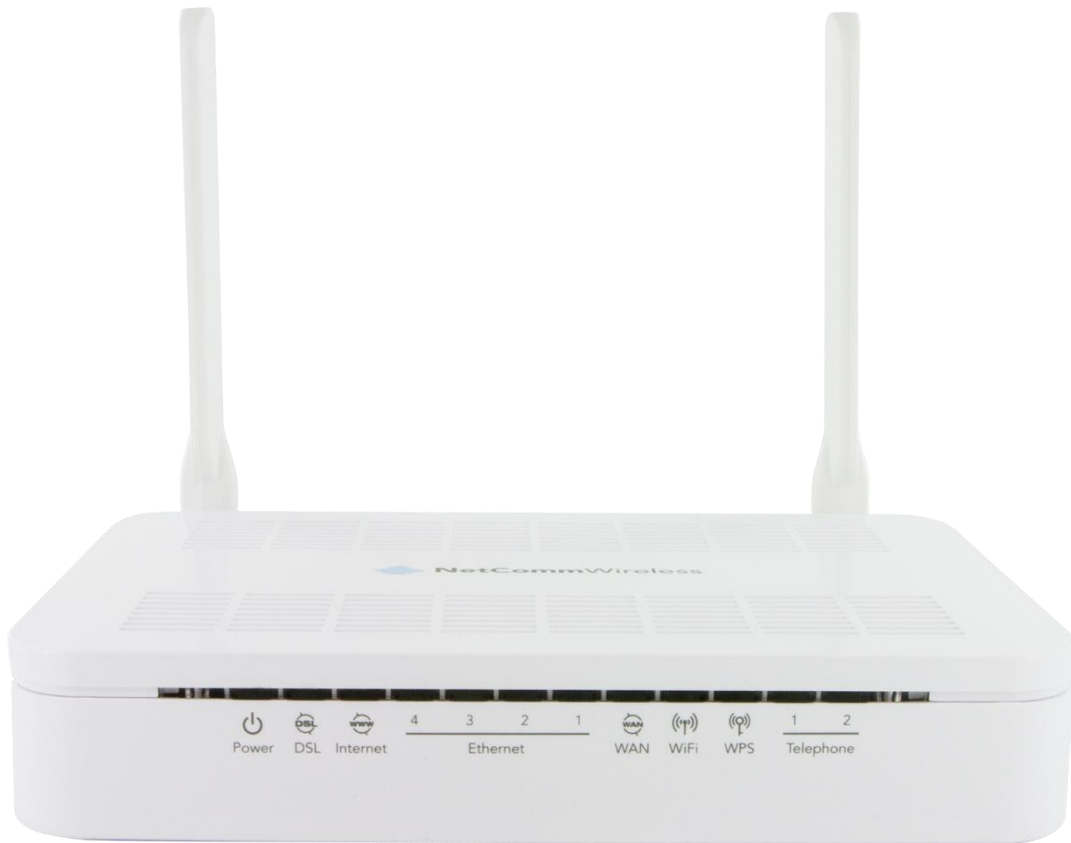


# VDSL/ADSL Dual Band AC1200 WiFi Gigabit Modem Router with VoIP

NF15ACV



## User Guide

## Important Notice

This device, like any wireless device, operates using radio signals which cannot guarantee the transmission and reception of data in all conditions. While the delay or loss of signal is rare, you should not rely solely on any wireless device for emergency communications or otherwise use the device in situations where the interruption of data connectivity could lead to death, personal injury, property damage, data loss, or other loss. NetComm Wireless accepts no responsibility for any loss or damage resulting from errors or delays in transmission or reception, or the failure of the NetComm Wireless device to transmit or receive such data.

#### Copyright

Copyright © 2016 NetComm Wireless Limited. All rights reserved.

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

Trademarks and registered trademarks are the property of NetComm Wireless Limited or their respective owners. Specifications are subject to change without notice. Images shown may vary slightly from the actual product.



**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 domestic 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 Wireless VDSL/ADSL Dual Band AC1200 WiFi Gigabit Modem Router with VoIP (NF15ACV)

DOCUMENT VERSION	DATE
1.0 - Initial document release	5 May 2016

*Table 1 - Document Revision History*

# Table of contents

<b>Overview</b> .....	<b>5</b>
Introduction .....	5
Target audience.....	5
Prerequisites .....	5
Notation .....	5
<b>Product introduction</b> .....	<b>6</b>
Product overview.....	6
Product features.....	6
Package contents.....	7
<b>Safety and product care</b> .....	<b>8</b>
<b>Transport and handling</b> .....	<b>8</b>
<b>Physical dimensions and indicators</b> .....	<b>9</b>
Physical dimensions .....	9
LED indicators.....	10
Interfaces .....	11
<b>Setting up your router</b> .....	<b>12</b>
Connecting the router to the Internet .....	14
<b>Advanced configuration</b> .....	<b>16</b>
<b>Status</b> .....	<b>17</b>
Device.....	17
IPv6 .....	18
ARP Table.....	18
<b>LAN</b> .....	<b>19</b>
<b>Wireless</b> .....	<b>20</b>
Wireless 2.4GHz/Wireless 5GHz .....	20
<b>WAN</b> .....	<b>26</b>
Ethernet WAN .....	26
DSL Settings .....	31
<b>Services</b> .....	<b>32</b>
VLAN on LAN .....	32
Dynamic DNS.....	32
Firewall.....	33
uPnP .....	37
RIP.....	38
<b>VoIP</b> .....	<b>39</b>
Phone 1/Phone 2 .....	39
Ring Tone.....	43
SIP Advance Setting .....	43
Call History.....	44
<b>Advanced</b> .....	<b>45</b>
Bridging .....	45
Routing .....	46
SNMP .....	47
Bridge Grouping .....	48
IP QoS .....	48
IPv6 .....	52
<b>Diagnostics</b> .....	<b>55</b>
Ping .....	55
Tracert .....	55
ATM Loopback.....	55
DSL Tone.....	57
ADSL Connection.....	57
<b>Admin</b> .....	<b>58</b>
Commit/Reboot.....	58
Backup/Restore .....	58
System Log.....	58
Password.....	60
Firmware Upgrade .....	60
ACL .....	61
Time Zone.....	61
TR-069.....	62
<b>Statistics</b> .....	<b>63</b>
Interface .....	63
DSL .....	64
<b>Appendix A: Default Settings</b> .....	<b>65</b>
<b>Legal &amp; Regulatory Information</b> .....	<b>66</b>
<b>Contact</b> .....	<b>69</b>

# Overview

## Introduction





This document provides you all the information you need to set up, configure and use the NetComm Wireless VDSL/ADSL Dual Band AC1200 WiFi Gigabit Modem Router with VoIP.

## Target audience

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

## Prerequisites

Before continuing with the installation of your device, please confirm that your equipment meets the minimum requirements below.

-  A configured Ethernet WAN connection.
-  A computer with Windows®, Mac OS®, or Linux-based operating systems with a working Ethernet adapter with TCP/IP Protocol installed.
-  A web browser such as Internet Explorer®, Google Chrome™, Mozilla Firefox®, Safari®, etc.
-  Wireless computer system requirements:
  - Computer with a working 802.11 b/g/n/ac wireless adapter.

## Notation

The following symbols are used in this user guide:



The following note requires attention.



The following note provides a warning.



The following note provides useful information.

# Product introduction

## Product overview

The NetComm Wireless NF15ACV residential VDSL2/ADSL2+ wireless 802.11ac gateway brings an advanced and reliable broadband experience to the home.

### UFB READY

Featuring VDSL2/ADSL2+ technologies as well as a Gigabit WAN port, the NF15ACV is a three-in-one gateway that provides access to DSL networks and all UFB fibre network options: FTTN, FTTB, FTTH.

### TRIPLE PLAY SERVICES

The NF15ACV is a triple play services enabler that supports the transmission of high-speed data with 4 Gigabit LAN ports, multi HD IPTV/OTT video streaming, VoIP feature for HD quality voice calls connecting up to 2 phones.

### ENHANCED WIRELESS EXPERIENCE

The NF15ACV embeds the newest generation of 802.11 AC WiFi for powerful access point and video grade wireless capabilities. The NF15ACV gateway allows both 2.4GHz and 5GHz bands to work concurrently, ensuring interoperability with all wireless equipment in the house.

The 2 x 2 external omni-directional antennas allow flexibility of configuration for an optimum reception and powerful signal across the home. Create a combined high-speed 1200 Mbps\* Wi-Fi home network and connect multitude of wireless devices such as TV, set top box, laptops, tablets, computers, NAS, smart phones and gaming consoles with great coverage and performance.

### MEDIA SHARING

Access and share A/V media and file content with all the connected devices in the house in real time. The NF15ACV becomes the media hub of the house using UPnP standard and enhanced wireless capabilities to create a reliable high-speed home network.








\* Maximum wireless signal rate and coverage values are derived from IEEE Standard 802.11n and 802.11ac 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.

## Product features

- 📶 Fully featured VDSL2 / ADSL2+/Ethernet WAN gateway – 4 x Gigabit Ethernet 10/100/1000 LAN ports
- 📶 VoIP Feature for HD quality voice calls. Connect up to 2 phones devices
- 📶 Wireless connectivity - next generation WiFi 802.11 AC1200 for multiple high-speed wireless connections
- 📶 WPS push button connect for the quick and easy secure connection of wireless devices
- 📶 Access and share media and file content across the wireless home network
- 📶 Device performance monitoring and management through TR-069\* optional

## Package contents




The NF15ACV package includes:

-  1 x NetComm Wireless NF15ACV VDSL/ADSL Dual Band AC1200 WiFi Gigabit Modem Router with VoIP
-  1 x 1.5m RJ45 Ethernet cable
-  1 x WiFi Security card
-  1 x Warranty card
-  1 x Power supply (12V/1.5A)
-  1 x RJ11 Telephone cable
-  1 x Quick start guide

If any of these items are missing or damaged, please contact NetComm Wireless Support immediately. The NetComm Wireless Support website can be found at: <http://support.netcommwireless.com>.

# 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.
-  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 router, 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.



# Physical dimensions and indicators

## Physical dimensions

Below is a list of the physical dimensions of the NF15ACV router.



DIMENSIONS	
Length	128 mm
Depth	184 mm
Height	34 mm
Weight	350 grams

*Table 2 - Device Dimensions*

## LED indicators

The NF15ACV router uses 12 LEDs to display the current system and connection status.







LED ICON	NAME	COLOUR / STATE	DESCRIPTION
	Power	Off	Powered off.
		Green	Powered on.
		Flashing Green	Device booting up.
	DSL	Green	Connected to DSLAM.
		Flashing green	Connecting to DSLAM
	Internet	Off	No internet connection present.
		Green	Internet is connected
		Flashing green	Transmitting/receiving data to/from the Internet.
Ethernet 1-4	Ethernet 1-4	Off	No device is connected to the Ethernet LAN port.
		Green	A device is connected to the Ethernet LAN port.
		Flashing green	Data is being sent or received via the Ethernet LAN port.
	WAN	Off	No device is connected to the Ethernet WAN port.
		Green	A device is connected to the Ethernet WAN port.
		Flashing green	Transmitting/receiving data to/from the WAN interface.
	WiFi	Off	WiFi is disabled.
		Green	2.4GHz WLAN access point operational
		Red	5GHz WLAN access point operational
		Amber	2.4GHz and 5GHz WLAN access points operational
		Flashing green	Transmitting/receiving data to/from the WLAN interface.
		Flashing red	Transmitting/receiving data to/from the WLAN interface
		Flashing amber	Transmitting/receiving data to/from the WLAN interface
	WPS	Green	WPS is enabled
		Flashing green	WPS function triggered. Trigger the WPS function on another with 2 minutes device to connect them.
Telephone 1-2	Telephone 1-2	Off	No VoIP service is configured.
		Green	VoIP registration successful.
		Flashing green	A telephone is in use.

Table 3 - LED Indicators

## Interfaces

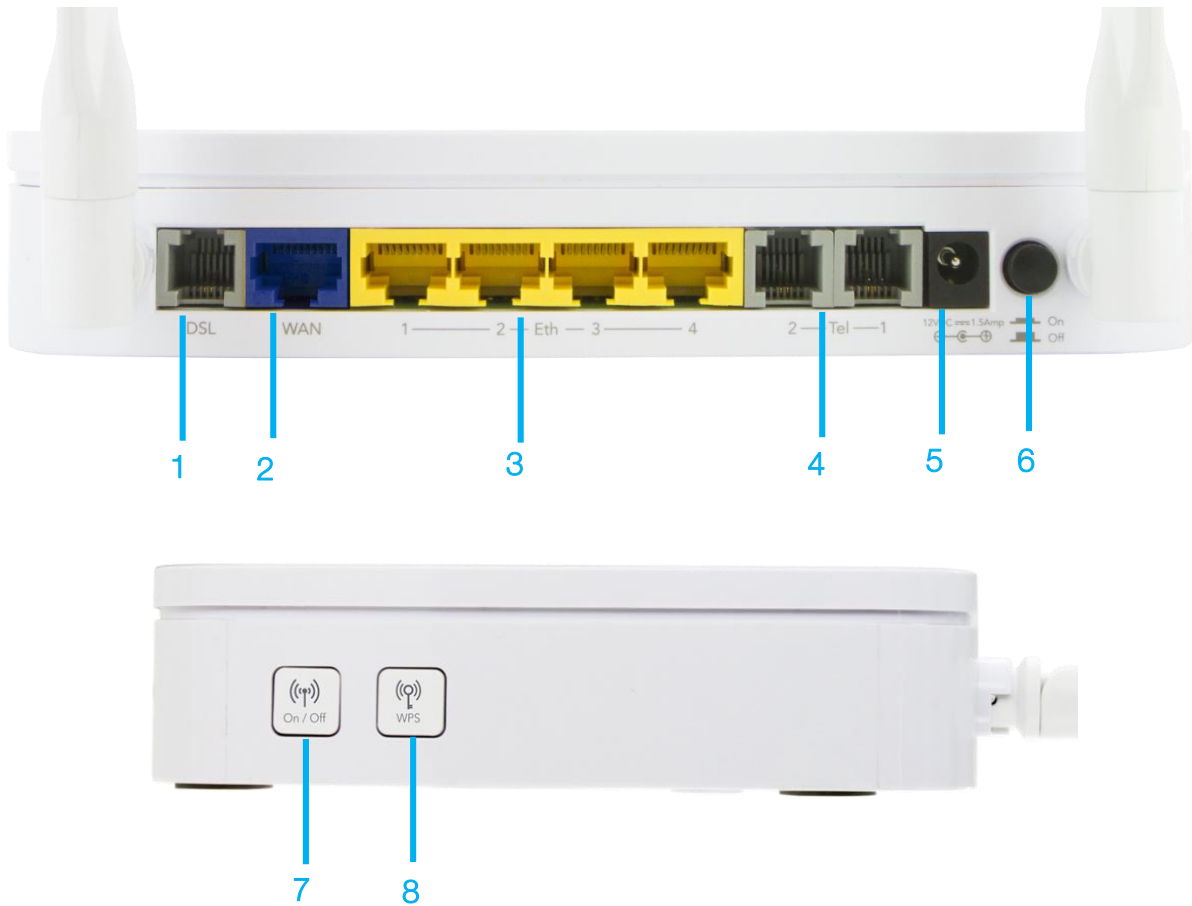


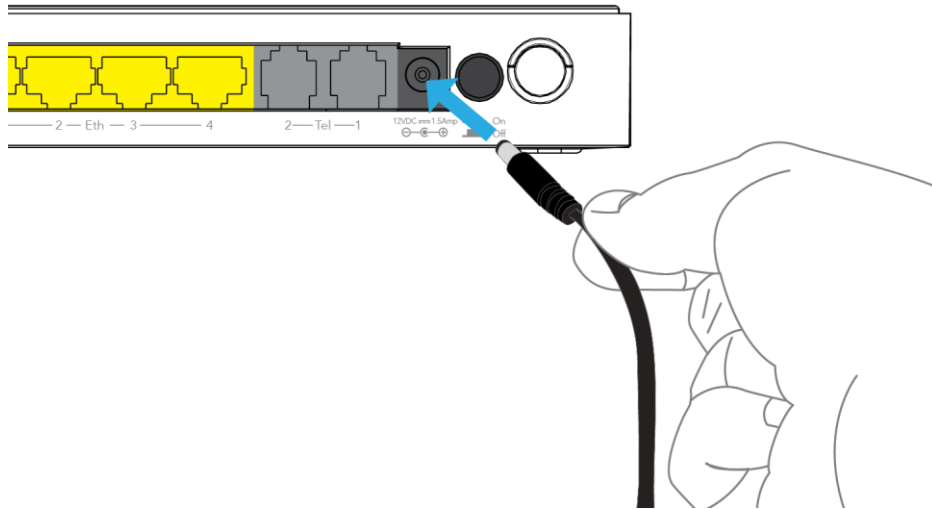
Figure 1 - Interfaces

NO.	ITEM	DESCRIPTION
1	DSL	Connect the included RJ11 cable here then connect the other end to the telephone wall socket or modem port of a DSL filter to provide the DSL connection for the modem.
2	WAN	Gigabit WAN port for connection to a WAN network.
3	LAN 1-4	Gigabit Ethernet LAN ports. Connect your Ethernet based devices to one of these ports for Gigabit-speed internet access.
4	Telephone 1-2	Phone ports for a standard PSTN analogue telephone handset. Connect phones to these ports with a VoIP provider to make use of a VoIP service.
5	Power jack	Connection point for the included power adapter. Connect the power supply here.
6	Power button	Turns the router on or off.
7	WiFi button	Hold button down for 3 seconds to turn Wireless radio on or off.
8	WPS button	Hold button down for 3 seconds to trigger the WPS function. When WPS has been triggered, press the WPS button on your other device to initiate a connection between the two devices.

Table 4 – Interfaces

# Setting up your router

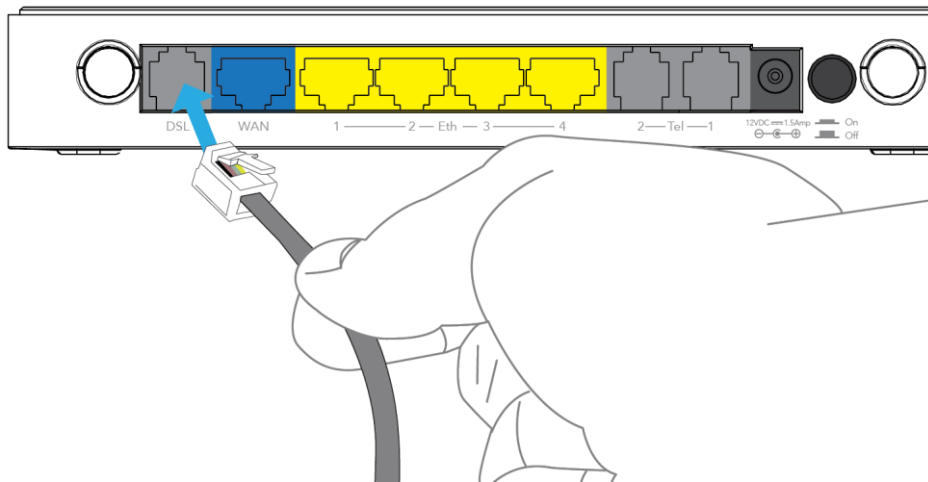
1. Connect the included power adapter to the power socket on the rear of the router then connect the other end of it to a wall power outlet.



2. Connect your internet service to the router.

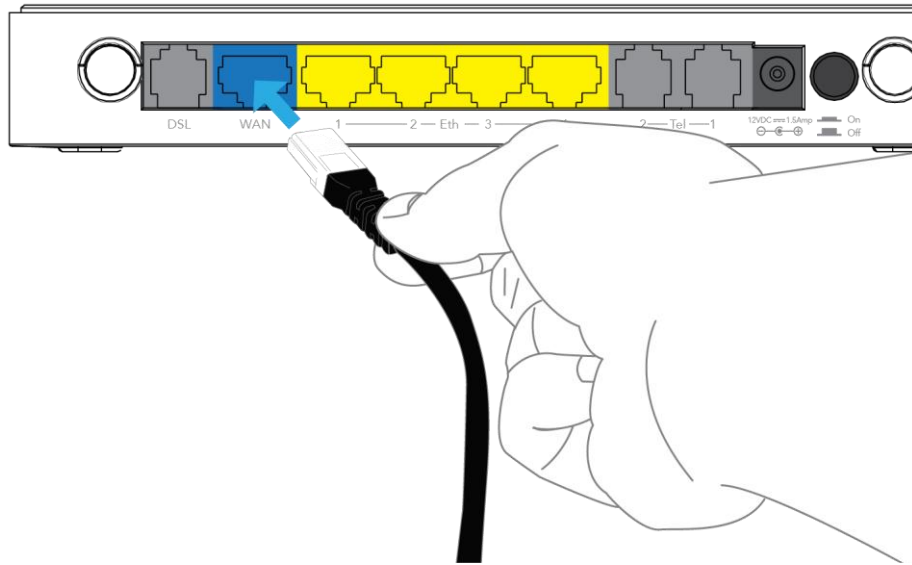
## DSL connections

- a. Attach one end of the included **Telephone cable** to the **DSL** port on the back of the router. Attach the other end to the telephone wall socket.



#### WAN/Fixed line connections (such as UFB)

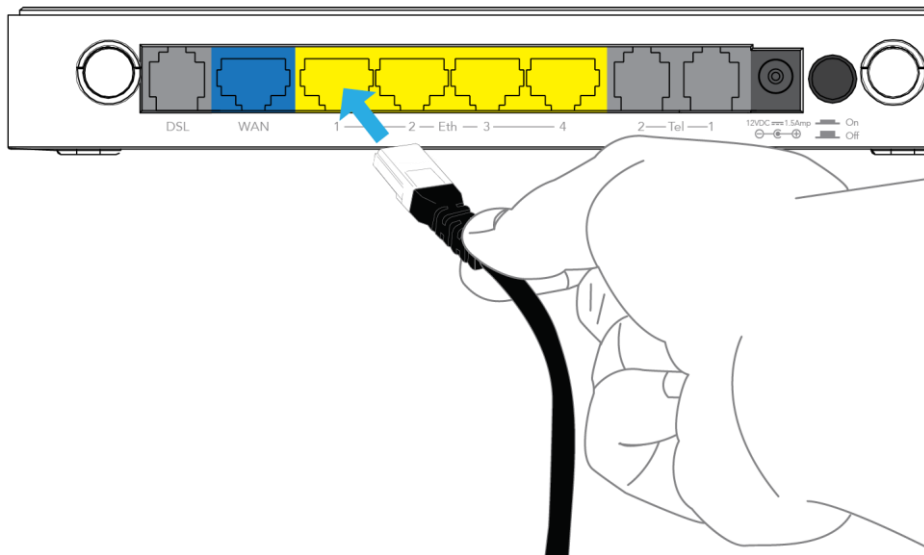
- b. Attach one end of the included **Ethernet cable** to the blue **WAN** port on the back of the router. Attach the other end to your UFB's Network Termination device.



#### Connecting via an Ethernet cable

If you want to connect your computer to the router via Ethernet cable, follow these instructions.

1. Connect an **Ethernet cable** to one of the yellow **LAN** ports on the back of the NF15ACV router.



2. Connect the other end of the **Ethernet cable** to your computer.

NOTE: There is only one Ethernet cable supplied. If you require more than one Ethernet cable, any standard CAT5e or CAT6 Ethernet cable is suitable.

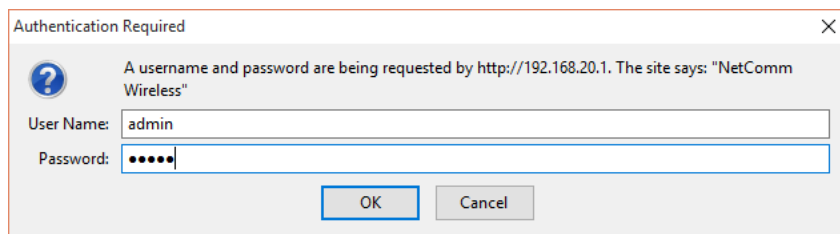
## Connecting via WiFi

1. Ensure WiFi is enabled on your device (e.g. computer/smartphone/gaming console).
2. Scan for wireless networks in your area and connect to the network name that matches the **Wireless Network Name** found on the **Wireless Security Card** (included in the box).
3. When prompted for your wireless security settings, enter the **Wireless Security Key** listed on your **Wireless Security Card**.

## Connecting the router to the Internet

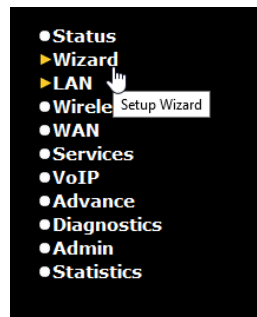
These steps guide you through configuring an Internet connection for your router.

1. After you have established a connection to the router using the previous steps, open your web browser and type **http://192.168.20.1** into the address bar at the top of the web browser window and press **Enter**.
2. Enter **admin** into both the Username and Password fields and click **OK**.



The Status page is displayed.

3. From the menu on the left side of the screen, select the **Wizard** item.



The Wizard is displayed.

4. From the **WAN Interface** drop down list, select your internet connection type.

### Wizard WAN Setup

This page is used to configure the parameters for WAN of your Router.

WAN Interface:

VPI:  VCI:

WAN Connection Type:

PPP User Name:  Password:

Enable VLAN:  VLAN ID:

5. Enter the details in the remaining fields as required by your ISP. If you do not have the details required, contact your ISP.

- By default, the 2.4GHz WiFi radio is turned on and the SSID (network name) is being broadcast. This means it is discoverable by wireless client devices when they perform a scan of nearby access points on the 2.4GHz spectrum. Use this page of the wizard to enable or disable the 2.4GHz WiFi radio and SSID Broadcast status or change the SSID name, Encryption type and the Pre-Shared Key. When you have finished, click the **Next** button.

### Wizard WiFi 2.4GHz Setup

This page is used to configure the parameters for WLAN clients which may connect to your Access Point.

Disable WLAN Interface

SSID:

Broadcast SSID:  Enabled  Disabled

Encryption:

Pre-Shared Key:

- By default, the 5GHz WiFi radio is turned on and the SSID (network name) is being broadcast. This means it is discoverable by wireless client devices when they perform a scan of nearby access points on 5GHz spectrum. Use this page of the wizard to enable or disable the 5GHz WiFi radio and SSID Broadcast status or change the SSID name, Security key type and the Security key. When you have finished, click the **Next** button.

### Wizard WiFi 5GHz Setup

This page is used to configure the parameters for WLAN clients which may connect to your Access Point.

Disable WLAN Interface

SSID:

Broadcast SSID:  Enabled  Disabled

Encryption:

Pre-Shared Key:

- This page allows you to configure the “administrator” and “user” passwords used to access the configuration pages. We highly recommend that you change the password from the default setting to protect your router from unauthorized access. From the **User Name** drop down list, select the **admin** or **user** account then enter the old password and new passwords in the respective fields. When you have finished, click the **Submit** button.

### Wizard Router Security

This page is used to set the account to access the web server of your Router. Empty user name and password will disable the protection.

User Name:

Old Password:

New Password:

Confirmed Password:

A pop-up message is displayed informing you that the router must be rebooted for the changes to take effect.

- Click the **OK** button. The router reboots with the new settings and connects to the internet using the settings you specified.

# Advanced configuration

The NF15ACV router comes with pre-configured settings that should suit most customers. For advanced configuration, log in to the web-based user interface of the router.

To log in to the web-based user interface:

1. Open a web browser (e.g. Google Chrome™, Mozilla Firefox®), type <http://192.168.20.1> into the address bar and press **Enter**. The log in prompt is displayed.

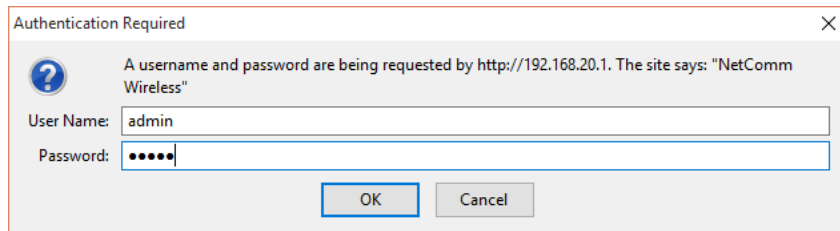


Figure 2 – Log in prompt for the web-based user interface

2. Enter the login username and password. If this is the first time you are logging in or you have not previously configured the password for the admin account, you can use the default account details to log in. The default log in credentials are:


Username: **admin**

Password: **admin**



Note: For security reasons, we highly recommend that you change the password of the admin account upon initial installation. You can do so by navigating to the Admin > Password.

The Status page is displayed when you have successfully logged in.

VDSL/ADSL Dual Band AC1200 WiFi Gigabit Modem Router with VOIP **NF15ACV**
 **NetCommWireless**

- **Status**
- ▶ Device
- ▶ IPv6
- ▶ ARP Table
- ▶ Wizard
- ▶ LAN
- Wireless
- WAN
- Services
- VoIP
- Advanced
- Diagnostics
- Admin
- Statistics

### Router Status

This page shows the current status and some basic settings of the device.

<b>System</b>	
Model Name	NF15ACV
Uptime	3 min
Firmware Version	NF15ACV_v1.2.42_NET712
HW Serial Number	18F14539EE01
DSP Version	v134f915
DNS Server	
IPv4 Default Gateway	
IPv6 Default Gateway	
<b>DSL</b>	
Operational Status	ACTIVATING
Upstream Speed	0 kbps
Downstream Speed	0 kbps
CO Vendor ID	
<b>LAN Configuration</b>	
IP Address	192.168.20.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC Address	18F14539EE00
<b>VoIP Port 1 Proxy0</b>	
Display Name	Phone1_Account1
Number	09103790
Register Status	VoIP Restart...
<b>VoIP Port 1 Proxy1</b>	
Display Name	Phone1_Account2
Number	
Register Status	Disabled
<b>VoIP Port 2 Proxy0</b>	
Display Name	Phone2_Account1
Number	09212697
Register Status	VoIP Restart...
<b>VoIP Port 2 Proxy1</b>	
Display Name	Phone2_Account2
Number	
Register Status	Disabled



# Status

## Device

The status page of the web interface provides system related information and is displayed when you log in to the NF15ACV router management console. The Device status page shows System, DSL, LAN Configuration, and VoIP port configuration details.

The menu on the left side of the screen can be used to navigate through the different configuration pages of the router.

VDSL/ADSL Dual Band AC1200 WiFi Gigabit Modem Router with VOIP **NF15ACV**

- Status
- ▶ Device
- ▶ IPv6
- ▶ ARP Table
- ▶ Wizard
- ▶ LAN
- Wireless
- WAN
- Services
- VoIP
- Advanced
- Diagnostics
- Admin
- Statistics

### Router Status

This page shows the current status and some basic settings of the device.

System	
Model Name	NF15ACV
Uptime	3 min
Firmware Version	NF15ACV_v1.2.42_NET712
HW Serial Number	18F14539EE01
DSP Version	v134f915
DNS Server	
IPv4 Default Gateway	
IPv6 Default Gateway	
DSL	
Operational Status	ACTIVATING.
Upstream Speed	0 kbps
Downstream Speed	0 kbps
CO Vendor ID	
LAN Configuration	
IP Address	192.168.20.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC Address	18F14539EE00
VoIP Port 1 Proxy0	
Display Name	Phone1_Account1
Number	09103790
Register Status	VoIP Restart...
VoIP Port 1 Proxy1	
Display Name	Phone1_Account2
Number	
Register Status	Disabled
VoIP Port 2 Proxy0	
Display Name	Phone2_Account1
Number	09212697
Register Status	VoIP Restart...
VoIP Port 2 Proxy1	
Display Name	Phone2_Account2
Number	
Register Status	Disabled

Figure 3 - Router status page

## IPv6

The IPv6 Status page displays LAN IPv6 addresses, prefix delegation and WAN configuration.

### IPv6 Status

This page shows the current system status of IPv6.

LAN Configuration					
IPv6 Address	fc01::1af1:45ff:fe39:ee00/64				
IPv6 Link-Local Address	fe80::1af1:45ff:fe39:ee00/64				
Prefix Delegation					
Prefix					
WAN Configuration					
Interface	VPI/VCI	Encapsulation	Protocol	IP Address	Status
ppp0_vc0_0	8/35	LLC	PPPoE		down
ppp1_ptm0_0	---	---	PPPoE		down
nas0_0	---	---	IPv6		down
<input type="button" value="Refresh"/>					

## ARP Table

The ARP Table displays a list of resolved MAC addresses.

### ARP Table

This table shows a list of learned MAC addresses.

IP Address	MAC Address
192.168.20.100	2c-44-fd-12-3c-6e
<input type="button" value="Refresh"/>	

# LAN

The LAN Interface Settings page displays information about your LAN IP address and allows you to change the address and subnet mask assigned to your device.

Here you can also configure the DHCP mode. DHCP may be disabled, set to DHCP Relay or run as a DHCP server (default). DHCP is an automatic method of assigning an IP address to devices on your network when they are connected. In most cases, these settings will not need to be changed.

## LAN Interface Settings

This page is used to configure the LAN interface of your Router. Here you may change the setting for IP addresses, subnet mask, etc..

---

IP Address:	<input type="text" value="192.168.20.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
<input type="checkbox"/> Secondary IP	
IGMP Snooping:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Ethernet to Wireless Blocking:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

---

DHCP Mode:  None  DHCP Relay  DHCP Server

Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

---

IP Pool Range:	<input type="text" value="192.168.20.100"/> - <input type="text" value="192.168.20.200"/>
	<input type="button" value="Show Client"/>
Max Lease Time:	<input type="text" value="86400"/> seconds (-1 indicates an infinite lease)
Domain Name:	<input type="text" value="NetComm.Wireless"/>
option 60(Network):	<input type="text" value="network_id"/>
option 60(Local):	<input type="text" value="local_id"/>
DNS option:	<input checked="" type="radio"/> Use DNS Relay <input type="radio"/> Set Manually
<input type="button" value="Port-Based Filter"/>	<input type="button" value="MAC-Based Assignment"/>
<input type="button" value="Apply Changes"/>	

# Wireless

## Wireless 2.4GHz/Wireless 5GHz

### Basic Settings

The WLAN Basic Settings page for both the 2.4GHz and 5GHz wireless radios provide the most common settings that you might need to configure in setting up your wireless network.

#### WLAN Basic Settings

This page is used to configure the parameters for WLAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Disable WLAN Interface

Band:

Mode:

SSID:

Channel Width:

Control Sideband:

Channel Number:

Radio Power (%):

Associated Clients:

#### WLAN Basic Settings

This page is used to configure the parameters for WLAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Disable WLAN Interface

Band:

Mode:

SSID:

Channel Width:

Control Sideband:

Channel Number:

Radio Power (%):

Associated Clients:

Refer to the table below for a description of each field.

FIELD	DESCRIPTION
Disable Wireless LAN Interface	Enable/disable the wireless LAN interface.
Band	Select the desired band from the list. Using a combination of bands allows for compatibility with legacy devices.
Mode	Configures the mode of the Wireless LAN interface.
Multiple AP	Enables multiple access points. When enabled, you can have up to four separate access points (networks). See the Multiple Aps screenshot below.
SSID	Specifies the network name. Each Wireless LAN network uses a unique Network Name to identify the network. This name is called the Service Set Identifier (SSID). When you set up your wireless adapter, you specify the SSID. If you want to connect to an existing network, you must use the name for that network. If you are setting up your own network you can make up your own name and use it on each computer. The name can be up to 32 characters long and contain letters and numbers.
Channel Width	Choose a channel width from the drop down list. Generally speaking, this should not be changed from the default setting unless you are aware of the effect that the change will have.
Control Sideband	Select a control sideband. Generally speaking, this should not be changed from the default setting unless you are aware of the effect that the change will have.
Channel Number	Select a channel number for the wireless network. When using multiple APs, ensure that you assign a different channel number to each AP to avoid signal interference.
Radio Power (mW)	The maximum output power of the radio. Generally speaking, this should not be changed from the default setting unless you are aware of the effect that the change will have.

To enable multiple APs, click the Multiple AP button. You can enable up to four APs and configure each AP from the page displayed. Refer to the screenshot below.

### Multiple APs

This page shows and updates the wireless setting for multiple APs.

Blocking between VAP:  Disable  Enable

No.	Enable	Band	SSID	Data Rate	Broadcast SSID	WMM	Relay Blocking	Active Client List
AP1	<input type="checkbox"/>	2.4 GHz (B+G+N) ▾	AP-1	Auto ▾	Enabled ▾	Enabled ▾	Disabled ▾	Show
AP2	<input type="checkbox"/>	2.4 GHz (B+G+N) ▾	AP-2	Auto ▾	Enabled ▾	Enabled ▾	Disabled ▾	Show
AP3	<input type="checkbox"/>	2.4 GHz (B+G+N) ▾	AP-3	Auto ▾	Enabled ▾	Enabled ▾	Disabled ▾	Show
AP4	<input type="checkbox"/>	2.4 GHz (B+G+N) ▾	AP-4	Auto ▾	Enabled ▾	Enabled ▾	Disabled ▾	Show

Apply Changes

Reset

## Advanced Settings

These settings are for technically advanced users who would like to fine tune their network. These settings should not be changed from the default setting unless you are aware of the effect that the change will have.

### WLAN Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about WLAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Fragment Threshold:  (256-2346)  
 RTS Threshold:  (0-2347)  
 Beacon Interval:  (20-1024 ms)  
 Data Rate:  ▾  
 Preamble Type:  Long Preamble  Short Preamble  
 Broadcast SSID:  Enabled  Disabled  
 Relay Blocking:  Enabled  Disabled  
 Protection:  Enabled  Disabled  
 Aggregation:  Enabled  Disabled  
 Short GI:  Enabled  Disabled  
 WMM Support:  Enabled  Disabled

Apply Changes

FIELD	DESCRIPTION
Fragment Threshold	When transmitting a packet over a network medium, sometimes the packet is broken into several segments, if the size of packet exceeds that allowed by the network medium. The Fragmentation Threshold defines the number of bytes used for the fragmentation boundary for directed messages. This value should remain at its default setting of 2346. It specifies the maximum size for a packet before data is fragmented into multiple packets.  If you experience a high packet error rate, you may slightly reduce the "Fragment Threshold" value within the value range of 256 to 2346. Setting this value too low may result in poor network performance. Only minor modifications of this value are recommended.
RTS Threshold	This value should remain at its default setting of 2347. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the preset "RTS threshold" size, the RTS/CTS mechanism will not be enabled. The DSL modem (or AP) sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.
Beacon Interval	The Beacon Interval value indicates the broadcast frequency of the SSID beacon. Enter a value between 20 and 1024. The default is 100.
Data Rate	The rate of data transmission should be set depending on the speed of your wireless network. You should select from a range of transmission speeds, or you can select Auto to have the Access Point automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the AP and a wireless client. The default setting is Auto.
Preamble Type	Specify the Preamble type is short preamble or long preamble.
Broadcast SSID	Broadcast or Hide SSID to your Network. Default: Enabled Broadcast
Relay Blocking	Disable or enable Relay blocking.
Protection	A protection mechanism which prevents collisions among 802.11g nodes.
Aggregation	Disable or enable Aggregation.
Short GI	Disable or enable Short guard interval.
WMM Support	Enables or disables WiFi Multimedia support.

## Security

This page allows you to configure wireless security. We recommend using WPA2 or WPA2 Mixed for the highest security.

### WLAN Security Settings

This page allows you setup the WLAN security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

---

SSID Type:

---

Encryption:

Authentication Mode:  Enterprise (RADIUS)  Personal (Pre-Shared Key)

WPA Cipher Suite:  TKIP  AES

WPA2 Cipher Suite:  TKIP  AES

Pre-Shared Key Format:

Pre-Shared Key:  [Click it to display](#)

FIELD	DESCRIPTION
SSID Type	Select the SSID when multiple SSID is used.
Encryption	There are 4 types of security to be selected. To secure your WLAN, it's strongly recommended to enable this feature. WEP: Make sure that all wireless devices on your network are using the same encryption level and key. Click Set WEP Key button to set the encryption key. WPA /WPA2: WPA/WPA2, also known as 802.11i, uses Advanced Encryption Standard (AES) for data encryption. AES utilized a symmetric 128-bit block data encryption. The most secure choice is WPA2. WAP2 Mixed: The AP supports WPA and WPA2 for data encryption. The actual selection of the encryption methods will depend on the clients.
Use 802.1x Authentication	Check it to enable 802.1x authentication. This option is selectable only when the "Encryption" is choose to either None or WEP. If the "Encryption" is WEP, you need to further select the WEP key length to be either WEP 64bits or WEP 128bits.
WPA Authentication Mode	There are 2 types of authentication mode for WPA. Enterprise (RADIUS): WPA RADIUS uses an external RADIUS server to perform user authentication. To use WPA RADIUS, enter the IP address of the RADIUS server, the RADIUS port (default is 1812) and the shared secret from the RADIUS server. Please refer to "Authentication RADIUS Server" setting below for RADIUS setting. The WPA algorithm is selected between TKIP and AES, please refer to "WPA cipher Suite" below. Personal (Pre-Shared Key): Pre-Shared Key authentication is based on a shared secret that is known only by the parties involved. To use WPA Pre-Shared Key, select key format and enter a password in the "Pre-Shared Key Format" and "Pre-Shared Key" setting respectively. Please refer to "Pre-Shared Key Format" and "Pre-Shared Key" setting below.
Pre-Shared Key Format	PassPhrase: Select this to enter the Pre-Shared Key secret as user-friendly textual secret. Hex (64 characters): Select this to enter the Pre-Shared Key secret as hexadecimal secret.
Pre-Shared Key	Specify the shared secret used by this Pre-Shared Key. If the "Pre-Shared Key Format" is specified as PassPhrase, then it indicates a passphrase of 8 to 63 bytes long; or if the "Pre-Shared Key Format" is specified as PassPhrase, then it indicates a 64-hexadecimal number.
Authentication RADIUS Server	If "WPA Authentication Mode" is set to WPA-RADIUS, the port (default is 1812), IP address and password of external RADIUS server are specified here.

## Access Control

Access Control is a means of securing your wireless network such that only the devices listed (by MAC address) are allowed to join the network. You may also use this function to block connection from specified devices. While this is not an entirely foolproof method of securing a network, it should be used in conjunction with other measures as an additional layer of security to decrease the risk of attack. MAC Address can be spoofed to change a computer's identity.

### WLAN Access Control

If you choose 'Allowed Listed', only those WLAN clients whose MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these WLAN clients on the list will not be able to connect the Access Point.

Mode:

MAC Address:  (ex. 00E086710502)

#### Current Access Control List:

MAC Address	Select
<input type="button" value="Delete Selected"/>	<input type="button" value="Delete All"/>

To edit the access control list:

- From the **Mode** drop down list, select either Allow Listed or Deny Listed. When Allow Listed is selected, all other MAC Addresses will be blocked.
- In the **MAC address** field, enter the MAC address of the device to allow or deny. The MAC address should be entered with no spaces or symbols between the characters, e.g. 00E086710502.
- Click on the **Add** button. The MAC address is listed in the Current Access Control List. To remove a device from the list, you can click the box in the **Select** column and then select **Delete Selected**.

## WPS

While WiFi networks have become ubiquitous around the world, many users still have difficulty in configuring a connection between two devices. WPS is a method of simplifying the connection so that the user needs no knowledge of specific settings. The simplest way of connecting two WPS certified devices is by pressing the WPS button (PBC) on each device within two minutes of each other. If Push Button Connect is not supported by both devices, you can use the PIN method where a PIN is set on one device and the other device must enter the PIN in order to authenticate on the network.

### Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your WLAN client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

---

**Disable WPS**

**WPS Status:**                       Configured     UnConfigured

**Auto-lock-down state:**        Unlocked   

**Self-PIN Number:**                 

**Push Button Configuration:**   

**Current Key Info:**

Authentication	Encryption	Key
WPA2-Mixed PSK	AES	TESTING123

---

**Client PIN Number:**               

The NF15ACV supports both PIN and Push Button Connect (PBC) methods. To use PBC, no configuration is required.

To use the PIN method as the registrar:

1. Ensure that the **Disable WPS** item is not selected.
2. Press the **Regenerate PIN** button to have a random PIN generated automatically.
3. Click the **Start PBC** button to begin the WPS connection.
4. On your other device, press the WPS button and enter the Self-PIN Number to connect when prompted.

To use the PIN method as a client:

1. In the **Client PIN Number** field, enter the PIN from the other device.
2. Press the WPS button on the other device.
3. Press the **Start PIN** button on the NF15ACV interface.



## Status

The WLAN Status pages display a summary of the configuration of each wireless network.

### WLAN Status

This page shows the WLAN current status.

---

WLAN Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	NF15ACV
Channel Number	1
Encryption	WPA2 Mixed
BSSID	18:f1:45:39:ee:05
Associated Clients	0

### WLAN Status

This page shows the WLAN current status.

---

WLAN Configuration	
Mode	AP
Band	5 GHz (A+N+AC)
SSID	NF15ACV 5G
Channel Number	36
Encryption	WPA2 Mixed
BSSID	18:f1:45:39:ee:00
Associated Clients	0

# WAN

## Ethernet WAN

This section discusses how to configure your NF15ACV to use the WAN port to connect to the Internet.

### Ethernet WAN

This page is used to configure the parameters for Ethernet WAN of your Router.

---

nas0\_0 ▾

Enable VLAN:       VLAN ID:       802.1p\_Mark

Channel Mode:  ▾

Enable NAPT:       Enable QoS:

Admin Status:  Enable  Disable      MTU:(max: PPPoE 1492, IPoE 1500)

Connection Type:  ▾

---

IP Protocol:  ▾

---

**WAN IP Settings:** Type:  Fixed IP  DHCP

Local IP Address:       Remote IP Address:

Subnet Mask:       Unnumbered

Send option60:  Enable  Disable      option60:

Request DNS:  Enable  Disable

Primary DNS Server:

Secondary DNS Server:

---

**IPv6 WAN Setting:**

Address Mode:  Slaac  Static

Enable DHCPv6 Client:

To connect to the Internet using DHCP:

1. From the **Channel Mode** drop down list, select **IPoE**.
2. Select **Enable NAPT**.
3. From the **Connection Type** drop down list, select **VOICE\_INTERNET\_TR\_069**.
4. From the **IP Protocol** drop down list, select **IPv4/IPv6** for IPv6 dual stack, else select **IPv4**.
5. From the **WAN IP Settings Type** settings, select **DHCP**.
6. Configure the IPv6 WAN Settings as per your ISPs requirements.
7. Click **Apply Changes**.

To connect to the Internet using a Fixed IP:

1. From the **Channel Mode** drop down list, select **IPoE**.
2. Select **Enable NAPT**.
3. From the **Connection Type** drop down list, select **VOICE\_INTERNET\_TR\_069**.
4. From the **IP Protocol** drop down list, select **IPv4/IPv6**.
5. From the **WAN IP Settings Type** settings, select **Fixed IP**.

6. Enter **Local IP Address**, **Subnet Mask** and **Remote IP Address** as provided by your ISP.
7. Configure the IPv6 WAN Settings as per your ISPs requirements.
8. Click **Apply Changes**.

To connect using a PPPoE connection:

1. From the **Channel Mode** drop down list, select **PPPoE**.
2. Select **Enable NAPT**.
3. From the **Connection Type** drop down list, select **VOICE\_INTERNET\_TR\_069**.
4. From the **IP Protocol** drop down list, select **IPv4/IPv6**.
5. Enter the PPPoE Authentication Username and Password provided by your ISP.
6. Configure the IPv6 WAN Settings as per your ISPs requirements.
7. Click **Apply Changes**.

Configuring a Bridged connection:

1. From the **Channel Mode** drop down list, select **Bridged**.
2. From the **Connection Type** drop down list, select **VOICE\_INTERNET\_TR\_069**.
3. Click **Apply Changes**.
4. Load your PPPoE client software on your PC and follow its set up instructions.

## VDSL WAN

If you have a VDSL connection, use this page to configure the connection settings.

### VDSL WAN

This page is used to configure the parameters for VDSL WAN of your Router.

---

ptm0\_0 ▾

Enable VLAN:       VLAN ID:       802.1p\_Mark  ▾

Channel Mode: PPPoE ▾

Enable NAPT:       Enable QoS:

Admin Status:  Enable  Disable      MTU:(max:PPPoE 1492, IPoE 1500)

Connection Type: VOICE\_INTERNET\_TR069 ▾

---

IP Protocol: IPv4/IPv6 ▾

---

**PPP Settings:** User Name:       Password:

Type: Continuous ▾      Idle Time (sec):

Authentication Method: AUTO ▾      AC-Name:

Service-Name:

---

**IPv6 WAN Setting:**

Address Mode:  Slaac  Static

Enable DHCPv6 Client:

To configure a VDSL WAN connection:

1. From the **Channel Mode** drop down list, select the type of VDSL connection.
2. Select **Enable NAPT**.
3. From the **Connection Type** drop down list, select **VOICE\_INTERNET\_TR\_069**.
4. From the **IP Protocol** drop down list, select **IPv4/IPv6**.
5. Configure the remaining settings as per your ISPs requirements.
6. Click **Apply Changes**.

## ADSL WAN

### ADSL WAN

This page is used to configure an ADSL WAN connection. Before continuing, ensure that you have the VPI, VCI, Encapsulation, Channel Mode (most commonly PPPoE or PPPoA), PPPoE/A Authentication Username and Password for your account. These can be obtained from your Internet Service Provider.

#### ADSL WAN Configuration

This page is used to configure the parameters for ADSL WAN of your Router.

VPI:  VCI:  Encapsulation:  LLC  VC-Mux Channel Mode:

Enable NAPT:  Enable QoS:

Admin Status:  Enable  Disable

Connection Type:

Enable VLAN:  Disable  Enable VLAN ID(0-4095):  802.1p\_Mark:

Enable IGMP:

IP Protocol:

**PPP Settings:** User Name:  Password:

Type:  Idle Time (sec):

#### IPv6 WAN

##### Setting:

Address Mode:  Slaac  Static

Enable DHCPv6 Client:

Request Options:

Request Address

Request Prefix

#### Current ATM VC Table:

Select	Interface	Mode	VPI	VCI	Encapsulation	NAPT	Connection Type	IGMP	IP Address	Remote IP	Subnet Mask	User Name	Default Route	Status	Actions
<input checked="" type="radio"/>	ppp0_vc0_0	PPPoE	8	35	LLC	On	VOICE_INTERNET_TR069	Off				username	On	Enabled	

To configure an ADSL WAN connection:

1. Enter the **VCI** and **VPI** settings provided by your ISP.
2. Select the **Encapsulation** provided by your ISP.
3. From the **Channel Mode** drop down list, select the type of connection you have been assigned.
4. Select **Enable NAPT**.
5. Use the **Connection Type** drop down list to select the appropriate type of connection.
6. From the **IP Protocol** drop down list, select the IP Protocol, IPv4, IPv6 or dual stacks IPv4/IPv6 determined by your ISP.
7. Enter the **Username** and **Password** provided by your ISP.
8. Configure the **IPv6 WAN** setting determined by your ISP.

To modify an ADSL WAN connection:

1. Select Existing ATM/VC entry.
2. Modify values on fields.
3. Click "**Modify**" to save changes.

## ADSL Settings

This page assists in configuring QoS settings for the ADSL connection. These settings should not be changed unless you are aware of the effect they will have on your ADSL connection.

### ATM Settings

This page is used to configure the parameters for the ATM of your Router. Here you may change the setting for VPI, VCI, QoS etc ...

VPI:  VCI:  QoS:

PCR:  CDVT:  SCR:  MBS:

#### Current ATM VC Table:

Select	VPI	VCI	QoS	PCR	CDVT	SCR	MBS
<input type="radio"/>	8	35	UBR	6000	0	---	---

FIELD	DESCRIPTION
VPI	Virtual Path Identifier. This is field displays the VPI from the selected ATM VC from the Current ATM VC Table.
VCI	Virtual Channel Identifier. This is field displays the VCI from the selected ATM VC from the Current ATM VC Table.
QoS	Quality of Service is a characteristic of data transmission that measures how accurately and how quickly a message or data is transferred from a source host to a destination host over a network. The four QoS options are: –UBR (Unspecified Bit Rate): When UBR is selected, the SCR and MBS fields are disabled. –CBR (Constant Bit Rate): When CBR is selected, the SCR and MBS fields are disabled. –nrt-VBR (non-real-time Variable Bit Rate): When nrt-VBR is selected, the SCR and MBS fields are enabled. –rt-VBR (real-time Variable Bit Rate): When rt-VBR is selected, the SCR and MBS fields are enabled.
PCR	Peak Cell Rate, measured in cells/sec., is the cell rate which the source may never exceed.
SCR	Sustained Cell Rate, measured in cells/sec., is the average cell rate over the duration of the connection.
MBS	Maximum Burst Size, a traffic parameter that specifies the maximum number of cells that can be transmitted at the peak cell rate.

## DSL Settings

This page is used to configure the parameters for the bands of your router. Generally speaking, these settings should be left alone unless you are aware of the effect changing them will have on your service.

### DSL Settings

This page is used to configure the parameters for the bands of your Router.

---

**DSL Modulation:**

- G.Lite
- G.Dmt
- T1.413
- ADSL2
- ADSL2+
- VDSL2

**AnnexL Option:**

(Note: Only ADSL 2 supports AnnexL)

- Enabled

**AnnexM Option:**

(Note: Only ADSL 2/2+ support AnnexM)

- Enabled

**VDSL2 Profile:**

- 8a
- 8b
- 8c
- 8d
- 12a
- 12b
- 17a
- 30a

**ADSL Capability:**

- Enable Bitswap
- Enable SRA

Apply Changes

# Services

## VLAN on LAN

This service allows you to create up to 4 virtual LANs. Select the **Enable** option for the desired LAN number then enter a VLAN ID in the appropriate field. Click the Apply Changes button to save your configuration when you have finished.

### VLAN on LAN Configuration

This page be used to configure VLAN on LAN.

LAN1 VLAN ID:	<input type="text" value="0"/>	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
LAN2 VLAN ID:	<input type="text" value="0"/>	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
LAN3 VLAN ID:	<input type="text" value="0"/>	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
LAN4 VLAN ID:	<input type="text" value="0"/>	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable

## Dynamic DNS

If your Internet connection has a dynamic IP address that is an address which is frequently changing each time a connection is made, it can be difficult to keep up to date with the current IP address. Using a Dynamic DNS service allows your router to broadcast its current IP address to the dynamic DNS service and you are able to access your router with a static hostname.

### Dynamic DNS Configuration

This page is used to configure the Dynamic DNS address from DynDNS.org or TZO. Here you can Add/Remove to configure Dynamic DNS.

Enable:

DDNS Provider:

Hostname:

Interface:

DynDns Settings:

User Name:

Password:

#### Dynamic DNS Table:

Select	State	Hostname	User Name	Service	Status
--------	-------	----------	-----------	---------	--------

To configure a Dynamic DNS service:

1. Check the **Enable** check box.
2. From **DDNS Provider** drop-down list, select the dynamic DNS service provider.
3. Enter the **Hostname**.
4. Enter the **Username**.
5. Enter the **Password**.
6. Click the **Add** button.



# Firewall

## Port Forwarding

Port forwarding is a method of sending network packets to a specific machine behind a NAT (network address translation) firewall. It is only necessary to create a port forwarding rule if you are hosting a server of some sort, such as a web server, email server or game server on your private local network.

### Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Port Forwarding:  Enable  Disable

Enable  Application:

Comment	Local IP	Local Port from	Local Port to	Protocol	Remote IP	Remote Port from	Remote Port to	Interface
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any

**Current Port Forwarding Table:**

Select	Comment Local	IP Address	Protocol	Local Port	Enable	Remote Host	Public Port	Interface

To configure a port forwarding rule:

1. Check the option **Enable Port Forwarding** to enable port forwarding.
2. Click the **Apply Changes** button.
3. Use the **Comment** field to enter any comments about the rule to help you remember what it is for.
4. Enter the IP Address and port you want to be forwarded in **Local IP / Local Port to / Local Port from** fields. (Ensure IP Address is reserved or static before port forwarding)
5. From the **Protocol** drop-down list, select the whether to allow TCP packet, UDP packets or both.
6. Click the **Add** button.

## DMZ

A Demilitarized Zone (DMZ) Host is a computer without the protection of a firewall. It allows that particular computer unrestricted 2-way communication to the internet. It is mostly used for Hosting servers, Internet games, Video conferencing, Internet telephony and other special applications. When enabled, all packets sent to the router are forwarded to the DMZ Host IP Address.

### DMZ Configuration

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

DMZ Host:  Enable  Disable

DMZ Host IP Address:

To configure DMZ:

1. Check the **Enable** button for the **DMZ Host** option.
2. In the **DMZ Host IP Address** field, enter the IP Address of the DMZ Host that all packets will be forwarded to. (Ensure IP Address is reserved or static before DMZ will work)
3. Click the **Apply Changes** button.

## IP/Port Filtering

The IP/Port filtering page allows you to configure rules to deny or allow specific services or applications through the router firewall.

### IP/Port Filtering

Entries in this table are used to restrict certain types of data packets through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Outgoing Default Action  Deny  Allow

Incoming Default Action  Deny  Allow

Direction:  Protocol:  Rule Action  Deny  Allow

Source IP Address:  Subnet Mask:  Port:  -

Destination IP Address:  Subnet Mask:  Port:  -

**Current Filter Table:**

Select	Direction	Protocol	Source IP Address	Source Port	Destination IP Address	Destination Port	Rule Action
<input type="button" value="Delete Selected"/>	<input type="button" value="Delete All"/>						

Refer to the table below for a description of each field.

FIELD	DESCRIPTION
Outgoing Default Action	Specifies the default action on the LAN to WAN forwarding path.
Incoming Default Action	Specifies the default action on the WAN to LAN forwarding path.
Direction	The direction of the traffic rule.
Protocol	Select the desired protocol option. Available options are TCP, UDP and ICMP.
Rule Action	Deny or allow traffic when matching this rule.
Source IP Address	The source IP address assigned to the traffic for which filtering is applied.
Source Subnet Mask	The Subnet mask of the source IP.
Source Port	Starting and ending source port numbers.
Destination IP Address	The destination IP address assigned to the traffic for which filtering is applied.
Destination Subnet Mask	The Subnet mask of the destination IP.
Destination Port	Starting and ending destination port numbers.

## MAC Filtering

MAC Filtering is a method of allowing or denying a device access to the network by its MAC address. This method applies to both LAN and WLAN clients.

### MAC Filtering for bridge mode

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Outgoing Default Action  Deny  Allow  
 Incoming Default Action  Deny  Allow

---

Direction:    
 Source MAC Address:   
 Destination MAC Address:   
 Rule Action  Deny  Allow

**Current Filter Table:**

Select	Direction	Source MAC Address	Destination MAC Address	Rule Action
<input type="button" value="Delete Selected"/>	<input type="button" value="Delete All"/>			

FIELD	DESCRIPTION
Outgoing Default Action	Specifies the default action on the LAN to WAN bridging/forwarding path.
Incoming Default Action	Specifies the default action on the WAN to LAN bridging/forwarding path.
Direction	The direction of the traffic.
Source MAC Address	The source MAC address assigned to the traffic for which filtering is applied.
Destination MAC Address	The destination MAC address assigned to the traffic for which filtering is applied.
Rule Action	Deny or allow traffic when matching this rule.

## URL Filtering

The URL filtering feature allows you to specify keywords that appear in a site's domain name which are allowed or blocked when someone on the network attempts to access the site.

### URL Blocking Configuration

This page is used to configure the Blocked filtered keyword. Here you can add/delete filtered keyword.

URL Blocking:  Enable  Disable

---

Keyword:

**Keyword Filtering Table:**

Select	Filtered Keyword
<input type="button" value="Delete Selected"/>	<input type="button" value="Delete All"/>

To add a keyword to the URL blocking list:

1. Select the **Enable** option.
2. Click the **Apply Changes** button.
3. In the **Keyword** field, enter the keyword you wish to block.
4. Click the **Add** button.

## Domain Filtering

This feature is used to block a specific domain name.

### Domain Blocking Configuration

This page is used to configure the Blocked domain. Here you can add/delete the blocked domain.

Domain Blocking:  Enable  Disable

---

Domain:

**Domain Blocking Configuration:**

Select	Domain
<input type="checkbox"/>	

To add a domain name to the blocking list:

1. Select the **Enable** option.
2. Click the **Apply Changes** button.
3. In the **Domain** field, enter the domain name you wish to block, for example, www.domain.com
4. Click the **Add** button.

## Parental Control

Parental Control allows you to specify a combination of a time period and MAC/IP address to apply access restrictions. The MAC addresses you enter and the time periods restrict those devices from accessing the Internet at those times.

### Parental Control

Entries in this table are used to restrict access to Internet from your local PCs/devices by mac address and time interval. Use of such filters can be helpful for parents to control children's usage of Internet.

Parental Control:  Enable  Disable

---

Rule Name:

Specified PC:  IP Address  MAC Address

IP Address:  --

MAC Address:  (ex. 00e086710502)

Controlled Days: Sun  Mon  Tue  Wed  Thu  Fri  Sat

Start Blocking time:  :

End Blocking time:  :

#### Current Parent Control Table:

Name	IP Address	MAC Address	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start	End	Select

FIELD	DESCRIPTION
Parental Control	To use the parental control feature, select the <b>Enable</b> option then click the <b>Apply Changes</b> button.
Rule Name	Enter a display name for the rule. This should be descriptive of the rule so that is easily identifiable in the list of rules.
Specified PC	Select the method used to identify the computer on the network. Remember that IP addresses may change while the MAC address of a device is hard-coded and is more permanent.
IP Address	If you selected IP address for the Specified PC option, enter the IP address of the computer to restrict in this field.
MAC Address	If you selected MAC address for the Specified PC option, enter the MAC address of the network adapter to restrict in this field. The MAC address should be entered without any symbols between the characters.
Controlled Days	Select the days to which this rule should apply.
Start Blocking time	Enter the time (in 24-hour format) that the rule should begin taking effect.
End Blocking time	Enter the time (in 24-hour format) that the rule should stop taking effect.

When you have added all the details in the table above, click the **Add** button to add the rule to the Parental Control table. If you wish to turn on the parental control feature, ensure that you have selected the **Enable** option at the top of the screen and then click the **Apply Changes** button.

## uPnP

Universal Plug and Play is designed to support zero-configuration “invisible” networking and automatic discovery for a wide range of devices. This means that a device can dynamically join a network, obtain an IP address and broadcast its capabilities while learning about the presence and capabilities of other network devices.

### UPnP Configuration

This page is used to configure UPnP. The system acts as a daemon when you enable it and select WAN interface (upstream) that will use UPnP.

UPnP:  Enable  Disable

WAN Interface:

**Apply Changes**

## RIP

Routing Information Protocol is an Internet protocol you can set up to share routing table information with other routing devices on your LAN, at your ISP's location, or on remote networks connected to your network. Most small home or office networks do not need to use RIP; they have only one Router, such as the DSL Router, and one path to an ISP. In these cases, there is no need to share routes, because all Internet data from the network is sent to the same ISP gateway.

### RIP Configuration

Enable the RIP if you are using this device as a RIP-enabled Router to communicate with others using the Routing Information Protocol. This page is used to select the interfaces on your device that use RIP, and the version of the protocol used.

RIP:  Enable  Disable

Apply Changes

Interface:

Receive Mode:

Send Mode:

Add

#### RIP Config Table:

Select	Interface	Receive Mode	Send Mode
<input type="button" value="Delete Selected"/>	<input type="button" value="Delete All"/>		

FIELD	DESCRIPTION
Interface	The name of the interface on which you want to enable RIP.
Receive Mode	Indicate the RIP version in which information must be passed to the routing device in order for it to be accepted into its routing table.
Send Mode	Indicate the RIP version this interface will use when it sends its route information to other devices.

# VoIP

The NF15ACV provides a software architecture for telephony applications. The software consists of real-time voice and signal processing software that perform many of the required telephony data processing functions.

VoIP enables telephone calls to be made over an IP network. The phones connected to the NF15ACV are standard analogue phones that are identical to the other telephones connected to the Home telephone wiring system. The phones can use DTMF dialling to make VoIP calls. The NF15ACV routes or receive calls over VoIP depending on the dialled telephone number or the way in which an incoming call is received. QoS (Quality of Service) is also used to ensure voice calls are placed at a higher priority than data traffic routed between the LAN and WAN interface.

## Phone 1/Phone 2

### VoIP Phone 1 Settings

You can configure settings here.

Default Account	
Select Default Account	Account1 ▾
Account1	
Account	<input type="checkbox"/> Enable
Display Name	Phone1_Account1
Number	<input type="text"/>
Login ID	<input type="text"/>
Password	<input type="text"/>
Proxy Addr	<input type="text"/>
Proxy Port	5060
SIP Domain	<input type="text"/>
Reg Expire (sec)	3600
Outbound Proxy	<input type="checkbox"/> Enable
Outbound Proxy Addr	<input type="text"/>
Outbound Proxy Port	5060
Enable Session timer	<input checked="" type="checkbox"/> Enable
Session Expire (sec)	1800
Register Status	Disabled

FIELD	DESCRIPTION
Display Name	Enter user name to be displayed.
Number	Enter user name (or phone number) of the user.
Login ID	Enter user name for authentication, maximum 39 characters.
Password	Enter user password for authentication, maximum 39 characters.
Proxy	Enable/Disable Proxy. Default: Disables
Proxy Addr	The IP address of SIP proxy
Proxy Port	The port number used by SIP Proxy. Default: 5060
SIP Domain	Assign domain name for the URL to be registered.
Reg Expire (sec)	SIP registration expired time. Assigns the time interval from 1 – 65535. Default setting is 3600 seconds.
Outbound Proxy	Enable: All outgoing requests will be sent to this outbound proxy. Default: Disabled
Outbound Proxy Addr	Specify the IP Address of SIP Outbound Proxy server. This field contains the URI string or the IP of the outbound proxy.
Outbound Proxy Port	The port number of Outbound Proxy Server, assign a number from 1024 to 65535, default setting is 5060.
Register Status	The phone's registration status

## SIP Advanced

SIP Advanced	
SIP Port	<input type="text" value="5060"/>
Media Port	<input type="text" value="9000"/>
DTMF Relay	<input type="text" value="Inband"/> ▾
DTMF RFC2833 Payload Type	<input type="text" value="96"/>
DTMF RFC2833 Packet Interval	<input type="text" value="10"/> (msec) (Must be multiple of 10msec)
Use DTMF RFC2833 PT as Fax/Modem RFC2833 PT	<input checked="" type="checkbox"/> Enable
Fax/Modem RFC2833 Payload Type	<input type="text" value="101"/>
Fax/Modem RFC2833 Packet Interval	<input type="text" value="10"/> (msec) (Must be multiple of 10msec)
SIP INFO Duration (ms)	<input type="text" value="250"/>
Call Waiting	<input checked="" type="checkbox"/> Enable
Call Waiting Caller ID	<input checked="" type="checkbox"/> Enable
Reject Direct IP Call	<input type="checkbox"/> Enable

FIELD	DESCRIPTION
SIP Port	Assign the SIP port number of terminal adapter. Its range is 1024 to 65535, default setting is 5060 for FX0 and 5061 for FXS1.
Media Port	Enter the port for RTP Port number for initial of sending RTP packet. Its range is 1024 to 65535. Default: 9000.
DTMF Relay	DTMFs are the tones generated by your telephone's keypad. Select the DTMF relay method. ATA supports 4 methods: SIP INFO RFC 2833 In-band pass through mode Default: In-band pass through mode.
RFC2833 Payload Type	Specify the Out-band 2833 payload type value. Default: 96
SIP Info Duration (ms)	Specify the Duration (ms) SIP INFO sounds on the telephony end of the call.
Call Waiting	Enable/Disable Call Waiting. Check with your VoIP Provider for Call Waiting support. Default: Enable
Call Waiting Caller ID	Enable/Disable Call Waiting Caller ID. Check with your VoIP Provider for Call ID support. Default: Disable
Reject Direct IP Call	Enable/Disable Reject Direct IP Call. Check with your VoIP Provider for IP Call check. Default: Disable



## Forward Mode

Forward Mode	
Forward all	<input checked="" type="radio"/> Off <input type="radio"/> On
Immediate Number	<input type="text"/>
Forward busy	<input checked="" type="radio"/> Off <input type="radio"/> On
Busy Number	<input type="text"/>
Forward no answer	<input checked="" type="radio"/> Off <input type="radio"/> On
Forward to number	<input type="text"/>
No answer timeout (minimal 4 seconds)	<input type="text" value="4"/>

FIELD	DESCRIPTION
Immediate Forward to	Enable/Disable Call Forwarding for all calls. Check with your VoIP Provider for Call Forwarding support. Default: Disable
Immediate Number	Assigns a phone number; if you want all incoming calls of the port always be redirected. Or You can specify a phone URI in this field. A URI look like SIP:21343@10.20.0.13 or <a href="#">SIP:PHONENUMBR@PROXYSERVER</a>
Busy Forward to	Enable/Disable Busy Forward to. Check with your VoIP Provider for Call Forwarding support. Default: Disable
Busy Number	When the port is busy in call, the incoming call will be redirected to the specified phone number. Or You can specify a phone URI in this field. A URI look like SIP:21343@10.20.0.13 or <a href="#">SIP:PHONENUMBR@PROXYSERVER</a>
No Answer Forward to	Enable/Disable No Answer Forward to. Check with your VoIP Provider for Call Forwarding support. Default: Disable
No Answer Number	When the call is not answered, the incoming call will be redirected to the specified phone number. Or You can specify a phone URI in this field. A URI look like SIP:21343@10.20.0.13 or SIP:PHONENUMBR@PROXYSERVER
No Answer Time (sec)	When the phone is ring unattended a period of time, the incoming call will timeout and redirected to the specified phone number. Default setting is 0 seconds.

## Speed Dial

### Speed Dial

Position	Name	Phone Number	Select
0	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
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"/>

FIELD	DESCRIPTION
Position	There are 10 Speed Dial number from 0 to 9. Pick up the phone and dial the speed dial number for example 5 and then dial # to make the call for the Phone Number in Speed dial number 5.
Name	Enter the Name of the called party.
Phone Number	Assigns a phone number or you can specify a phone URI in this field. A URI looks like SIP:21343@10.20.0.13 or <a href="#">SIP:PHONENUMBR@PROXYSERVER</a>
Select	Delete a specified entry.

## Abbreviated Dial

Here you can set up shortcuts to dial specific numbers or devices.

### Abbreviated Dial

Abbreviated Name	Phone Number
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

FIELD	DESCRIPTION
Abbreviated Name	Enter the Speed Dial Number
Phone Number	Enter the URL, VoIP Phone Number, Remote WAN IP Address of the VoIP Gateway For example: <ul style="list-style-type: none"> <li>• 2222</li> <li>• 192.168.10.222</li> <li>• <a href="#">2222@192.168.10.101</a></li> <li>• voipuser</li> </ul>

## Ring Tone

The Ring Tone settings page lets you configure the ring cadence. The ring cadence is the pattern that the phone rings in and there are standards in each country. You can select the default cadence for your country, a preset cadence or manually specify the cadence in milliseconds. Cadence ON specifies the time that phone is ringing while Cadence OFF specifies the interval between rings.

### VoIP Ring Tone Settings

You can configure settings here.

---

**Select Country**

Country  ▼

**Ring Cadence(Detection) Setting**

Cadence  ▼

**Select Cadence**

Cadence  ▼

**Custom Cadence**

Cadence ON (msec)

Cadence OFF (msec)

## SIP Advance Setting

The SIP Advance Setting page provides advanced settings for the SIP functions of your device. As these are advanced features, only change these settings if you are aware of the impact they will have on your service.

### SIP Advance Setting

You can configure settings here.

---

**Function Key**  
Must be \* + 0-9

Call Transfer  (Default: \*1)

**Dial Option**

Auto Dial Time  (3-9 sec, 0 is Disable)

Dial-out by Hash Key  Enabled

**Off-Hook Alarm**

Off-Hook Alarm Time  (10-60 sec, 0 is Disable)

**FXS Pulse Dial Detection**

Disable  Enable

Interdigit Pause Duration  (msec)

**SIP setting**

SIP Prack  Disabled

SIP Server Redundacy  Enabled

SIP CLIR anonymouse from header  Enabled

Hook Flash Relay setting:  ▼

**SIP OPTIONS**

Disable  Enable

Options interval time  (sec)

**DSCP Flag**

SIP DSCP  ▼

RTP DSCP  ▼

**Enable/Disable HW-NAT**

HWNAT  ▼

## Call History

The call history page displays a list of incoming and outgoing calls made on both voice ports of the router.

### VoIP Call History

This page shows the VoIP Call log.

#### Port 1

DateTime	From	To	Type	Status	Duration
----------	------	----	------	--------	----------

#### Port 2

DateTime	From	To	Type	Status	Duration
----------	------	----	------	--------	----------

# Advanced

## Bridging

The Bridging page provides the option to enable or disable the Spanning Tree Protocol and set MAC address ageing time.

### Bridging Configuration

This page is used to configure the bridge parameters. Here you can change the settings or view some information on the bridge and its attached ports.

Ageing Time:  (seconds)

802.1d Spanning Tree:  Enabled  Disabled

FIELD	DESCRIPTION
Ageing Time	Set the Ethernet address ageing time, in seconds. After [Ageing Time] seconds of not having seen a frame coming from a certain address, the bridge will time out (delete) that address from Forwarding DataBase (fdb).
802.1d Spanning Tree	Enable/disable the spanning tree protocol.

Click the **Show MACs** button to display the Bridge Forwarding Database

### Bridge Forwarding Database

This table shows a list of learned MAC addresses for this bridge.

Port No	MAC Address	Is Local?	Ageing Timer
2	18-f1-45-39-ee-00	yes	---
1	2c-44-fd-12-3c-6e	no	0.02
6	18-f1-45-39-ee-05	yes	---

## Routing

The routing page enables you to define a specific route for your Internet and network traffic. Most home users do not require the need to define static routes but you may need to if you have two or more networks or subnets, if you connect two or more ISP services, or if you connect to a remote corporate LAN.

### Routing Configuration

This page is used to configure the routing information. Here you can add/delete IP routes.

**Enable:**   
**Destination:**   
**Subnet Mask:**   
**Next Hop:**   
**Metric:**   
**Interface:**

#### Static Route Table:

FIELD	DESCRIPTION
Enable	Check to enable the selected route.
Destination	The network IP address of the subnet. The destination can be specified as the IP address of a subnet or a specific host in the subnet. It can also be specified as all zeros to indicate that this route should be used for all destinations for which no other route is defined (this is the route that creates the default gateway).
Subnet Mask	The network mask of the destination subnet. The default gateway uses a mask of 0.0.0.0.
Next Hop	The IP address of the next hop through which traffic will flow towards the destination subnet.
Metric	Defines the priority of the route.
Interface	The interface to which a static routing subnet is to be applied.

## SNMP

Simple Network Management Protocol (SNMP) is a troubleshooting and management protocol that uses the UDP protocol on port 161 to communicate between clients and servers. The NF15ACV can be managed locally or remotely by SNMP protocol.

### SNMP Configuration

This page is used to configure the SNMP. Here you may change the settings for system description, trap ip address, community name, etc..

<b>SNMP:</b>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<b>System Description</b>	<input type="text" value="System Description"/>
<b>System Contact</b>	<input type="text" value="System Contact"/>
<b>System Name</b>	<input type="text" value="NF15ACV"/>
<b>System Location</b>	<input type="text" value="System Location"/>
<b>System Object ID</b>	<input type="text" value="1.3.6.1.4.1.16972"/>
<b>Trap IP Address</b>	<input type="text" value="192.168.1.254"/>
<b>Community name (read-only)</b>	<input type="text" value="public"/>
<b>Community name (write-only)</b>	<input type="text" value="public"/>

FIELD	DESCRIPTION
System Description	A description of the router. This may be anything you like and is used for identification purposes.
System Contact	Contact person and/or contact information for the NF15ACV.
System Name	An administratively assigned name for the NF15ACV.
System Location	The physical location of the NF15ACV.
Trap IP Address	Destination IP address of the SNMP trap
Community name (read-only)	Name of the read-only community. This read-only community allows read operation to all objects in the MIB.
Community name (write-only)	Name of the write-only community. This write-only community allows write operation to the objects defines as read-writable in the MIB.

## Bridge Grouping

The Bridge Grouping page lets you select interfaces for grouping.

### Bridge Grouping Configuration

To manipulate a mapping group:

1. Select a group from the table.
2. Select interfaces from the available/grouped interface list and add it to the grouped/available interface list using the arrow buttons to manipulate the required mapping of the interfaces.
3. Click 'Apply Changes' button to save the changes.

**Note that the selected interfaces will be removed from their existing groups and added to the new group.**

**Grouped Interfaces**

->

<-

**Available Interfaces**

Select	Interfaces
Default	LAN1, LAN2, LAN3, LAN4, wlan0, wlan1, nas0_0, ppp1, ppp0
<input type="radio"/>	
<input type="radio"/>	
<input type="radio"/>	
<input type="radio"/>	

## IP QoS

### QoS Policy

Entries in this table are used to assign the precedence for each incoming packet based on specified policy.

To configure the QoS policy:

1. Ensure IP QoS is enabled.
2. Select PRIO or WRR.
3. If PRIO is selected, a lower number implies greater precedence. If WRR policy is selected, input the weight of the queue. The default is 40:30:20:10.
4. Click the Apply button.



## IP QoS Configuration

IP QoS:  Disable  Enable

### QoS Queue Config

This page is used to configure the QoS policy and Queue. If select PRIO of policy, the lower numbers imply greater precedence. If select WRR of policy, please input the weight of this queue. Default is 40:30:20:10. After configuration, please click 'Apply Changes'

Policy:  PRIO  WRR

Queue	Priority	Enable
Q1	1	<input type="checkbox"/>
Q2	2	<input type="checkbox"/>
Q3	3	<input type="checkbox"/>
Q4	4	<input type="checkbox"/>

**Apply Changes**

## QoS Classification

To configure QoS classification:

Click the **Add** button.

### IP QoS Classification

This page is used to add or delete classification rule. (After add a new rule, please click 'Apply Changes' to take effect.)

ID	Name	Mark			Classification Rules										Delete	Edit	IP Version
		DSCP Mark	IP Precedence	802.1P Mark	LAN	Protocol	DSCP	Source IP/Mask	Source Port	Destination IP/Mask	Destination Port	Source MAC	Destination MAC	802.1p			

**Add**

**Apply Changes**

The Add IP QoS Classification Rules screen is displayed.

### Add IP QoS Classification Rules

This page is used to add a IP QoS classification rule.

---

IP Version:	<input type="text" value="Please select IP version"/>
Rule Name:	<input type="text" value="rule_"/>

#### Assign IP Precedence/DSCP/802.1p to Egress Traffic

Precedence:	<input type="text" value="Queue 1"/>
DSCP:	<input type="text"/>
802.1p:	<input type="text"/>

#### Specify Ingress Traffic Classification Rules

Please specify Configuration - 1 Or Configuration - 2

##### Configuration - 1

WAN:	<input type="text" value="Any"/>
Physical Port:	<input type="text"/>
Protocol:	<input type="text"/>
DSCP:	<input type="text"/>
Source IP:	<input type="text"/>
Source Mask:	<input type="text"/>
Destination IP:	<input type="text"/>
Destination Mask:	<input type="text"/>
Source Port:	<input type="text"/>
Destination Port:	<input type="text"/>
Source MAC:	<input type="text"/>
Destination MAC:	<input type="text"/>

##### Configuration - 2

802.1p:	<input type="text"/>
---------	----------------------

FIELD	DESCRIPTION
IP Version	Select IPv4 or IPv6.
Rule Name	Enter a name for the rule to identify it in the list.
Precedence	Select this field to mark the IP precedence bits in the packet that match this classification rule.
DSCP	Select the Differentiated Services Code Point (DSCP) marking applied.
802.1p	Select this field to mark the 3-bit user-priority field in the 802.1p header of the packet that match this classification rule. Note that this 802.1p marking is workable on a given PVC channel only if the VLAN tag is enabled in this PVC channel.
WAN	Select the Interface.
Physical Port	The incoming ports. The selections include LAN ports, and blank for not applicable.
Protocol	The selections are TCP, UDP, ICMP and blank for none. This field is required if the source port or destination port has been entered.
DSCP	Select the Differentiated Services Code Point (DSCP).
Source IP	The IP address of the source traffic.
Source Netmask	The source IP subnet netmask. This field is required if the source IP has been entered.
Destination IP	The IP address of the traffic destination.
Destination Netmask	The destination IP subnet netmask. This field is required if the destination IP has been entered.
Source Port	The source port of the select protocol. You cannot configure this field without entering the protocol first.
Destination Port	The destination port of the selected protocol. You cannot configure this field without entering the protocol first.
Source MAC	The MAC address of the traffic source.
Destination MAC	The MAC address of the traffic destination.
802.1p	Select this field to mark the 3-bit user-priority field in the 802.1p header of the packet that match this classification rule. Note that this 801.p marking is workable on a given PVC channel only if the VLAN tag is enabled in this PVC channel.

## Traffic Shaping

### IP QoS Traffic Shaping

Total Bandwidth Limit: 1024 Kbps

ID	WAN Interface	Protocol	Source Port	Destination Port	Source IP	Destination IP	Rate(kb/s)	Delete	IP Version
<div style="display: flex; justify-content: space-around; margin-top: 5px;"> <span>Add</span> <span>Apply Changes</span> <span>Apply Total Bandwidth Limit</span> </div>									

To configure traffic shaping:

1. Click the **Add** button. The Add IP QoS Traffic Shaping Rule screen is displayed.

#### Add IP QoS Traffic Shaping Rule

IP Version:    
 Interface:    
 Protocol:    
 Source IP:    
 Source Mask:    
 Destination IP:    
 Destination Mask:    
 Source Port:    
 Destination Port:    
 Uplink Rate:  kb/s

- Enter the details as required. A description of each field is listed in the table below. Click the **Apply Changes** button when you have finished.

FIELD	DESCRIPTION
IP Version	Select IPv4 or IPv6.
Protocol	The selections are TCP, UDP, ICMP and blank for none. This field is required if the source port or destination port has been entered.
Source IP	The IP address of the source traffic.
Source Mask	The source IP netmask. This field is required if the source IP has been entered.
Destination IP	The IP address of the traffic destination.
Destination Mask	The destination IP netmask. This field is required if the destination IP has been entered.
Source Port	The source port of the select protocol. You cannot configure this field without entering the protocol first.
Destination Port	The destination port of the selected protocol. You cannot configure this field without entering the protocol first.
Uplink Rate	Enter a figure in kilobytes per second to restrict the uplink rate. Leave this blank for no restriction.

## Others

Here you can configure IP passthrough. Select the interface then enter a lease time in seconds.

### Other Advanced Configuration

Here you can set some other advanced settings.

**IP PassThrough:**  Lease Time:  seconds  
 Allow LAN access

**Apply Changes**

## IPv6

### IPv6

This page is used to enable or disable IPv6.

### IPv6Configuration

This page be used to configure IPv6 enable/disable

IPv6:  Enable  Disable

**Apply Changes**

## RADVD

This page is used to configure the RADVD settings on the router.

### RADVD Configuration

This page is used to setup the RADVD's configuration of your Router.

MaxRtrAdvInterval:	<input type="text" value="600"/>
MinRtrAdvInterval:	<input type="text" value="198"/>
AdvCurHopLimit:	<input type="text" value="64"/>
AdvDefaultLifetime:	<input type="text" value="1800"/>
AdvReachableTime:	<input type="text" value="0"/>
AdvRetransTimer:	<input type="text" value="0"/>
AdvLinkMTU:	<input type="text" value="0"/>
AdvSendAdvert:	<input type="radio"/> off <input checked="" type="radio"/> on
AdvManagedFlag:	<input checked="" type="radio"/> off <input type="radio"/> on
AdvOtherConfigFlag:	<input type="radio"/> off <input checked="" type="radio"/> on
Enable ULA:	<input type="radio"/> off <input checked="" type="radio"/> on
ULA Prefix:	<input type="text" value="fc01::"/>
ULA Prefix Len:	<input type="text" value="64"/>
ULA Prefix Valid Time:	<input type="text" value="2592000"/>
ULA Prefix Preferred Time:	<input type="text" value="604800"/>
Prefix Mode:	<input type="text" value="Auto"/> ▼
<input type="button" value="Apply Changes"/>	

## DHCPv6

This page is used to configure DHCPv6 Server and DHCPv6 Relay.

### DHCPv6 Settings

This page is used to configure DHCPv6 Server and DHCPv6 Relay.

DHCPv6 Mode:  None  DHCP Relay  
 DHCP Server (Manual)  DHCP Server (Auto)

Auto Config by Prefix Delegation for DHCPv6 Server.

## MLD Proxy

This page is used to configure the Multicast Listener Discovery (MLD) proxy for discovering multicast listeners.

### MLD Proxy Configuration

This page be used to configure MLD Proxy.

MLD Proxy:  Enable  Disable

WAN Interface:

## MLD Snooping

This page is used to enable or disable MLD snooping. MLD Snooping limit the flooding of multicast traffic.

### MLD Snooping Configuration

This page be used to configure MLD Snooping.

MLD Snooping:  Enable  Disable

**Apply Changes**

## IPv6 Routing

This page is used to configure IPv6 Static Routing. Enter the details of the route then click the **Add Route** button to add it to the list.

### IPv6 Static Routing Configuration

This page is used to configure the IPv6 static routing information. Here you can add/delete static IP routes.

Enable:   
 Destination:   
 Next Hop:   
 Metric:   
 Interface:

**Add Route** **Update** **Delete Selected** **Delete All**  
**Show Routes**

Static IPv6 Route Table:

Select	State	Destination	Next Hop	Metric	Interface
--------	-------	-------------	----------	--------	-----------

## IP/Port Filtering

Entries in this table are used to restrict certain types of data packets through the Gateway. Use of such filters can be helpful in securing or restricting your local network. Enter the details of the rule then click the **Add** button.

### IPv6 IP/Port Filtering

Entries in this table are used to restrict certain types of data packets through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Outgoing Default Action  Deny  Allow  
 Incoming Default Action  Deny  Allow **Apply Changes**

Direction:  Protocol:  Rule Action  Deny  Allow

Source Interface ID:  -   
 EX: 1111:2222:3333:4444-fff.fff.fff.fff

Destination Interface ID:  -   
 EX: 1111:2222:3333:4444-fff.fff.fff.fff

Source Port:  -   
 Destination Port:  -

**Add**

Current Filter Table:

Select	Direction	Protocol	Source Interface ID	Source Port	Destination Interface ID	Destination Port	Rule Action
--------	-----------	----------	---------------------	-------------	--------------------------	------------------	-------------

**Delete Selected** **Delete All**

# Diagnostics

## Ping

When troubleshooting your internet connection, it is a good idea to make sure you can ping the network. A ping command sends a message to the host you specify. If the host receives the message, it sends messages in reply. To use it, you must know the IP address of the host you are trying to communicate with and enter the IP address in the Host Address field. Enter the IPv4 or IPv6 host address in the appropriate field then click “Go!” to start the ping command. The ICMP ping results are displayed on this page.

### Ping Diagnostics

This page is used to send ICMP ECHO\_REQUEST packets to network host. The diagnostic result will then be displayed.

---

IPv4 Host Address:	<input type="text"/>	<input type="button" value="Go !"/>
IPv6 Host Address:	<input type="text"/>	<input type="button" value="Go !"/>

## Tracert

The Tracert (or trace route) command displays the hops that a message takes when it travels from your router to a remote destination. Enter the host address that you wish to trace and click the “Go!” button. This allow you to identify the route taken for a packet from your router to arrive at its destination.

### Tracert Diagnostics

This page is used to print the route packets trace to network host. The diagnostic result will then be displayed.

---

Host Address:	<input type="text"/>
<input type="button" value="Go !"/>	

## ATM Loopback

Connectivity verification is supported by the user of the ATM OAM loopback capability for both VP and VC connections. This page is used to perform the VCC loopback function to check the connectivity of the VCC.

### ATM Loopback Diagnostics - Connectivity Verification

Connectivity verification is supported by the use of the ATM OAM loopback capability for both VP and VC connections. This page is used to perform the VCC loopback function to check the connectivity of the VCC.

---

Select PVC:

8/35

Flow Type:

F4 Segment     F4 End-to-End

F5 Segment     F5 End-to-End

Loopback Location ID:



## DSL Tone

This page is used to test the DSL tones, and help identify specific frequency interference. Click the **Start** button to begin the test.

### DSL Tone Diagnostics

DSL Tone Diagnostics. Only ADSL2/ADSL2+/VDSL2 support this function.

	Downstream	Upstream
Hlin Scale		
Loop Attenuation(dB)		
Signal Attenuation(dB)		
SNR Margin(dB)		
Attainable Rate(Kbps)		
Output Power(dBm)		

Tone Number	H.Real	H.Image	SNR	QLN	Hlog
0					
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					

## ADSL Connection

The ADSL Connection diagnostics page lets you run some tests to check the status of your ADSL connection. To begin the tests, select the ADSL interface then click the **Go** button.

### ADSL Connection Diagnostics

The Router is capable of testing your connection. The individual tests are listed below. If a test displays a fail status, click 'Go' button again to make sure the fail status is consistent.

Select the ADSL Connection:

ADSL Connection Check	
Test ADSL Synchronization	PASS
Test ATM OAM F5 Segment Loopback	PASS
Test ATM OAM F5 End-to-end Loopback	PASS
Test ATM OAM F4 Segment Loopback	PASS
Test ATM OAM F4 End-to-end Loopback	PASS

Internet Connection Check	
Test PPP Server Connection	PASS
Test Authentication with ISP	PASS
Test the assigned IP Address	PASS
Ping Default Gateway	PASS
Ping Primary Domain Name Server	PASS

# Admin

## Commit/Reboot

This page is used to commit any configurational changes you have made and reboot the router so that they take effect. Click the Commit and Reboot button to save settings and reboot the router.

### Commit and Reboot

This page is used to commit changes to system memory and reboot your system.

---

## Backup/Restore

You can save the current configuration of your Router to a file on your computer. This is highly recommended before you change any configuration settings on the Router or before you upgrade your firmware. If any problem should occur after you have made changes, you can use this page to restore the router to your previous settings.

### Backup and Restore Settings

This page allows you to backup current settings to a file or restore the settings from the file which was saved previously. Besides, you could reset the current settings to factory default.

---

Backup Settings to File:

Restore Settings from File:  No file selected.

Reset Settings to Default:

## System Log

The System Log page is useful for troubleshooting and is used to display a log of events that occur on the router. You can change the level of logging as a means of filtering out the types of messages that you want to see. Additionally, you may save the log file to your hard drive using the **Save** button.

### System Log

---

System Log :  Enable  Disable

Log Level :  ▾

Display Level :  ▾

Save Log to File:

Clear Log:

---

System Log

Date/Time	Facility	Level	Message
-----------	----------	-------	---------

## Password

The Password configuration page is used to change the password for the admin and user accounts on the router. For your security, we highly recommend changing these passwords from their original settings to prevent unauthorized access to your router.

Select the account username then enter the old and new passwords in the designated fields. Click the **Apply Changes** button when you have finished.

### Password Configuration

This page is used to set the account to access the web server of your Router. Empty user name and password will disable the protection.

User Name:

admin ▾

Old Password:

New Password:

Confirmed Password:

Apply Changes

Reset

## Firmware Upgrade

The firmware is software that is stored on the router and governs the way it operates. New firmware files can be uploaded to the router using this page.

To update the router firmware:

1. Click the **Browse** button then locate the firmware file on your computer.
2. Click the **Upgrade** button to begin the firmware upgrade process.

### Firmware Upgrade

This page allows you upgrade the firmware to the newer version. Please note that do not power off the device during the upload because this make the system unbootable.

Browse... No file selected.

Upgrade

Reset

## ACL

This page is used to configure the Remote Management feature listed in the Access Control List (ACL). If ACL is enabled, only the IP addresses in the ACL table can access the Customer Premises Equipment (CPE). Use this page to enable or disable ACL and add or remove IP addresses from the list.

### ACL Configuration

This page is used to configure the IP Address for Access Control List. If ACL is enabled, only the IP address in the ACL Table can access CPE. Here you can add/delete the IP Address.

ACL Capability:  Enable  Disable

---

Enable:

Interface:

IP Address:

Subnet Mask:

Service Name	LAN
Any	<input type="checkbox"/>
TELNET	<input type="checkbox"/>
FTP	<input type="checkbox"/>
TFTP	<input type="checkbox"/>
HTTP	<input type="checkbox"/>
SNMP	<input type="checkbox"/>
Secure Shell(SSH)	<input type="checkbox"/>
PING	<input checked="" type="checkbox"/>

---

ACL Table:

Select	State	Interface	IP Address	Services	Port
<input type="checkbox"/>	Enable	LAN	0.0.0.0/0	any	--
<input type="checkbox"/>	Enable	WAN	0.0.0.0/0	ping	

## Time Zone

Certain systems may not have a date or time mechanism or may be using inaccurate time/day information. The Simple Network Time Protocol feature provides a way to synchronize the router's own time of day setting with a remote time server as described in RFC 2030 (SNTP) and RFC 1305 (NTP). Correct time is needed for Schedule, Parental control, and System logging.

### Time Zone Configuration

You can maintain the system time by synchronizing with a public time server over the Internet.

Current Time : Year  Month  Day   
 Hour  Min  Sec

Time Zone Select :

Enable Daylight Saving Time

Enable SNTP Client Update

WAN Interface:

SNTP Server :    
  (Manual Setting)

## TR-069

TR-069 is a protocol for communication between customer premises equipment (CPE) and an Auto Configuration Server (ACS). It allows the auto configuration server to push requests to the router to perform certain activities, for example, a firmware upgrade.

### TR-069 Configuration

This page is used to configure the TR-069 CPE. Here you may change the setting for the ACS's parameters.

**TR069:**  Enabled  Disabled

#### ACS:

URL:   
 User Name:   
 Password:   
 Periodic Inform:  Enabled  Disabled  
 Periodic Inform Interval:

#### Connection Request:

User Name:   
 Password:   
 Path:   
 Port:

#### Certificate Management:

CPE Certificate Password:     
 CPE Certificate:  No file selected.   
 CA Certificate:  No file selected.

FIELD	DESCRIPTION
<b>ACS</b>	
URL	The Auto Configuration Server URL. For example, <a href="http://10.0.0.1:80">http://10.0.0.1:80</a> or <a href="https://10.0.0.1:443">https://10.0.0.1:443</a>
User Name	The username that the NF15ACV should use when connecting to the ACS.
Password	The password that the NF15ACV should use when connecting to the ACS.
Periodic Inform	When this field is enabled, the NF15ACV will send an Inform RPC to the ACS server at the system startup, and will continue to send it periodically at an interval defined in Periodic Inform Interval field; When this field is disabled, the NF15ACV will only send Inform RPC to the ACS server once at the system startup.
Periodic Inform Interval	Time interval in seconds to send the Inform message.
<b>Connection Request</b>	
User Name	The username the remote ACS should use when connecting to the NF15ACV.
Password	The password the remote ACS should use when connecting to the NF15ACV.
Path	The path of the device ConnectionRequestURL. The device ConnectionRequestURL should be configured based on the Device_IP, Path and Port as follows: <a href="http://Device_IP:Port/Path">http://Device_IP:Port/Path</a>
Port	The port of the device ConnectionRequestURL.

# Statistics

## Interface

This page shows the packet statistics for transmission and reception for each configured interface.

### Interface Statistics

This page shows the packet statistics for transmission and reception regarding to network interface.

Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
eth0.2	0	0	0	0	0	0
eth0.3	0	0	0	0	0	0
eth0.4	2117	0	0	2889	0	0
eth0.5	0	0	0	0	0	0
wlan0	23125	0	0	1838	0	0
ppp0_vc0_0	781	0	0	762	0	0
ptm0_0	0	0	0	0	0	0
nas0_0	0	0	0	0	0	0

## DSL

This page shows statistics and information pertaining to the DSL connection.

### DSL Statistics

Mode	ADSL2 Annex A
TPS-TC	ATM
Latency	Fast
Status	SHOWTIME.
Power Level	L0
Uptime	00:08:13
G.Vector	Off

	Downstream	Upstream
Trellis	On	On
SNR Margin (dB)	7.2	6.0
Attenuation (dB)	54.0	29.0
Output Power (dBm)	18.0	12.0
Attainable Rate (Kbps)	3480	924
G.INP	Off	Off
Rate (Kbps)	3248	825
R (number of check bytes in RS code word)	14	16
N (RS codeword size)	230	224
L (number of bits in DMT frame)	870	231
S (RS code word size in DMT frame)	2.11	7.75
D (interleaver depth)	16	1
Delay (msec)	8.50	2.00
INP (DMT frame)	1.029	0.277
FEC errors	0	0
OH Frame	28500	27445
CRC (OH Frame) errors	0	0
Total ES	0	1
Total SES	0	0
Total UAS	52	0
Total LOSS	--	--
Last Link Rate	0	0
Full Init	0	
Failed Full Init	0	
Synchronized time(Second)	493	
Synchronized number	1	



# Appendix A: Default Settings

The following tables list the default settings for the NF15ACV router.

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

*Table 5 - LAN Management Default Settings*

ADMIN MANAGER ACCOUNT	
Username:	admin
Password:	admin

*Table 6 - Web Interface Default Settings*

# Legal & Regulatory Information

## 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 (ACN 002490486) (NetComm Wireless Limited) (or its licensors). This Manual does not transfer any right, title or interest in NetComm Wireless Limited's (or its licensors') intellectual property rights to you.

You are permitted to use this Manual for the sole purpose of using the NetComm Wireless 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 Wireless Limited.

NetComm, NetComm Wireless and NetComm Wireless Limited are a trademark of NetComm Wireless Limited. All other trademarks are acknowledged to be the property of their respective owners.

## 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 incorporates a radio transmitting device, in normal use a separation distance of 20cm will ensure radio frequency exposure levels complies with Australian and New Zealand standards.
3. 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:
  - i. Change the direction or relocate the receiving antenna.
  - ii. Increase the separation between this equipment and the receiver.
  - iii. Connect the equipment to an alternate power outlet on a different power circuit from that to which the receiver/TV is connected.
  - iv. Consult an experienced radio/TV technician for help.
4. 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 Wireless. Failure to do so may cause damage to this product, fire or result in personal injury.
5. This equipment may not work when mains power fails.

## 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.

## Product Warranty

All NetComm Wireless 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 Wireless Limited within 30 days of the original purchase date by registering online via the NetComm Wireless web site at [www.netcommwireless.com](http://www.netcommwireless.com). 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 Consumer Protection Laws Section above).

Subject to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see the [Consumer Protection Laws](#) Section 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 Wireless Limited 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 Wireless Limited 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 Wireless Limited;
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 Wireless Limited; or
6. the serial number has been defaced or altered in any way or if the serial number plate has been removed.

## 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 the [Consumer Protection Laws](#) Section above), NetComm Wireless Limited accepts no liability or responsibility, for consequences arising from the use of this product. NetComm Wireless Limited 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 Wireless'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 Wireless's liability for any breach of that guarantee, condition or warranty is limited to: (i) in the case of a supply of goods, NetComm Wireless Limited 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 Wireless Limited 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 Wireless Limited is unable to limit its liability as set out above, NetComm Wireless Limited 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

Phone: +61(0)2 9424 2070

Fax: +61(0)2 9424 2010

Email: [sales@netcommwireless.com](mailto:sales@netcommwireless.com) [techsupport@netcommwireless.com](mailto:techsupport@netcommwireless.com)