



**This manual serves the following
ComNet Model Numbers:**

NW7
NW7E

INSTALLATION AND OPERATION MANUAL



ENVIRONMENTALLY HARDENED HIGH THROUGHPUT 802.11A/N WIRELESS ETHERNET DEVICE

Thank you for purchasing NetWave® from ComNet. This installation guide applies to the following models:

NW7: Individual Hardened Single Radio, Two Gb Ethernet Ports, One internal 19dBi 17° beamwidth directional antenna, Includes power injection module, line cord and mounting assembly, Port 1 Supports 802.3af/at PD PoE Power, Port 2 provides IEEE802.3at PSE PoE Power, FCC certified for use in the NA Region.

NW7E: Individual Hardened Single Radio, Two Gb Ethernet Ports, One internal 19dBi 17° beamwidth directional antenna, Includes power injection module, line cord and mounting assembly, Port 1 Supports 802.3af/at PD PoE Power, Port 2 provides IEEE802.3at PSE PoE Power, ETSI certified for use in the EU Region.

The NetWave® NW7[E] environmentally hardened high throughput (HT) 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 multi-point applications and comes with an integrated 19dBi, 17° beamwidth antenna. The NW7[E] supports up to 240Mbps throughput using MIMO technology. The units can be powered by an 802.3af/at PoE Compliant device or through a supplied power injection module with the second Ethernet port serving as an IEEE802.3at power source. The NW7 is FCC certified for use in North America and the NW7E is ETSI, DFS and TPC certified for use in the European Union.

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:

- » NW7/NW7E Datasheets
- » NW7/NW7E Quick Start Guides

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	4
Legal Information	4
1.0 Introduction	5
2.0 Point to Multi-Point - NW7 and NW7E	6
3.0 Point-to-Point Systems - NW7 and NW7E	7
4.0 PoE Pass-through Port - NW7 and NW7E	8
5.0 Cabling Requirements	9
6.0 Hardware Installation	10
6.1 NW7 and NW7E Outdoor Ethernet Gland Installation	10
6.2 NW7 and NW7E Indicating LED Details	12
6.3 NW7 and NW7E Outdoor Standard Mounting Hardware	13
6.4 NW7 and NW7E Outdoor Upgrade Mounting Hardware	14
7.0 Detailed Power Requirements	15
8.0 Key Default Configurations	16
9.0 Quick Configuration	17
10.1 STATUS Page - Access Point	18
10.2 STATUS Client Page - Client	21
10.3 WIRELESS SETTINGS Page - Access Point	24
10.4 WIRELESS SETTINGS - Client Page - Client	29
10.5 NETWORK SETTINGS - Client or Access Point	33
10.6 SYSTEM TOOLS Page - Client and Access Point	36
10.7 ADMIN Page - Client or Access Point	41
11.0 Agency Compliance	46
12.0 GPL (General Public License) Statement	48

Overview

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 © 2013 ComNet. All rights reserved.

Disclaimer

ComNet reserves the right to make changes in specifications at any time without notice. The information furnished by ComNet in this material is believed to be accurate and reliable. However, ComNet assumes no responsibility for its use.

1.0 Introduction

The NetWave® environmentally hardened high throughput (HT) 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 multi-point applications and comes with an integrated 19dBi, 17° beamwidth antenna. The NW7[E] supports up to 240Mbps throughput using MIMO technology. The units can be powered by an 802.3af/at PoE Compliant device or through a supplied power injection module with the second Ethernet port serving as an IEEE802.3at power source. The NW7 is FCC certified for use in North America and the NW7E is ETSI, DFS and TPC certified for use in the European Union.

This manual contains detailed operational and configuration information not covered in the quick start guides.

This guide applies to the following models:

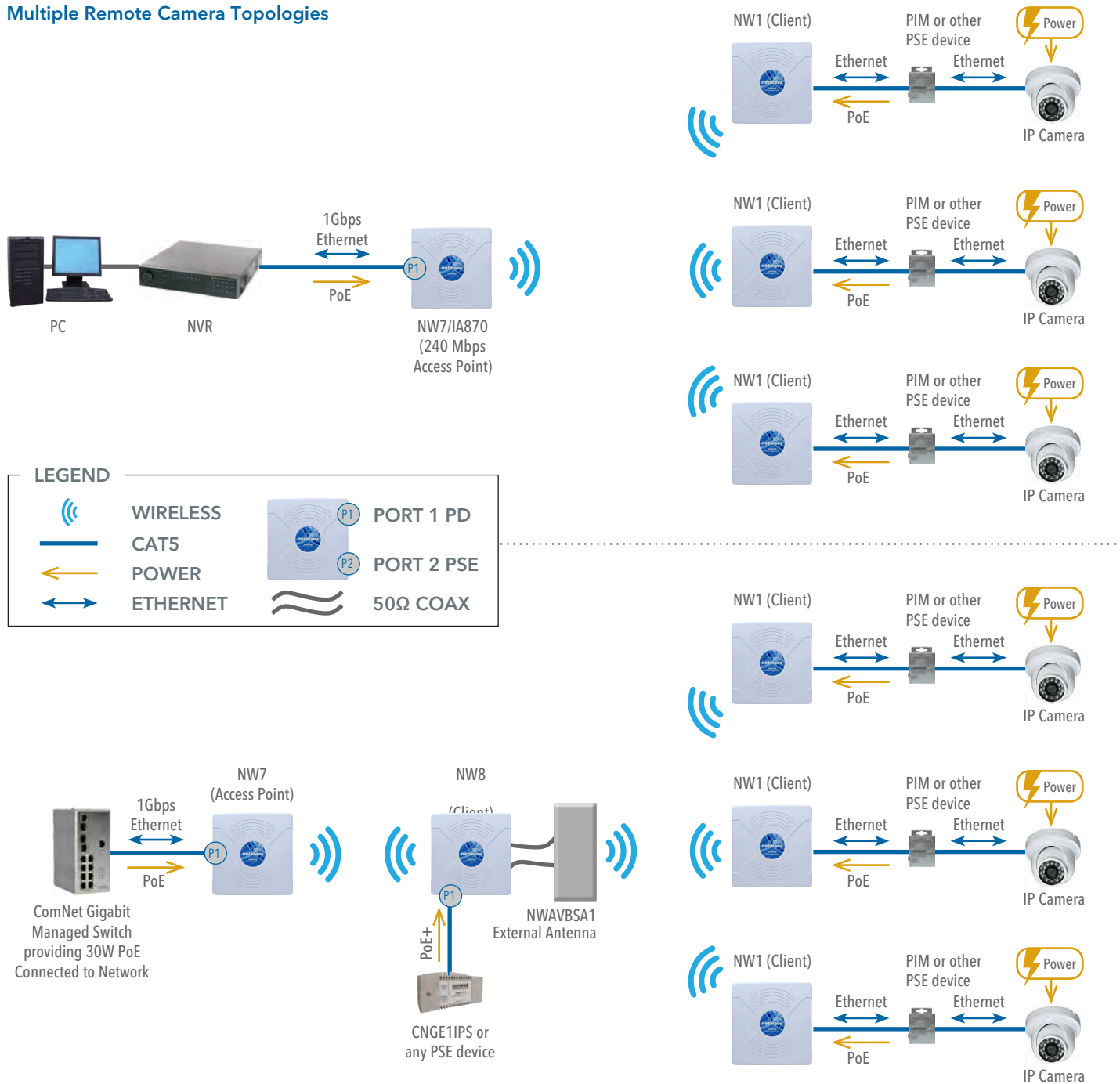
- NW7 - Individual Hardened Single Radio, Two Gb Ethernet Ports, one internal 19dBi 17° beamwidth directional antenna, Includes power injection module, line cord and mounting assembly, Port 1 Supports 802.3af/at PD PoE Power, Port 2 provides IEEE802.3at PSE PoE Power, FCC certified for use in the NA Region.

- NW7E - Individual Hardened Single Radio, Two Gb Ethernet Ports, one internal 19dBi 17° beamwidth directional antenna, Includes power injection module, line cord and mounting assembly, Port 1 Supports 802.3af/at PD PoE Power, Port 2 provides IEEE802.3at PSE PoE Power, ETSI certified for use in the EU Region.

2.0 Point to Multi-Point - NW7 and NW7E

These individual units allow the user to configure for either multipoint access point or client operation. The NW7[E] supports integrated 19dBi 17° directional antenna or an optional 8dBi 70° internal antenna. See the ComNet website for the latest information regarding antenna support.

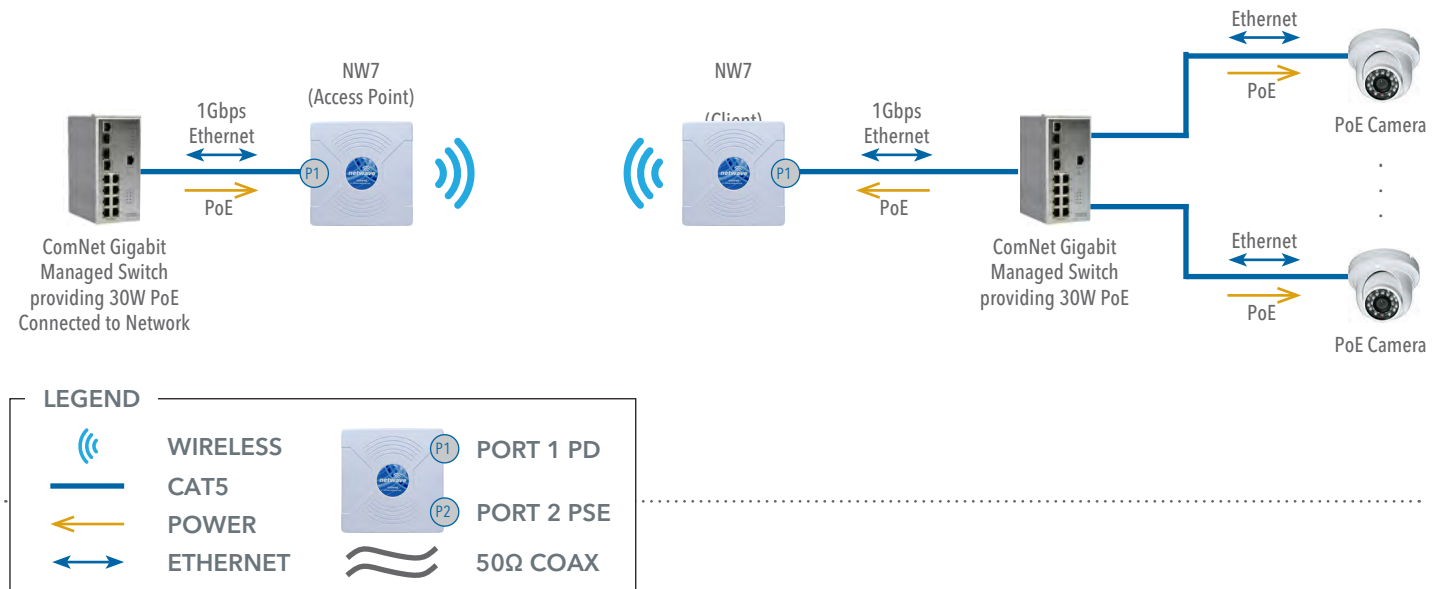
Multiple Remote Camera Topologies



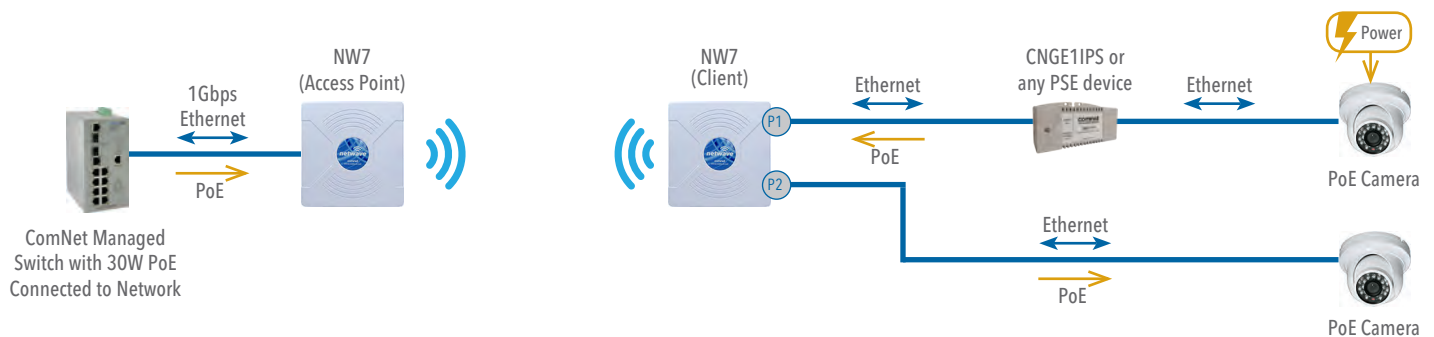
3.0 Point-to-Point Systems - NW7 and NW7E

In a point-to-point design, the client has the added feature of MAC Address Locking which is not available in a point to multipoint design. MAC Lock enables higher operating EIRP and increased security for FCC versions.

High Throughput Point-to-Point Topology (Shown with PoE Cameras)

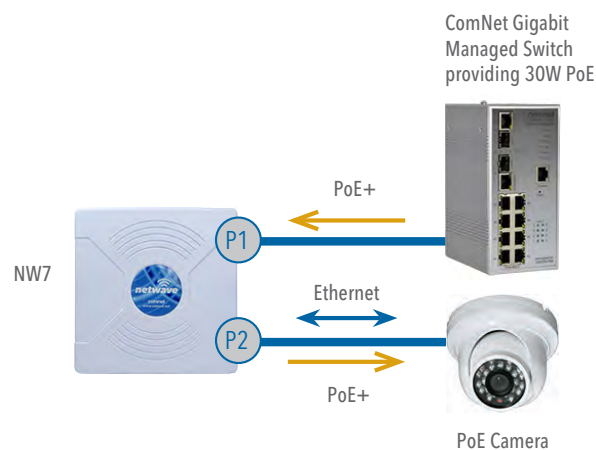
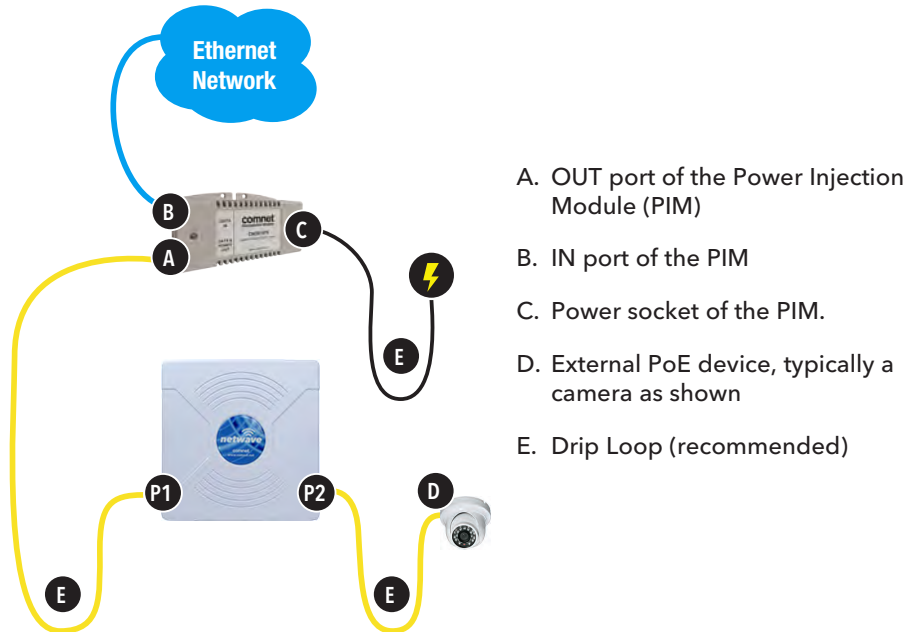


Point-to-Point Topology (Shown with PoE Injector and PoE Powered Cameras)



4.0 PoE Pass-through Port - NW7 and NW7E

The NetWave NW7 and NW7E come with dual Gigabit Ethernet ports. Port 1 supports IEEE 802.3af/at PD PoE power and Port 2 is a Power over Ethernet IEEE 802.3at PSE (Power Sourcing Equipment) port that acts as a voltage source and supplies PoE PD devices with power via the Ethernet cable.



5.0 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 www.comnet.net/comnet-products/cables



6.0 Hardware Installation

6.1 NW7 and NW7E Outdoor Ethernet Gland Installation

There will be two cable glands and a weather seal cap included with each outdoor enclosure. The provided weather seal cap should be used when Port 2 is not in use to prevent damage to the port and the wireless device.

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 as shown, push the split rubber gasket into place and loosely screw the cap that goes over the rubber washer.



Below is an image with the Ethernet connection made to the node and the gland assembly about to be installed.



Once the RJ45 connection has been made, screw in the gland into the housing making sure it is tight enough for a water tight seal but not so tight to cause the rubber seal to squeeze off.

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 below.

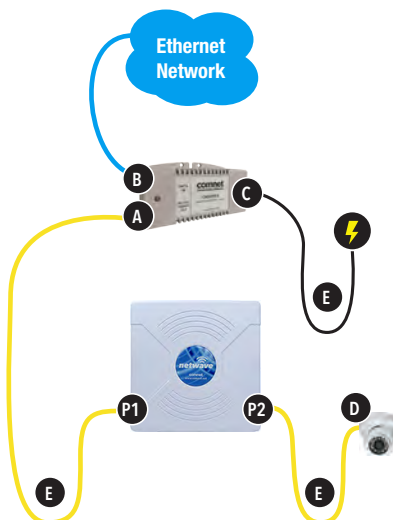


Connect one end of an RJ-45 Ethernet cable to the LAN OUT port of the Power Injection Module (PIM) and the other end to LAN of the access point - as shown below.

Note: : *Maximum length of the RJ-45 CAT5 cable is 100 meters without powering a second device connected to port 2.*

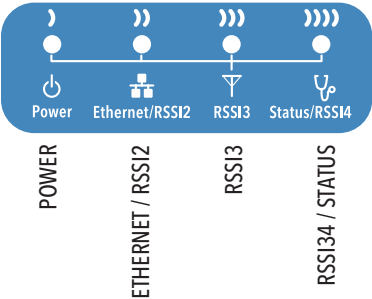
Connect the RJ-45 Ethernet cable attached to the PIM to a network device, such as a switch or to the configuration PC. Then plug the power cord to an AC power outlet and IEC plug into the socket of the PIM - as shown in the diagram below.

Note: *DC Passive PoE input is 48 to 57 VDC. If powering a second device from Port 2, it is recommended not to exceed 20 meters from the PIM/PoE+ PSE to the Access Point and not to exceed 5 meters from the AP to the Camera or secondary device.*



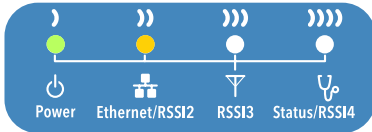
When mounting the hardware outdoors, it is highly recommended to create a drip loop with the Ethernet cable to prevent moisture from getting into the gland.

6.2 NW7 and NW7E Indicating LED Details

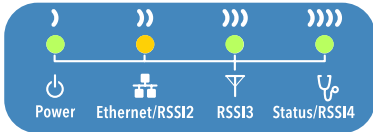
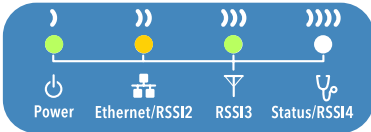


LED	VISUAL CUE	INDICATION
POWER	SOLID GREEN	Power is supplied to the NW7/NW7E
	OFF	No power is supplied to the NW7/NW7E
ETHERNET / RSSI2	FLASH GREEN	Ethernet connection is established
	SOLID YELLOW	Ethernet connection is established and there is activity present RSSI Level is > Yellow LED Threshold
	OFF	No Ethernet connection established. RSSI Level is < Yellow LED Threshold
RSSI3	SOLID GREEN	Good signal strength
RSSI4 / STATUS	FLASH GREEN	Unit is booting up
	SOLID GREEN	Excellent signal strength (Advisable to check Status Page to confirm RSSI is <70)

SIGNAL STRENGTH:



MINIMUM SIGNAL



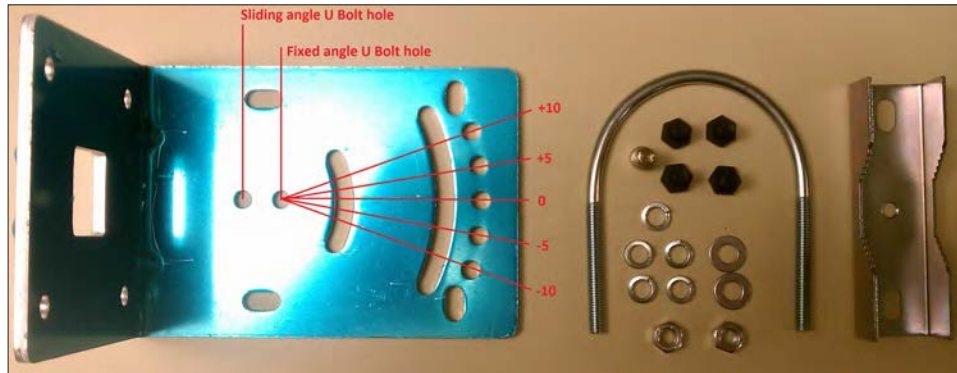
MAXIMUM SIGNAL

- Power - will illuminate when there is power applied to the Ethernet port
- Ethernet - will illuminate when there is an active Ethernet connection
- RSSI3 - will illuminate when the RSSI threshold goes above what is set in the RSSI LED Setting section of the WIRELESS SETTINGS page
- Status/RSSI4 - Provided status during boot and will illuminate solid when the RSSI threshold goes above what is set in the RSSI LED Setting section of the WIRELESS SETTINGS page

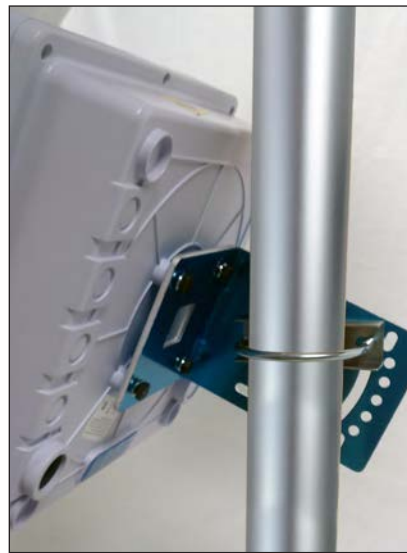
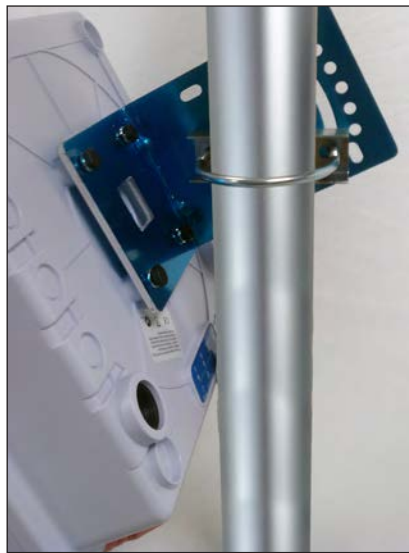
6.3 NW7 and NW7E Outdoor Standard Mounting Hardware

This mounting hardware will support pole diameters up to 3 in (7.6 cm).

Below are the parts contained in the standard mounting hardware



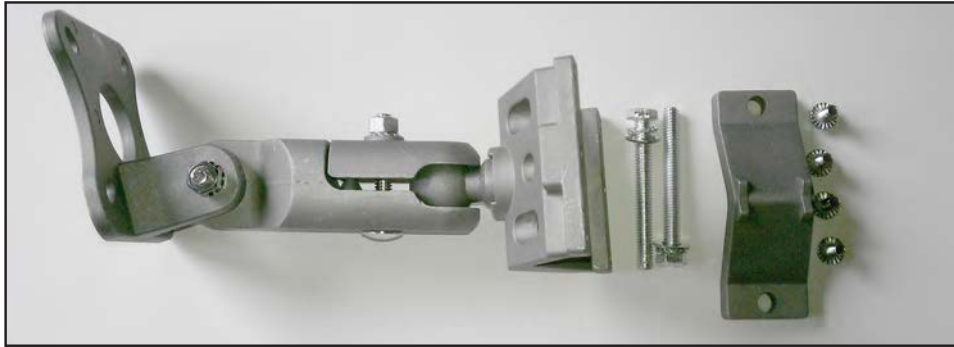
Here is the mounting hardware assembled shown in a $+45^\circ$ and -45° vertical position



6.4 NW7 and NW7E Outdoor Upgrade Mounting Hardware

An upgrade to the outdoor mounting hardware is available. This optional version is of heavier construction supporting an articulating joint and is designed for wall or pole mount supporting up to a 3 inch (76 mm) pole.

Note: *This hardware is sold separately under part number NWBKT1*



7.0 Key Default Configurations

IP Address of Web Server	192.168.10.101
LAN Mode for Web Server	Static Addressing
Web Server User ID	admin
Web Server Password	admin
Web Server Guest User ID	guest
Web Server Guest Password	guest
SSID	NetWave-1
WPA Pre-shared Key	12345678
Channel-Frequency (AP)	Auto
Channel Spectrum Width	20/40M
Long Range Parameters	Enabled and defaulted to 1000m
STP	Disabled

Note: A Reset to defaults (performed on the ADMIN page) will erase all user configurations.

8.0 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 mains power 90 – 240 VAC to the Power Injection Module with the provided power cord. 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.
5. Point the browser to 192.168.10.101. This is the default address.
6. A login prompt will pop up. Enter:
ID admin
Password admin
7. Select the NETWORK SETTINGS tab and set the desired network settings.
Select Apply Settings
Select 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 WIRELESS SETTINGS tab and set:
 - Wireless mode – Set to AP or Client
 - Country code – Only required if setting up the NW7E (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 RSSI is greater than 70, it is recommended to reduce RF TX power at the remote/ connected node.
 - Set SSID – if changing from the default setting
 - Channel Spectrum Width – May want to reduce to 20M or even 10M from the default 20/40M if the 5GHz spectrum is crowded or experiencing unstable connections across the link.
 - Wireless Security – if changing from default settings
 - Select Apply Settings
 - Select Save

Note: *: NW7 and NW7E nodes may need to have the Wireless Mode set to either AP or Client (default is Client). The unit IP addresses will need to be all set to different addresses (default address is 192.168.10.101). This is the IP address of the embedded configuration web server. Therefore, it is recommended that configuration be performed one at a time and prior to deployment.*

9.0 Detailed Configuration

9.1 STATUS Page - Access Point

comnet netwave

STATUS WIRELESS SETTINGS NETWORK SETTINGS SYSTEM TOOLS ADMIN

MAIN

Uptime: 0 Days 22:06:21
System Time: 01/01/2000 14:06:22

VERSION

Firmware Version: NW3_V1.0.2

LAN SETTING

LAN MAC: 00-22-3b-0d-00-03
Address Mode: static
IP Address: 192.168.10.101
Gateway IP Address: 192.168.10.1
LAN Port Connection Status: Plugged

Radio 1

Wireless Mode: Access Point WDS
Local AP SSID: Netwave-1
Frequency: 5.765 GHz
MAC: 00-22-3b-0d-00-04
Local AP MAC: 00-22-3b-0d-00-04
Security: WPA2
Refresh

CONNECTED STATIONS {0}

MAC Address	Signal Strength	Tx Rate	Tx CCQ(Client Conn Quality)	Rx Rate	Channel Width
LOCAL AP STATISTICS					
	Bytes	Packets	Errors		
Received:	0	0	0		
Transmitted:	0	0	0		
LOCAL AP ERRORS					
RX Invalid NWID:	1	TX Excessive Retries:		0	
RX Invalid Crypt:	0	Missed Beacons:		0	
RX Invalid Frag:	0	Other Errors:		0	

9.1.1 STATUS_AP Page MAIN Section

This section will list the unit uptime as well as the system time which can be set on the SYSTEM TOOLS page.

9.1.2 STATUS_AP Page LAN SETTING Section

LAN MAC	Lists the MAC address for the electrical copper Ethernet port
Address Mode	Shows the current setting for setting the IP address for the embedded web server. This is configured on the NETWORK SETTINGS page
IP Address	Current IP address for the embedded web server
Gateway IP Address	IP address for the network gateway
LAN Port Connections	Shows connection status for copper Ethernet ports 1 and 2.

9.1.3 STATUS_AP Page RADIO Section

Wireless Mode	Shows the operational mode for the radio. This can be set on the WIRELESS SETTINGS page.
Local AP SSID	SSID that this AP is broadcasting.
Frequency	Frequency that the AP is operating on
MAC	MAC address of the AP radio
Local AP MAC	MAC address of the AP radio
Security	Operating security. This can be selected on the WIRELESS SETTINGS page

9.1.4 STATUS_AP Page CONNECTED STATIONS Section

MAC Address	Lists the MAC addresses of the connected stations
Signal Strength	Lists the RSSI values of the connected stations
Tx Rate	Displays the transmit radio connection rate
Tx CCQ	Client Connection Quality. Given in % and provide the radio connection quality with the connected AP with 100% being the best.
Channel Width	The channel width that the radio connection is using. This is automatically determined based on the radio connection quality when 20/40M channel bandwidth is selected on the WIRELESS SETTINGS page. Possible connections that may be displayed are listed below starting with the best/fastest connection HT40+ HT40 HT40- HT20 HT10
Refresh Button	This will cause the data that feeds this page to be refreshed.

9.1.5 STATUS_AP Page LOCAL AP ERRORS Section

RX Invalid NWID	Shows the number of SSIDs detected that is different from the Remote AP SSID. This number will continually count up and will count up faster in congested RF environments. It is normal to see this count increase.
RX Invalid Crypt	Represents the number of transmitted and received packets which were encrypted with the wrong encryption key and failed the decryption routines. It can be used to detect invalid wireless security settings and encryption break attempts.
RX Invalid Frags	This value represents dropped packets due to packet reassembly failure due to link layer fragments.
TX Excessive Retries	Represents the number of packet delivery failures. Undelivered packets are retransmitted a set number of times before an error is logged and counted.
Missed Beacons	Beacons are management packets sent by an AP and this value represents the number of beacons which were not received by the client. Missed Beacon counts could indicate that there is too much distance between the Client and AP.
Other Errors	This count represents the total number of transmitted and received packets that were lost or discarded for reasons other than what is listed above.

9.2 STATUS Client Page - Client

comnet netwave

STATUS | NETWORK | SYSTEM | ADMIN

MAIN

Uptime: 0 Days 00:09:26
System Time: 12/31/1999 16:09:37

VERSION

Firmware Version: Nw3_v1.0.2

LAN SETTING

LAN MAC: 00-22-39-0d-00-03
Address Mode: static
IP Address: 192.168.10.101
Gateway IP Address: 192.168.10.1
LAN Port Connection Status: Plugged

Antenna Alignment

Signal Strength: 47 dBm
Left/Right Chain: 46,37
Noise Level: -120 dBm

Radio 1

Wireless Mode: Station WDS
Remote AP SSID: Trunkline 2
Signal Strength: 45(45,35)
TX Rate: 300M
TX CQ (Client Conn Quality): 94%
Frequency: 5.760 GHz

MAC: 00-22-39-0d-00-04
Remote AP MAC: 00-22-39-01-6C-08
Noise level: -120 dBm
RX Rate: 6M
Channel Width: HT40+
Security: WPA2

LOCAL STATION STATISTICS

	Bytes	Packets	Errors
Received:	20716	174	0
Transmitted:	9553	72	0

LOCAL STATION ERRORS

RX Invalid MFRM:	0	TX Frame Retries:	0
RX Invalid Crypt:	0	Missed Beacons:	0
RX Invalid Page:	0	Other Errors:	0

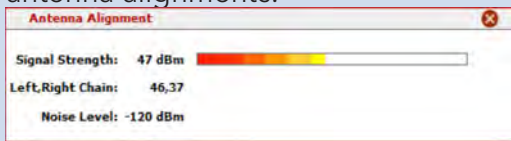
9.2.1 STATUS-Client Page MAIN Section

This section will list the unit uptime as well as the system time which can be set on the SYSTEM TOOLS page.

9.2.2 STATUS-Client Page LAN SETTING Section

LAN MAC	Lists the MAC address for the electrical copper Ethernet port
Address Mode	Shows the current setting for setting the IP address for the embedded web server. This is configured on the NETWORK SETTINGS page
IP Address	Current IP address for the embedded web server
Gateway IP Address	IP address for the network gateway
LAN Port Connections	Shows connection status for copper Ethernet ports 1 and 2.

9.2.3 STATUS-Client Page RADIO Section

Wireless Mode	Lists the operational mode for the radio. This can be set on the WIRELESS SETTINGS page.
Remote AP SSID	SSID for that the client will scan and connect to.
Noise Level	Receiver noise floor. A higher number indicates an operating environment with more RF noise/congestion.
Signal Strength	Received signal strength.
TX Rate	Radio connect rate for the transmit portion
RX Rate	Radio connect rate for the receive portion
TX CCQ	Client Connection Quality. Given in % and provide the radio connection quality with the connected AP with 100% being the best.
Frequency	Frequency the client is using to connect to the AP
MAC	MAC address of the client radio
Remote AP MAC	MAC address of the connected AP radio
Channel Width	channel width the radio connection is using. This is automatically determined based on the radio connection quality when 20/40M channel bandwidth is selected on the WIRELESS SETTINGS page. Possible connections that may be displayed are listed below starting with the best/fastest connection HT40+ HT40 HT40- HT20 HT10
Security	Operating security. This can be selected on the WIRELESS SETTINGS page
Align Button	<p>This will produce a pop up Antenna Alignment window (shown below) that will render a graphical RSSI meter. This meter will present a scale between 0 and 100. This tool may be helpful when performing antenna alignments.</p>  <p>NOTE: RSSI values above 70 will begin to cause reduction of link throughput. RSSI values greater than 75 will significantly reduce link throughput but RSSI values this high are normally experienced during bench testing.</p>
Refresh Button	This will cause the data that feeds this page to be refreshed.

9.2.4 STATUS-Client Page LOCAL STATION STATICS Section

Received	Shows Bytes, Packets, and Errors received
Transmitted	Shows Bytes, Packets, and Errors transmitted

9.2.5 STATUS-Client Page LOCAL STATION ERROR Section

RX Invalid NWID	Shows the number of SSIDs detected that is different from the Remote AP SSID. This number will continually count up and will count up faster in congested RF environments. It is normal to see this count increase.
RX Invalid Crypt	Represents the number of transmitted and received packets which were encrypted with the wrong encryption key and failed the decryption routines. It can be used to detect invalid wireless security settings and encryption break attempts.
RX Invalid Frags	This value represents dropped packets due to packet reassembly failure due to link layer fragments.
TX Excessive Retries	Represents the number of packet delivery failures. Undelivered packets are retransmitted a set number of times before an error is logged and counted.
Missed Beacons	Beacons are management packets sent by an AP and this value represents the number of beacons which were not received by the client. Missed Beacon counts could indicate that there is too much distance between the Client and AP.
Other Errors	This count represents the total number of transmitted and received packets that were lost or discarded for reasons other than what is listed above.

9.3 WIRELESS SETTINGS Page - Access Point

comnet
netwave

STATUS WIRELESS SETTINGS NETWORK SETTINGS SYSTEM TOOLS ADMIN

Apply Settings

BASIC WIRELESS SETTINGS (RADIO 1)

Wireless Mode: Access Point

Local AP-ESSID: Airwave-1 ☐ Hide SSID

Country Code: United States of America

Wireless Profile: 1a

Channel Spectrum Width: 20/40M

Guard Interval: Short

Channel-Frequency: 11000 ☐ Auto 5745 5755 5765 5775 5785 5795

Transmit Power: 18 2x2 Dual - Aggregate Dual Chain Power

LOCAL AP - WIRELESS SECURITY (RADIO 1)

Security: WPA2

WPA Authentication: PSK Cipher Type: AES

WPA Pre-shared Key: 12345678

Pri. Radius Server IP: 0.0.0.0

Sec. Radius Server IP: 0.0.0.0

Authentication Port: 1812

Accounting Port: 1813

Radius Secret Key: 12345678

LONG RANGE PARAMETERS (RADIO 1)

Long Range Parameters: ☒ Enable

Beacon Interval: 100

RTS Threshold: 2346 ☐ off

Fragmentation Threshold: 2346 ☐ off

Distance: 1000 meters

Slot Time(us): 13

ACK Timeout(us): 29 ☒ Auto Adjust for Slottime, ACK Timeout, CTS Timeout

CTS Timeout (us): 29

RSSI LED SETTINGS (RADIO 1)

Signal Strength Indicator (RSSI): LED1: 10 LED2: 30 LED3: 30 LED4: 40

Apply Settings

9.3.1 WIRELESS SETTINGS - AP Page BASIC WIRELESS SETTINGS Section

Note: Any settings changes made on this page will require the hitting Apply Settings button then Select Save.

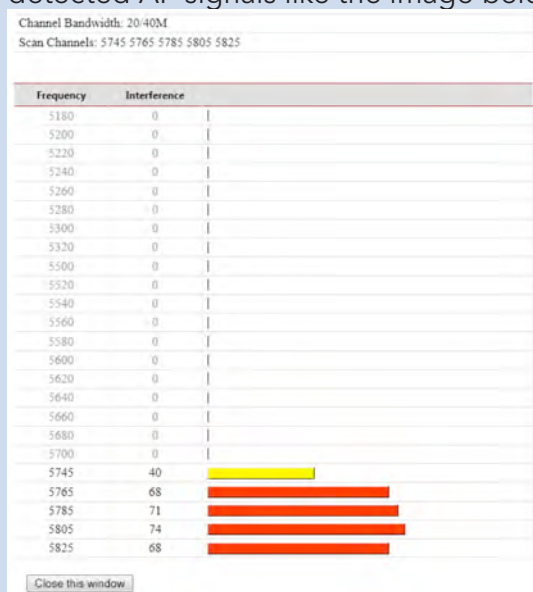
Wireless Mode	The user can select either Access Point or Client mode of operation.
Local AP-ESSID	The SSID this AP will broadcast.
Country Code	A country of operation can be selected from the pull down. NOTE: For the FCC version, only United States will be in the list while countries participating in the ETSI harmonized standards will populate this list for the ETSI version.
Wireless Profile	Select either NA or NG operation. NA is 802.11a and 802.11n (5GHz operation). NG is 802.11g and 802.11n (2.4GHz operation). NOTE: Some models may only support the NA (5GHz) option.
Channel Spectrum Width	The user can select the operation channel width. 20/40M lets the units determine the best channel width with the maximum 40MHz as an option under good RF conditions. One may want to choose 20MHz for noisy or congested RF environments. Options available are 20/40M, 20M, and 10M.
Guard Interval	This represents the guard interval between packets. The options are Short and Long. The Long option is recommended for links greater than 2Km in distance.
Channel Frequency	Auto is enabled by default. When Auto is unchecked, the user can select from a number of frequencies available from the drop down list. When Auto is checked and during boot up, the AP will select the operational channel with least interference.
Select Button	When pressed, a pop up screen comes up like the one below:

☒ 5745 MHz ☒ 5765 MHz ☒ 5785 MHz ☒ 5805 MHz ☒ 5825 MHz

This allows the user to select which frequencies the AP will scan for during reboot and when Auto mode is checked/enabled.

Interference
Analyzer Button

When pressed, will generate a pop up window showing all the detected AP signals like the image below:



Transmit Power

This section will set the RF transmit power. The maximum RF power available will be limited in software based on the gain of the integrated antenna and the region the unit was programmed to operate in. The default will set the unit to maximum allowed RF power. Here the user can reduce the RF power in case the RX RSSI levels on the remote unit exceed 65.

Remember to select Apply Settings if any changes were made.

9.3.2 WIRELESS SETTINGS - AP Page WIRELESS SECURITY Section

Security

Here the end user can select the wireless security mode. Options available are None, WEP, WPA, WPA2, and 802.1x port-based security. 802.1x is for secure user-based authentication through a centralized authentication server.

WPA
Authentication

Options here will set the authentication depending on the security selected above. PSK (Pre-Shared Key) is the default for WPA/WPA2 security. EAP-TTLS and EAP-PEAP are the two authentication methods for 802.1x security.

NOTE: Operating with 802.1x security will limit link throughput to a maximum of 54Mbps.

Cipher Type

Options for WPA/WPA2 are TKIP (Temporal Key Integrity Protocol) which uses the RC4 encryption algorithm and AES (Advanced Encryption Standard). AES is the default setting and is the recommended cipher allowing the highest link throughput. TKIP will limit throughput to a maximum of 54Mbps.

Remember to select Apply Settings if any changes were made.

Pre-shared Key	(For use with WPA security) Here an alpha-numeric between 8 and 63 character long pre-shared key can be entered.
Identity	(For use with 802.1x security) identification credential and be entered here to be used by the WPA supplicant for EAP authentication.
User Name	(For use with 802.1x security) Identification credential used by the APA supplicant for EAP – tunnelled authentication in an unencrypted form.
User Password	(For use with 802.1x security) Password credential used by the WPA supplicant for EAP authentication.

Remember to select Apply Settings if any changes were made.

9.3.3 WIRELESS SETTINGS - AP Page LONG RANGE PARAMETERS Section

Long Range Parameters	Check box to enable long range parameters. This is enabled and set to 1000m by default. 1000m should meet a majority of the system link distances but if the link distance goes beyond 1000m, this section will need to be adjusted on both ends of the link – see Distance and the Calculate Button section below.
Beacon interval	Defines the time interval (in ms) between AP beacon broadcasts. Not recommended to change the default 100ms setting.
RTS Threshold	RTS (Request to Send) threshold. This parameter controls what size data packet the low level RF protocol issues to an RTS packet. The default is 2346 with the valid range of 0-2346. There are several trade-offs to consider setting this parameter. Using a small value causes RTS packets to be sent more often, consuming more of the available bandwidth potentially reducing the throughput of the network packet. However, the more RTS packets that are sent, the quicker the system can recover from interference or collisions -- as would be the case in a wireless network with interference.
Fragmentation Threshold	Default is 2346 with a valid range is 256-2346. This parameter sets the threshold where the wireless transmission will fragment any packet if the packet size exceeds the threshold value. This setting/rule will not apply to broadcast and multicast packets.
Distance and the Calculate Button	Distance in meters that will be used to calculate Slot time, ACK timeout and CTS timeout. The default is 1000 meters but this value should be increased if the link distance goes beyond 1000m. Settings above 4000m will gradually start to affect link throughput. Once the distance value has been entered, press the Calculate button. This will update the Slot time, ACK Timeout, and CTS Timeout fields. Once these have been updated, press the Apply Settings button.

Remember to select Apply Settings if any changes were made.

9.3.4 WIRELESS SETTINGS - AP Page RSSI LED INDICATOR Section

This section allows the user to set the LED threshold for the RSSI Indicating LEDs.

Note: *LED1 on this page is not brought out on the external LED label, LED2 corresponds to Ethernet/RSSI2 on the LED label, LED3 corresponds to RSSI3, and LED4 corresponds to Status/RSSI4.*

Remember to select Apply Settings if any changes were made.

9.4 WIRELESS SETTINGS - Client Page - Client

comnet
netwave

STATUS WIRELESS NETWORK SYSTEM ADMIN
SETTINGS SETTINGS TOOLS

Apply Settings

BASIC WIRELESS SETTINGS (RADIO 1)

Wireless Mode: Client

Remote AP-ESSID: Netwave-1

Remote AP-Lock to MAC: ☐ Enabled

Country Code: United States of America

Wireless Profile: NA

Channel Spectrum Width: 20/40M

Guard Interval: Short

Transmit Power: 18 dBm Chainmask: 2x2 Dual - Aggregate Dual Chain Power

Channel Scan List: ☒ Enabled

Site Survey

20.00.30-24.00.25

Select Channels to Scan

REMOTE AP - WIRELESS SECURITY:

Security: WPA2

WPA Authentication: PSK

Preshared Key: 12345678

Identity: Anonymous

User Name: user@example.com

User Password: password

Cipher Type: AES

LONG RANGE PARAMETERS (RADIO 1)

Long Range Parameters: ☒ Enable

Beacon Interval: 100

RTS Threshold: 2346 ☐ off

Fragmentation Threshold: 2346 ☐ off

Distance: 1000 meters

Slot Time(us): 13

ACK Timeout(us): 29

CTS Timeout (us): 29

Calculate

☒ Auto Adjust for Slottime, ACK Timeout, CTS Timeout

RSSI LED SETTINGS (RADIO 1)

Signal Strength Indicator (RSSI):

LSD1: 10 LSD2: 20 LSD3: 30 LSD4: 40

Apply Settings

9.4.1 WIRELESS SETTINGS - Client Page BASIC WIRELESS SETTINGS Section

Note: Any settings changes made on this page will require selecting the 'Save' pop up button then the 'Apply Settings' button.

Wireless Mode The user can select either Access Point or Client mode of operation.

Remote AP-ESSID Remote Access point SSID can be entered here.

Site Survey Button When pressed, will generate a pop up screen showing all the potential APs that it can connect to like the image below:

Scanned channels: 5745 5765 5785 5805 5825

MAC address	ESSID	Encryption	ALG	Signal, dbm	Channel	Frequency
00:22:3b:0d:00:19	Netwave-1	WPA2-PSK	AES	-40	149	5745
00:22:3b:01:6c:58	Netwave-1	WPA2-PSK	AES	-30	153	5765
00:22:3b:01:6c:59	Netwave-Eng2	WPA2-PSK	AES	-67	161	5805

Close this window

NOTE: If there is an AP you wish to connect to, just double click on the desired AP line this window will close and auto populate the Remote AP-SSID box and the Remote AP-Lock to MAC address box.

MAC Lock When enabled this feature allows for a higher operating EIRP for FCC versions and a more secure link between the AP and Client.

Country Code A country of operation can be selected from the pull down.
NOTE: for the FCC version, only United States will be in the list while countries participating in the ETSI harmonized standards will populate this list for the ETSI version.

Wireless Profile Select either NA or NG operation. NA is 802.11a and 802.11n (5GHz operation). NG is 802.11g and 802.11n (2.4GHz operation).

NOTE: Some models may only support the NA (5GHz) option.

Channel Spectrum Width The user can select the operation channel width. 20/40M lets the units determine the best channel width with the maximum 40MHz as an option under good RF conditions. One may want to choose 20MHz for noisy or congested RF environments. Options available are 20/40M, 20M, and 10M.

Guard Interval This represents the guard interval between packets. The options are Short and Long. The Long option is recommended for links greater than 2Km in distance.

Transmit Power This section will set the RF transmit power. The maximum RF power available will be limited in software based on the gain of the integrated antenna and the region the unit was programmed to operate in. The default will set the unit to maximum RF power and here the user can reduce the RF power in case the RX RSSI levels on the remote unit exceed 65.

Channel Scan List When enabled, the client will only scan the channels selected.

Select Channels To Scan Button When this button is pressed, a new client scan window will pop up shown below:

☒ 5745 MHz ☒ 5765 MHz ☒ 5785 MHz ☒ 5805 MHz ☒ 5825 MHz

Select all Clean all Apply Close this window

Here the user can select which channels the client will scan. This can reduce link lock times if the desired AP is fixed to a known frequency.

Remember to select Apply Settings if any changes were made.

9.4.2 WIRELESS SETTINGS - Client Page WIRELESS SECURITY Section

Security	Here the end user can select the wireless security mode. Options available are None, WEP, WPA, WPA2, and 802.1x port-based security. 802.1x is for secure user-based authentication through a centralized authentication server.
WPA Authentication	Options here will set the authentication depending on the security selected above. PSK (Pre-Shared Key) is the default for WPA/WPA2 security. EAP-TTLS and EAP-PEAP are the two authentication methods for 802.1x security. <i>Note: Operating with 802.1x security will limit link throughput to a maximum of 54Mbps.</i>
Cipher Type	Options for WPA/WPA2 are TKIP (Temporal Key Integrity Protocol) which uses the RC4 encryption algorithm and AES (Advanced Encryption Standard). AES is the default setting and is the recommended cipher allowing the highest link throughput. TKIP will limit throughput to a maximum of 54Mbps.

Remember to select Apply Settings if any changes were made.

Pre-shared Key	(For use with WPA security) Here an alpha-numeric between 8 and 63 character long pre-shared key can be entered.
Identity	(For use with 802.1x security) identification credential and be entered here to be used by the WPA supplicant for EAP authentication.
User Name	(For use with 802.1x security) Identification credential used by the APA supplicant for EAP - tunnelled authentication in an unencrypted form.
User Password	(For use with 802.1x security) Password credential used by the WPA supplicant for EAP authentication.

Remember to select Apply Settings if any changes were made.

9.4.3 WIRELESS SETTINGS - Client Page LONG RANGE PARAMETERS Section

Long Range Parameters	Check box to enable long range parameters. This is enabled and set to 1000m by default. 1000m should meet a majority of the system link distances but if the link distance goes beyond 1000m, this section will need to be adjusted on both ends of the link - see Distance and the Calculate Button section below.
Beacon interval	Defines the time interval (in ms) between AP beacon broadcasts. Not recommended to change the default 100ms setting.
RTS Threshold	RTS (Request to Send) threshold. This parameter controls what size data packet the low level RF protocol issues to an RTS packet. The default is 2346 with the valid range of 0-2346. There are several trade-offs to consider setting this parameter. Using a small value causes RTS packets to be sent more often, consuming more of the available bandwidth potentially reducing the throughput of the network packet. However, the more RTS packets that are sent, the quicker the system can recover from interference or collisions -- as would be the case in a wireless network with interference.
Fragmentation Threshold	Default is 2346 with a valid range is 256-2346. This parameter sets the threshold where the wireless transmission will fragment any give packet if the packet size exceeds the threshold value. This setting/rule will not apply to broadcast and multicast packets.
Distance and the Calculate Button	Distance in meters that will be used to calculate Slot time, ACK timeout and CTS timeout. The default is 1000 meters but this value should be increased if the link distance goes beyond 1000m. Settings above 4000m will gradually start to affect link throughput. Once the distance value has been entered, press the Calculate button. This will update the Slot time, ACK Timeout, and CTS Timeout fields. Once these have been updated, press the Apply Settings button.

Remember to select Apply Settings if any changes were made.

9.4.4 WIRELESS SETTINGS - Client Page RSSI LED INDICATOR Section

This section allows the user to set the LED threshold for the RSSI Indicating LEDs.

Note: *LED1 on this page is not brought out on the external LED label, LED2 corresponds to Ethernet/RSSI2 on the LED label, LED3 corresponds to RSSI3, and LED4 corresponds to Status/RSSI4.*

Remember to select Apply Settings if any changes were made.

9.5 NETWORK SETTINGS - Client or Access Point

The screenshot displays the 'comnet netwave' web interface. At the top, there is a navigation bar with tabs: STATUS, WIRELESS, NETWORK, SYSTEM, and ADMIN. Below these are sub-tabs: SETTINGS, SETTINGS, and TOOLS. The 'NETWORK' tab is selected. The main content area is titled 'LOCAL AREA NETWORK' and contains several configuration sections. The 'LAN Mode' section has radio buttons for 'DHCP Client' (selected) and 'Static'. Below this are input fields for IP Address (192.168.10.101), Netmask (255.255.255.0), Gateway IP (192.168.10.1), and DHCP Fallback IP (192.168.10.302). The 'DHCP Mode' section has radio buttons for 'NONE' (selected) and 'DHCP Server (LAN Mode needs to be Static)'. Below this are input fields for DHCP Start IP Address (192.168.10.100), DHCP End IP Address (192.168.10.254), DHCP Netmask (255.255.255.0), DHCP Gateway IP, and DHCP Lease Time (3600 seconds). The 'DHCP SERVER RESERVATIONS' section has a table with columns for IP Address, Hardware: MAC, and Description, and an 'Add' button. The 'BANDWIDTH CONTROL' section has a checkbox for 'Bandwidth Control' which is checked and labeled 'Enabled', and a 'Configure' button. There are 'Apply Settings' buttons at the top right and bottom right of the main content area.

comnet netwave

STATUS WIRELESS **NETWORK** SYSTEM ADMIN
SETTINGS SETTINGS TOOLS

Apply Settings

LOCAL AREA NETWORK

LAN Mode: ☒ DHCP Client ☐ Static

IP Address: 192.168.10.101

Netmask: 255.255.255.0

Gateway IP: 192.168.10.1

DHCP Fallback IP: 192.168.10.302

DHCP Mode: ☒ NONE ☐ DHCP Server (LAN Mode needs to be Static)

DHCP Start IP Address: 192.168.10.100

DHCP End IP Address: 192.168.10.254

DHCP Netmask: 255.255.255.0

DHCP Gateway IP:

DHCP Lease Time: 3600 seconds

DHCP SERVER RESERVATIONS:

IP Address	Hardware: MAC	Description

Add

BANDWIDTH CONTROL:

Bandwidth Control: ☒ Enabled

Apply Settings

9.5.1 NETWORK SETTINGS - Local Area Network (LAN) Section

LAN Mode	Embedded web server addressing mode. Options are static or dynamic for an address from a local DHCP server.
IP Address	For setting the static address for the embedded web server.
Netmask	Static network mask
Gateway IP	Static gateway IP address
DHCP Fallback IP	This will be the address the web server will default to if it cannot establish communications with a DHCP server
DHCP Mode	This enables an option to make the node act as a DHCP server. Note: Can only set DHCP server if the node is statically addressed. Once the DHCP Server option has been selected, DHCP option fields below are enabled for entry.
DHCP Start IP Address	DHCP address block start address
DHCP Stop IP Address	DHCP address block stop address
DHCP Netmask	DHCP Network mask that the DHCP sever will pass to the DHCP clients
DHCP Gateway IP	IP address for the network segment gateway that the DHCP sever will pass to the DHCP clients
DHCP Lease Times	Lease time for the DHCP addresses. Default is 1 hour or 3600 seconds.

Remember to select Apply Settings if any changes were made.

9.5.2 NETWORK SETTINGS Page DHCP SERVER RESERVATIONS Section

Here one can assign IP addresses to specific MAC addresses. Once the IP address and MAC address has been entered, click the ADD button. Make sure the IP address assigned is within the DHCP start and end address block.

Remember to select Apply Settings if any changes were made.

9.5.3 NETWORK SETTINGS Page BANDWIDTH CONTROL Section

When enabled is checked, this will limit up and download speeds specified by the page that will launch when the configure button is pressed as shown below:




The screenshot shows a web-based configuration interface titled "BANDWIDTH CONTROL SETUP". It contains two input fields for setting traffic limits. The first field is labeled "Ethernet to WirelessTraffic Limit (kbit)-Download:" and has a value of "0". The second field is labeled "Wireless to EthernetTraffic Limit (kbit)-Upload:" and also has a value of "0". Both fields are enclosed in a blue border. At the bottom right of the configuration area, there is a button labeled "Apply Setting".

BANDWIDTH CONTROL SETUP	
Ethernet to WirelessTraffic Limit (kbit)-Download:	0
Wireless to EthernetTraffic Limit (kbit)-Upload:	0

Apply Setting

Enter in the throughput limiting values for upload and download then hit the Apply Setting button. This feature could be useful when configuring clients connecting to a single multipoint AP or in a repeating system thus keeping within the maximum throughput of any one hop or multipoint AP.

9.6 SYSTEM TOOLS Page - Client and Access Point



[STATUS](#) [WIRELESS SETTINGS](#) [NETWORK SETTINGS](#) **[SYSTEM TOOLS](#)** [VLAN SETTINGS](#) [ADMIN](#)

SPANNING TREE PROTOCOL (STP) SETUP

Enable STP:

☐

Root Priority:

(Range : 0 to 65536)

Root Hello Time:

(Range : 1 to 10)

Root Forward Delay:

(Range : 4 to 30)

Root Maximum Age:

(Range : 6 to 40)

DIAGNOSTIC TOOLS

Throughput Test:

Throughput Monitor:

Ping Utility:

Bridge Table:

DHCP Active Leases:

ARP Table:

PING WATCHDOG

Enable Ping Watchdog:

☐

IP Address To Ping:

Ping Interval:

seconds

Startup Delay:

seconds

Failure Count To Reboot:

AUTO-REBOOT

Auto Reboot Mode:

SNMP SETUP

Enable SNMP:

☐

Read Password:

Write Password:

Engine ID:

Enable SNMP Trap:

☐

Trap Destination IP:

Community:

NTP SETUP

Select Your Time Zone:

Current Router Time:

GMT-07:00

Proposed Router Time:

Enable NTP Client:

☐

Known Time Server:

Time Server:

TELNET SERVER

Enable Telnet Server:

☒

Server Port:

SYSTEM LOG

Enable System Log:

☐

Logging IP/Domain Name:

Logging Port:

9.6.1 SYSTEM TOOLS Page STP Section

Enable STP	Not enabled by default
Root Priority	Allows the user to set priorities in each node used during the root bridge selection process.
Root Hello Timer	For setting STP hello times. Default is 2
Root Forward Delay	For setting STP forward delay. Default is 15
Root Max Age	For setting STP maximum age timer. Default is 20

Remember to select Apply if any changes were made.

9.6.2 SYSTEM TOOLS Page PING WATCHDOG Section

The ping watchdog utility can be a useful tool if a node needs to be periodically rebooted. Wireless equipment can sometimes require reboot to re-establish a connection if operating in noisy environments

Enable Ping Watchdog	Not enabled by default.
IP Address to ping	Network address that the watchdog utility will ping.
Ping Interval	Interval in seconds that the watchdog utility will send ICMP ping requests out. Default is 5 seconds
Startup Delay	One time delay after node is booted. Default is 60 seconds.
Failure Count to Reboot	The number of successive ping failures before the node will initiate a reboot.

Remember to select Apply if any changes were made.

9.6.3 SYSTEM TOOLS Page AUTO-REBOOT Section

This can be set to reboot a certain time every day or by a set number of hours. This is disabled by default.

Remember to select Apply if any changes were made.

9.6.4 SYSTEM TOOLS Page SNMP SETUP Section

Enable SNMP	Not enabled by default
Read Password	Password to query the device
Engine ID	Engine ID for the SNMP agent. Default is 800007e5BD00002704D000007c
Enable SNMP trap	Not enabled by default.
Trap Destination IP	Destination IP address where the trap messages will be sent.
Community	Enter the SNMP community string

Remember to select Apply if any changes were made.

9.6.5 SYSTEM TOOLS Page NTP SETUP Section

Select your Time Zone:

Current Router Time	This is the time the node is set to. This will be updated and displayed in the STATUS page by either setting to the browsing computer system clock or by a connected NTP server.
Proposed Router Time	This will display the system clock of the device that is browsing to the node. If the Adjust button is pressed, The time displayed in this box will overwrite the clock on the device.
Enable NTP Client	not enabled by default.
Known Time Server	Select a time server from the drop down list. Note: The node will need to have access to the internet to connect to any one of these servers.
Time server	Manually enter in a time server if the desired one is not in the Known Timer Server list.

Remember to select Apply if any changes were made.

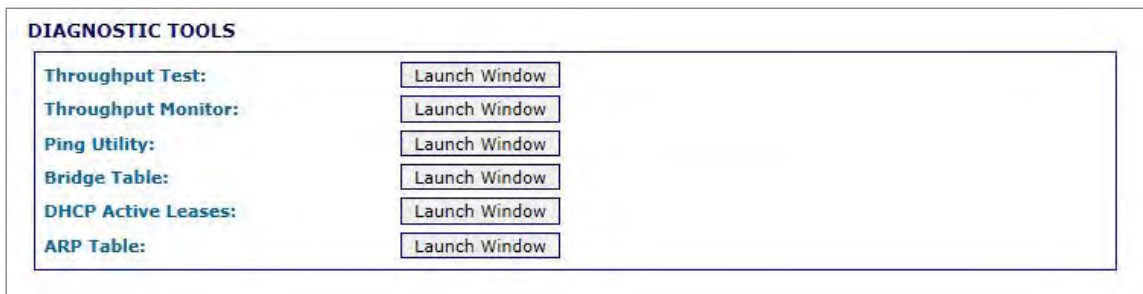
9.6.6 SYSTEM TOOLS Page TELNET SERVER Section

Enable Telnet Server	Enabled by default
Telnet server port	Port 23 is the default

9.6.7 SYSTEM TOOLS Page SYSTEM SERVER Section

Enable Syslog	Not enabled by default
Logging IP/ Domain Name	Enter in the destination IP address of the device to receive the system log
Logging port	Port 514 is the default. Port 514 is common for receiving UDP system logs

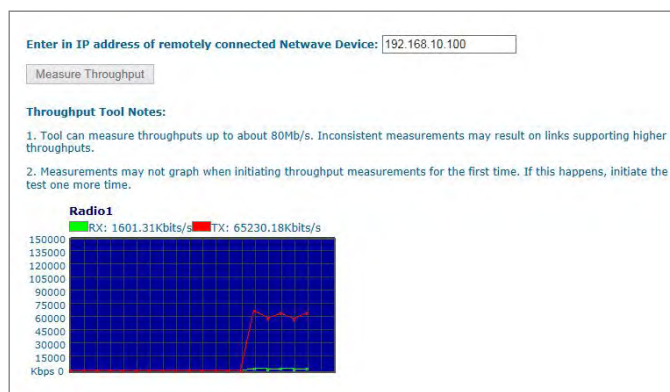
9.6.8 SYSTEM TOOLS Page Diagnostic Tools Section



Throughput Test

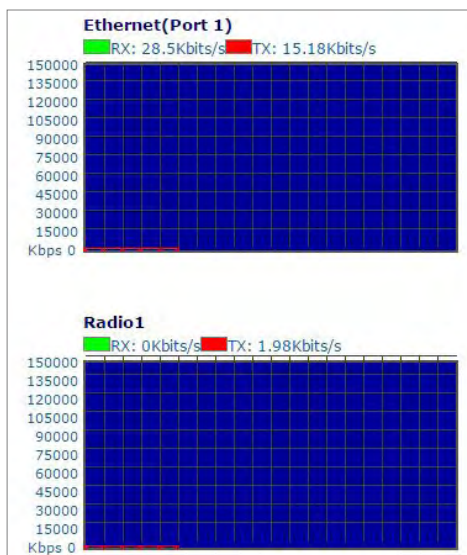
Throughput Test can measure throughput between radios.

Enter the IP address of the remote device and pre Measure Throughput.



Throughput Monitor

Displays currently used throughput used by the Ethernet Port and Wireless Radio.



Ping Utility

Use this utility to test network connections using ICMP ping.

When Ping Utility is selected, a pop up screen with come up as shown below:

NETWORK PING

Destination IP/HOST: 192.168.10.70

Packet Count: 5

continuous

Packet Size: 4096 bytes

Host	Time	TTL
192.168.10.70	3.326 ms	128
192.168.10.70	5.836 ms	128
192.168.10.70	3.067 ms	128
192.168.10.70	3.054 ms	128
192.168.10.70	3.038 ms	128

5 of 5 packets received, 0% loss

Min: 3.038 ms

Avg: 3.664 ms

Max: 5.836 ms

Start

ARP Table

When ARP Table is selected, the below pop up screen comes up listing all ARP entries:

ARP TABLE

IP address	HW type	Flags	HW address	Mask	Device
192.168.10.70	0x1	0x2	00:24:9B:06:95:98	*	br0

Close

Bridge Table

This table displays a list of devices connected to the node bridge interface as shown below

BRIDGE TABLE

Port No	Mac Address	Is Local	Agein Timer
2	00:10:83:5b:ee:46	no	87.48
2	00:13:21:0d:51:48	no	7.23
2	00:18:f8:a9:c3:bf	no	104.87
2	00:19:d1:6b:13:32	no	63.66
2	00:1a:a0:de:2d:86	no	29.82
2	00:1b:78:30:40:e6	no	33.78
2	00:1b:78:ba:20:8a	no	5.62

DHCP Active Leases

This table displays a list of active DHCP leases if this node were configured as a DHCP server.

DHCP ACTIVE LEASES

Host Name	IP Address	Hardware MAC	Lease Expired Time
-----------	------------	--------------	--------------------

Close

9.7 ADMIN Page - Client or Access Point

The screenshot displays the 'ADMIN' page of a comnet netwave device. The page has a navigation bar at the top with links: STATUS, WIRELESS SETTINGS, NETWORK SETTINGS, SYSTEM TOOLS, and ADMIN (highlighted). The main content area is divided into several sections:

- FIRMWARE UPGRADE**: Contains a 'Firmware Version:' field with the value 'NW3_V1.0.2', a 'Browse...' button, and an 'Upload' button.
- HOST NAME**: Contains a 'Host Name:' field with the value 'NW3' and an 'Apply' button.
- ADMINISTRATIVE ACCOUNT**: Contains fields for 'Administrator Username:' (value: admin), 'Current Password:', 'New Password:', and 'Verify New Password:', with an 'Apply' button.
- READ-ONLY ACCOUNT**: Contains a checkbox for 'Enable Read-Only Account:' (checked), a 'Read-Only Username:' field (value: guest), a 'Password:' field, and an 'Apply' button.
- CONFIGURATION MANAGEMENT**: Contains buttons for 'Backup Configuration:' (backup...), 'Backup System Log:' (backup...), an 'Upload Configuration:' field with a 'Browse...' button, and a 'Restore' button.
- DEVICE REBOOT/RESET**: Contains a 'Reboot...' button and a 'Reset to defaults...' button.

9.7.1 ADMIN Page FIRMWARE UPGRADE Section

Firmware Version: Displays the version currently running

Firmware Upgrade procedure:

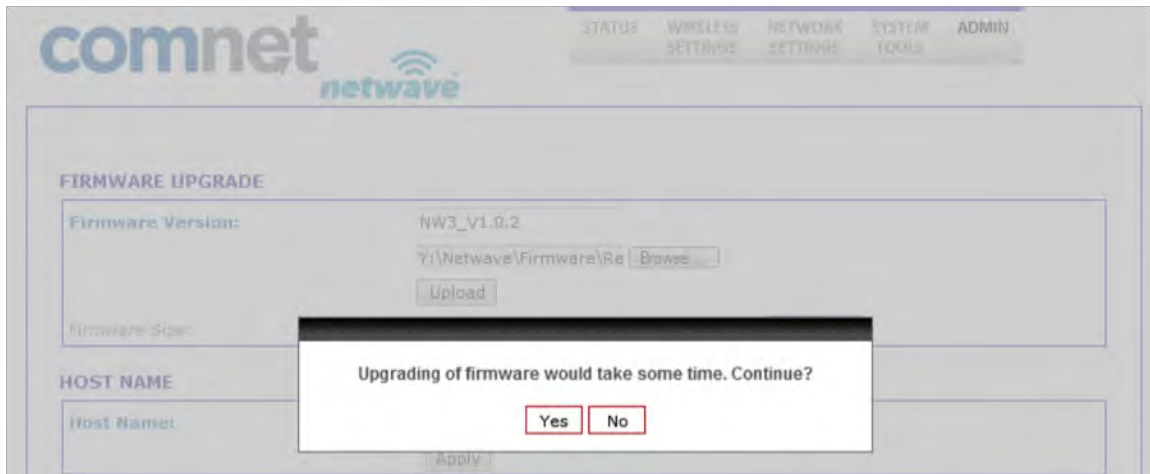
- Press the browse button to browse to a location where the upgrade image is located
- Once the file has been located hit the Upload button. You should see the following screen while the image is uploading:



- Once the image has been uploaded, an Upgrade button will appear as shown:



- Press the upgrade button and you should see a prompt confirming the upgrade to continue. Select Yes:



- The following screen will now show reminding the user to not reboot during an upgrade process. This screen should render for at least 60 seconds if the PC browsing to this particular node is locally connected.

Note: *If a firmware upgrade is being performed on a node connected on the remote end of a wireless connection, It may take several minutes for this screen to clear as the link needs to re-establish and connections to restart. One may have to clear ARP cash on the connected PC by issuing arp -d command at the command prompt.*



- The last screen will confirm to reboot. Hit Yes.



- Unit will reboot and the page will refresh after about 60 seconds.
- It is recommended that a factory reset be performed by hitting the Restore to Default button at the bottom of the ADMIN page but may not be required. Consult ComNet tech support for further detail on the particular upgrade or refer to the firmware release notes.
- End of Firmware upgrade procedure

9.7.2 ADMIN Page HOST NAME Section

Enter in the desired host name.

Remember to select Apply if any changes were made.

9.7.3 ADMIN Page ADMIN ACCOUNT Section

Administrator Username	Default is admin
Current Password	Default is admin

Remember to select Apply if any changes were made.

9.7.4 ADMIN Page READ-ONLY ACCOUNT Section

The read only account is for monitoring only with no configuration authorization

Enable Read-Only Account	Enabled by Default
Read-only Username	Default is guest
Password	Default is guest

Remember to select Apply if any changes were made.

9.7.5 ADMIN Page CONFIG MANAGEMENT Section

This section allows the user to save the current configuration of the node in a file allowing backup of node configuration.

Backup Configuration	When the Backup button is pressed, a prompt will pop up asking where to store the configuration file.
Backup System Log	When Backup is pressed, a page showing the contents of the current log files will be displayed. This then can be saved. One will have to hit the back button to get to the previous ADMIN page.
Upload Configuration	Hit browse to the location of a backup configuration file then hit restore. This will restore the unit configuration to the stored configuration.

9.7.6 ADMIN Page DEVICE REBOOT/RESET Section

Reboot Button	Will reboot the node
Reset to defaults	Will restore the node to factory defaults erasing all user set parameters.

10.0 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 conforme 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 installées en considérant une distance de séparation de toute personnes d'au moins 2.52m et ne doivent pas être localisées ou utilisées 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.

11.0 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 <http://www.gnu.org/philosophy/free-sw.html> 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 <http://www.gnu.org/licenses/licenses.html>. 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 machine-readable 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

Contact Information

ComNet - www.comnet.net

		Tel: +1-203-796-5300
North America	ComNet Corporate Headquarters and Customer Support Center	Tel: +1-888-6789427
		Email: info@comnet.net
		Tel: +44 (0)113 307 6400
EMEA, PACRIM, South America	ComNet Europe Ltd, Leeds	Tel: +44 (0)113 307 6409
		Email: info-europe@comnet.net



3 CORPORATE DRIVE | DANBURY, CT 06810 | USA
T: 203.796.5300 | F: 203.796.5303 | TECH SUPPORT: 1.888.678.9427 | INFO@COMNET.NET
8 TURNBERRY PARK ROAD | GILDERSOME | MORLEY | LEEDS, UK LS27 7LE
T: +44 (0)113 307 6400 | F: +44 (0)113 253 7462 | INFO-EUROPE@COMNET.NET