



This manual serves the following ComNet Series:

NW1[IC] NW2 NWK1[IC] NWK2 NWK11/M[IC]

INSTALLATION AND OPERATION MANUAL

RETUVAVE INDUSTRIAL OUTDOOR ULTRA-HIGH THROUGHPUT, IMPACT RESISTANT HARDENED 802.11AC WIRELESS ETHERNET DEVICE

Thank you for purchasing NetWave from ComNet. This installation guide applies to all Generation 4 NetWave Radios. NW1 Shown in examples.

The NetWave® NW(1,2)[IC] Industrial Grade high performance wireless radio is ideal for high capacity and scalable deployments where channel overlapping and interference typically cause our discounted competitors radios to become unstable. The wide range of channel spectrum widths available on the NW(1,2)[IC] series of radios gives you the option of narrowing channel bandwidths as your network grows which will increase the number of non-overlapping channels and improve stability.

The NW(1,2)[IC] comes standard with an integrated antenna and an IP67 rated impact resistant polycarbonate enclosure that is designed to survive the most extreme conditions.

The NW1 is FCC certified for use in the United States. The NW2 is ETSI, DFS and TPC certified for use in the European Union. The NW1IC is certified for use in Canada.

About This Guide

This guide is intended for different users such as engineers, integrators, developers, IT managers, and technicians.

It assumes that users have some PC competence and are familiar with Microsoft Windows operating systems and web browsers such as Windows Internet Explorer and Mozilla Firefox, as well as have knowledge of the following:

- » Installation of electronic equipment
- » Electrical regulations and guidelines
- » Knowledge of Local Area Network technology

Related Documentation

The following documentation is also available:

- » NW(1,2) Series (Gen 4) Datasheet
- » NW(1,2) Series (Gen 4) Quick Start Guide

Website

For information on ComNet's entire product line, please visit the ComNet website at http://www.comnet.net

Support

For any questions or technical assistance, please contact your sales person (sales@comnet.net) or the customer service support center (techsupport@comnet.net)

Safety

- » Only ComNet service personnel can service the equipment. Please contact ComNet Technical Support.
- » The equipment should be installed in locations with controlled access, or other means of security, and controlled by persons of authority.

Contents

About This Guide	2
Related Documentation	2
Website	2
Safety	2
Overview	5
Regulatory Compliance Statement	5
Warranty	5
Disclaimer	5
Legal Information	5
1.0 Introduction	6
System Requirements	6
2.0 Deployments	7
Point to Multi-Point	7
Point to Point Topology Utilizing Dual Ports for Passthrough PoE	8
4.0 Cabling Requirements	9
5.0 Hardware Installation	9
Outdoor Ethernet Gland Installation	9
NetWave Indicating LED Details	11
Outdoor Standard Mounting Hardware	11
6.0 Key Default Settings	13
IP Address	13
Login Credentials	13
Default Wireless Settings	13
7.0 Quick Configuration	14
8.0 Detailed Configuration	15
Logging Into a Radio	15
Operating Modes	16
Reset and Save Settings	16
Logout	16
Reset Button	16
Web GUI	17

Navigation Tabs	17
Status - Routes	18
Status - Kernel Log	18
Status - Realtime Graphs	19
System	22
Network	30
Network - Wifi	35
WiFi Configuration	36
Agency Compliance	43
GPL (General Public License) Statement	45

Overview

Regulatory Compliance Statement

Product(s) associated with this publication complies/comply with all applicable regulations. Please refer to the Technical Specification section for more details.

Warranty

ComNet warrants that all ComNet products are free from defects in material and workmanship for a specified warranty period from the invoice date for the life of the installation. ComNet will repair or replace products found by ComNet to be defective within this warranty period, with shipment expenses apportioned by ComNet and the distributor. This warranty does not cover product modifications or repairs done by persons other than ComNet-approved personnel, and this warranty does not apply to ComNet products that are misused, abused, improperly installed, or damaged by accidents.

Please refer to the Technical Specifications section for the actual warranty period(s) of the product(s) associated with this publication.

Disclaimer

Information in this publication is intended to be accurate. ComNet shall not be responsible for its use or infringements on third parties as a result of its use. There may occasionally be unintentional errors on this publication. ComNet reserves the right to revise the contents of this publication without notice.

Legal Information

No part of this document may be reproduced or transmitted in any form or by any means, electronic and mechanical, for any purpose, without the express written permission of ComNet.

Copyright

Copyright © 2020 Communication Networks, LLC (dba ComNet). All rights reserved.

1.0 Introduction

The NetWave® ultra-high throughput, impact-resistant hardened wireless Ethernet transmission device can be configured through the embedded User Interface as a Client or as an Access Point. This single radio model was designed for high throughput point-to-point or multipoint applications and comes with an integrated 19dBi, 17° beamwidth antenna. The NetWave Radios supports up to 500 Mbps throughput using 802.11ac MIMO technology. The units can be powered by an 02.3af/at PoE compliant device or through a sold-separately PoE injector with the second Ethernet port serving as an IEEE802.3af power source. NW1 is FCC certified for use in North America, NW1IC is certified for use in Canada, and the NW2 is ETSI, DFS and TPC certified for use in the European Union.

This user manual is a guide for the NetWave Generation 4 wireless Ethernet devices as well as the preconfigured kits. ComNet NetWave Wireless offers OpenWRT with the most advanced Qualcomm Atheros wireless drivers. NetWave now includes a new user-friendly LuCI web interface for configuring the device. OpenWRT is an extensible GNU/Linux distribution for embedded devices. It is built from the ground up to be a full featured, easily modifiable operating system. It is powered by a Linux kernel that's more recent than most other distributions. LuCI is a free, clean, extensible and easily maintainable web user interface for embedded devices. It has high performance, small installation size, fast runtimes, and good maintainability. The units come configured for either point to point or point to multipoint applications. This manual contains detailed operational and configuration information not covered in the quick start guides.

System Requirements

Web Browser: Mozilla Firefox, Google Chrome, Apple Safari, or Microsoft Internet Explorer 8 or above.

2.0 Deployments

Point to Multi-Point

These individual units allow the user to configure for either multipoint access point or client operation. There is a MAC address lock feature that can be enabled through the user interface but is not enabled by default. The NW(1,2)[IC] radios includes a 19dBi 17° internal antenna. See the ComNet website for the latest information regarding antenna support. Preconfigured NWK kits do not support point-to multipoint topologies out of the box. They will need to add the additional clients to a whitelist on the access point.



Image 1

Point to Point Topology Utilizing Dual Ports for Passthrough PoE





4.0 Cabling Requirements

Shielded CAT 5 or better should be used for all out of plant Ethernet connection and should be properly grounded through the PoE AC ground. Industrial grade shielded Ethernet cable is recommended to help prevent ESD damage commonly experienced with outdoor installations. Visit <u>www.comnet.net/comnet-products/cables</u>

5.0 Hardware Installation

Outdoor Ethernet Gland Installation

There will be at least one cable gland included with each outdoor enclosure. Below is an image of the individual parts of the gland with an Ethernet cable routed through.

Note: The split rubber washer allows a pre-terminated Ethernet cable to be used.

Once the cable has been routed through the weather connection, and the RJ45 connection has been made, screw in the gland into the housing making sure it is tight enough for a water tight seal. Push the split rubber gasket into place and loosely screw the cap that goes over the rubber washer.





Once the gland is tight in the housing, tighten the outer nut/cap making sure the rubber seal squeezes and seals the Ethernet cable to the gland as shown.

Connect one end of an RJ-45 Ethernet cable to the LAN OUT port of the Power Injection Module (PIM) and the other end to LAN of the access point – as sown below.

Note: Maximum length of the RJ-45 CAT5 cable is 90 meters.

Connect the RJ-45 Ethernet cable attached to the PIM to a network device, such as a switch or to the configuration PC. Then plug the power adaptor to an AC power outlet and power plug into the socket of the PIM – as shown in the diagram below.

Note: DC PoE input for the NW(1,2,9) and NWK(1,2,9) is 48 VDC.



- A. Connect one end of an RJ-45 Ethernet cable to the OUT port of the Power Injection Module (PIM) and the other end to LAN of the access point. Maximum length of the RJ-45 CAT5 cable is 100 meters.*
- B. Connect the RJ-45 Ethernet cable attached to the PIM to a network device, such as to a switch or to the PC you will use to configure the access point.
- C. Connect the power adaptor to the main electrical supply and the power plug into the socket of the PIM. PoE power input: Passive PoE (range 36 to 48 VDC). The unit can also be powered by a suitable IEEE 802.3af/at PSE device such as a PoE switch or injector.
- D. A Drip Loop is recommended as additional precaution against moisture entering the Access Point housing.
- * Up to 200mW radio. For higher power radio upgrade to higher rating power adapter.

Image 5

IMPORTANT: Only plug PoE power to Port 1. Connecting a PoE power source to the PSE Port (#2) will cause a major device malfunction and void the warranty.

NetWave Indicating LED Details



SIGNAL STRENGTH:



WEAK SIGNAL

EXCELLENT SIGNAL

Image 6

Outdoor Standard Mounting Hardware

This mounting hardware will support pole diameters up to 2 in (5.8 cm). Below are the parts contained in the standard mounting hardware.



Image 7

Here is the mounting hardware assembled shown with a NW1/M in a +30° and -30° vertical position





6.0 Key Default Settings

IP Address

Defaulted Radio	192.168.10.101
IP Address of Web Server	192.168.10.100 (AP) 192.168.10.101 (CL)

Login Credentials

Username	root
Password	root

Default Wireless Settings

SSID	NetWave-1
WPA Pre-shared Key	12345678
Channel-Frequency (AP)	Auto
Channel Spectrum Width	Auto

Note: A Reset to defaults will erase the user config and reset the radio to a 192.168.10.101 address and set the wireless card to Client mode.

7.0 Quick Configuration

- 1. Connect an Ethernet cable from the port labelled as IN on the power Injection Module to either a laptop or a PC LAN port.
- 2. Connect the second Ethernet cable from the OUT port on the Power Injection Module to the NetWave LAN port.
- 3. Apply 48 VDC to the Power Injection Module with the provided power supply. You should notice the green LED illuminate in the Power Injection Module and the power LED on the NetWave unit.
- 4. Set the IP address of the laptop being used to configure NetWave to static and the subnet to 192.168.10.x/24 subnet.
- Point the browser to 192.168.10.101. This is the default address.
 For preconfigured kits (NWKX_AP and NWKX_CL) point the Browser to 192.168.10.100 for the Access Point or 192.168.10.101 for the Client.
- 6. A login prompt will pop up. Enter: Username root

Password root

7. Select the NETWORK » WIFI tab and set the desired network settings. Select Apply & Save.

Note: This will be the network address for the NetWave web server. It is not necessary to set to the same subnet as the operating network, but it is recommended.

- 8. Select the NETWORK -> WIFI tab and set:
 - Wireless mode Set to AP or Client
 - Country code Only required if setting up the NW2 (ETSI) model

Note: It is the user's responsibility to ensure that the correct country is chosen. ComNet accepts no liability for incorrect equipment set up.

- Output RF power if received signal strength is greater than 80, it is recommended to reduce RF TX power
- Set SSID if changing from the default setting
- Channel Spectrum Width May want to reduce to 20M from the default 20/40/80MHz if the 5GHz spectrum is crowded
- Wireless Security if changing from default settings
- Select Apply Settings
- Select Save

Note: Multipoint nodes will need to have the Wireless Mode set to either AP or Client (default is Client). And the IP addresses will need to be all set to different addresses (default address is 192.168.10.101). Once this is done, all the clients will connect to the multipoint AP with all other setting kept at default.

8.0 Detailed Configuration

Logging Into a Radio

To access the NetWave configuration interface, perform the following steps:

- 1. Connect an Ethernet cable from the Data In port on the Midspan Injector or Port 2 on the radio directly to your laptop.
- 2. If you are using a Midspan Power Injector, connect the power cable to an outlet and turn on power.
- 3. Assign the Ethernet adapter on your computer with a static IP address on the 192.168.1.x network, e.g. 192.168.10.10 and with a subnet mask 255.255.255.0.
- 4. Launch a web browser and enter the default IP address of the device, 192.168.10.101, into the address bar.

The login page will look like the following image:

	t Chaos Calmer 15.05.1 unknown Load: 2.26 1.38 0.56	
FROM COMNET Authorization Required Please enter your username and password.		
Username	<mark>⊜</mark> root	
Password	2	
		🙆 Reset 💷 Logir

Image 9

The default authorization details are:

Username: root

Password: root

Operating Modes

The Netwave Radio can operate in the following modes:

- 1. Access Point WDS
- 2. Client WDS
- An Access Point can have multiple clients.
- A Client Radio can only link to one access point.

Reset and Save Settings

The buttons are described here.

Reset	Save	Save & Apply
In	ge 10	

Reset	Undo the changes.
Save	Saves the changes but does not take effect till settings are applied
Save & Apply	Saves and applies the changes. Please use this button so that the changes are applied immediately.

- Note: At the top right corner of the NetWave configuration web page, there may be either of the following texts displayed:
 - Changes: 0: Means that all changes on the configuration web page have been applied to the Wireless Device.

Unsaved Changes: Shows the number of changes that have not yet been Save & Apply.

Logout

There are two ways to logout of the radio, most will simply close the browser or browser tab. There is also a logout button on the navigation bar.

Reset Button G

The reset button is a physical hardware button on the enclosure of the radio. Depending on how long the button is pressed, you can reboot the board or reset it to factory default. First make sure, that the power is on and wait a minute for the board to finish starting up. The following table shows the duration of the button press and the corresponding action.

Button Press Duration	Effect
0 - 3 Seconds	Power cycles the radio
5 - 20 Seconds	Reset to factory default

Web GUI

After login, the browser will display the Status - Overview page. This is the default information page that shows your connected stations and their connection quality.

Status System	Network						
Overview Rou	ites Kernel Log Realtime Graphs						
Wireless							
Generic 802.11	ac Wireless Controller (wifi0)	SSID: M Mode: M Icone Birtarie: BSSID: Com Encrypti	<u>ttwave-1</u> iaster 3 36 (5.180 GHz) 866 Mbit/s 24.48/D1.00.42:28 ion: WPA2 NONE (CCMP)				
Associated St	ations						
none							
	MAC-Address	Network	Noise Level	RSSI (0-100)	RX Rate	TX Rate	Up Time
	C4:4B:D1:00:42:0F	Master "Netwave-1"	-95 dBm	60(0,0,0)	866.0 Mbit/s	866.0 Mbit/s	51 mins 38 s
Status System							
Router Name		OpenWrt					
Firmware Version		NW1Gen4_v5.0.3-8					
Kernel Version		3.14.77					
Local Inne							
Memory							
Total Available							
Network							
IPv4 WAN Stat	JS	Not connect	cted				
IPv6 WAN Stat	us	Not connec	cted				
Active Connect	ions						

Image 11

Navigation Tabs

The navigation tabs assist with locating the specific settings that need to checked or updated.





The Status - Overview Page is the default page and is divided into the following sections.

Wireless	Displays the wireless settings for the Ath0 wireless card
Associated Stations	Shows connected stations
System	Displays host name, Firmware, and Kernel versions
Memory	Displays total and free onboard memory
Network	Shows WAN configurations if configured
DHCP Leases	Shows IPv4 DHCP Leases
DHCPv6 Leases	Shows IPv6 DHCP Leases

Status - Routes

The Routes page will display current ARP Table, IPv4, and IPv6 Routes.

	MAC-Address	Int	erface	
	00:0c:29:c3:fa:7d	b	br-lan	
	c4:4b:d1:00:42:0c	b	ır-lan	
102.100.10.0029			mider.	
	Source	Metric	Table	
larget	boulde			
fdd9:3d5c:7b34::/64	Source	1024	main	
fdd9:3d5c:7b34::/64 ff00::/8	Source	1024 256	main local	
	Target 192.168.10.0/24	MAC_Address 00:00:29:031a:7d c4/4b:d1:00:42:0c Target IPy4-Gateway 192:168:10:0/24	MAC_Address Into 000.c29c3ta.7d b c4:4b:d100.42:0c b 7arget IPy4-Gateway Metric 192:168.10.024 0 0	

Image 13

Status - Kernel Log

The Kernel Log displays operational messages from the processor.

Status System	n Network Logout
Overview Rou	utes Kernel Log Realtime Graphs
Kernel Lo	g
000000.0] 000000.0] 000000.0] 000000.0] 000000.0] 000000.0] 000000.0] 000000.0]	D) Booting Linux on physical CPU 0x0 D) Linux version 3.14.77 (benku@benku-VirtualBox) (gcc version 4.8.3 (OpenWrt/Linaro GCC 4.8-2014.04 unknown)) #100 SMP PREEMPT Sat Apr 3 14:22:51 PDT 2021 D) Linux version 3.14.77 (benku@benku-VirtualBox) (gcc version 4.8.3 (OpenWrt/Linaro GCC 4.8-2014.04 unknown)) #100 SMP PREEMPT Sat Apr 3 14:22:51 PDT 2021 D) CPU: ARWY Processor [410fc075] revision 5 (ARMv7), cr=10c5387d D) CPU: PIPT / VIPT nonaliasing data cache, VIPT aliasing instruction cache D) Machine model: Qualcomm Technologies, Inc. IPQ40xx/AP-DK07.1-C1 D) Memory policy: Data cache writealloc D) On node 0 totalpages: 126976 D) free_area_init_node: node 0, pgdat c08af740, node_mem_map dfbfa000 D) Normal zone: 1024 pages used for memmap D) Normal zone: 1024 pages reserved

lmage 14

Status - Realtime Graphs

Realtime graphs has the 4 following categories: Load, Traffic, Wireless, and Connections.

Load

Realtime Load displays current CPU usae. 1.00 would be considered 100% utilization.



Image 15

Traffic

The Traffic tab displays throughput load for each of the interfaces.

Ath0 is the wireless interface.

Eth0 is port 1.

Eth1 is port 2.

Status System Network	Logout			
Overview Routes Kernel Log	Realtime Graphs			
Load Traffic Wireless Co	nnections			
Realtime Traffic				
ath0 bond0 br.lan eth0	eth1 aretap0 in6tal0 miirea teal0			
	4m	3m	2m	1m
0 kbit/s (0 kB/s)				
0 kbit/s (0 kB/s)				
0 kbit/s (0 kB/s)				
				(4 minute window, 3 second interval)
Int	bound: 0 kbit/s	Average: 0 kbit/s		Peak: 0 kbit/s
Out	bound: 0 kbit/s	Average: 0 kbit/s		Peak: 0 kbit/s
	(0 kB/s)	(0 kB/s)		(0 kB/s)



Wireless

The Wireless tab has 2 sections. The upper section displays the Signal Strength and Noise Levels in dBm.

- » The Signal Strength is shown as a negative number that ranges from -95 (Weakest) to 0 (Strongest).
- » The Noise Level is also rated from -95 to 0 with -95 being the noise floor (No interference).
- » The Signal to Noise Ratio is also shown and is rated from 0 to 100 with 100 being the strongest signal possible.

The lower section displays the data rate of the wireless connection and varies greatly depending on throughput demand and processor load.



Image 17

Connections

The connections tab is a graphical display of the ARP table and the number of devices connected.



Image 18

System

Settings for managing the device will be found under the Systems Tab.

Under the Systems Main tab, there are 6 sub-categories: System, Administration, SNMP, LED Configuration, Backup/Flash Firmware, and Reboot.

System Properties

General Settings

The System Properties Section has two tabs, General Settings and Logging.

The General Settings Tab is used to designate a Hostname for the radio and specify a timezone.

You can also sync the radio time with your browser.

System Properties	
General Settings	
Local Time	Sat Apr 3 20:04:10 2021
Hostname	OpenWrt
Timezone	UTC

Image 19

Logging

The logging page allows you to configure what type of messages are sent and where to send it to.

System Properties		
General Settings Logging		
System log buffer size	64	
	W KiB	0110110101011011010101010101010101010101
External system log server	0.0.0.0	
External system log server port	514	
Log output level	Debug	
Cron Log Level	OpenWrt	



Time Synchronization

The NTP Settings are under the Time Synchronization section. The device is able to act as an NTP Client or Server. If connected to the internet, the radio may synchronize with an outside server.

Enable NTP client		
Provide NTP server		
TP server candidates	0.openwrt.pool.ntp.org 🔹 1.openwrt.pool.ntp.org 🔹	
	2.openwrt.pool.ntp.org	

Image 21

System - Administration

The Administration page allows you to change the password to your radio and configure SSH Access.

Router Password				
Changes the administrator password for accessing the device				
Password	2	2		
Confirmation	<i>ø</i>	<i>#</i>		
SSH Access				
Dropbear offers SSH network shell access and an integrated SCP ser	ver			
Dropbear Instance			∞ Delet _f	
Interface	Ian: J. J. M.			
	② Listen only on the given inte	face or, if unspecified, on all		
Port	22 ② Specifies the listening port c	this Dropbear instance		
Password authentication	🗹 💿 Allow SSH password au	hentication		
Allow root logins with password	Allow the root user to lor	Allow the root user to login with password		
Gateway ports	Allow remote hosts to cr	anect to local SSH forwarded ports		
b44				
CCLL Vave				
Here you can paste public SSH-Keys (one per line) for SSH public-key	authentication.			

Image 22

Administration - Router Password

To update the device login password, Enter the new password in both the Password and Confirmation sections. The green circular arrows to the right of the input box will reveal/hide the password entered.

changes the administrator password for accessing the device			
Password	»····	<u>a</u>	
Confirmation	P ••••		

Image 23

Administration - SSH Access

SSH Access is available via Dropbear and an integrated SCP server.

SSH can be disabled by deleting all SSH instances. To delete, select the delete button on the top right.

○ Ian: 周 周 @
○ Ian: 周恩●
unspecified
Usten only on the given interface or, if unspecified, on all
22 Specifies the listening port of this Dropbear Instance
C (a) Allow SSH password authentication
Allow the root user to login with password
Allow remote hosts to connect to local SSH forwarded ports

Image 24

SSH	Allows you to access the device's Linux shell and file system using the Secure Shell protocol. For example, the programs PuTTY and WinSCP can be used.
Interface	Lets the device listen on a given interface or all interaces.
Port	Specifies the listening port, the default being 22.
Password Authentication	Allows SSH password authentication.
Allow root logins with password	This is enabled by default.
Gateway ports	Allow remote hosts to connect to local SSH forwarded ports.

System - SNMP

The Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

In the System » SNMP Page, you can configure SNMP V2c and SNMP V3.

SNMP Information

In the SNMP Information section, the text fields for the SNMP Enterprise ID, Contact, and Location information is shown.

SNMP Configuration

eneral Settings Trap			
nable SNMP			
NMP V2c Read Password	public		
MP V2c Write Password	private		
NMP V3 Username	admin		
MP V3 Auth Algorithm	MD5		
NMP V3 Auth Password	» ••••••	20 20	
NMP V3 Privacy Algorithm	DES		
NMP V3 Privacy Password	<i>"</i>	2	

Image 25

Enable SNMP	Enables SNMP
SNMP V2c Read Password	Sets the community string for read-only access (to the variables on the SNMP agent) by the network management station (NMS). The NMS is the software which runs on the SNMP manager. (default: public)
SNMP V2c Write Password	Sets the community string for read-write access by the SNMP manager. (default: private) A community string identifies a group of SNMP agents. It is sent in clear text. It should be changed from the default string "public" or "private". The variables on the SNMP agent can be classified into read-only or read-write variables.
SNMP V3 Username	Sets the username for authentication. (default: admin)
SNMP V3 Auth Algorithm	Shows the authentication algorithm used e.g. MD5.
SNMP V3 Password	Configures the password for user authentication. (default: password)
SNMP V3 Privacy Algorithm	Shows the data encryption algorithm used e.g. DES.
SNMP V3 Privacy Password	Sets the password for data encryption. (default: password)

SNMP Trap

1	SNMP Configuration		
	General Settings Trap		
	Enable SNMP Trap		
	SNMP Trap IP Address	192.168.1.10	
	SNMP Trap Port	162	

Image 26

Enable SNMP Trap	Allows the SNMP agent to notify the SNMP manager of events.
SNMP Trap IP Address	Sets the IP address of the SNMP Manager which receives the trap messages
SNMP Trap Port	Sets the port number.

System - LED Configuration

Strength indicator for LEDs 1, 2, 3, and 4.

The LED Configuration page customizes how the LEDs indicate the received SNR signal strength (0 to 100 with 0 being weakest).

stomizes the behaviour of the device LEDs.		
Signal strength indicator interface		
LEDRSSI		
Wireless interface	Master "Netwave-1" (ath0)	
Pignal atrongth indicator I EDa		
Signal strength indicator LEDs	10	
Signal strength indicator LEDs	[10	
Signal strength Indicator LEDs LED#1 LED#2	10 20	
Signal strength Indicator LEDs LED#1 LED#2 LED#3	10 20 30	

Image 27

Wireless InterfaceChooses the interface which the LEDs will report.Signal StrengthSets the SNR Values for radio. These values should be adjusted to help fine tuneIndicator LEDsthe alignment of the radio.

Summary of LED Indicators



LED	VISUAL CUE	INDICATION
POWER	SOLID GREEN	Power is supplied to the unit
	OFF	No power is supplied to the unit
	SOLID GREEN	LAN Connected
LAN	OFF	No Connectivity
RSSI1	SOLID RED	Weak Connection
RSSI2	SOLID ORANGE	Moderate Connection
RSSI3	SOLID GREEN	Solid Connection
RSSI4	COUD ODEEN	Excellent Connection
	SOLID GREEN	(Advisable to check Status Page to confirm RSSI is > -55)

SIGNAL STRENGTH:



WEAK SIGNAL

EXCELLENT SIGNAL

System - Backup / Flash Firmware

The Backup /Flash Firmware Page allows you to download your config, upload a config, load firmware, and reset the radio to factory defaults.

system Administration SNMP LED Configuration	Backup / Flash Firmware Reboot	
lash operations		
ctions Configuration		
Click TDPDUMP" to download tcp dumped file.		
Download TCPDUMP:	Generate tcpdump	
Backup / Restore	ent configuration files. To reset the firmware to its initial state, click "Derform reset" (only possible with r	reuschle imanaet
Download backup:	Generate archive	μασιια integes).
Reset to defaults:	@Perform reset	
To restore configuration files, you can upload a previously gen-	verated backup archive here.	
Restore backup:	Browse No file selected.	Upload archive
Flash new firmware image Upload a sysupgrade-compatible image here to replace the ru	unning firmware. Check "Keep settings" to retain the current configuration (requires an OpenWrt compa	tible firmware image).
Keep settings:		
Image:	Browse No file selected	Elash image

Image 29

Download TCP Dump	Generates a text file with TCP Dump Data.
Download Backup	Generates an archive of your configuration file.
Reset To Defaults	Resets radio to factory defaults.
Restore Backup	Restores config based on the loaded configuration file.
Keep Settings	When checked and image is loaded, the configuration will be preserved when a new image is loaded. Uncheck if the radios should be set to defaults, Recommended.
Image	Loads new software image and installs.

System - Reboots

Power cycles the radio clearing all unsaved changed.



Network

You can view and configure the interfaces of the local area network (LAN) zone.

Network address translation (NAT) occurs between these two network zones. The router that performs the NAT is called a gateway. A gateway is a network point that acts as an entrance to another network.

Status System Network Interfaces Will Static Routes LAN Interfaces	Logout Diagnostics Firewall			
Interface Overview Netw LAI B ^P (L) b-la	ork N I ∰) n	Status Uptime: 4h 4m 28s MAC-Address: C4-4B:D1:00:42:28 RX: 381 MB (2399 Pkts.) TX: 6.75 MB (21299 Pkts.) IPv4: 192:168.10.100/24 IPv6: fdd9:3d5c:7b34::1/60	Actions 🖉 Connect 🎯 Stop 🛛 🛃	Edit 🗷 Delete
Global network options		fdd9:3d5c:7b34::/48		
Reset				Save 🛛 Save & Ap

Image 31

The LAN zone (icon with two Ethernet ports) has the bridged interface "br-lan" which

consists of one physical port (icon with one Ethernet port) and two wireless networks (each icon looking like a short standing fan) on the device. Hovering the mouse over each icon would give the name of the interface it represents.

Selecting Edit or The Lan tab will direct you to the Network Interfaces Tab

Network - General Setup

LAN	
Interfaces - LAN	
On this page you can configure the network interfaces. You can bridge several intereth0 , 1).	s by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use <u>VLAN</u> notation INTERFACE. VLANNR (e.g.
Common Configuration	
General Setup Advanced Settings Physical Settings Firewall Setting	
Status	Uptime: 4h 11m 4s MAC-Address: C4.48:D1:00.42:28 ⁸⁵ Rx: 397 MS (3126 Ptks) tr-tam TX: 7.06 MB (22376 Ptks) (Ptw4: 122.468.10.1002/4 IPv6: tdd9:3d5c:7b34::1/60
Protocol	Static address
IPv4 address	192.168.10.100
IPv4 netmask	255.255.255.0
IPv4 gateway	
IPv4 broadcast	
Use custom DNS servers	*
IPv6 assignment length	60 Sign a part of given length of every public IPv6-prefix to this interface
IPv6 assignment hint	Assign prefix parts using this hexadecimal subprefix ID for this interface.
DHCP Server	
General Setup IPv6 Settings	
Ignore interface	Compared DHCP for this interface.

Image 32

Common Configuration

Status	Shows a summary of the interface for the LAN zone. This includes uptime, MAC address, bytes and packets received by the device, bytes and packets transmitted by the device, and its IPv4 and IPv6 addresses.
Protocol	Choose between various networking protocols. Static is most common but DHCP is also supported.
IPv4 Address	Static IP Address
IPv4 Netmask	Static Subnet Mask
IPv4 Gateway	Static Gateway Address
IPv4 Broadcast	Static Broadcast Address
Custom DNS	DNS Server Address
IPv6 Assignment Length	Assigns a part of a given length of every public IPv6-prefix to this interface.
IPv6 Assignment Hint	Assign a prefix using hexadecimal subprefix ID for this interface.

DHCP Server - General Setup

Ignore Interface Disabled by default, when unchecked it will provide DHCP to your network.

DHCP Server	
General Setup Advanced Settings IPv6 Settings	
Ignore interface	Disable DHCP for this interface.
Start	100 Superst leased address as offset from the network address.
Limit	150 a Maximum number of leased addresses.
Leasetime	12h Expiry time of leased addresses, minimum is 2 minutes (2m).

Image 33

With DHCP Enabled (unchecked).

Start	Lowest leased address in your DHCP pool.
Limit	Maximum number of leased addresses.
Lease time	Expiration time of leases.

DHCP Advanced Settings

General Setup Advanced Settings IPv6 Settings	
Dynamic DHCP	🗹 🔞 Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.
Force	Force DHCP on this network even if another server is detected.
IPv4. Netmask	Override the netmask sent to clients. Normally it is calculated from the subnet that is served.
DHCP-Options	Define additional DHCP options, for example "6, 192.168.2.1, 192.168.2.2" which advertises different DNS servers to clients.

Dynamic DHCP	Dynamically allocate DHCP Addresses for clients, if disabled, only clients having static leases will be served.
Force	Force DHCP ont his network even if another server is detected.
IPv4 Network	Override the netmask sent to clients.
DHCP Options	Define additional DHCP Options.

DHCP IPv6 Settings

disabled 🔹	
disabled	
disabled 💌	
	disabled • disabled • disabled •



Router Advertisement	Router Advertisement service enable and select mode; Server, Relay, or Hybrid.
DHCPv6-Service	DHCPv6 service enable and select mode; Server, Relay, or Hybrid.
NDP-Proxy	NDP Proxy enable and select mode, Relay or Hybrid.
Announced DNS Servers	List of available DNS Servers used.
Announced DNS Domain	List of domains available.

Network - LAN - Advanced Settings

General Setup Advanced Settings Physical Settings Firewall Settings	
ring up on boot	
ise builtin IPv6-management	
verride MAC address	C4:4B:D1:00:42:28
verride MTU	1500
lse gateway metric	0

Image 36

Note: Advanced settings should only be changed by Network Engineers familiar with the settings and typically do not need to be changed.

Bring up on boot	Enables the LAN interface on boot. Radio will be inaccessible if this is changed.
Use IPv6 Management	Uses the default IPv6 script for configuration.
Override MAC Address	Disabled by default, Overrides the Eth0 LAN MAC
Override MTU	Disable by default, Overwide MTU Size.
Use gateway metric	Sets the cost of using the device as a gateway.

Network - LAN - Physical Settings

Note: Physical settings should only be changed by Network Engineers familiar with the settings and typically do not need to be changed.

Image: Second
Generating Tree Protocol on this bridge
Ethernet Adapter: "bond0"
Z JE Ethernet Adapter: "etho" (lan)
2010 VLAN Interface: "eth0.1"
Ethernet Adapter: "eth1" (lan)
Ethernet Adapter: "gretap0"
Ethernet Adapter: "jp6tnl0"
Ethernet Adapter: "milireg"
Custom Interface:

Image 37

Bridge Interfaces	Allows communication between interfaces.
Enable STP	Enables Spanning Tree Protocol over the interfaces
Interfaces	List of all interfaces, please leave as defaults!

Network - LAN - Firewall Settings

Firewall settings page assigns your Firewall Rules to a particular interface. Almost all applications will want the LAN Interface checked.

 Common Configuration	
General Setup Advanced Settings Physical Settings Firewall Settings	
Create / Assign firewall-zone	● Ian: [Ian:] [] ● ()
	wan: (empty)
	unspecified -or- create:
	Choose the firewall zone you want to assign to this interface. Select unspecified to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it.

Image 38

Network - Wifi

The Network - Wifi tab is the most used tab on this webserver. All wireless provisioning will start on this page. The wireless overview page will highlight the radios current performance which helpful when configuring the devices.

Status	System Network	Logout								
	Wifi Static Routes									
wifi0: Mas	er "Netwave-1"									
Wirele	ss Overview									
	Generic Atheros 802 Channel: 36 (5.180 GHz)	2.11anac (wifi0) Bitrate: 866 Mbit/s							Scan	bbA 🖆
	SSID: Netwave-1 100% BSSID: C4:4B:D1:	Mode: Master :00:42:28 Encryption: WPA2 NONE (Co	CMP)					Disable	e 🗹 Edit	Remove
Associ	ated Stations									
	SSID	MAC-Address	IPv4-Address	Noise	Rssi	RX Rate	TX Rate	TxCCQ	Up Tir	me
	Netwave-1	C4:4B:D1:00:42:0F	?	-95 dBm	52(0,0,0)	650.0 Mbit/s	585.0 Mbit/s	87%	5 hours 23 n	nins 52 s
L										

Image 39

Network - Wifi - Wireless Overview

The Wireless Overview page will show the current wireless interface (Ath0) and its settings.

Channel	Channel the radio is communicating on.	
Bitrate	Data Rate the radio is transmitting. This will adjust depending on signal quality.	
SSID	Service Set Identifier is the broadcast ID Access Points transmit and clients receive.	
BSSID	MAC Address of the AP that is broadcasting the SSID.	
Encryption	Current encryption used.	
Scan	(Client Only) Scans channels in the selected scanlist to find available AP's.	
Add	Adds a wireless interface, for future use.	
Remove	Deletes the selected interface.	
Disable/Enable	Disable/Enable the wireless interface.	
Edit	Brings you to the Wireless Interface Settings page.	

Network - Wifi - Associated Stations

Lists the stations connected to the device. Clients will only have one associated station, the AP. AP's can have multiple Associated Stations.

Associated Stations TX Rate SSID MAC-Address IPv4-Address Noise Rssi RX Rate TxCCQ Up Time 1 C4:4B:D1:00:42:0F -95 dBm 55(0,0,0) 585.0 Mbit/s 585.0 Mbit/s 5 hours 34 mins 37 s Netwave-1 90%

WiFi Configuration

General Setup

Inaces Will Static Routes Diagnostics Firewail						
ifi0: Master "Netwave-1"						
/ireless Network: Master "Netwave-1"	(ath0)					
Davies Configuration section covers physical settings of the radio here	turner such as channel and transmit nower. Network settings like	o operation and operation mode are	grouped in the Interface Configuration	n contian		
Device Configuration - United States / Mexico	Wale such as challing and utalismic power, receiper securitys in	e encryption and operation mode are	grouped in the memore comparation	r section.		
General Setun						
Status	Mode: Master SSID: BSSID: C4/48:D1:00: Channet: 36 (5.180 G 100% Signat: 43 dBm (No Bitrate: 866.0 Mbit/s	Netwave-1 42:28 Encryption: WPA2 NONE (C Hz) Tx-Power: 24 dBm se: -95 dBm Country: US	CMP)			
Wireless network is enabled	Disable					
WIFI Standard	auto	2				
Frequency	auto	auto				
Block Dfs Channel list	🗹 😰 Block Dfs Channel list					
AP Background ACS scan	🗌 🎯 Automatically scan and s	witch to best channel after a period of tim	e, default is 60 seconds			
Scan List:	Enable Scan List					
	36 (5.180 GHz)	40 (5.200 GHz)	44 (5.220 GHz)	48 (5.240 GHz)		
	🔽 149 (5.745 GHz)	153 (5.765 GHz)	157 (5.785 GHz)	161 (5.805 GHz)		
	I65 (5.825 GHz)					
Transmit Power	27 dBm (501 mW)	1				

Image 41

Status	Shows current radio settings with connection quality icon.
Enable/Disable Wireless	Should read "Wireless network is enabled" if enabled.
WIFI Standard	Auto, 802.11a, 802.11an, 802.11ac
Spectrum Width	20,40,80MHz (Depending on Standard) *Only shown if Wifi Standard isn't in Auto.
Frequency	Select broadcast channel, leave to auto if you would like to use the Scan List.
Block DFS	Blocks DFS Channels for quicker boot.
AP Background Scan	Automatically scan and switch to best channel. Only recommended for European Countries using DFS.
Scan List	If enabled, allows you to select which channels are available to use.
Transmit Power	Sets the output power of the radio.

Wifi Advanced Settings

 Device Configuration - United States / Mexico	
General Setup Advanced Settings	
Distance Optimization	1000

Image 42

Distance	Specify the distance of the link to increase stability.
Optimization	1000 equal 1 kilometer. Only needs to be adjusted for long range links over 1 km

Wifi - Interface Configuration

The Interface Configuration section contains the section tabs for General Setup, Wireless Security, MAC-Filter, and Advanced Settings

1	Interface Configuration	
	General Setup Wireless Security MAC-Filter Advanced Settings	
	ESSID	Netwave-1
	Mode	Access Point (WDS)
	Guard Interval	Short y
	Data Rate (Mbps)	Auto
	Hide ESSID	

Image 43

ESSID	Specifies the name or extended service set identifier (ESSID) of the wireless network as it is provided in the beacon message. The network name can be up to 32 characters in length and can contain spaces. When running in AP mode, it is the name of the network as advertised in the beacon message. In Client mode, it is the network name that the client associates with.
Mode	Selects whether the device is operating as an Access Point WDS or Client WDS
BSSID	Sets the MAC address of the AP. This option is available for a device operating as a client. This is useful because there can be multiple APs with the same ESSID. Setting the MAC address would prevent the client from roaming to other APs. (Client Mode Only)
Guard Interval	Chooses between Short and Long guard intervals. Guard intervals are used to ensure that distinct transmissions do not interfere with one another. Data rate is improved in downlink and uplink if both AP and client use the Short Guard Interval.
Data Rate (Mbps)	Selects the data rate or the modulation and coding scheme (MCS). The default setting of Auto is recommended. The MCS and data rates are adjusted automatically depending on the wireless channel conditions.
Hide ESSID	Hides the network name (ESSID) from being broadcast publicly. (This option is for a device operating as an AP.)

Note: If the goal is securing your network, use WPA or preferably WPA2 encryption. Hiding the ESSID does not provide complete security.

Wireless Security

 Interface Configuration	
General Setup Wireless Security MAC-Filter Advanced Settings	
Encryption	WPA2-PSK 🔽
Cipher	Force CCMP (AES)

Image 44

Encryption Chooses between No Encryption (open) and the following encryptions: WPA-PSK, WPA2-PSK, WPA2-PSK Mixed Mode.

WPA or WPA2 with PSK

Wifi protected access (WPA) is a stronger encryption than WEP.

Furthermore, WPA2 was developed to strengthen the security of WPA and is stronger than WPA

and WEP.

For WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK Mixed Mode encryptions, we have the following options

options.

Cipher	Set to Forced CCMP (AES)
Кеу	The pre-shared key (PSK) is the password for the wireless network. This may consist
	of 8 to 63 ASCII characters. (Default: 123455678)

MAC-Filter

Interfere Configuration

MAC Filter allows you to Whitelist (Allow Listed Only) or Blacklist (Allow All Except Listed) stations.

	interface configuration		
	General Setup Wireless Security MAC-Filter Advanced Settings		
	MAC-Address Filter	Disable	
		Disable	
		Allow listed only	
*	Back to Overview 🞯 Reset	Allow all except listed	Save Dave & Apply

Interface Configuration - Advanced Settings

Interface Configuration	
General Setup Wireless Security MAC-Filter Advanced Settings	
802.11h (Transmit Power Control)	
Multicast Rate	1000
Fragmentation Threshold	2346 C Default is 2346 bytes. Range is 256 to 2346
RTS/CTS Threshold	2346 C Default is 2347 bytes. Range is 0 to 2347
WMM Mode (WIFI Multimedia)	🗹 🕲 Ensures applications that require better throughput are inserted in queues with higher priority.

Image 46

802.11H	Transmit Power Control, can modulate power based on interference with satellites and radar.
Multicast Rate	Set a baseline for wifi devices to be able to connect to router.
Fragmentation Threshold	The default size of the fragmentation threshold is 2346 bytes and the standard range is 256 - 2346 bytes. It is used to specify the maximum size for a data packet before being fragmented into multiple packets.
RTS/CTS Threshold	The RTS/CTS packet size threshold is 0-2347 octets. Typically, sending RTS/CTS frames does not occur unless the packet size exceeds this threshold. If the packet size that the node wants to transmit is larger than the threshold, the RTS/CTS handshake gets triggered. Otherwise, the data frame gets sent immediately.
WMM Mode	Provides Quality of Service (QoS) features, checked by default. Wireless multimedia enables the classification of the network traffic into 4 main types, voice, video, best effort, and background, in decreasing order of priority. Higher priority traffic has a higher transmission opportunity and would have to wait less time to transmit. As a result, an existing video stream would not be interrupted by additional background processes.

Routing

The NetWave radio is a full gateway with Static Route capabilities.

Routing should be configured by certified Network Professionals.

Status System Network Logout	ilos Firewall				
loutes					
outes specify over which interface and gateway a	a certain host or network can be reached.				
Static IPv4 Routes	5 - 3.61				
Interface 📹	Target Host-IP or Network	IPv4-Netmask if target is a network	IPv4-Gateway	Metric	мто
		This section contains no values vet			
Add		,			
Static IPv6 Routes					
Interface 🖷	Targ	jet	IPv6-Gateway	Metric	MTU
	IPv6-Address or M	Network (CIDR)			
		This section contains no values yet			
Add					
Reset					Save Save & A

Image 47

Diagnostic Tools

The following Diagnostic tools are available:

- » Ping
- » TraceRoute
- » NSLookup

Status System Network Logout Interfaces W/fi Static Routes Diagnostics Firew	ali				
Diagnostics					
Network Utilities					
dev.openwrt.org	dev.openwrt.org	dev.openwrt.org			
IPv4 - Ping	Traceroute	INSlookup			
	Install iputils-traceroute6 for IPv6 traceroute				

Firewall

The Network - Firewall page contains the subpages for General Firewall Settings, Port Forwards, and Traffic Rules.

General Settings

terfaces Wifi St	atic Routes Diagnostics Firew	all		te da tada ta ta ta ta ta ta ta ta ta	ter hante hannen ter her her her hande, her hande her h	alle lle lle lle lle lle le le le le le l	e, e
eneral Settings Po	rt Forwards Traffic Rules Cus	iom Rules					
rowall - Zon	o Cottings						
rewaii - Zon	e settings						
firewall creates zones	over your network interfaces to cont	rol network traffic flow.					
Seneral Settings							
Enable SYN-flood pro	tection						
Drop invalid packets							
Input			accept		-		
Output			accept		-		
Convord			becepe				
Forward			reject		ĭ		
Zones							
	Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan:	lan: 🚂 🚂 🙊 ⇒ wan	accept	• accept	accept -			Edit Delete
w	an: (empty) ⇒ REJECT	reject	- accept	• reject •			ZEdit Delete
bba	L						
Decet							Save Save &

Image 49

Enable SYN-Flood	Prevents SYN DDoS Attacks
Drop invalid Packets	Blocked forged packets
Input	Accept Inbound traffic
Output	Forward outbound traffic
Forward	Forward all traffic

Zones

Topos

Specify your network zone rules.

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan: lan: 🛃 🛃 🙊 🔿 wan	accept	• accept	accept 🔹			ZEdit Delete
wan: (empty) ⇒ REJECT	reject	 accept 	reject -			ZEdit Delete

Firewall Port Forward

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

The Network » Firewall » Port Forwards page lets you define the protocol and port number to access an internal IP address.

Status System Network Logout				
Interfaces Wifi Static Routes Diagnostics Firewall				
General Settings Port Forwards Traffic Rules Custom Rul	les			
Firewall - Port Forwards				
Port forwarding allows remote computers on the Internet to connect to	o a specific computer or service within the private LAN.			
Port Forwards				
Name	Match		Forward to	Enable Sort
	This secti	on contains no values yet		
	New port forward:			
Name Protocol External zone	External port Internal zone Internal IP address	Internal port		
New port forward TCP+UDP wan	lan 🛃	bbA		
Reset				Save Save & Apply
マインレント しんしん しんしん しんしん しんしん しんしん	しにん さんせい さん ひん ひん ひん ひん ひん ひん ひん ひん	さんだいにたいかだいだいにたいにたいにたい	ささださんたいかたちたたたたたたた しんしいたん	ささたいいににたいにににんにたいにの

Image 51

Traffic Rules

Traffic rules define policies for packets travelling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

Firewall	-	Traffic	Rul	es

Match IPv4.UCP From any host in wan To any router IP at port 68 on this device IPv4.UCM with type acho-request From any host in wan To any router I/ on this device IPv4.4GMP From any host in wan To any router // on this device IPv4.4GMP From any host in wan To any router // on this device IPv4.4GMP	Action Accept input Accept input Accept input Accept input		Sort	☑Edit ×Delei ☑Edit ×Delet
IPv4.UDP From any host in wan To any router IP at port 89 on this device IPv4.CMP with type acto-request From any host in wan To any router I/e on this device IPv4.4CMP From any host in wan To any router I/e on this device	Accept input Accept input Accept input	2	••	Edit Delei
From any host in wan To any couter of the at port 68 on this device IEV-44-CMB with type actio-request From any host in wan To any nouter IP on this device IEV-4-GMB From any host in wan To any nouter IP on this device IEV-4-GMB	Accept input Accept input Accept input		•••	Edit Delei
To any router / Part port 36 on his device IIP-4-LOW with type acho-request From any host in wan To any router / Fon this device IIP-4-LOWP From any host in wan To any router / Fon this device	Accept input Accept input		•	Edit Dele
IIP-V41CMP with type acto-request Form any host in wan To any router / for on this device IIP-V44CMP Form any host in wan To any router / for a this device IIP-V4-UDP	Accept input Accept input		•	Edit Dele
From any hosts in wan To any router /P on this device IPV4-HOMP From any hosts in wan To any router /P on this device IPV4-UDP	Accept input		99	Edit Dele
ito any notice in on source IPV4-IGMP From any host in wan To any notice / From this device IPV4-UDP	Accept input	-		
Form any host in wan To any notatin i wan To any notatin / i on a his device	Accept input	-		
To any router IP on this device	Mocopt input			
Prove DP		-		
IFW-ODF				
From IP rance (e80*/10 in way with source port 547	Accept input	$\overline{\checkmark}$		
To IP range fe80://20 at port 546 on this device				
IPv64CMP with types 130/0, 131/0, 132/0, 143/0				
From IP range /e80::/10 in wan	Accept input	\sim	* *	ZEdit > Dele
To any router IP on this device		_		
with types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type, router-solicitation, neighbour-solicitation, router-advertisement,				
neighbour-advertisement	Accept input and limit to 1000 pkts, per second			
From any host in wan	Accept input and inflit to 1000 pkts, per second			
To any router IP on this device				
IPv6-ICMP with types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type		_		
From any host in wan	Accept forward and limit to 1000 pkts. per second	\sim	4 -	ZEdit Dele
To any host in any zone				
Any IPSEC-ESP	NUCLEAR DRAWLER	-		
From any host in wan	Accept forward	\sim	0	ZEdit ZDele
To any host in lan				
Any UDP	1000120001			
From any host in wan	Accept forward	×		
	I OF Hage ROUCT VARIANT ON UTING VARIANT I OF A CHARM WIT ON UTING VARIANT I ON UTING VARIANTI I ON UTING VARIANT I ON UTING VARIANTI I ON UTING VA	IN Prediction With Spee Sold(13) (130) (130) (130) (130) Accept input IP Vei-ICM With Spee Sold(13) (130) (130) (130) (130) Accept input With Spee Sold(13) (130) (130) (130) (130) (130) Accept input With Spee Sold(13) (130)	In the index inde	IDENTIFY IDENTIFY <td< td=""></td<>

Agency Compliance

FCC

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

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

Industry Canada

This Class A digital apparatus complies with Canadian ICES-003. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that permitted for successful communication. This device complies with Industry Canada license-exempt RSS standard(s).

Operation is subject to the following two conditions:

- This device may not cause interference, and
- This device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil numérique de la classe A est confrome à la norme NMB-003 Canada. Pour réduire le risque d'interférence aux autres utilisateurs, le type d'antenne et son gain doivent être choisies de façon que la puissance isotrope rayonnée équivalente (PIRE) ne dépasse pas ce qui est nécessaire

pour une communication réussie. Cet appareil est conforme à la norme RSS Industrie Canada exempts de licence norme(s). Son fonctionnement est soumis aux deux conditions suivantes:

17 Compliance

- Cet appareil ne peut pas provoquer d'interférences et
- Cet appareil doit accepter toute interférence, y compris les interférences qui peuvent

causer un mauvais fonctionnement du dispositif.

RF Exposure Warning

The antennas used for this transmitter must be installed to provide a separation distance of at least 2.52m from all persons and must not be located or operating in conjunction with any other antenna or transmitter.

Les antennes utilisées pour ce transmetteur doivent être installé en considérant une distance de séparation de toute personnes d'au moins 2.52m et ne doivent pas être localisé ou utilisé en conflit avec tout autre antenne ou transmetteur.

CE Marking

CE marking on this product represents the product is in compliance with all directives that are applicable to it.

This equipment may be operated in the following countries:

Great Britain and Northern Ireland, Austria, Belgium, Denmark, Finland, France, Germany, Ireland, Italy, Netherlands, Norway, Portugal, Romania, Switzerland, Sweden

Installer Compliance Responsibility

Devices must be professionally installed and it is the professional installer's responsibility to make sure the device is operated within local country regulatory requirements.

RoHS/WEEE Compliance Statement

European Directive 2002/96/EC requires that the equipment bearing this symbol on the product and/or its packaging must not be disposed of with unsorted municipal waste. The symbol indicates that this product should be disposed of separately from regular household waste streams. It is your responsibility to dispose of this and other electric and electronic equipment via designated collection facilities appointed by the government or local authorities. Correct disposal and recycling will help prevent potential negative consequences to the environment and human health. For more detailed information about the disposal of your old equipment, please contact your local authorities, waste disposal service, or the shop where you purchased the product.

GPL (General Public License) Statement

You may have received from ComNet products that contained - in part - free software (software licensed in a way that ensures your freedom to run, copy, distribute, study, change and improve the software). Such products include NetWave series of products.

As part of these products, ComNet may have distributed to you hardware and/or software that contained a version of free software programs developed by the Free Software Foundation, a separate not-for-profit organization without any affiliation to ComNet.

See <u>http://www.gnu.org/philosophy/free-sw.html</u> for more details. If ComNet distributed any portions of these free software programs to you, you were granted a license to that software under the terms of either the GNU General Public License or GNU Lesser General Public License "License", copies of which are available from <u>http://www.gnu.org/licenses/licenses.html</u>. The Licenses allow you to freely copy, modify and redistribute that software without any other statement or documentation from us.

ComNet will provide to anyone who contacts us at the contact provided below, for a charge of no more than our cost of physically performing source code distribution, a complete machinereadable copy of the complete corresponding source code for the free software programs used in the version of the programs that we distribute to you. The cost will be free if the delivery medium of the machine-readable copy is through the Internet.

Contact information:

Email: techsupport@comnet.net

Tel: 203-796-5300

Address: 3 Corporate Drive, Danbury, CT 06810 USA

We will reply within 7 working days once the request has been made through email or telephone.

ComNet Customer Service

Customer Care is ComNet Technology's global service center, where our professional staff is ready to answer your questions at any time. Email ComNet Global Service Center: customercare@comnet.net



© 2021 Communication Networks Corporation. All Rights Reserved.

"ComNet" and the "ComNet Logo" are registered trademarks of Communication Networks, LLC.

3 CORPORATE DRIVE | DANBURY, CT 06810 | USA T: 203.796.5300 | F: 203.796.5303 TECH SUPPORT: 1.888.678.9427 INFO@COMNET.NET

SUITE 7, CASTLEGATE BUSINESS PARK CALDICOT | SOUTH WALES, UK | NP26 5AD T: +44 (0) 2036 300 695 | F: +44 (0)113 253 7462 INFO-EUROPE@COMNET.NET



NETWAVE