Wireless security - WEP, WPA, WPA2
- Browser based interface for configuration and management: OS independent and easy to use
- File server (FTP / NAS)
- Download assistant
- Web HDD function

Speeds are dependent on network coverage. See your 3G provider coverage maps for more details. The total number of Wi-Fi users can also affect data speeds. Maximum wireless signal rate and coverage values are derived from IEEE Standard 802.11g and 802.11n specifications. Actual wireless speed and coverage are dependent on network and environmental conditions included but not limited to volume of network traffic, building materials and construction/layout.

Package Contents

The NP805N package consists of:

- Gigabit Wireless Router - NP805N
- Quick Start Guide
- Power Supply Unit
- Ethernet Cable (RJ-45)
- Wireless Security Card
- Warranty Card

If any of these items are missing or damaged, please contact NetComm Support immediately by visiting the NetComm Support website at: <http://www.netcomm.com.au/contact-us/technical-support>

Product Features

The NetComm NP805N integrates a Wireless LAN and gigabit WAN into one unit. Connection to the Internet is achieved through a connection to the NP805N's WAN port.

Users are able to share a single Internet connection via both a wired and wireless connection to the NP805N. With a built in and external antenna providing a 2 transmit, 2 receive (2T2R) 802.11n wireless access point, this router provides wireless speeds of up to 300Mbps.

On top of this, the NP805N has four LAN ports for wired connections to multiple devices. The NP805N allows the user to simply connect an Ethernet based WAN device for Internet connectivity.

The NP805N also includes advanced security features such as VPN pass-through, a full complement of wireless security options and a built in firewall.

Physical Dimensions and Indicators

LED Indicators

The NP805N has been designed to be placed on a desktop. All of the cables exit from the rear for better organization. The display is visible on the front of the NP805N to provide you with information about network activity and the device status. See below for an explanation of each of the indicator lights.



LED INDICATOR	ICON	COLOUR	ACTIVITY	DEFINITION
WIFI		Green	Off	The WiFi function is disabled.
			On	The WiFi function is enabled.
			Flashing	The NP805N is waiting for a WPS PBC connection.
USB		Green	Off	No USB device is connected.
			On	A USB device has been connected.
			Flashing	The USB device is being accessed by a connected client.
POWER		Green	Off	The NP805N is powered off.
			On	The NP805N is powered on and operating normally.
			Flashing	The NP805N is starting up.
WWW		Green	Off	No Internet configuration present.
			On	The NP805N is connected via an Ethernet WAN based service.
			Flashing	Data is being sent or received via the Ethernet WAN port.
LAN 1 - 4		Green	Off	No device is connected to the Ethernet LAN port.
			On	A device is connected to the Ethernet LAN port.
			Flashing	Data is being sent or received via the Ethernet LAN port.

Physical Dimensions

The following page lists the physical dimensions of the NP805N.



NP805N	
Length	215 mm
Width	145 mm
Height	37 mm
Weight	403 grams

NP805N Default Settings

The following tables list the default settings for the NP805N.

LAN (MANAGEMENT)	
Static IP Address:	192.168.20.1
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.20.1

WIRELESS (WI-FI)	
SSID:	(Refer to the included Wireless Security Card)
Security:	WPA-SPK/WPA2-PSK (mixed mode)
Security Key:	(Refer to the included Wireless Security Card)

NP805N WEB INTERFACE ACCESS	
Username:	admin
Password:	admin

Integrated Interfaces

The following integrated interfaces are available on the NP805N:



REAR PANEL	
INTERFACE	FUNCTION
WIFI Antenna	Connect one of the supplied WIFI antennas here; It should be screwed on in a clockwise direction.
LAN 1-4	Connect Ethernet based devices here
WAN	Connect an Ethernet based WAN device here
Power Jack	Connect the power supply here
Power button	Power the NP805N on or off
WIFI Antenna	Connect one of the supplied WIFI antennas here; It should be screwed on in a clockwise direction.



FRONT PANEL	
INTERFACE	FUNCTION
USB	Connect a USB storage based device here to provide access to connected clients.
RESET	Press and hold the reset button for 5 seconds to restore the NP805N to Factory Defaults.
WPS / USB OFF	<ul style="list-style-type: none"> - Press for WPS mode - Hold for 5 seconds to disable the USB functionality.

Safety and Product Care

With reference to unpacking, installation, use and maintenance of your electronic device, the following basic guidelines are recommended:

- Do not use or install this product near water to avoid fire or shock hazard. For example, near a bathtub, kitchen sink, laundry tub, or near a swimming pool. Also, do not expose the equipment to rain or damp areas (e.g. a wet basement).
- Do not connect the power supply cord on elevated surfaces. Allow it to lie freely. There should be no obstructions in its path and no heavy items should be placed on the cord. In addition, do not walk on, step on or mistreat the cord.
- To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are unobstructed.



WARNING

Disconnect the power line from the device before servicing.

Transport and Handling

When transporting the NP805N, it is recommended to return the product in the original packaging. This ensures the product will not be damaged.



In the event the product needs to be returned, ensure it is securely packaged with appropriate padding to prevent damage during courier transport.

Installation and Configuration of the NP805N

Placement of your NP805N

The wireless connection between your NP805N and your Wi-Fi devices will be stronger the closer your connected devices are to your NP805N. Your wireless connection and performance will degrade as the distance between your NP805N and connected devices increases. This may or may not be directly noticeable, and is greatly affected by the individual installation environment.

If you have concerns about your network's performance that might be related to range or obstruction factors, try moving the computer to a position between three to five meters from the NP805N in order to see if distance is the problem.



Please note: While some of the items listed below can affect network performance, they will not prohibit your wireless network from functioning; if you are concerned that your network is not operating at its maximum effectiveness, this checklist may help.

If you experience difficulties connecting wirelessly between your Wi-Fi Devices and your NP805N, please try the following steps:

- In multi-storey homes, place the NP805N on a floor that is as close to the centre of the home as possible. This may mean placing the NP805N on an upper floor.
- Try not to place the NP805N near a cordless telephone that operates at the same radio frequency as the NP805N (2.4GHz).

Avoid obstacles and interference

Avoid placing your NP805N near devices that may emit radio “noise,” such as microwave ovens. Dense objects that can inhibit wireless communication include:

- Refrigerators
- Washers and/or dryers
- Metal cabinets
- Large aquariums
- Metallic-based, UV-tinted windows
- If your wireless signal seems weak in some spots, make sure that objects such as those listed above are not blocking the signal's path (between your devices and the NP805N).

Cordless Phones

If the performance of your wireless network is impaired after considering the above issues, and you have a cordless phone:

- Try moving cordless phones away from your NP805N and your wireless-enabled computers.
- Unplug and remove the battery from any cordless phone that operates on the 2.4GHz band (check manufacturer's information). If this fixes the problem, your phone may be interfering with the NP805N.
- If your phone supports channel selection, change the channel on the phone to the farthest channel from your wireless network. For example, change the phone to channel 1 and move your NP805N to channel 11. See your phone's user manual for detailed instructions.
- If necessary, consider switching to a 900MHz or 5GHz cordless phone.

Choose the “Quietest” Channel for your Wireless Network

In locations where homes or offices are close together, such as apartment buildings or office complexes, there may be wireless networks nearby that can conflict with your wireless network. Use the Site Survey capabilities found in the Wireless Utility of your wireless adapter to locate any other wireless networks that are available (see your wireless adapter's user manual), and switch your Router and computers to a channel as far away from other networks as possible.

Experiment with more than one of the available channels, in order to find the clearest connection and avoid interference from neighbouring cordless phones or other wireless devices.

Hardware installation

1. Connect the power adapter to the Power socket on the back of the NP805N. Plug the power adapter into the wall socket and switch on the power.
2. Wait approximately 60 seconds for the NP805N to power up.

Connecting via a cable

1. Connect the yellow Ethernet cable provided to one of the ports marked 'LAN' at the back of the NP805N.
2. Connect the other end of the yellow Ethernet cable to your computer.
3. Wait approximately 30 seconds for the connection to establish.
4. Open your Web browser, and enter <http://192.168.20.1> into the address bar and press enter.
5. Follow the steps to set up your NP805N.

Connecting wirelessly

1. Ensure Wi-Fi is enabled on your device (computer/laptop/Smartphone).
2. Scan for wireless networks in your area and connect to the network name that matches the Wireless network name configured on the NP805N.



Please note: Refer to the included Wireless Security Card for the default SSID of your NP805N

3. When prompted for your wireless security settings, enter the Wireless security key configured on the NP805N.



Please note: Refer to the included Wireless Security Card for the default wireless security key of your NP805N

4. Wait approximately 30 seconds for the connection to establish.
5. Open your Web browser, and enter <http://192.168.20.1> into the address bar and press enter.
6. Follow the steps to set up your NP805N.

Web Based Configuration Interface

First-time Setup Wizard

Please follow the steps below to configure your NP805N Wireless router via the web based configuration wizard.

Open your web browser (e.g. Internet Explorer/Firefox/Safari) and type <http://192.168.20.1/> into the address bar at the top of the window.

At the login screen, type "admin" (without quotes) in the username and password field. Then click on Login.



Please note: admin is the default username and password for the unit.

1. Click on “Yes, let’s get started with the wizard”.



This page enables you to enter the information needed to setup your Internet connection.



2. From the WAN type pull down menu, select the type of Internet connection you would like to utilise. You can select from:
 - Dynamic IP Address
 - Static IP Address
 - PPP over Ethernet
 - PPTP
 - L2TP

Dynamic IP Address



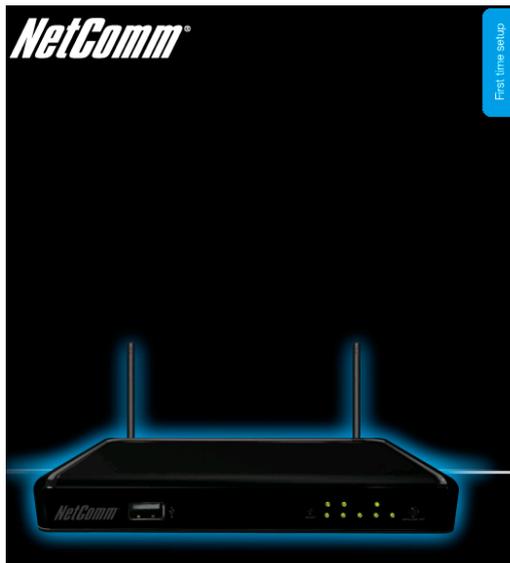
1. Enter the Host Name (if required).
2. Enter the ISP registered MAC Address (if required).
3. Click "Next".

Static IP Address



1. Enter the Static IP Address for your connection.
2. Enter the Subnet Mask for your connection.
3. Enter the Static Gateway for your connection.
4. Enter the Static Primary DNS for your connection.
5. Enter the Static Secondary DNS for your connection (if available).
6. Click "Next".

PPP over Ethernet



NetComm

First time setup

Step 1 of 5

Select your internet connection type:

WAN type:

Username

Password

1. Enter the Username required for your PPPoE connection.
2. Enter the Password required for your PPPoE connection.
3. Click "Next".

PPTP



NetComm

First time setup

Step 1 of 5

Select your internet connection type:

WAN type:

IP Mode:

Server IP Address/Name

PPTP Account

PPTP Password

1. Select to use either a static or dynamically assigned IP address for your connection. When selecting to utilise a static IP address, you will also need to enter the PPTP IP Address, PPTP Subnet Mask and PPTP Default gateway in use for the connection (*Refer to your PPTP administrator for more information*).
2. Enter the Username required for your PPTP connection.
3. Enter the Password required for your PPTP connection.
4. Click "Next".

L2TP

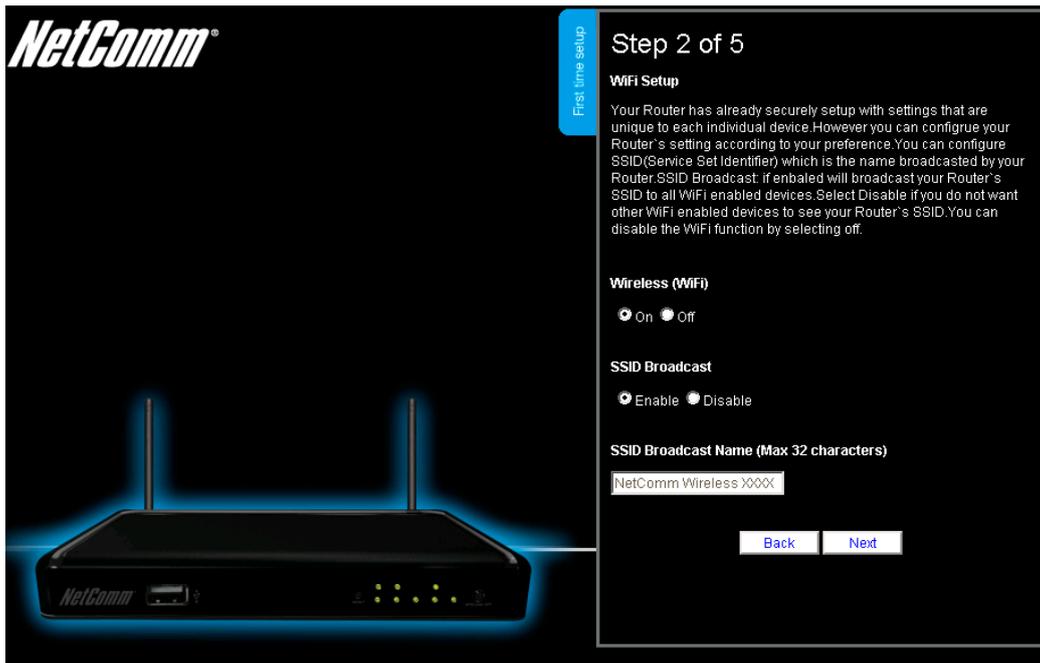


The image shows a black NetComm NP805N Gigabit Wireless Router with two antennas and a blue glow. To its right is a screenshot of the router's web interface during the 'First time setup' process, specifically 'Step 1 of 5'. The interface is dark-themed and contains the following fields:

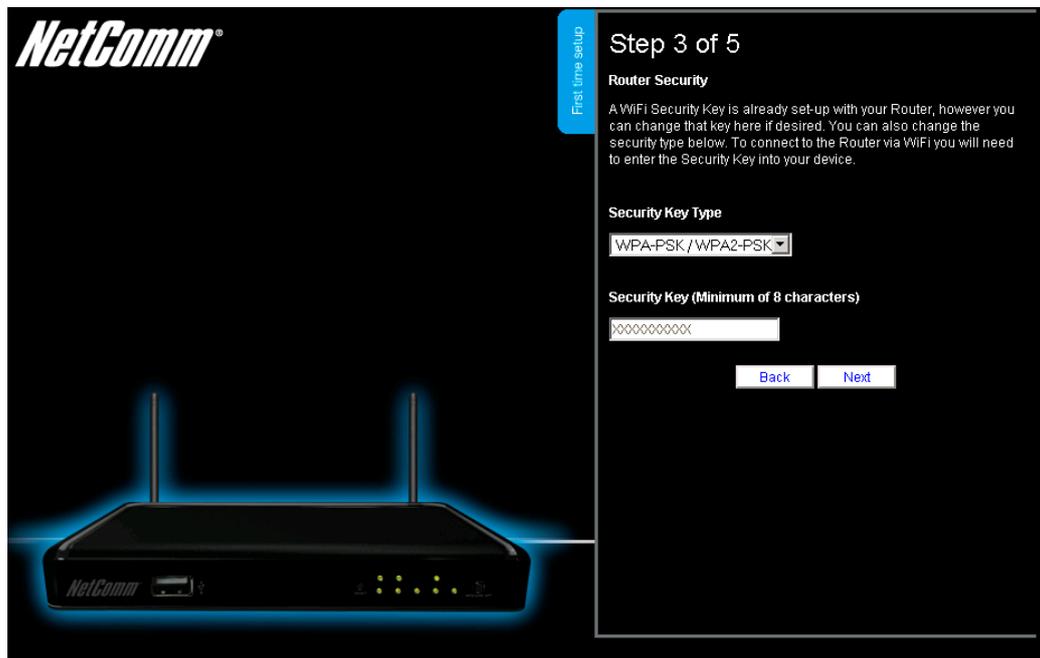
- WAN type:** A dropdown menu with 'L2TP' selected.
- IP Mode:** A dropdown menu with 'Dynamic IP Address' selected.
- Server IP Address/Name:** A text input field.
- L2TP Account:** A text input field.
- L2TP Password:** A text input field.

At the bottom of the form is a blue 'Next' button. A vertical blue bar on the left side of the form contains the text 'First time setup'.

1. Select to use either a static or dynamically assigned IP address for your connection. When selecting to utilise a static IP address, you will also need to enter the L2TP IP Address, L2TP Subnet Mask and L2TP Default gateway in use for the connection (*Refer to your L2TP administrator for more information*).
2. Enter the Username required for your L2TP connection.
3. Enter the Password required for your L2TP connection.
4. Click "Next".



3. If you want to change the Wireless network settings, you can do so on this page. You can enable or disable the Wireless network, select whether to broadcast your SSID or not and change the Wireless network name. Change the settings as needed and click “Next”.
(If you wish to use the default settings, click “Next”)



4. If you want to change the Wireless network security settings, you can do so on this page. You can change the type of Wireless network security in use or the Wireless Security key. Change the settings as needed and click “Next”.
(If you wish to use the default settings, click “Next”)



5. If you want to change the system username or password, enter the new username to use or the current system password into the "Old Password" field and then enter the new password into both the "Desired Password" and "Retype Password" fields and then click "Next".

(If you do not wish to change the password, leave the fields blank and click "Next")



6. Confirm the setup information and click "Finish" if everything is correct. You can also click "Back" to go back and change any of the previously configured settings.

Your device is restarting.

Remaining time: 65 seconds

7. The router will then apply your configured settings and restart.

System is ready

8. Once completed, your router is configured and should be connected to the Internet.

Advanced Configuration

To access the advanced configuration options of your NP805N, you need to login to the web configuration and change to Advanced view.

To do this, open your web browser (e.g. Internet Explorer/Firefox/Safari), type <http://192.168.20.1/> into the address bar at the top of the window and press the enter key.



At the login screen, type "admin" (without quotes) in the Username and Password field. Then click on Login.



Please note: admin is the default username and password for the unit.



Click on any of the top menu items to access the respective function configuration pages.

Status

[Status](#)
[Network Setup](#)
[Forwarding Rules](#)
[Security Settings](#)
[Advanced Settings](#)
[PNAS SETTINGS](#)
[Toolbox](#)

IPv4 System Status		
Item	WAN Status	Sidenote
Remaining Lease Time	-	Renew
IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Gateway	0.0.0.0	
Domain Name Server	0.0.0.0, 0.0.0.0	

IPv6 System Status		
Item	WAN Status	Sidenote
WAN Link-Local Address		Dynamic IPv6
Global IPv6 Address	/64	
LAN IPv6 Link-Local Address		
Link Status		Connect

Wireless Status		
Item	WLAN Status	Sidenote
Wireless mode	Enable	(B/G/N Mixed)
SSID	NetComm Wireless 8529	
Channel	Auto	
Security	WPA-PSK / WPA2-PSK	(TKIP/AES)

Statistics Information		
Statistics of WAN	Inbound	Outbound
Octets	0	720
Unicast packets	0	8
Multicast packets	0	0

[View Log...](#)
[Clients List...](#)
[NAT Status...](#)
[Refresh](#)

Device Time: Fri, 02 Jan 2009 21:53:27 +1100

ITEM	DESCRIPTION
IP Address	The current WAN IP address of the router
Subnet Mask	The current subnet mask in use by the router
Gateway	The gateway in use by the router to access the internet
Domain Name Server	The Domain name server converts
Connection Time	The time the current connection to the internet has been active
WAN Link-Local Address	The current WAN IPv6 address
Global IPv6 Address	The current IPv6 subnet mask in use
LAN IPv6 Link-Local Address	The current LAN IPv6 address of the NP805N
Link Status	The current IPv6 WAN connection status
Wireless mode	The current status of the wireless network (enabled or disabled)
SSID	The current wireless network name is use by the router
Channel	The current wireless channel in use on your wireless network
Security	The currently selected wireless security in use on your wireless network
Octets	The number of data packets which have passed into and out of the router
Unicast Packets	The number of unicast packets which have passed into and out of the router
Multicast packets	The number of multicast packets which have passed into and out of the router.

Network Setup

Network Setup

This page allows you to change the LAN (Local Area Network) and WAN (Wide Area Network) connection settings as well as the automatic failover function on the NP805N.



Item	Setting
LAN IP Address	192.168.1.1
Subnet Mask	255.255.255.0

OPTION	DEFINITION
LAN IP Address	The local IP address of the NP805N. <i>(The computers on your network must use this IP address as their Default Gateway. You can change it if necessary.)</i>
Subnet Mask	Enter the subnet mask for use on the local network. This would usually be set to 255.255.255.0.

WAN Interface Types

Ethernet WAN (xDSL/Cable/Satellite)

WAN Type: You can select from the following WAN types:-

- Dynamic IP
- Static IP
- PPP over Ethernet
- PPTP
- L2TP

Dynamic IP



Item	Setting
LAN IP Address	192.168.20.1
Subnet Mask	255.255.255.0
WAN Interface	Ethernet WAN
WAN Type	Dynamic IP Address
Host Name	<input type="text"/> (optional)
ISP registered MAC Address	<input type="text"/> <input type="button" value="Clone"/>
NAT	<input checked="" type="checkbox"/> Enable
Multicast	Auto
IGMP Snooping	<input type="checkbox"/> Enable
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

OPTION	DEFINITION
Host Name	Set the hostname for your connection <i>(Optional - Refer to your ISP for more information).</i>
ISP Registered MAC Address	You can change the WAN port MAC address if needed to clone your 3G modem <i>(Optional - Refer to your ISP for more information).</i>
NAT	This option enables or disables "Network Address Translation" for this connection type.
Multicast	Enable multicast support for this connection. Select the appropriate IGMP protocol version from the pull down menu.
IGMP Snooping	This option enables or disables "IGMP" for this connection type.

Static IP

Item	Setting
LAN IP Address	<input type="text" value="192.168.20.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
WAN Interface	<input type="text" value="Ethernet WAN"/>
WAN Type	<input type="text" value="Static IP Address"/>
WAN IP Address	<input type="text"/>
WAN Subnet Mask	<input type="text"/>
WAN Gateway	<input type="text"/>
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
NAT	<input checked="" type="checkbox"/> Enable
Multicast	<input type="text" value="Auto"/>
IGMP Snooping	<input type="checkbox"/> Enable

OPTION	DEFINITION
WAN IP Address	Enter the WAN IP address used for your connection.
WAN Subnet Mask	Enter the WAN Subnet mask used for your connection.
WAN Gateway	Enter the WAN Gateway address used for your connection.
Primary DNS	Enter the Primary DNS used for your connection.
Secondary DNS	Enter the Secondary DNS (if available) used for your connection.
NAT	This option enables or disables "Network Address Translation" for this connection type.
Multicast	Enable multicast support for this connection. Select the appropriate IGMP protocol version from the pull down menu.
IGMP Snooping	This option enables or disables "IGMP" for this connection type.

PPP over Ethernet

Status ▶ Network Setup ▶ Forwarding Rules ▶ Security Settings ▶ Advanced Settings ▶ NAS SETTINGS ▶ Toolbox

Item	Setting
LAN IP Address	<input type="text" value="192.168.20.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
WAN Interface	<input type="text" value="Ethernet WAN"/>
WAN Type	<input type="text" value="PPP over Ethernet"/>
IPv6 Dualstack	<input checked="" type="checkbox"/> Enable
Username	<input type="text"/>
Password	<input type="text"/>
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
Service Name	<input type="text"/> (optional)
Assigned IP Address	<input type="text"/> (optional)
MTU	<input type="text" value="0"/> (0 is auto)
NAT	<input checked="" type="checkbox"/> Enable
Multicast	<input type="text" value="Auto"/>
IGMP Snooping	<input type="checkbox"/> Enable

OPTION	DEFINITION
IPv6 Dualstack	Select to enable or disable the IPv6 Dualstack function for this connection type.
Username	The account name given to you by your ISP.
Password	The password given to you by your ISP.
Primary DNS	This feature allows you to manually assign a Primary DNS Server <i>(Optional - Refer to your ISP for more information).</i>
Secondary DNS	This feature allows you to manually assign a Secondary DNS Server <i>(Optional - Refer to your ISP for more information).</i>
Service Name	Enter the service name if your ISP requires it <i>(Optional - Refer to your ISP for more information).</i>
Assigned IP Address	Enter the IP address assigned to your service. This is usually left blank.
MTU	The default MTU value is 0 (auto). It is set automatically when you connect.
NAT	This option enables or disables "Network Address Translation" for this connection type
Multicast	Enable multicast support for this connection. Select the appropriate IGMP protocol version from the pull down menu.
IGMP Snooping	This option enables or disables "IGMP" for this connection type.

PPTP

Item	Setting
LAN IP Address	<input type="text" value="192.168.20.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
WAN Interface	<input type="text" value="Ethernet WAN"/>
WAN Type	<input type="text" value="PPTP"/>
IP Mode	<input type="text" value="Dynamic IP Address"/>
Server IP Address/Name	<input type="text"/>
PPTP Account	<input type="text"/>
PPTP Password	<input type="text"/>
Connection ID	<input type="text"/> (optional)
Connection Control	<input type="text" value="Auto Reconnect (always-on)"/>
MTU	<input type="text" value="0"/> (0 is auto)
MPPE	<input type="checkbox"/>
Multicast	<input type="text" value="Auto"/>
IGMP Snooping	<input type="checkbox"/> Enable

OPTION	DEFINITION
IP Mode	Select to use either a static or dynamically assigned IP address for your connection. When selecting to utilise a static IP address, you will also need to enter the PPTP IP Address, PPTP Subnet Mask and PPTP Default gateway in use for the connection <i>(Refer to your PPTP administrator for more information).</i>
Server IP Address/Name	Enter the PPTP server name or IP Address.
PPTP Account	Enter the PPTP username supplied by your PPTP administrator.
PPTP Password	Enter the PPTP password supplied by your PPTP administrator.
Connection ID	Enter an Optional name to identify the PPTP connection.
Maximum Idle Time	The amount of inactivity on the internet connection before it is disconnected. Set it to zero or enable "Auto-reconnect" to disable this feature.
Connection Control	There are 3 modes to select from: <ul style="list-style-type: none"> ▪ Connect-on-demand: The NP805N will connect to the internet when a client sends outgoing packets. ▪ Auto Reconnect (Always-on): The NP805N will automatically reconnect to the internet until the connection is manually disconnected. ▪ Manually: The NP805N will not connect to the internet until someone clicks the connect button in the Status-page.
MTU	The default MTU value is 0 (auto). It is set automatically when you connect.
MPPE	Select to enable or disable the MPPE security extensions for the PPTP connection.
Multicast	Enable multicast support for this connection. Select the appropriate IGMP protocol version from the pull down menu.
IGMP Snooping	This option enables or disables "IGMP" for this connection type.

L2TP



Item	Setting
LAN IP Address	<input type="text" value="192.168.20.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
WAN Interface	<input type="text" value="EthernetWAN"/>
WAN Type	<input type="text" value="L2TP"/>
IP Mode	<input type="text" value="Dynamic IP Address"/>
Server IP Address/Name	<input type="text"/>
L2TP Account	<input type="text"/>
L2TP Password	<input type="text"/>
Maximum Idle Time	<input type="text" value="600"/> seconds
Connection Control	<input type="text" value="Connect-on-Demand"/>
MTU	<input type="text" value="0"/> (0 is auto)
MPPE	<input type="checkbox"/>
Multicast	<input type="text" value="Auto"/>
IGMP Snooping	<input type="checkbox"/> Enable

OPTION	DEFINITION
IP Mode	Select to use either a static or dynamically assigned IP address for your connection. When selecting to utilise a static IP address, you will also need to enter the L2TP IP Address, L2TP Subnet Mask and L2TP Default gateway in use for the connection <i>(Refer to your L2TP administrator for more information).</i>
Server IP Address/Name	Enter the L2TP server name or IP Address.
L2TP Account	Enter the L2TP username supplied by your L2TP administrator.
L2TP Password	Enter the L2TP password supplied by your L2TP administrator.
Connection ID	Enter an Optional name to identify the L2TP connection.
Maximum Idle Time	The amount of inactivity on the internet connection before it is disconnected. Set it to zero or enable "Auto-reconnect" to disable this feature.
Connection Control	There are 3 modes to select from: <ul style="list-style-type: none"> ▪ Connect-on-demand: The NP805N will connect to the internet when a client sends outgoing packets. ▪ Auto Reconnect (Always-on): The NP805N will automatically reconnect to the internet until the connection is manually disconnected. ▪ Manually: The NP805N will not connect to the internet until someone clicks the connect button in the Status-page.
MTU	The default MTU value is 0 (auto). It is set automatically when you connect.
MPPE	Select to enable or disable the MPPE security extensions for the L2TP connection.
Multicast	Enable multicast support for this connection. Select the appropriate IGMP protocol version from the pull down menu.
IGMP Snooping	This option enables or disables "IGMP" for this connection type.

DHCP Server

This Page allows you to change the Dynamic Host Configuration Protocol (DHCP) server settings on the NP805N. The DHCP Server enables computers or devices connecting to the NP805N to automatically obtain their network configuration settings. By default, the DHCP server is enabled.

[Status](#)
[▶ Network Setup](#)
[▶ Forwarding Rules](#)
[▶ Security Settings](#)
[▶ Advanced Settings](#)
[▶ NAS SETTINGS](#)
[▶ Toolbox](#)

Item	Setting
DHCP Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
IP Pool Starting Address	<input type="text" value="100"/>
IP Pool Ending Address	<input type="text" value="200"/>
Lease Time	<input type="text" value="86400"/> Seconds
Domain Name	<input type="text"/>

OPTION	DEFINITION
DHCP Server	Enable or disable the DHCP server.
IP Pool Starting/Ending Address	Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting / ending address of the IP address pool
Lease Time	Length of the DHCP lease time
Domain Name	Optional, this information will be passed to the client

Click "Save" to save these settings or "Undo" to cancel.

You can also check the DHCP client list by clicking the "Client List" button.

 Please note: See the section "DHCP Client List" below for more information

The "Fixed Mapping..." button allows you to map a specific IP address to a specific MAC address.

 Please note: See the section "DHCP Fixed Mapping" below for more information

Click the "More..." button for the following extended options:

Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
Primary WINS	<input type="text"/>
Secondary WINS	<input type="text"/>
Gateway	<input type="text"/> (optional)

OPTION	DEFINITION
Primary DNS	Optional, this information will be passed to the client
Secondary DNS	Optional, this information will be passed to the client
Primary WINS	Optional, this information will be passed to the client
Secondary WINS	Optional, this information will be passed to the client
Gateway	Optional, this information will be passed to the client

DHCP Client List

This is the list of currently connected devices utilising DHCP.

Status ▶ Network Setup ▶ Forwarding Rules ▶ Security Settings ▶ Advanced Settings ▶ NAS SETTINGS ▶ Toolbox					
IP Address	Host Name	MAC Address	Type	Lease Time	Select
Delete Back Refresh Fixed Mapping					

If you wish to set a permanent IP address for a particular DHCP client (or device), select the appropriate DHCP client by clicking in the "Select" box. This will ensure the clients current IP address is always assigned to it.

DHCP Fixed Mapping

DHCP Fixed Mapping allows you to reserve a specific IP address for a specific device.

Status ▶ Network Setup ▶ Forwarding Rules ▶ Security Settings ▶ Advanced Settings ▶ NAS SETTINGS ▶ Toolbox			
DHCP clients — select one — Copy to ID —			
ID	MAC Address	IP Address	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
<< Previous Next >> Save Undo Back			

The DHCP Server will reserve a specific IP for a device based on that devices unique MAC address.

You can enter a new Fixed Mapping by entering the MAC address of the device and the IP address you wish to allocate to it.

Click on the "Enable" checkbox to activate the DHCP fixed mapping entry.

Wireless

The Wireless LAN settings page allows you to configure the wireless network features of the router.

Status
▶ Network Setup
▶ Forwarding Rules
▶ Security Settings
▶ Advanced Settings
▶ NAS SETTINGS
▶ Toolbox

Item	Setting
Wireless Module	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Network ID (SSID)	<input type="text" value="NetComm Wireless XXXX"/>
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	<input type="text" value="Auto"/>
Wireless Mode	<input type="text" value="B/G/N mixed"/>
Authentication	<input type="text" value="WPA-PSK / WPA2-PSK"/>
Encryption	<input type="text" value="TKIP"/>
Preshare Key	<input type="text" value="XXXXXXXXXX"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="WDS Setting..."/> <input type="button" value="WPS Setup..."/> <input type="button" value="Wireless Client List..."/>	

OPTION	DEFINITION
Wireless Module	Select to enable or disable the Wireless network function of the NP805N.
Network ID (SSID)	Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this product and other Access Points that have the same Network ID. <i>(Please refer to the included Wireless Security Card insert for your default SSID)</i>
SSID Broadcast	The router will broadcast the SSID so that wireless clients can find the wireless network.
Channel	The wireless radio channel in use by your network.
Wireless Mode	Choose B/G Mixed, B only, G only, and N only, G/N Mixed or B/G/N mixed. <i>(The factory default setting is B/G/N mixed)</i>
Authentication	<p>You may select from the following authentication types to secure your wireless network:</p> <ul style="list-style-type: none"> ▪ Open ▪ Shared ▪ Auto ▪ WPA ▪ WPA-PSK ▪ WPA2 ▪ WPA2-PSK ▪ WPA/WPA2 ▪ WPA-PSK/WPA2-PSK. <p>WPA-PSK/WPA2-PSK is a newer type of security. This type of security gives a more secure network compared to WEP. Use TKIP Encryption Type for WPA-PSK and AES for WPA2-PSK.</p> <p>Please enter the key in the "Preshare Key". The key needs to be more than 8 characters and less than 63 characters. It can be any combination of letters and numbers.</p> <p><i>(Please refer to the included Wireless Security Card insert for your default WPA-PSK2 key)</i></p>



Please Note: The configuration for WPA-PSK and WPA2-PSK is identical

After configuring wireless security, you also need to configure your wireless adapter to use the same security settings before you can connect wirelessly. Not all wireless adapters support WPA-PSK/WPA2-PSK/WPA/WPA2 security. Please refer to your wireless adapter user guide for more information.

It is strongly recommended to set up wireless security such as WPA-PSK (when the wireless client supports WPA) in order to secure your network.

Click "Save" to save these settings or click "Undo" to cancel.

WDS (Wireless Bridging)

Status Network Setup Forwarding Rules Security Settings Advanced Settings **NAS SETTINGS** Toolbox

Item	Setting
Wireless Bridging	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Remote AP MAC 1	<input type="text"/>
Remote AP MAC 2	<input type="text"/>
Remote AP MAC 3	<input type="text"/>
Remote AP MAC 4	<input type="text"/>
Encryption type	TKIP
Encryption key	<input type="text"/>

Save Undo Back

Wireless Distribution System (WDS) allows you to connect to other wireless access points (Remote APs), and in doing so extend a wired infrastructure to locations where cabling is not possible or inefficient to implement.

Enter the MAC address of the other wireless access points taking part in the WDS network and then click “Save”.

WPS Setup

Status Network Setup Forwarding Rules Security Settings Advanced Settings **NAS SETTINGS** Toolbox

Item	Setting
WPS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP PIN	Generate New PIN
Config Mode	Registrar
Config Status	CONFIGURED Release
Config Method	Push Button
WPS status	NOT USED

Save Trigger Cancel

Wi-Fi Protected Setup (WPS) offers safe and easy way to connect wirelessly.

Simply push the WPS button on the router and then press the WPS on your wireless device within 2 minutes and the WLAN connection should be completed automatically.

OPTION	DEFINITION
AP PIN	The current PIN used to connect. ▪ Click “Generate New PIN” to force the router to create a new PIN.
Config Mode	Set the router to be either the Registrar or Enrollee.
Config Status	You can discard the current WPS configuration by clicking “Release”.
Config Method	Set the WPS configuration method to either Push Button or PIN code.

 Please note: These settings should not need to be changed.

Wireless Client List

Status Network Setup Forwarding Rules Security Settings Advanced Settings **NAS SETTINGS** Toolbox

ID	MAC Address
Back Refresh	

The list of currently connected wireless devices is shown here.

Change Password

This page allows you to change the NP805N web configuration password.

Item	Setting
Username	<input type="text" value="admin"/> (*Change this if you need to change Username.)
Old Password	<input type="password"/>
New Password	<input type="password"/>
Reconfirm	<input type="password"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

Please type in the old password (*the factory default username and password is admin*) and then type in the new password. Type the same new password in the “Reconfirm field” and click “Save”.

Forwarding Rules

The Forwarding Rules page allows you to configure the port forwarding management on the router. Click on any of the menu items on the left to access the respective settings page.

Forwarding rules are a necessary feature as by default NAT (Network Address Translation) will automatically block incoming traffic from the Internet to the LAN unless a specific port mapping exists in the NAT translation table. Because of this, NAT provides a level of protection for computers that are connected to your LAN.

However this also creates a connectivity problem when you want to make LAN resources available to Internet clients. For example, to play network games or host network applications.

There are three ways to work around NAT and to enable certain LAN resources available from the Internet:

- **Port Forwarding** (available in the Virtual Server page)
- **Port Triggering** (available in the Special AP page)
- **DMZ Host** (available in the Miscellaneous page)

Virtual Server

A virtual server is defined as a Service Port, and all requests to this port will be redirected to the computer specified by the Server IP.

Virtual Servers can also work with Scheduling Rules, and give you more flexibility on Access control.



Please note: For further instructions on scheduling rules, please refer to the “Scheduling” section later in this guide

Well known services --select one-- Copy to ID -

ID	Service Ports	Server IP	Enable	Use Rule#
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always ▾
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always ▾
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always ▾
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always ▾
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always ▾
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always ▾
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always ▾
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always ▾
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always ▾
10	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always ▾
11	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always ▾
12	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always ▾
13	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always ▾
14	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always ▾
15	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always ▾
16	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always ▾
17	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always ▾
18	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always ▾
19	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always ▾
20	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always ▾

Save Undo

For example, if you have an FTP server (the default port is 21) at 192.168.20.10, a Web server (the default port is 80) at 192.168.20.40, and a VPN server (the default port is 1723) at 192.168.20.60, then you would need to specify the following virtual server mappings:



Please note: At any given time, only one IP address can bind to a particular Service Port.

SERVICE PORT	SERVER IP	ENABLE	USE RULE#
21	12.168.1.10	✓	(0) Always
80	192.168.20.40	✓	(0) Always
1723	192.168.20.60	✓	(0) Always

Click "Save" to save the settings or "Undo" to cancel.

Special AP

Some applications like On-line games, Video conferencing and Internet telephony require multiple connections to the internet. As such, these applications cannot work with a pure NAT router such as the NP805N.

ID	Trigger	Incoming Ports	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

The Special Applications feature allows some of these applications to work with this router.

 Please Note: If this fails to make the application work, try to set up that computer as the DMZ host instead.

(For further instructions on setting up a DMZ host, please refer to the "Miscellaneous" section below)

OPTION	DEFINITION
Trigger	The outbound port number that will be triggered by the application..
Incoming Ports	When the trigger packet is detected, the inbound packets sent to the specified port numbers will be allowed to pass through the firewall.
Enable	Select to enable or disable the configured special application entry.

The NP805N also provides predefined settings for some popular applications.

To use the predefined settings, select your application from the Popular application pull down list, select an unused ID from the list and then click Copy to. The predefined settings will then be added to the list.

Click "Save" to save the settings or "Undo" to cancel.

Miscellaneous

A Demilitarized Zone (DMZ) Host is a computer without the protection of firewall. It allows that particular computer to be exposed to unrestricted 2-way communication to the internet. It is mostly used for Internet games, Video conferencing, Internet telephony and other special applications.

Item	Setting	Enable
IP Address of DMZ Host	<input type="text"/>	<input type="checkbox"/>
UPnP setting		<input checked="" type="checkbox"/>

To enable DMZ, enter the IP address of the computer you want to be live on the internet and click on "Enable".

 Please Note: This feature should be used only when necessary.

OPTION	DEFINITION
IP Address of DMZ Host	Enter the IP address of the computer you wish to put in the DMZ.
UPnP Setting	The device also supports uPnP. If the DMZ host operating system supports this function enable it to automatically configure the required network settings.

Click "Save" to save the settings or "Undo" to cancel.

Security Settings

The Security Setting page allows you to configure the security management on the router such as Packet filters and MAC Control. Click on any of the menu items on the left to access the respective setting page.

Status

The Status page lists any currently configured filtering for the Outbound, Inbound and Domain filters.

Status ▶ Network Setup ▶ Forwarding Rules ▶ Security Settings ▶ Advanced Settings ▶ NAS SETTINGS ▶ Toolbox			
Item	Status		
Outbound Filter	Disable		
Local Client	Only Deny Remote Host	Service	Working Time
Item	Status		
Inbound Filter	Disable		
Remote Host	Deny Remote Host to access	Service	Working Time
Item	Status		
Domain Filter	Disable		
Domain	Access		
All other Domains	Yes		
<input type="button" value="Refresh"/>			

Packet Filters

The Packet Filter enables you to control what packets are allowed to pass through the router. There are two types of packet filter, Outbound Packet Filter which applies to all outbound packets and the Inbound Packet Filter which only applies to packets that are destined for a Virtual Server or DMZ host only.



Please note: For further instructions on setting up MAC Level Filtering, please refer to the “MAC Control” section below

Outbound Filter:

To enable an Outbound Filter, tick the “Enable” tick box at the top of the page.

Status
▶ Network Setup
▶ Forwarding Rules
▶ Security Settings
▶ Advanced Settings
▶ NAS SETTINGS
▶ Toolbox

Item		Setting		
Outbound Packet Filter		<input type="checkbox"/> Enable		
<input checked="" type="radio"/> Allow all data through the router except data that matches the specified rules. <input type="radio"/> Deny all data through the router except data that matches the specified rules.				
ID	Source IP	Destination IP : Ports	Enable	Use rule#
1	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
2	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
3	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
4	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
5	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
6	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
7	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
8	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
Save Undo Inbound Filter... MAC Level...				

There are two types of filtering policies:

- Allow all data traffic to pass except those that match the specified rules.
- Deny all data traffic to pass except those that match the specified rules.

You can specify up to 48 filtering rules for each direction (Inbound or Outbound). For each rule you will need to define the following:

- Source IP address
- Source port
- Destination IP address
- Destination port
- Protocol: TCP or UDP or both.
- Use Schedule Rule#

For source or destination IP address, you can define a single IP address (192.168.20.1) or a range of IP addresses (192.168.20.100-192.168.20.200). Leaving these fields empty implies all IP addresses are matched.

For source or destination port, you can also define a single port (80) or a range of ports (1000-1999). Use the prefix "T" or "U" to specify either the TCP or UDP protocol e.g. T80, U53, U2000-2999. No prefix indicates both TCP and UDP are defined. Leaving this field empty implies all ports are matched.

The Packet Filter also works with Scheduling Rules, and gives you more flexibility on Access control.



Please note: For further instructions on scheduling rules, please refer to the “Scheduling” section later in this guide

Click "Save" to save the settings or "Undo" to cancel.

Inbound Filter:

To access the Inbound Packet Filter page, click on the "Inbound Filter" button on the bottom of the Outbound Filter page. All the settings on this page are the same as those for the Outbound Filter shown on the previous page.

Status
▶ Network Setup
▶ Forwarding Rules
▶ Security Settings
▶ Advanced Settings
▶ NAS SETTINGS
▶ Toolbox

Item		Setting		
Inbound Packet Filter		<input type="checkbox"/> Enable		
<input checked="" type="radio"/> Allow all data through the router except data that matches the specified rules. <input type="radio"/> Deny all data through the router except data that matches the specified rules.				
ID	Source IP	Destination IP : Ports	Enable	Use rule#
1	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
2	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
3	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
4	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
5	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
6	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
7	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
8	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
Save Undo Outbound Filter... MAC Level...				

Click "Save" to save the settings or "Undo" to cancel.

Domain Filters

Domain Filters enable you to prevent users from accessing specific domain addresses.

To enable the Domain Filter, tick the "Enable" tick box at the top of the page.

Status ▶ Network Setup ▶ Forwarding Rules ▶ Security Settings ▶ Advanced Settings ▶ NAS SETTINGS ▶ Toolbox

Item	Setting
Domain Filter	<input type="checkbox"/> Enable
Log DNS Query	<input type="checkbox"/> Enable
Privilege IP Addresses Range	From <input type="text"/> To <input type="text"/>

ID	Domain Suffix	Action	Enable
1	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
6	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
7	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
8	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
9	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
10	* (all others)	<input type="checkbox"/> Drop <input type="checkbox"/> Log	-

OPTION	DEFINITION
Domain Filter	Select to enable or disable domain filtering.
Log DNS Query	Enable this if you want to log when someone accesses filtered URLs.
Privilege IP Addresses Range	Set a group of computers that has unrestricted access to the internet

To set a Domain Filter, you need to specify the following:

OPTION	DEFINITION
Domain Suffix	Please type the suffix of the URL that needs to be restricted. For example, ".com", "xxx.com".
Action	The router action that you want when someone is accessing a URL that matches the specified domain suffix. Select Drop to block the access and/or select Log to log this access.
Enable	Tick to enable the rule.

Click "Save" to save the settings or "Undo" to cancel.

URL Blocking

URL Blocking will block LAN computers from connecting to a pre-defined website. The major difference between the Domain Filter and URL Blocking is that Domain Filtering require users to input a suffix (e.g. xxx.com, yyy.net) while URL Blocking only requires you to input a keyword.

To enable URL Blocking, tick the “Enable” tick box at the top of the page.

Status ▶ Network Setup ▶ Forwarding Rules ▶ Security Settings ▶ Advanced Settings ▶ NAS SETTINGS ▶ Toolbox

Item	Setting	
URL Blocking	<input type="checkbox"/> Enable	
ID	URL	Enable
1	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>		

To set a URL Blocking rule, you need to specify the following:

OPTION	DEFINITION
URL	If any part of the Website's URL matches the pre-defined word then the connection will be blocked. For example, you can use pre-defined word "sex" to block all websites if their URLs contain the pre-defined word "sex".
Enable	Tick to enable the rule.

Click "Save" to save the settings or "Undo" to cancel.

MAC Control

MAC Control allows you to assign different access rights for different users and to assign a specific IP address to a specific MAC address.

To enable MAC Address Control, tick the "Enable" tick box at the top of the page.

Status ▶ Network Setup ▶ Forwarding Rules ▶ Security Settings ▶ Advanced Settings ▶ NAS SETTINGS ▶ Toolbox

Item	Setting		
MAC Address Control	<input type="checkbox"/> Enable		
<input type="checkbox"/> Connection control	Wireless and wired clients with C checked can connect to this device; and <input type="text" value="allow"/> unspecified MAC addresses to connect.		
<input type="checkbox"/> Association control	Wireless clients with A checked can associate to the wireless LAN; and <input type="text" value="allow"/> unspecified MAC addresses to associate.		
DHCP clients <input type="text" value="- select one -"/> <input type="button" value="Copy to"/> ID <input type="text" value="-"/>			
ID	MAC Address	C	A
1	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="button" value=" << Previous"/> <input type="button" value=" Next >>"/> <input type="button" value=" Save"/> <input type="button" value=" Undo"/>			

Two types of MAC Control are available:

OPTION	DEFINITION
Connection control (C column)	Use this to control which clients (wired and wireless) can connect to the unit. If a client is denied access to connect to this device, it means the client cannot access the Internet either. Choose to allow or deny clients with MAC addresses that are not in the list to connect to this device.
Association control (A column)	Check Association Control to control which wireless client can associate with the unit. If a client is denied access to associate with the unit, it means the client cannot send or receive any data via this device. Choose to allow or deny the clients with MAC addresses that are not in the list to associate to the wireless LAN.



Please note: Click the "Next Page" or the "Previous Page" buttons to see the entire list

Click "Save" to save the settings or "Undo" to cancel.

Miscellaneous

This page allows you to change various miscellaneous security settings on the unit.

▶ Status
▶ Network Setup
▶ Forwarding Rules
▶ Security Settings
▶ Advanced Settings
▶ NAS SETTINGS
▶ Toolbox

Item	Setting	Enable
Administrator Time-out	<input type="text" value="300"/> seconds (0 to disable)	
Remote Administration	<input type="text"/> / <input type="text"/> : <input type="text"/>	<input type="checkbox"/>
Discard PING from WAN side		<input type="checkbox"/>
DoS Attack Detection		<input checked="" type="checkbox"/>
Keep WAN in stealth mode		<input checked="" type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>		

OPTION	DEFINITION
Administrator Time-out	The period of time with no activity in the web configuration page to logout automatically, set this to zero to disable this feature.
Remote Administrator Host/Port	Normally only Intranet users can browse the built-in web pages to perform administration tasks. This feature enables you to perform administration tasks from a remote host. If this feature is enabled, only the specified IP address can perform remote administration.
Discard PING from WAN side	When this feature is enabled, your router will not respond to ping requests from remote hosts.
DoS Attack Detection	When this feature is enabled, the router will detect and log where the DoS attack comes from on the Internet.
Keep WAN in stealth mode	Prevent the WAN interface from responding to remote probes.



Please note: If the specified IP address is 0.0.0.0, any host can connect to the router to perform administration tasks. You can also use a subnet mask (/nn) to specify a group of trusted IP addresses for example, "10.1.2.0/24".

When Remote Administration is enabled, the web server port will be shifted to 80.

You can also change the web server port.

When enabled, the router can detect the following (and more) DoS attack types:

- SYN Attack
- WinNuke
- Port Scan
- Ping of Death
- Land Attack

Click "Save" to save the settings or "Undo" to cancel.

Advanced Settings

The Advanced Setting page allows you to configure the advanced settings on the router such as the System log, Dynamic DNS and SNMP options. Click on any of the menu items on the left to configure the access the respective setting page.

Status

The Status page displays the current System time, and lists any configured Dynamic DNS (DDNS) accounts, any Static or Dynamic Routes added or any Quality of Service (QoS) rules in place.

Item	Status
System Time	Thu, 03 Nov 2011 11:30:19 +1100

Item	Status
DDNS	Disable
Provider	-

Item	Status
Dynamic Routing	Disable
Static Routing	Disable

Destination	Subnet Mask	Gateway	Hop

Item	Status
QoS Control	Disable

Local Client	Remote Host	Service	Priority	Working Time

System Log

This enables you to set up the system log features of the router. You can also choose to send the system log to a remote syslog server (via a UDP connection) or email a copy to a recipient.

Status
▶ Network Setup
▶ Forwarding Rules
▶ Security Settings
▶ Advanced Settings
▶ NAS SETTINGS
▶ Toolbox

Item	Setting	Enable
IP address for syslogd server	<input style="width: 80%;" type="text"/>	<input type="checkbox"/>
Email address to send syslog to		<input type="checkbox"/>
• SMTP Server : port	<input style="width: 60%;" type="text"/> : <input style="width: 20%;" type="text"/>	
• SMTP Username	<input style="width: 90%;" type="text"/>	
• SMTP Password	<input style="width: 90%;" type="text"/>	
• E-mail addresses	<div style="border: 1px solid black; height: 40px; width: 100%;"></div>	
• E-mail subject	<input style="width: 90%;" type="text"/>	
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="View Log..."/> <input type="button" value="Email Log Now"/>		

OPTION	DEFINITION
IP Address for remote System Logs (syslog)	The IP address of the syslog server where the system log data will be sent. Click the "Enable" checkbox to enable this function.
Email address to send syslog to	Click the "Enable" checkbox to enable this function.
SMTP Server : port	Enter the IP address or fully qualified domain name (FQDN) and port for the selected email server.
SMTP Username	The SMTP username required to send email <i>(if required)</i> .
SMTP Password	The SMTP password required to send email <i>(if required)</i> .
Email Addresses	Enter the email addresses to send a copy of the current syslog to.
Email Subject	Enter the email subject to show on any sent emails.
View Log...	View the current system log.
Email Log Now	Email the current syslog to the entered email addresses.

Dynamic DNS

The Dynamic DNS feature enables users to set a static domain name for their internet connection even when the ISP only provides a dynamic IP address.

By mapping the host name to the current public IP address of the router, users who want to connect to the router or any services behind the router from the internet can just use the Dynamic DNS hostname instead of the IP Address which might change every time the router connects to the Internet.

Before you can use Dynamic DNS service, you need to register an account on one of the many supported Dynamic DNS providers such as DynDNS.org, TZO.com or dhs.org.

Item	Setting
DDNS	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Provider	DynDNS.org(Dynamic)
Host Name	<input type="text"/>
Username / E-mail	<input type="text"/>
Password / Key	<input type="text"/>

Save Undo

After registering the account, the Dynamic DNS provider will provide you with the following details:

- Host Name
- Username/Email
- Password/Key

To enable the Dynamic DNS feature on the unit, click the "Enable" check box, choose the appropriate Dynamic DNS Provider and enter the details supplied by your Dynamic DNS provider.

Click "Save" to save the settings or "Undo" to cancel.

QoS

Quality of Service (QoS) provides different priority to different users or data flows. It can also guarantee a certain level of performance.

Status ▶ Network Setup ▶ Forwarding Rules ▶ Security Settings ▶ Advanced Settings ▶ NAS SETTINGS ▶ Toolbox

Item	Setting
Cross-layer QoS	Disable ▼
QoS Mode	Smart-QoS ▼
Bandwidth of Upstream	<input type="text"/> Kbps (Kilobits per second)
Bandwidth of Downstream	<input type="text"/> Kbps (Kilobits per second)
Flexible Bandwidth Management	Disable ▼

Item	Select	Setting
Game	<input type="checkbox"/>	<input type="text" value="0"/> %
Chat	<input type="checkbox"/>	<input type="text" value="0"/> %
VoIP	<input type="checkbox"/>	<input type="text" value="0"/> %
P2P	<input type="checkbox"/>	<input type="text" value="0"/> %
Video	<input type="checkbox"/>	<input type="text" value="0"/> %
Web	<input type="checkbox"/>	<input type="text" value="0"/> %

Save

OPTION	DEFINITION
Cross-layer QoS	Select to enable or disable cross-layer Quality of Service support on the connection.
Flexible Bandwidth Management	Select to enable or disable flexible bandwidth management control on the connection.
Average Bandwidth	Select to enable or disable bandwidth averaging on the connection.

You can also control the whether certain types of network traffic are given priority or even forbidden on your network. Put a tick in the checkbox to either grant the specified traffic type priority over others or to forbid the traffic altogether.

Click the “Advanced Setting” button to display the QoS rules table and configure advanced QoS settings. Click the “Add New Rule” to configure a new QoS rule or “Group Setting” to create a group of traffic to apply the entered QoS rules to.

To create a group, click the “Group Setting” button, and then click “New Add” and select to group via IP address or MAC address.

OPTION	DEFINITION
Rule	Select to enable or disable the QoS rule.
Class	Select the class of traffic you would like to prioritise.
Class Info	Enter the applicable class information to apply QoS to.
Function	Select the appropriate function from the class to apply QoS to.
Function data	Enter the appropriate data required to match your selected function.
Direction	Select the applicable traffic direction to prioritise.
Schedule	Select the previously configured schedule rule to determine when to apply the traffic management. The QoS rules can work in conjunction with Scheduling Rules.



Please note: For further instructions on scheduling rules, please refer to the “Scheduling” section later in this guide

Click on “Save” to store your setting or “Undo” to discard your changes.

SNMP

SNMP (Simple Network Management Protocol) is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

[Status](#)
[▶ Network Setup](#)
[▶ Forwarding Rules](#)
[▶ Security Settings](#)
[▶ Advanced Settings](#)
[▶ NAS SETTINGS](#)
[▶ Toolbox](#)

item	Setting
Enable SNMP	<input type="checkbox"/> Local <input type="checkbox"/> Remote
Get Community	<input type="text"/>
Set Community	<input type="text"/>
IP 1	<input type="text"/>
IP 2	<input type="text"/>
IP 3	<input type="text"/>
IP 4	<input type="text"/>
SNMP Version	<input checked="" type="radio"/> V1 <input type="radio"/> V2c
WAN Access IP Address	<input type="text"/>

OPTION	DEFINITION
Enable SNMP	You must check Local, Remote or both to enable SNMP function. If Local is checked, this device will only respond to requests from LAN connected hosts. If Remote is checked, this device will respond to requests from the WAN connection.
Get Community	Sets the community string your device will respond to for Read-Only access.
Set Community	Sets the community string your device will respond to for Read/Write access.
IP 1, IP 2, IP 3, IP 4	Input your SNMP Management host IP here. You will need to configure the address where the device should send SNMP Trap messages to.
SNMP Version	Please select proper SNMP Version that your SNMP Management software supports.
WAN Access IP Address	You can limit remote access to a specific IP address by entering it here.



Please note: If "Remote" access is enabled, the default setting of 0.0.0.0 means any IP obtain SNMP protocol Information.

Click on "Save" to store your setting or "Undo" to discard your changes.

Routing

Routing tables allow you to determine which physical interface address to use for outgoing IP data. If you have more than one router and subnet, you will need to configure the routing table to allow packets to find the proper routing path and allow different subnets to communicate with each other.

These settings are used to setup the static and dynamic routing features of the NP805N.

Status
▶ Network Setup
▶ Forwarding Rules
▶ Security Settings
▶ Advanced Settings
▶ NAS SETTINGS
▶ Toolbox

Item		Setting			
Dynamic Routing		<input checked="" type="radio"/> Disable <input type="radio"/> RIPv1 <input type="radio"/> RIPv2			
Static Routing		<input checked="" type="radio"/> Disable <input type="radio"/> Enable			
ID	Destination	Subnet Mask	Gateway	Hop	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>					

Dynamic Routing:

Routing Information Protocol (RIP) will exchange information about different host destinations for working out routes throughout the network.



Please note: Only select RIPv2 if you have a different subnet in your network. Otherwise, please select RIPv1.

Static Routing:

For static routing, you can specify up to 8 routing rules.

You need to enter the **destination IP address**, **subnet mask**, **gateway**, and **hop** for each routing rule, then enable the rule by clicking the Enable checkbox.

Click on "Save" to store your setting or "Undo" to discard your changes.

System Time

This page allows you to change the System time setting on the NP805N.

Status
▶ Network Setup
▶ Forwarding Rules
▶ Security Settings
▶ Advanced Settings
▶ NAS SETTINGS
▶ Toolbox

Item	Setting
Time Zone	(GMT+10:00) Canberra, Melbourne, Sydney
Auto-Synchronization	<input checked="" type="checkbox"/> Enable Time Server (RFC-868): 0.netcomm.pool.ntp.org

Sync Result

OPTION	DEFINITION
Time Zone	Select the time zone where this device is located.
Auto-Synchronization	Select the "Enable" checkbox to enable this function.
Time Server	Select a NTP time server to obtain the current UTC time from.
Sync with Time Server	Select if you want to set Date and Time by NTP Protocol.
Sync with my PC	Select if you want to set Date and Time using your computers Date and Time

Click "Save" to save the settings or "Undo" to cancel.

Scheduling

You can use scheduling to enable or disable a service at a specific time or on a specific day.

Item		Setting
Schedule		<input type="checkbox"/> Enable
Rule#	Rule Name	Action
1		<input type="button" value="Add New"/>
2		<input type="button" value="Add New"/>
3		<input type="button" value="Add New"/>
4		<input type="button" value="Add New"/>
5		<input type="button" value="Add New"/>
6		<input type="button" value="Add New"/>
7		<input type="button" value="Add New"/>
8		<input type="button" value="Add New"/>
9		<input type="button" value="Add New"/>
10		<input type="button" value="Add New"/>

Select "Enable" and then click the "New Add" button.

Item		Setting	
Name of Rule 1		<input type="text"/>	
Policy		<input type="button" value="Inactivate"/> except the selected days and hours below.	
ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	<input type="button" value="- choose one -"/>	<input type="text"/>	<input type="text"/>
2	<input type="button" value="- choose one -"/>	<input type="text"/>	<input type="text"/>
3	<input type="button" value="- choose one -"/>	<input type="text"/>	<input type="text"/>
4	<input type="button" value="- choose one -"/>	<input type="text"/>	<input type="text"/>
5	<input type="button" value="- choose one -"/>	<input type="text"/>	<input type="text"/>
6	<input type="button" value="- choose one -"/>	<input type="text"/>	<input type="text"/>
7	<input type="button" value="- choose one -"/>	<input type="text"/>	<input type="text"/>
8	<input type="button" value="- choose one -"/>	<input type="text"/>	<input type="text"/>

Select a name for the rule and enter the details such as the day, start time or end time and click "Save"

In the example below, the rule is called "Work Hours" and it is only active between 08:00 and 17:30.

You are then able to select the scheduling rule name specified from the Packet Filter configuration section to perform the configured filtering at the scheduled time as per the screenshot below.

Item		Setting	
Name of Rule 1		<input type="text" value="Work Hours"/>	
Policy		<input type="button" value="Inactivate"/> except the selected days and hours below.	
ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	<input type="button" value="Every Day"/>	<input type="text" value="08:00"/>	<input type="text" value="17:30"/>

This example would prevent any access to the IP address 66.102.11.104 from any device connected to the router, 7 days a week, only between the hours of 08:00 and 17:30.

Click "Save" to save the settings or "Undo" to cancel.

IPv6

The IPv6 page enables you to configure the settings used for an IPv6 connection (if supported by your Internet Service Provider).

[Status](#)
[▶ Network Setup](#)
[▶ Forwarding Rules](#)
[▶ Security Settings](#)
[▶ Advanced Settings](#)
[▶ NAS SETTINGS](#)
[▶ Toolbox](#)

Item	Setting
IPv6	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
IPv6 Connection	<input type="text" value="DHCPv6"/>
DNS Setting	<input checked="" type="radio"/> Obtain DNS Server address Automatically <input type="radio"/> Use the following DNS address
Primary DNS Address	<input type="text"/>
Secondary DNS Address	<input type="text"/>
LAN IPv6 Address	<input type="text" value=""/> /64
LAN IPv6 Link-Local Address	<input type="text"/>
Autoconfiguration	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Autoconfiguration Type	<input type="text" value="Stateless"/>
Router Advertisement Lifetime	<input type="text" value="200"/> Seconds
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

OPTION	DEFINITION
IPv6	Select to enable or disable IPv6 functionality.
IPv6 Connection	Select the type of IPv6 connection to utilise for your service. You can select from: <ul style="list-style-type: none"> ▪ Static IPv6 ▪ DHCPv6 ▪ PPPoE ▪ 6 to 4 ▪ IPv6 in IPv4 Tunnel Select the type of connection as required by your Internet Service Provider for their IPv6 service and then enter the appropriate details are provided by them in the applicable fields.
LAN IPv6 Address	The IP Address to use for the IPv6 service connection.
LAN IPv6 Link-Local Address	The current local LAN IPv6 address of the NP805N.
Autoconfiguration	Select to enable or disable IPv6 auto configuration (if supported by your Internet Service Provider).
Autoconfiguration Type	Select the applicable type of auto configuration mode as required by your Internet Service Provider for their IPv6 service.
Router Advertisement Lifetime	Enter the length of time between the router advertising its availability on the IPv6 connection.

TR-069

The TR-069 client enables the NP805N to be automatically configured from an appropriate TR-069 server. Enter the applicable configuration options to enable the router to contact the TR-069 server and retrieve any configuration options.

Status ▶ Network Setup ▶ Forwarding Rules ▶ Security Settings ▶ Advanced Settings ▶ NAS SETTINGS ▶ Toolbox

Item	Setting
TR-069	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
ACS URL	<input type="text"/>
ACS UserName	<input type="text"/>
ACS Password	<input type="text"/>
ConnectionRequest Port	<input type="text" value="8099"/>
ConnectionRequest UserName	<input type="text"/>
ConnectionRequest Password	<input type="text"/>
Inform	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Interval	<input type="text" value="900"/> seconds

OPTION	DEFINITION
TR-069	Select to enable or disable the TR-069 automatic configuration function.
ACS URL	Enter the URL of the ACS server for automatic configuration.
ACS User Name	The username required to login to the ACS server.
ACS Password	The password required to login to the ACS server.
Connection Request Port	The port number the ACS server is running on.
Connection Request Username	The username to use when a connection request is made to the CPE.
Connection Request Password	The password to use when a connection request is made to the CPE.
Inform	Select to enable or disable the Inform function for ACS connections.
Interval	Select the interval between Inform requests if Inform has been enabled.

Once configured, click the “Save” button to store any changes to the settings.

VLAN

The VLAN page enables you to configure VLAN tagging for the Ethernet ports. VLAN tagging can be used to separate network traffic so that it is not visible to other VLANs. The currently configured VLAN tagging settings are shown at the bottom of the page.

Status ▶ Network Setup ▶ Forwarding Rules ▶ Security Settings ▶ Advanced Settings ▶ NAS SETTINGS ▶ Toolbox

Ethernet	WAN/LAN	VID	Tx TAG
Port 1	WAN	<input type="text" value="2"/>	<input type="checkbox"/>
Port 2	LAN	<input type="text" value="1"/>	<input type="checkbox"/>
Port 3	LAN	<input type="text" value="1"/>	<input type="checkbox"/>
Port 4	LAN	<input type="text" value="1"/>	<input type="checkbox"/>
Port 5	LAN	<input type="text" value="1"/>	<input type="checkbox"/>

VLAN ID on LAN	LAN/Wireless LAN(Interface)	Tag	Type	Internet or ISP map WAN(VLAN ID)
1	Port2, Port3, Port4, Port5	No	NAT	0

1. Enter the VLAN ID to be used for a particular Ethernet port.
2. Select whether or not to mark transmitted packets with the selected VLAN ID.
3. Click "Save".

You can also set the WAN port to a particular VLAN (if needed). To do this, perform the following steps:

1. Click the "WAN VLAN Settings" button.

Status ▶ Network Setup ▶ Forwarding Rules ▶ Security Settings ▶ Advanced Settings ▶ NAS SETTINGS ▶ Toolbox

Item	Setting
VID	<input type="text" value="1"/>
Routing Type	<input type="text" value="NAT"/>

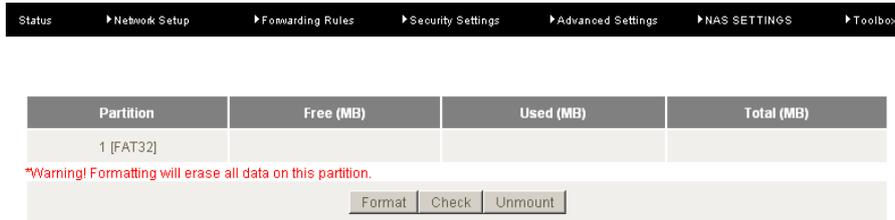
2. Select the appropriate VLAN ID.
3. Select the appropriate Routing Type for the WAN interface to use.
4. Click "Save".

NAS Settings

The NAS Settings page enables you to configure the network area storage (NAS) function of the NP805N. This function can be used to remotely access files stored on an attached USB hard drive. Click on any of the menu items to access the respective configuration page.

Disk Utility

The Disk Utility function enables you to check any attached USB storage for errors. The NP805N will scan the attached storage and determine if there are any file system errors present. File System errors can prevent you being able to access stored content. You can also format (erase) any attached storage if needed. Simply click the appropriate button to perform either task.

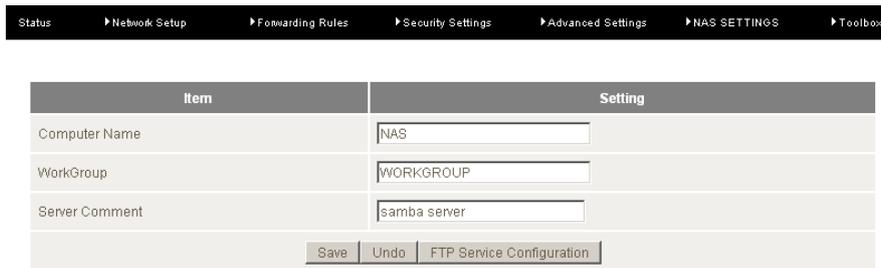


File Sharing

The File Sharing function enables the NP805N to take part in a Windows networking environment. Once configured, the attached USB Storage can be viewed from Windows by typing:

\\<Configured NP805N Computer Name>\Storage\

Files can then be dragged and dropped onto the attached USB storage.



OPTION	DEFINITION
Computer Name	Enter the computer name the NP805N is to use on the network.
WorkGroup	Enter the network workgroup the NP805N is to be a member of.
Server Comment	Enter the comment to be displayed when a list of network hosts is shown.

The File Sharing configuration also enables you to enable the built-in FTP server function and the associated settings:



OPTION	DEFINITION
FTP	Select to enable or disable the FTP server function.
FTP Port	Enter the network port the FTP server should run on.
FTP Max Connections per IP	Enter the maximum number of concurrent connections which can be used by a particular IP address.
FTP Max Clients	Enter the maximum number of clients which can connect to the FTP concurrently.
Client Support UTF8	Enable Unicode support for connected clients.
Codepage	Select the appropriate codepage to use for the filenames of files stored on the FTP server.

Access Control

The Access Control function enables control over which users can access any attached USB Storage. By default, the NP805N is in "Guest Mode" which means anyone can access the attached hard drive.

Status ▶ Network Setup ▶ Forwarding Rules ▶ Security Settings ▶ Advanced Settings ▶ NAS SETTINGS ▶ Toolbox

Item	Setting
Security Level	<input checked="" type="radio"/> Guest mode <input type="radio"/> Authorization mode
<input type="button" value="Save"/> <input type="button" value="User Configuration"/>	

Enabling "Authorization Mode" allows the creation of specific user accounts with a password to further control access permissions. To enable this, click on the "Authorization Mode" radio button and click "Save". You can then click on the "User Configuration" button in order to create the required user accounts.

Status ▶ Network Setup ▶ Forwarding Rules ▶ Security Settings ▶ Advanced Settings ▶ NAS SETTINGS ▶ Toolbox

Item	Setting		
User Name	<input type="text"/> (Max. 20 users)		
Password	<input type="text"/>		
ID	Username	Password	Select
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Cancel"/> <input type="button" value="Back"/>			

Add the user name and password and then click "Add". Alternatively, to remove a user, click on the radio button to the right of the username and then click "Delete".

iTunes Server

The iTunes Server function enables any applicable media on any attached USB storage to be directly access from within iTunes. To enable this, click on the "Enable" radio button in the "Service" section. Click the "Save" button to save any configuration changes you have made.

Status ▶ Network Setup ▶ Forwarding Rules ▶ Security Settings ▶ Advanced Settings ▶ NAS SETTINGS ▶ Toolbox

Item	Setting
Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
iTunes Shared Library Name	<input type="text"/>
iTunes Shared Library Password (required)	<input type="text"/>
Service Port (default = 3689)	<input type="text" value="3689"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

OPTION	DEFINITION
Service Name	Enter the name that will show up in iTunes for a library list.
Service Port	Enter the port number to run your iTunes server on (<i>This will usually be left as 3369</i>).
Access Password	Enter the password required to access your iTunes server content.

Download Assistant

The Download Assistant enables you to schedule the NP805N to perform a download from an Internet host.

You are able to select from two download types:

- FTP
- HTTP

Each type of download job requires different configuration options.

FTP

Status
▶ Network Setup
▶ Forwarding Rules
▶ Security Settings
▶ Advanced Settings
▶ NAS SETTINGS
▶ Toolbox

Item	Setting
Download Type	<input checked="" type="radio"/> FTP <input type="radio"/> HTTP
Job Name	<input type="text"/>
URL	<input type="text"/> Port <input type="text" value="21"/>
Save To	<input type="text" value="/C/Downloads/FTP"/>
Login method	<input checked="" type="radio"/> Anonymous <input type="radio"/> Account
Username	<input type="text"/>
Password	<input type="text"/>
Start Time	<input type="radio"/> Schedule <input checked="" type="radio"/> At Once
	Time <input type="text" value="2011"/> / <input type="text" value="Nov"/> / <input type="text" value="03"/> - <input type="text" value="12"/> : <input type="text" value="01"/>

*Please make sure the files that you download are legal before proceeding to download them.

OPTION	DEFINITION
Job Name	A name to identify the download job.
URL	The address to download from.
Port	The port required for the FTP server (<i>This would usually be left as 21</i>).
Save To	The location on the NP805N to save the downloaded file to.
Login Method	Select the type of authentication required by the FTP server (<i>Selecting anonymous means a username and password are not required</i>).
Username	The username required to access the FTP server.
Password	The password required to access the FTP server.
Start Time	Select to either schedule a time for the download to begin or start the download immediately.

HTTP

Item	Setting
Download Type	<input type="radio"/> FTP <input checked="" type="radio"/> HTTP
Job Name	<input type="text"/>
URL	<input type="text"/>
Save To	<input type="text" value="/C/Downloads/HTTP"/>
Start Time	<input type="radio"/> Schedule <input checked="" type="radio"/> At Once
	Time: <input type="text" value="2011"/> / <input type="text" value="Nov"/> / <input type="text" value="08"/> - <input type="text" value="17"/> : <input type="text" value="14"/>
*Please make sure the files that you download are legal before proceeding to download them.	
<input type="button" value="E-mail Alert Configuration"/> <input type="button" value="Save"/> <input type="button" value="Undo"/>	

OPTION	DEFINITION
Job Name	A name to identify the download job.
URL	The address to download from.
Save To	The location on the NP805N to save the downloaded file to.
Start Time	Select to either schedule a time for the download to begin or start the download immediately.

You can also configure the NP805N to send an e-mail on completion of the scheduled download. Click on the "E-mail Alert Configuration" button to setup this option.

Item	Setting
HTTP download alert	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
FTP download alert	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
SMTP Server Address	<input type="text"/>
SMTP Server Port	<input type="text"/>
SMTP User Name	<input type="text"/>
SMTP Password	<input type="text"/>
Email Address	<input type="text"/>
Email Subject	<input type="text"/>
Reservation Disk space	<input type="text" value="200"/> MB
<input type="button" value="Back"/> <input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Test E-mail"/>	

OPTION	DEFINITION
HTTP Download Alert	Select to enable or disable an alert to be sent for a completed HTTP download.
FTP Download Alert	Select to enable or disable an alert to be sent for a completed FTP download.
USB Download Alert	Select to enable or disable an alert to be sent for a completed USB download.
SMTP Server Address	Enter the address of the email server to be used to send the alerts.
SMTP Server Port	Enter the port which the email server is running on.
SMTP User Name	Enter the username required to login to the email server.
SMTP Password	Enter the password required to login to the email server.
Email Address	Enter the email address any alerts are to be sent to.
Email Subject	Enter the subject to be used on any email alerts sent out.
Reservation Disk Space	Enter the amount of disk space to reserve on the NP805N for the specified download.

Download Status

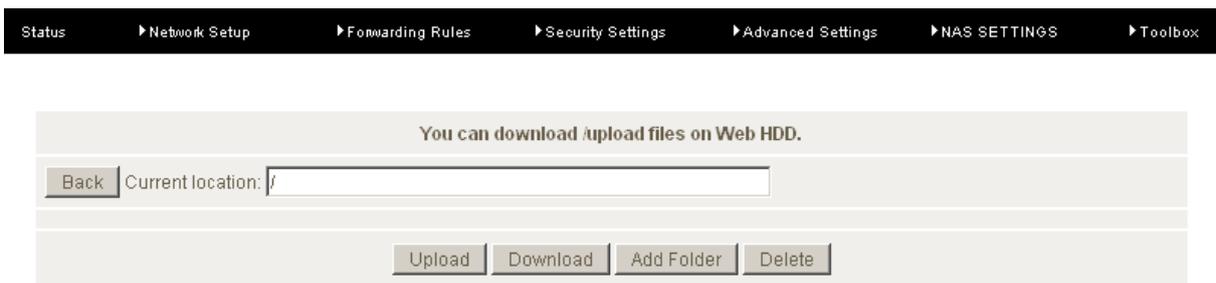
The Download Status page enables you to monitor previously scheduled Download Assistant jobs. From this page you are able to Start, Pause, Resume or Delete any Download Assistant jobs.



The View drop-down menu enables you to select whether currently running jobs, waiting jobs or scheduled jobs are displayed. Once listed, click on the checkbox on the left hand side of the listed jobs and then click the appropriate function button.

Web HDD

The Web HDD function provides a web page based Windows Explorer type view of the content of any attached USB storage. Using this interface you are able to upload, download or delete files and folders as well as create directories. Click through the displayed folders to show any stored files.



Single click on any items to select them and click the appropriate button or double click folders to view any content.



To upload files to your Web HDD. To do this, click the Upload button. You can then click the “Browse” button and then navigate to the file you would like to upload. Once selected, this file will be copied to the Web HDD and become available to download by connected devices.

Toolbox

System Info

From this page you can view the current System log entries for the router.

The screenshot shows the 'System Info' page with a navigation bar containing: Status, Network Setup, Forwarding Rules, Security Settings, Advanced Settings, NAS SETTINGS, and Toolbox. Below the navigation bar is a table with two sections:

Item	Setting
WAN Type	Dynamic IP Address
Display time	Thu, 03 Nov 2011 11:38:35 +1100

Time	Log

Below the table are navigation buttons: << Previous, Next >>, First Page, Last Page, Refresh, Download, and Clear logs.

You can also select to save a copy of the syslog data to your computer by clicking the "Download" button or clear the current syslog data by clicking the "Clear Logs" button.

Restore Settings

This page enables you to restore a previously saved backup of the NP805N's configuration.

The screenshot shows the 'Restore Settings' page with a navigation bar containing: Status, Network Setup, Forwarding Rules, Security Settings, Advanced Settings, NAS SETTINGS, and Toolbox. The main content area is titled 'Config Filename' and features a text input field and a 'Browse...' button. Below this is a note: 'Note! Do not interrupt the process or power off the unit when it is being upgraded. When the process is done successfully, the unit will be restarted automatically.' At the bottom are 'Restore' and 'Cancel' buttons.

Click the "Browse" button and navigate to the location you previously saved the configuration file. Click the "Restore" button once you have selected the appropriate .bin file to use.

Firmware Upgrade

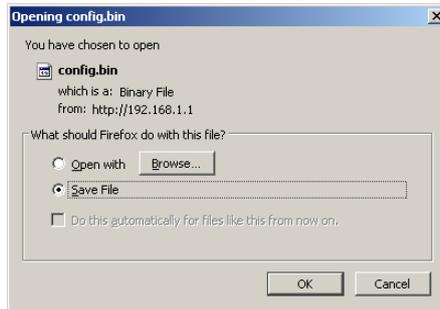
This page enables you to update the firmware on the NP805N.

The screenshot shows the 'Firmware Upgrade' page with a navigation bar containing: Status, Network Setup, Forwarding Rules, Security Settings, Advanced Settings, NAS SETTINGS, and Toolbox. The main content area is titled 'Firmware Filename' and features a text input field and a 'Browse...' button. Below this is the text: 'Current firmware version is R0.05a6.' followed by a note: 'Note! Do not interrupt the process or power off the unit when it is being upgraded. When the process is done successfully, the unit will be restarted automatically.' There is a checkbox labeled 'Accept unofficial firmware.' and 'Upgrade' and 'Cancel' buttons at the bottom.

Click the "Browse" button and navigate to the location you saved the firmware update file. You can then upgrade the routers firmware by clicking the "Upgrade" button.

Backup Settings

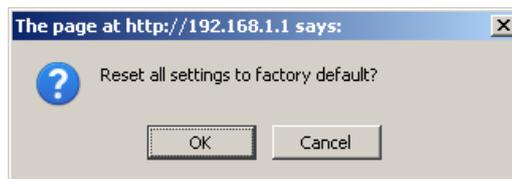
You can backup your current settings by clicking the "Backup Setting" button then and save it as a bin file.



When you want to restore these settings, click the "Restore Setting" link and use the bin file you saved.

Reset to Default

You can reset your NP805N to the factory default settings by clicking on this link.



After clicking "OK", the router will reset and start up with the default settings loaded.

Reboot

You can reboot your router by clicking on the "Reboot" link. This can be useful to ensure restore settings are loaded.

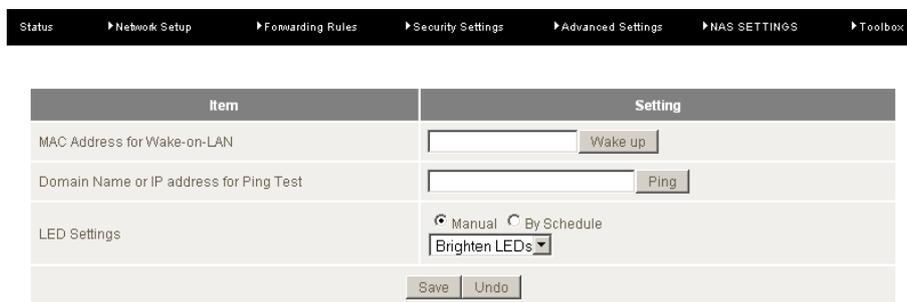


Startup Wizard

Click this link to re-run the First time Setup Wizard. You can use this to easily reconfigure your NP805N.

Miscellaneous

Wake-on-LAN enables the router to start-up a computer or device (if the computer supports it) when a WOL packet is detected on the network going to the client MAC you have entered.



You can also control the brightness of the LEDs on the router manually or via a scheduled time (Please refer to the scheduling section for instructions on setting up scheduled times).

OPTION	DEFINITION
MAC Address for Wake-On-LAN	Enter the MAC address of the computer you would like to be able to wake up from standby mode.
Domain Name or IP address for Ping Test	Enter the domain name or IP address you would like to attempt to ping.
LED Settings	Select to manually control the LED brightness.

Logout

Click this link to logout of the NP805N's Web based User Interface.

Additional Product Information

Establishing a wireless connection

Windows XP (Service Pack 2)

1. Open the Network Connections control panel (Start -> Control Panel -> Network Connections):
2. Right-click on your Wireless Network Connection and select View Available Wireless Networks:
3. Select the wireless network listed on your included wireless security card and click Connect.
4. Enter the network key (refer to the included wireless security card for *the default wireless network key*).
5. The connection will show Connected.

Windows Vista

1. Open the Network and Sharing Center (Start > Control Panel > Network and Sharing center).
2. Click on "Connect to a network".
3. Choose "Connect to the Internet" and click on "Next".
4. Select the wireless network listed on your included wireless security card and click Connect.
5. Enter the network key (refer to the included wireless security card for *the default wireless network key*).
6. Select the appropriate location. This will affect the firewall settings on the computer.
7. Click on both "Save this network" and "Start this connection automatically" and click "Next".

Windows 7

1. Open the Network and Sharing Center (Start > Control Panel > Network and Sharing center).
2. Click on "Change Adapter settings" on the left-hand side.
3. Right-click on "Wireless Network Connection" and select "Connect / Disconnect".
4. Select the wireless network listed on your included wireless security card and click Connect.
5. Enter the network key (refer to the included wireless security card for *the default wireless network key*).
6. You may then see a window that asks you to "Select a location for the 'wireless' network". Please select the "Home" location.
7. You may then see a window prompting you to setup a "HomeGroup". Click "Cancel" on this.
8. You can verify your wireless connection by clicking the "Wireless Signal" indicator in your system tray.
9. After clicking on this, you should see an entry matching the SSID of your NP805N with "Connected" next to it.

Mac OSX 10.6

1. Click on the Airport icon on the top right menu.
2. Select the wireless network listed on your included wireless security card and click Connect.
3. On the new window, select "Show Password", type in the network key (refer to *the included wireless security card for the default wireless network key*) in the Password field and then click on OK.
4. To check the connection, click on the Airport icon and there should be a tick on the wireless network name.



Please note: For other operating system (Windows 98SE, Windows ME, Windows 2000 etc) or if you use a wireless adaptor utility to configure your wireless connection, please consult the wireless adapter documentation for additional information.

Troubleshooting

Using the indicator lights (LEDs) to Diagnose Problems

The LEDs are useful aides for finding possible problem causes.

Power LED

The Power LED does not light up.

STEP	CORRECTIVE ACTION
1	Make sure that the NP805N power adaptor is connected to the device and plugged in to an appropriate power source. Use only the supplied power adaptor.
2	Check that the NP805N and the power source are both turned on and device is receiving sufficient power.
3	Turn the NP805N off and on.
4	If the error persists, you may have a hardware problem. In this case, you should contact technical support.

Web Configuration

I cannot access the web configuration pages.

STEP	CORRECTIVE ACTION
1	Make sure you are using the correct IP address of the NP805N. You can check the IP address of the device from the Network Setup configuration page.
2	Check that you have enabled remote administration access. If you have configured an inbound packet filter, ensure your computer's IP address matches it.
3	Your computer's and the NP805N's IP addresses must be on the same subnet for LAN access. You can check the subnet in use by the router on the Network Setup page.
4	If you have changed the devices IP address, then enter the new one as the URL you enter into the address bar of your web browser.

The web configuration does not display properly.

STEP	CORRECTIVE ACTION
1	Delete the temporary web files and log in again. In Internet Explorer, click Tools, Internet Options and then click the Delete Files ... button. When a Delete Files window displays, select Delete all offline content and click OK. (Steps may vary depending on the version of your Internet browser.)

Login Username and Password

I forgot my login username and/or password.

STEP	CORRECTIVE ACTION
1	Press the Reset button for ten seconds, and then release it. When the Power LED begins to blink, the defaults have been restored and the NP805N restarts. You can now login with the factory default username and password "admin" (without the quotes)
2	It is highly recommended to change the default username and password. Make sure you store the username and password in a safe place.

WLAN Interface

I cannot access the NP805N from the WLAN or ping any computer on the WLAN.

STEP	CORRECT ACTION
1	Check the Wi-Fi LED on the front of the unit and verify the WLAN is enabled as per the LED Indicator section.
2	If you are using a static IP address for the WLAN connection, make sure that the IP address and the subnet mask of the NP805N and your computer(s) are on the same subnet. You can check the routers configuration from the Network Setup page.

Technical Data

The following table lists the hardware specifications of the NP805N.

MODEL	NP805N
CPU	RT3052
Wireless LAN	IEEE 802.11n. Backwards compatible with IEEE 802.11b/g
Ethernet WAN	1 x Gigabit WAN port (10/100/1000 Mbps)
Connectivity	1 x USB 2.0, 4 x 10/100/1000 Mbps LAN, WLAN
LED Indicators	Power, WWW, LAN 1-4, WAN, WIFI, USB
Operating Temperature	Operating temperature: 0°C - 40°C, Humidity: 10%-90% non-condensing Storage temperature: -10°C - 70°C, Humidity: 0%-95% non-condensing
Power Input	12V DC - 1.5A
Dimensions & Weight	215 mm (L) x 145 mm (W) x 37 mm (H) 403 grams
Regulatory Compliance	C-Tick

Electrical Specifications

It is recommended that the NP805N be powered by the supplied 12V DC, 1.5A power supply. A replacement power supply is available from the NetComm Online shop.

Environmental Specifications / Tolerances

The NP805N housing enables it to operate over a wide variety of temperatures from 0°C - 40°C (operating temperature).

Legal & Regulatory Information

1. Intellectual Property Rights

All intellectual property rights (including copyright and trade mark rights) subsisting in, relating to or arising out of this Manual are owned by and vest in NetComm Wireless Limited (ACN 002490486) (**NetComm**) (or its licensors). This Manual does not transfer any right, title or interest in NetComm's (or its licensors') intellectual property rights to you.

You are permitted to use this Manual for the sole purpose of using the NetComm product to which it relates. Otherwise no part of this Manual may be reproduced, stored in a retrieval system or transmitted in any form, by any means, be it electronic, mechanical, recording or otherwise, without the prior written permission of NetComm.

NetComm is a trademark of NetComm. All other trademarks are acknowledged to be the property of their respective owners.

2. Customer Information

The Australian Communications & Media Authority (**ACMA**) requires you to be aware of the following information and warnings:

1. This unit may be connected to the Telecommunication Network through a line cord which meets the requirements of the AS/CA S008-2011 Standard.
2. This equipment has been tested and found to comply with the Standards for C-Tick and or A-Tick as set by the ACMA. These standards are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio noise and, if not installed and used in accordance with the instructions detailed within this manual, may cause interference to radio communications. However, there is no guarantee that interference will not occur with the installation of this product in your home or office. If this equipment does cause some degree of interference to radio or television reception, which can be determined by turning the equipment off and on, we encourage the user to try to correct the interference by one or more of the following measures:
 - Change the direction or relocate the receiving antenna.
 - Increase the separation between this equipment and the receiver.
 - Connect the equipment to an alternate power outlet on a different power circuit from that to which the receiver/TV is connected.
 - Consult an experienced radio/TV technician for help.
3. The power supply that is provided with this unit is only intended for use with this product. Do not use this power supply with any other product or do not use any other power supply that is not approved for use with this product by NetComm. Failure to do so may cause damage to this product, fire or result in personal injury.

3. Consumer Protection Laws

Australian and New Zealand consumer law in certain circumstances implies mandatory guarantees, conditions and warranties which cannot be excluded by NetComm and legislation of another country's Government may have a similar effect (together these are the **Consumer Protection Laws**). Any warranty or representation provided by NetComm is in addition to, and not in replacement of, your rights under such Consumer Protection Laws.

If you purchased our goods in Australia and you are a consumer, you are entitled to a replacement or refund for a major failure and for compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure. If you purchased our goods in New Zealand and are a consumer you will also be entitled to similar statutory guarantees.

4. Product Warranty

All NetComm products have a standard one (1) year warranty from date of purchase, however, some products have an extended warranty option (refer to packaging and the warranty card) (each a **Product Warranty**). To be eligible for the extended warranty option you must supply the requested warranty information to NetComm within 30 days of the original purchase by registering online via the NetComm web site at www.netcomm.com.au. For all Product Warranty claims you will require proof of purchase. All Product Warranties are in addition to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see Section 3 above).

Subject to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see Section 3 above), the Product Warranty is granted on the following conditions:

1. the Product Warranty extends to the original purchaser (you / the customer) and is not transferable;
2. the Product Warranty shall not apply to software programs, batteries, power supplies, cables or other accessories supplied in or with the product;
3. the customer complies with all of the terms of any relevant agreement with NetComm and any other reasonable requirements of NetComm including producing such evidence of purchase as NetComm may require;
4. the cost of transporting product to and from NetComm's nominated premises is your responsibility;
5. NetComm does not have any liability or responsibility under the Product Warranty where any cost, loss, injury or damage of any kind, whether direct, indirect, consequential, incidental or otherwise arises out of events beyond NetComm's reasonable control. This includes but is not limited to: acts of God, war, riot, embargoes, acts of civil or military authorities, fire, floods, electricity outages, lightning, power surges, or shortages of materials or labour; and
6. the customer is responsible for the security of their computer and network at all times. Security features may be disabled within the factory default settings. NetComm recommends that you enable these features to enhance your security.

Subject to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see Section 3 above), the Product Warranty is automatically voided if:

1. you, or someone else, use the product, or attempt to use it, other than as specified by NetComm;
2. the fault or defect in your product is the result of a voltage surge subjected to the product either by the way of power supply or communication line, whether caused by thunderstorm activity or any other cause(s);
3. the fault is the result of accidental damage or damage in transit, including but not limited to liquid spillage;
4. your product has been used for any purposes other than that for which it is sold, or in any way other than in strict accordance with the user manual supplied;
5. your product has been repaired or modified or attempted to be repaired or modified, other than by a qualified person at a service centre authorised by NetComm; or
6. the serial number has been defaced or altered in any way or if the serial number plate has been removed.

5. Limitation of Liability

This clause does not apply to New Zealand consumers.

Subject to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see Section 3 above), NetComm accepts no liability or responsibility, for consequences arising from the use of this product. NetComm reserves the right to change the specifications and operating details of this product without notice.

If any law implies a guarantee, condition or warranty in respect of goods or services supplied, and NetComm's liability for breach of that condition or warranty may not be excluded but may be limited, then subject to your rights and remedies under any applicable Consumer Protection Laws which cannot be excluded, NetComm's liability for any breach of that guarantee, condition or warranty is limited to: (i) in the case of a supply of goods, NetComm doing any one or more of the following: replacing the goods or supplying equivalent goods; repairing the goods; paying the cost of replacing the goods or of acquiring equivalent goods; or paying the cost of having the goods repaired; or (ii) in the case of a supply of services, NetComm doing either or both of the following: supplying the services again; or paying the cost of having the services supplied again.

To the extent NetComm is unable to limit its liability as set out above, NetComm limits its liability to the extent such liability is lawfully able to be limited.

Contact

Address: NETCOMM WIRELESS LIMITED Head Office
PO Box 1200, Lane Cove NSW 2066 Australia
P: +61(0)2 9424 2070 F: +61(0)2 9424 2010
E: sales@netcomm.com.au
W: www.netcomm.com.au