





Niveo Professional NWA 100 Wireless 900N Dual Band PoE Access Point

1

Manual v1.3



Copyright Statement

UIVGOI

is the registered trademark of Netstar Products BV. All products and product names mentioned herein are the trademarks or registered trademarks of their respective holders. Copyright of the whole product as integration, including its accessories and software, belongs to Netstar Products BV. No part of this publication can be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the prior written permission of Netstar Products BV. If you would like to know more about our product information, please visit our website at www.niveoprofessional.com.

Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, NIVEO PROFESSIONAL reserves the right to make changes to the products described in this document without obligation to notify any person or organization of such revisions or changes. NIVEO PROFESSIONAL does not assume any liability that may occur due to the use or application of the product or circuit layout(s) described herein. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information and recommendations in this document do not constitute the warranty of any kind, express or implied.

Warrantee, complaints and return of goods

Niveo warrants that the goods delivered by it are free of design, material and manufacturing faults, such for a period of 12 months following delivery. The Warrantee issued by Niveo will never exceed the Warrantee issued by Niveo's own supplier in respect of the goods, such in full compliance with the relevant terms of Warrantee of this supplier. The Warrantee is not valid if the damage is the result of incorrect handling by the buyer and/or if the buyer has acted contrary to the instructions (of use) for the products. Without prejudice to the above, Niveo will never be held to extend its Warrantee beyond replacement or crediting of the value of the faulty product delivered, such at the discretion of Niveo. The buyer will only have a right to replacement if it turns out impossible to repair the goods in question.

Details of the Niveo Professional warranty can be found on www.niveoprofessional.com.

Exclusions and Limitations

This limited warranty does not apply if: (a) the product assembly seal has been removed or damaged, (b) the product has been altered or modified, except by Niveo, (c) the product damage was caused by use with non-Niveo products, (d) the product has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Niveo, (e) the product has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident, (f) the serial number on the Product has

PROFESSIONAL

NWA100 Access Point

been altered, defaced, or removed, or (g) the product is supplied or licensed for beta, evaluation, testing or demonstration purposes for which Niveo does not charge a purchase price or license fee.

ALL SOFTWARE PROVIDED BY NIVEO WITH THE PRODUCT, WHETHER FACTORY LOADED ON THE PRODUCT OR CONTAINED ON MEDIA ACCOMPANYING THE PRODUCT, IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. Without limiting the foregoing, Niveo does not warrant that the operation of the product or software will be uninterrupted or error free. Also, due to the continual development of new techniques for intruding upon and attacking networks, Niveo does not warrant that the product, software or any equipment, system or network on which the product or software is used will be free of vulnerability to intrusion or attack. The product may include or be bundled with third party software or service offerings. This limited warranty shall not apply to such third party software or service offerings. This limited availability of a third party's service for which this product's use or operation may require.

TO THE EXTENT NOT PROHIBITED BY LAW, ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED TO THE DURATION OF THE WARRANTY PERIOD. ALL OTHER EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF NON-INFRINGEMENT, ARE DISCLAIMED.

Some jurisdictions do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to you. This limited warranty gives you specific legal rights, and you may also have other rights which vary by jurisdiction.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL NIVEO BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF THE THEORY OF LIABILITY (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT (INCLUDING ANY SOFTWARE), EVEN IF NIVEO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL NIVEO' LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. The foregoing limitations will apply even if any warranty or remedy provided under this limited warranty fails of its essential purpose. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Technical Support

Website: http://www.niveoprofessional.com Tel:+31 (0) 297 25 61 61 Email: <u>info@niveoprofessional.com</u>



Contents

CHAPTER 1 PRODUCT OVERVIEW	
1.1 PRODUCT FEATURES	
1.2 PACKAGE CONTENTS	
1.3 LEDS AND INTERFACES	
CHAPTER 2 INSTALLATION	
CHAPTER 3 CONFIGURATION GUIDELINES	
3.1 IP CONFIGURATION	
3.2 WEB LOGIN	
3.3 Status	9
3.3.1 System Status	9
3.3.2 Wireless Status	9
3.3.3 Traffic Statistics	10
3.3.4 Wireless Clients	
3.4 Network	
3.4.1 LAN Settings	11
3.5 WIRELESS	
3.5.1 Basic	
3.5.2 Security	14
3.5.3 WDS	
3.5.4 Universal Repeater	
3.5.5 Access Control	
3.5.6 Advanced	
3.6 SNMP	19
3.7 TOOLS	
3.7.1 Maintenance	19
3.7.2 Time	
3.7.3 Logs	
3.7.4 Configuration	
3.7.5 User Name & Password	
3.7.6 Diagnostics	
3.7.7 LED	
APPENDIX 1 GLOSSARY	
APPENDIX 2 CONFIGURE PC	
WIN7 OS CONFIGURATION	
WINDOWS XP OS CONFIGURATION	
APPENDIX 3 SAFETY AND EMISSION STATEMENT	



Chapter 1 Product Overview

The Wireless AP is a best-in-class 802.11n indoor access point designed specifically for wireless projects. With suspension installation and existed structure, the device saves time and costs. Versatile and powerful, the Wireless AP offers multiple security modes and supports 802.11n and 802.3at PoE power supply, which makes your data transmission safe..

1.1 Product Features

- Supports IEEE802.11n, IEEE802.11g, IEEE 802.11b and IEEE802.11a;
- 1000M Ethernet port for wired LAN connection;
- PoE Port for connecting to power supply or connecting to IEEE802.3at PoE_PSE switch;
- One RJ-45 10/100/1000 IEEE802.3ab, IEEE802.3u, IEEE802.3 auto-sensing Gigabit port for data transmission or power supply;
- Wireless rates of up to 450Mbps;
- Unified Management allows network administrators to centrally manage APs on LAN;
- Supports IP address, wireless SSID, device name, channel, wireless security and domain diagnostics;
- WEP, WPA-PSK, WPA2-PSK and WPA-PSK/WPA2-PSK encryptions secure wireless network against unauthorized accesses;
- Can be configured to select an optimum channel for device to operate on;
- Can be configured to adjust transmitting power;
- Supports AP and WDS mode.

1.2 Package Contents

Please verify that the package contains the following items:

- Wireless Access Point
- Power Adapter
- PoE Injector
- 5 screws
- Ethernet Cable
- Bracket
- Install Guide

If any of the above items are incorrect, missing, or damaged, please contact your reseller for immediate replacement.



1.3 LEDs and Interfaces

Side Panel:



Power

Solid: Receiving electrical power;

Blinking: Functioning properly;

Off: Receiving no electrical power or LED is disabled manually.

2.4GHz, 5GHz

Solid: Wi-Fi is enabled;

Blinking: Transferring data;

Back Panel:



RESET

Restores the device to the factory default settings when pushed and held for 7 seconds (This button has been hidden by the bracket of this device. Before pressing this button, you should remove the bracket.).

ΡοΕ

PoE Port for connecting to power supply or connecting to IEEE802.3at switch;

LAN

1000M Ethernet Port for connecting to an Ethernet LAN device such as a PC or switch, etc.



Chapter 2 Installation

Installation procedures:

- 1. Connect the injector to the power adapter.
- 2. Connect the PoE port of the injector to the PoE port on this device with an Ethernet cable.
- 3. Connect the LAN port of the injector to the switch.
- 4. Hang the AP:
 - (1) Install the bracket onto the ceiling or wall.
 - (2) Fix the AP onto the bracket.

The network topology is shown below:





Chapter 3 Configuration Guidelines

3.1 IP Configuration

The default IP address of your wireless access point is 192.168.2.200. If you are using the default IP subnet, the computer you are using to connect to the device should be configured with an IP address that starts with 192.168.2.x (where x can be any number between 1~253) and a Subnet Mask of 255.255.255.0; if you have changed the subnet of the wireless access point, the computer you are using to connect must be within the same subnet. If you are not clear about this configuration, please refer to <u>Appendix 2: Configure PC.</u>

3.2 Web Login

To connect to the Wireless AP using the defaults IP address:

- 1. Open a Web browser.
- 2. Enter 192.168.2.200 into your browser.
- 3. Enter the default User Name admin and default Password admin into the login window.

UIVGO	NWA100
	Username:
	Password:
	Login

4. Click Login and your Web browser shall automatically display the home page.



3.3 Status

3.3.1 System Status

This screen displays this device's current system status.

www.niveoprofe	ssional.com		
			PROFESSIONAL
	System Status		Administrator Name[admin] Version:V1.0.0.14_EN_NST01
Status			
System Status	Device Name	NWA100	
Wireless Status	System Time	2014-01-06 01:09:31	
Traffic Statistics	Up Time	ooh 10m 45s	
Wireless Clients	Number of Wireless Clients	0	
Network	Firmware Version	V1.0.0.14_EN_NST01	
Wireless	Hardware Version	1.0.0.0	
SNMP	MAC Address	00:B0:C6:12:B6:60	
Tools	IP Address	192.168.2.200	
	Subnet Mask	255.255.255.0	

- **1. Device Name:** Displays this device's name.
- 2. System Time: Displays system's current time.
- **3. Up Time:** Displays the device's uptime.
- 4. Number of Wireless Clients: Displays the information of connected wireless clients (if any).
- 5. Firmware Version: Displays Device's current firmware version.
- 6. Hardware Version: Displays Device's current hardware version.
- 7. MAC Address: Displays device's LAN MAC address.
- 8. IP Address: Displays device's LAN IP address.
- 9. Subnet Mask: Displays device's subnet mask.

3.3.2 Wireless Status

This section displays 2.4GHz and 5GHz wireless status.

ssional.	com			
				PROFESSIONAL
2.4GHz Wi	reless Status 5GHz Wireless Status			Administrator Name[admin] Version:V1.0.0.14_EN_NST01
-				
		Wireless Status		
	Network Mode	11b/g/n mixed		
	Channel	11		
ID	SSID	MAC Address	Security Mode	
1	Niveo 2.4 WLAN_1_12B660	00:B0:C6:12:B6:60	Disable	
			ĥ.	
	2.4GHz W	SSional.com	SSional.com 2.4GHz Wireless Status SGHz Wireless Status Wireless Status Wireless Status Wireless Status 10 SSID MAC Address 1 Niveo 2.4 WLAN_1_128660 00:80:C6:12:86:60	SSional.com Schz Wireless Status SGHz Wireless Status Wireless Status Wireless Status Wireless Status 100/0000000000000000000000000000000000



www.niveoprofe	ssional.c	com			
	2.4GHz Wir	eless Status 5GHz Wireless State	15		Administrator Name[admin] Version:V1.o.o.14_EN_NSTo1
Status					
System Status			Wireless Status		
Wireless Status		Network Mode	11a/n		
Traffic Statistics		Channel	44		
Wireless Clients					
Network	ID	SSID	MAC Address	Security Mode	
Wireless	1	Niveo 5 WLAN_1_12B668	00:B0:C6:12:B6:68	Disable	
SNMP					
Tools					

- 1. Network Mode: Displays device's current network mode.
- **2. Channel:** Displays device's current channel.
- 3. SSID: Displays device's network name.
- 4. MAC Address: Displays connected wireless client's MAC address.
- 5. Security Mode: Displays device's current security mode.

3.3.3 Traffic Statistics

This section displays each SSID's traffic statistics.

www.niveoprofe	essional.com				
	Statistics				
	SSID	Total RX Traffic (MB)	Total RX Packets	Total TX Traffic (MB)	Total TX Packets
	Niveo 2.4 WLAN_1_12B660	0.02MB	63	0.12MB	1252
	Niveo 5 WLAN_1_12B668	o.ooMB	o	0.12MB	1248
Wireless Clients					
Wireless					
INMP					

- 1. Total RX Traffic: Total RX bytes SSID has received.
- 2. Total RX Packets: Total RX packets SSID has received.
- 3. Total TX Traffic: Total TX bytes SSID has transmitted.
- 4. Total TX Packets: Total TX packets SSID has transmitted.

3.3.4 Wireless Clients

This section displays information of connected clients (if any). You can view 2.4GHz client list and 5GHz client list respectively here.



Status Status Status Status Administrator Name[admin] Version/V.Lo.o.14_EN_NSTot System Status Wireless Status I Traffic Statistics ID MAC Address Link Rate ID MAC Address Link Rate There is no wireless client connected to the device: There is no wireless client connected to the device: Help	www.niveoprofes	sional.com				P R 0	
Status Here you can see a list of wireless clients connected to the device. Hep System Status Currently connected Hosts: Refresh Hep Traffic Statistics ID MAC Address Link Rate Wireless Clients There is no wireless client connected to the device: Hep Wireless There is no wireless client connected to the device: Hep		2.4GHz Wireless Client Li	st 5GHz Wireless Client List				Administrator Name[admin] Version:V1.o.o.14_EN_NSTo1
Traffic Statistics ID MAC Address Link Rate Wireless Clients There is no wireless client connected to the device: Image: Client Statistics Network Image: Client Statistics Image: Client Statistics SNMP Image: Client Statistics Image: Client Statistics Tools Image: Client Statistics Image: Client Statistics	Status System Status Wireless Status	Here you can see a list of v	vireless clients connected to the device. s: Refresh			Help	
Network Wireless SNMP Tools		ID	ID MAC Address Link Rate				
SNMP Tools							
	SNMP Tools						

www.niveoprofe	ssional.cor	n		
	2.4GHz Wireles	s Client List 5GHz Wireless Client List		Administrator Name[admin] Version:V1.o.o.14_EN_NSTo1
 Status System Status Wireless Status 	Here you can : Currently Con	see a list of wireless clients connected to the device. nected Hosts Refresh		Help
Traffic Statistics	ID	MAC Address	Link Rate	
Wireless Clients		There is no wireless client connected to the device!		
Network				
Wireless				
SNMP				
Tools				

1. MAC Address: Displays connected wireless client's MAC address.

2. Link Rate: Displays the link speed rate between this device and the connected wireless client.



3.4 Network

3.4.1 LAN Settings

Here you can configure the LAN IP address, subnet mask, gateway and DNS servers.

www.niveo	professional.com			
	LAN Settings			Administrator Name[admin] Version:V1.o.o.14_EN_NSTo1
Status				
Network	IP Address	192.168.2.200	For example:192.168.1.1	Help
Wireless	Subnet Mask	255.255.255.0		OV.
SNMP	Gateway	192.168.2.254		UK
Tools	Preferred DNS Server	192.168.2.254		
	Alternate DNS Server		(Optional)	
A _{Note}				
1. Default I	LAN IP:192.168.2.20	o, default	subnet mask: 255.255	5.255.0.

2. If you change the default IP address, you must use the new IP address to re-log in.



3.5 Wireless

3.5.1 Basic

Select 2.4GHz or 5GHz to configure basic settings.

2.4GHz Wireless Basic

www.niveoprofe	ssional.com		
	2.4GHz Wireless Basic 5GHz V	Vireless Basic	Administrator Name[admin] Version:V1.o.o.14_EN_NST01
Status			
Network	Select Wireless Network	00:B0:C6:12:B6:60 (Niveo 2.4 WLAN_1_12B660 enabled) 🗸	Help
Wireless	Wireless	✓ Enable	ОК
Basic			
Security	SSID Broadcast	Enable Disable	
WDS	AP Isolation	Enable	
Universal Repeater	SSID	Niveo 2.4 WLAN_1_12B660	
Access Control	Country	Germany 🗸	
Advanced	Wireless Mode	11b/g/n mixed V	
SNMP	Channel	2462MHz (Channel 11)	
Tools	Channel Bandwidth		
	Extension Channel	2442MHZ (Channel 7)	
	WMM Capable	Enable Disable	
	APSD Capable	Enable Disable	
	Max Clients(1-124)	30	

1. Select Wireless Network: 8 SSIDs are available here.

2. Enable: Select it to enable wireless feature. As for 2.4GHz, only the first SSID is enabled by default and it can't be disabled. Up to 8 SSIDs can be enabled at the same time.

3. SSID Broadcast: This option allows you to have your network name (SSID) publicly broadcast or if you choose to disable it, the SSID will be hidden. It is enabled by default.

4. AP Isolation: Isolates clients connected to the same SSID.

5. SSID: This is the public name of your wireless network. Select the SSID you wish to configure from the drop-down list.

6. Wireless Mode: Select a right mode according to your wireless client. The default mode of 2.4GHz is 11b/g/n mixed.

11b mode: Select it if you have only 11b wireless devices in your wireless network. Up to 11Mbps wireless rate is supported on this mode.

11g mode: Select it if you have only 11g or 11n wireless devices in your wireless network. Up to 54Mbps wireless rate is supported on this mode.

11b/g mixed mode: Select it if you have 11b and 11g wireless devices in your wireless network. Up to 54Mbps wireless rate is supported on this mode.

11b/g/n mixed mode: Select it if you have 11b, 11g and 11n wireless devices in your wireless network. In this mode wireless connection rate is negotiated. Up to 450Mbps wireless rate is supported on this mode.

7. Channel: Select from 1~13 channels or Auto. The best selection is a channel that is the least used by neighboring networks.

8. Channel Bandwidth: Select a proper channel bandwidth to enhance wireless performance. Select 20/40M frequency width when device is operating in 11n, select 20M frequency width when device is operating in



non-11n mode.

9. Extension Channel: This is used to enhance data throughput ability for 802.11n devices on the network.

10. WMM-Capable: WMM is QoS for your wireless network. Enabling this option may better stream wireless multimedia data such as video or audio (recommended).

11. ASPD Capable: Select to enable/disable the auto power saving mode. By default, this option is disabled.

12. Maximum Clients: Total clients should be within 124.

5GHz Wireless Basic

www.niveoprofe	essional.com		CIVCO PROFESSIONAL
	2.4GHz Wireless Basic 5GHz V	Vireless Basic	Administrator Name[admin] Version:V1.0.0.14_EN_NST01
Status			
Network	Select Wireless Network	00:B0:C6:12:B6:68(Niveo 5 WLAN_1_12B668 enabled) V	Help
Wireless	Wireless	✓ Enable	ОК
Basic			
Security	SSID Broadcast	Enable Obisable	
WDS	AP Isolation	Enable	
Universal Repeater	SSID	Niveo 5 WLAN_1_12B668	
Access Control	Country	Germany 🗸	
Advanced	Wireless Mode		
SNMP	Channel		
Tools	channel		
	WMM Capable	Enable Disable	
	APSD Capable	Enable O Disable	
	Max Clients(1-124)	30	

1. Select Wireless Network: 8 SSIDs are available here.

2. Enable: Select it to enable wireless feature. As for 2.4GHz, only the first SSID is enabled by default and it can't be disabled. Up to 8 SSIDs can be enabled at the same time.

3. SSID Broadcast: This option allows you to have your network name (SSID) publicly broadcast or if you

choose to disable it, the SSID will be hidden. It is enabled by default.

4. AP Isolation: Isolates clients connected to the same SSID.

5. SSID: This is the public name of your wireless network. Select the SSID you wish to configure from the drop-down list.

6. Wireless Mode: Select a right mode according to your wireless client. The default mode of 5GHz is 11a/n.

11a mode: Select it if you have only 11a wireless devices in your wireless network. Up to 54Mbps wireless rate is supported on this mode.

11a/n mode: In this mode wireless connection rate is negotiated. Up to 450Mbps wireless rate is supported on this mode.

7. Channel: Select 149, 153, 157, 161, 165 or Auto in 11a mode and select 149, 157 or Auto in 11a/n mode. The best selection is a channel that is the least used by neighboring networks.

8. WMM-Capable: WMM is QoS for your wireless network. Enabling this option may better stream wireless multimedia data such as video or audio (recommended).

9. ASPD Capable: Select to enable/disable the auto power saving mode. By default, this option is disabled.10. Maximum Clients: Total clients should be within 124.



3.5.2 Security

This section allows you to secure your wireless network. Here we introduce 4 security modes to you.

www.niveoprol	fessional.com		<u>niveo</u> 1
Status	2-4GHz Wireless Security	SCH2 Wireless Security	Administrator Name(admin) Version/Version/Ling/STar
Metwork	Select Wireless Network	NV60 1.4 WLAN_1 125666	and the
Wireless Basis Security WDS troiversal Reporter Access Cantrol Access Cantrol SAUs Taols	Security Mode	Control 000 WWA-PSK WWA-PSK WWA-PSK WWA-PSK WWA-PSK WWA-PSK WWA-PSK WWA-PSK WWA-PSK WWA-PSK WWA-PSK WWA-PSK	OK.

WEP

WEP is intended to provide data confidentiality comparable to that of a traditional wired network. Two types of encryption can be used with WEP: Open and Shared Key.

www.niveoprofe	ssional.com				
	2.4GHz Wireless Security 5	GHz Wireless Security			Administrator Name[admin] Version:V1.o.o.14_EN_NSTo1
Status					
Network	Select Wireless Network	Niveo 2.4 WLAN_1_12B660 V		Help	
Wireless	Security Mode	WEP 🗸		ок	
Basic	Encryption Type	Open 🗸			
Security	802.1X Authentication	Disable 🗸			
WDS	Default Key	Key 1 🗸			
Universal Repeater	WEP Key 1	ASCII	ASCII 🗸		
Advanced	WEP Key 2	ASCII	ASCII 🗸		
SNMP	WEP Key 3	ASCII	ASCII 🗸		
Tools	WEP Key 4	ASCII	ASCII 🗸		

1. Encryption Type: Select Open or Shared from the drop-down list.

2. WEP Key: Select Hex or ASCII from the drop-down list. Enter 5 or 13 valid ASCII characters

(0-9,a-z,A-Z,@,*,-,_ can be included) if you select ASCII or enter 10 or 26 valid Hex characters (0-9,a-f,A-F can be included) if you select Hex.

WPA-PSK

The WPA (Wi-Fi Protected Access) protocol implements the majority of the IEEE 802.11i standard. It enhances data encryption through the Temporal Key Integrity Protocol (TKIP) which is a 128-bit per-packet key, meaning that it dynamically generates a new key for each packet. WPA also includes a message integrity check feature to prevent data packets from being tampered with. Only authorized network users can access the wireless network. WPA adopts enhanced encryption algorithm over WEP.



www.niveoprofe	ssional.com			
	2.4GHz Wireless Security	GHz Wireless Security		Administrator Name[admin] Version:V1.o.o.14_EN_NSTo1
	Select Wireless Network	Niveo 2.4 WLAN 1 12B660 V		Неір
Wireless Basic Security WDS Universal Repeater	Security Mode Cipher Type Security Key Key Update Interval	WPA-PSK V @ AES TKIP TKIP TKIP&AES	ו	ОК

- 1. Cipher Type: Select AES (advanced encryption standard) or TKIP (temporary key integrity protocol) &AES.
- 2. Security Key: Enter a security key, which must be between 8-63 ASCII characters long.
- **3. Key Update Interval:** Enter a valid time period for the key to be changed.

WPA2-PSK

WPA2 (Wi-Fi Protected Access version 2) is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP. It is more secured than WPA and WEP.

www.niveoprofe	ssional.com			
	2.4GHz Wireless Security	GHz Wireless Security		Administrator Name[admin] Version:V1.0.0.14_EN_NST01
Status				
Network	Select Wireless Network	Niveo 2.4 WLAN_1_12B660 V	Help	
Wireless	Security Mode	WPA - PSK 🗸	OK	
Basic	Cipher Type	● AES ○ TKIP ● TKIP&AES		
Security	Security Key	12345678		
WDS	Key Update Interval	3600 s		
Universal Repeater				
Access Control				
Advanced				
SNMP				
Tools				

- 1. Cipher Type: Select AES (advanced encryption standard) or TKIP (temporary key integrity protocol) &AES.
- 2. Security Key: Enter a security key, which must be between 8-63 ASCII characters long.
- **3. Key Update Interval:** Enter a valid time period for the key to be changed.

3.5.3 WDS

Wireless distribution system (WDS) is a system enabling the wireless interconnection of access points in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the traditional requirement for a wired backbone to link them. Note: The Access Points you select must support WDS.



www.niveopro	essional.com	<u>NIVCOI</u>
	3-4GHz Wireless WDS SCitz Wireless WDS	Administration Name[admin] Version/Version_EN_MSTore
Status Retwork Witcless Basis Security WSS Universal Reporter Access Control Advenced Easter Teals	Unable Duals Mode WDS Mode Duals Mode AP INAC Address Duals Mode Internatin Andress Address Address Antity Mode	инф Сах. а

1. WDS Mode: Select Disable, Repeater Mode or Bridge Mode.

2. AP MAC Address: Displays the remote AP's MAC address.

For Example:

Access Point 1 LAN IP: 192.168.2.200

Access Point 2 LAN IP: 192.168.2.223

WDS Mode: Repeater Mode

Configure Access Point 1:

1. Enter the remote AP's MAC address and click **OK**.

2. You can also scan the remote AP.

1) Click **Open Scan** to select the remote AP and click **OK** to add the corresponding MAC address

automatically.

Select	SSID	MAC Address	Channel	Security	Signal Strength
\bigcirc	Micasa31	50:7E:5D:4A:DF:28	1	wep/wpa	-73 dBm
۲	MICASA31	B8:8D:12:5D:D7:A3	1	wep/wpa	-67 dBm
\bigcirc	linksys19	00:23:69:2 Bericht van w	vebpagina	-	×
\bigcirc	Ziggo	C2:F8:DA:			
\bigcirc	Thomson7910A7	00:18:F6:E	Are you sure you	want to connec	t to this AP?
\bigcirc	snoetje	90:F6:52:F			
\bigcirc	VGV751926FDD5	84:9C:A6::	ſ	ОК	Annuleren
\bigcirc	draadloos	20:4E:7F:9			
\bigcirc	SpeedTouchBDB341	00:18:F6:03:03:16	6	wep/wpa	-32 dBm
\bigcirc	Sitecom	00:21:04:A2:89:28	6	wep/wpa	-84 dBm
\bigcirc	Arcus	o8:96:D7:29:99:7E	6	wep/wpa	-83 dBm
\bigcirc	Oud-1	Eo:CB:4E:94:87:EA	11	wep/wpa	-74 dBm
\bigcirc	Ziggo18C24	90:00:4E:7C:F1:F2	11	wep/wpa	-53 dBm
\bigcirc	Ziggo1B868	Co:F8:DA:63:5E:D7	11	wep/wpa	-79 dBm
0	Ziggo	C2:F8:DA:63:5E:D8	11	wep/wpa	-76 dBm

2) Click **OK** to save your settings.



www.niveoprofe	essional.com		P.R.O.F.E	
	2.4GHz Wireless WDS 5GHz V	/ireless WDS		Administrator Name[admin] Version:V1.o.o.14_EN_NSTo1
Status				
Network	WDS Mode	Repeater Mode 🗸	Help	
Wireless	AP MAC Address	B8:8D:12:5D:D7:A3	ок	
Basic	AP MAC Address			
Security	AP MAC Address			
WDS	AP MAC Address			
Universal Repeater		Re-scan		
Access Control		Re-scan		

Then follow the steps mentioned above to configure the Access Point 2. After the two APs have added each other, they can be bridged successfully.



2. Once the security mode has been changed, please reboot the device.

3. If one of the APs is in Bridge Mode, the remote one must be in Repeater Mode.

4. In Bridge mode, clients won't be able to access the device's primary SSID.

3.5.4 Universal Repeater

Select Universal Repeater and enable scan to automatically populate SSID and channel of the AP to connect or manually enter the AP's SSID, channel and security key.

www.niveoprofe	essional.com		<u>UIVGOI</u>
	Wireless Universal Repeater		Administrator Name[admin] Version:V1.0.0.14_EN_NST01
Status Network		✓ Enable	Help
 Wireless Basic 	Interface	● 2.4G ○ 5G	ОК
Security WDS	SSID MAC Address	Niveo 2.4 WLAN_1_128660	
Universal Repeater Access Control	Channel Security Mode	2462MHz (Channel 11)	
Advanced	Default Key	Key 1 V	
Tools	WEP Key 1 WEP Key 2	ASCII ASCII ASCII ASCII	
	WEP Key 3 WEP Key 4		
		Enable Scan	

ANote -----

1. Enabling scan does not populate the security key, so you must still manually enter it.

2. Make sure your (local) AP, PCs connected and the remote AP to connect are on the same subnet with

different IP addresses.

3. If ping requests sent from PCs connected to your local AP are properly replied by the targeted remote AP,



Universal Repeater is successfully operating; if not, check your settings again.

3.5.5 Access Control

Specify a list of devices to allow or disallow a connection to your wireless network via the device's MAC addresses. To deactivate this feature, select "Disable"; to activate it, select "Allow" or "Deny" (2.4GHz/5GHz).

www.niveoprofe	ssional.com	
	2.4GHz Access Control 5GHz Access Control	Administrator Name[admin] Version:V1.o.o.14_EN_NSTo1
Status		Kala
Network	Select Wireless Network Niveo 2.4 WLAN_1_12B660 V	ueb
Wireless	Configure wireless MAC address filter.	ОК
Basic	MAC Address Filter Disable 🗸	
Security	Mitalaus Claud Lat	
WDS	There is no client on the current network.	
Universal Repeater		
Access Control		
Advanced		
SNMP		
Tools		

MAC Filter Mode: Select Allow or Deny from the drop-down list.

 To permit a wireless device to connect to your wireless network, select Allow, enter its MAC address, click Add and then OK. Then only this device listed as "Allowed" will be able to connect to your wireless network; all other wireless devices won't be allowed.

To disallow a wireless device to connect to your wireless network, select **Deny**, enter its MAC address, click
 Add and then OK. Then this device listed as "Denied" will be unable to connect to your wireless network.

3.5.6 Advanced

This section allows you to configure advanced wireless settings (2.4GHz or 5GHz). If you are new to networking and have never configured these settings before, we recommend you to leave the default settings unchanged.

www.niveoprofe	ssional.com		
	2.4GHz Wireless Advance 5GH	z Wireless Advance	Administrator Name[admin] Version:V1.0.0.14_EN_NST01
Status			
Network	RF Preamble	Long 🗸	Help
Wireless	Beacon Interval	100 ms(Valid Range: 20 - 999 Default: 100)	ОК
Basic	Fragment Threshold	2346 (Valid Range: 256 - 2346 Default: 2346)	
Security	RTS Threshold	2347 (Valid Range: 1 - 2347 Default: 2347)	
WDS	DTIM Interval	1 (Valid Range: 1 - 255 Default: 1)	
Universal Repeater	TX Power Percentage	100 (Valid Range: 50 - 100 Default: 100)	
Access Control			
SNMP			
Tools			

- **1. RF Preamble:** This is used to synchronize frames. Do not change it unless necessary.
- 2. Beacon Interval: This is a time interval between any 2 consecutive Beacon packets sent by an Access Point



to synchronize a wireless network. Specify a valid Beacon Interval value between 20-999. The default value is 100.

3. Fragment Threshold: Specify a valid Fragment Threshold value between 256-2346. The default value is 2346. Any wireless packet exceeding the preset value will be divided into several fragments before transmission.

4. RTS Threshold: Specify a valid RTS Threshold value between 1-2347. The default is 2347. If a packet exceeds the preset value, RTS/CTS scheme will be used to reduce collisions. Set it to a smaller value if there are distant clients and interference.

5. DTIM Interval: A DTIM (Delivery Traffic Indication Message) Interval is a countdown informing clients of the next window for listening to broadcast and multicast messages. When such packets arrive at device's buffer, the device will send DTIM (delivery traffic indication message) and DTIM interval to wake clients up for receiving these packets. Specify a valid value between 1-255. The default is 1.

6. TX Power Percentage: Control TX power . Specify a value between 50 - 100. The default is 100.

3.6 SNMP

The Simple Network Management Protocol (SNMP) is widely used in local area networks (LANs) for collecting information, managing, and monitoring network devices, such as servers, control systems, hubs, switches, and routers. Specialized software in each SNMP capable device, known as an Agent, continuously monitors the status of the device and reports the results to the SNMP Manager software. This AP supports both SNMP v1 and SNMP v2c.

www.niveoprofe	ssional.com			
	SNMP Setting		Administrator Name[admin] Version:V1.o.o.14_EN_NSTo1	
Status	a statement of st		u.h	
Network	Support SNMP v1 and v2c.		нер	
Wireless	SNMP Setting	Enable	OK	
SNMP	Contact	admin	- On	
Tools	Device Name	NWA100		
	Location			
	Get Community	public		
	Set Community	private		
	Trap Destination	192.168.2.200		

Click **Enable** to enable the SNMP feature.

- 1. **Get Community:** Specify a community for reading SNMP agent information;
- 2. Set Community: Specify a community for writing SNMP agent information.

3.7 Tools

3.7.1 Maintenance

Upgrade

Upgrade is released periodically to improve the functionality of your device or to add new features



Click **Tools > Maintenance > Upgrade** to enter the screen below:

www.niveoprofes	ssional.com
	Upgrade Reboot Administrator Name[admin] Version:V1.0.0.14_EN_NSTo1
Network	Current Firmware Version: V1.0.0.14_EN_NST011 Release Date:May 14 2014
Wireless	Please select a firmware for upgrade:
SNMP	Reduces Develo
• Tools	He Name: Diducter Upgrave
	rou must select via ties from the rise of type and pown iss, otherwise you may not tink on the rise. Emmuners uncarfed lasts for second monitor and the normal time in the rise of the rest of the device while
	upgrade is in process.

To upgrade device software:

- 1. Click Browse to locate and select upgrade file on your hard disk.
- 2. Click **Upgrade** to upgrade device firmware.
- 3. When the firmware upgrade completes, your wireless access point will automatically restart.
- 4. Restore the AP back to factory default settings after reboot.

A_{Note} ------

When uploading software to the Wireless AP, it is important not to disconnect the device from power supply.

If the power supply is interrupted, the upload may fail, corrupt the software, and render the device

inoperable. When the upload completes, your wireless access point will automatically restart. The upgrade

process typically takes about several minutes.

Reboot

The Reboot option restarts the wireless access point using its current settings. Connections will be lost during reboot.

Click Tools > Maintenance > Reboot to display screen below:

www.niveoprofes	ssional.com	<u>UIVGO</u>
		PROFESSIONAL
	Upgrade Reboot	Administrator Name[admin] Version:V1.o.o.14_EN_NSTo1
Status		
Network	Click below button to force a reboot.	
Wireless	Reboot	
SNMP		
▶ Tools	Note: Connection to AP will be lost during device reboot Current settings will be lost after a reboot. So be sure to save them	
Maintenance	before you perform a reboot.	
Time		
Logs		
Configuration		
Username & Password		
Diagnostics		
LED		



3.7.2 Time

This page is used to set the device's system time. You can choose to set the time manually or get the GMT time from the Internet and the system will automatically connect to NTP server to synchronize the time.

www.niveoprofes	ssional.com
	Time Setting Administrator Name[admin] Version:V1.0.0.14_EN_NSTo1
Network	Inis page is used to set the device's system little. He from internet and notes will automatically Help
Wireless	concerts ONTP server to synchronize the time. OK
SNMP	Note: System time will be lost when the device is disconnected from power supply.
▶ Tools	However, it will be updated automatically when the device reconnects to internet.
	To activate time-based features, system time must be set correctly first, either manually or automatically on this page.
	Sync with Internet Time Servers Sync Interval: a hours
	Time Zone: [(GMT-osioo) North America, Eastern Standard Time, New York, Ottawa
	(Note: System time will not be accurate unless there is access to internet or you customize it.)
	Custom Time:
	2014 Year(s Month b: Davids h 20 m ha s Coov Local Time

- 1. Sync with Internet Time Servers: Gets the GMT time from the Internet
- 2. Sync Interval: The default sync interval is 2 hours.
- **3. Time Zone:** Select your local time zone.
- **4. Copy Local Time:** Copy time on your PC to the device.

▲_{Note}------

System time will be lost when the device is disconnected from power supply. However, it will be updated

automatically when the device reconnects to Internet.

3.7.3 Logs

Syslog

Here you can view the history of the device's actions. Click **Refresh** to display the latest logs and or click **Clear** to remove all logs.

www.niveoprofe	ssional.com	
	Syslog Log Setting	Administrator Name[admin] Version:V1.0.0.14_EN_NST01
Status		
Network	Here you can view the history of the device's actions. It may help troubleshoot network problems.	Help
Wireless	Index Time Type Log Content	Defeath
SNMP	1 2013-01-01 00:59:12 system init web server success!	NCI1031
▶ Tools	2 2013-01-01 00:59:12 system system start!	Clear
Maintenance	2 Entries,1 Pages,Page 1	1
Time		
Logs		
Configuration		
Username & Password		
Diagnostics		
LED		

Log Setting

Here you can set up number of logs and rules of log settings. Up to 300 entries can be logged. The default is 150.



www.niveoprofes	sional.com		
	Syslog Log Setting		Administrator Name[admin] Version:V1.0.0.14_EN_NST01
	To activate rules listed below, you must check this check	dox.	Help
Wireless	ID Log Server IP Log Server Port	Enable Action	ОК
Tools		Add	
Username & Password Diagnostics			

3.7.4 Configuration

Backup & Restore

This section allows you to save a copy of the device configurations on your local hard drive or to restore the previous configurations back to the device.

1. **Backup:** Once you have configured the device the way you want it, you can save these settings to a configuration file on your local hard drive that can later be imported to your device in case that the device is restored to factory default settings. To do so, click the **Backup** button and specify a directory to save settings on your local hardware.

2. **Restore:** Click the **Browse** button to locate and select a configuration file that is saved previously on your local hard drive and then click **Restore** to restore it. Configurations will be restored after device reboot.

www.niveoprofe	ssional.com	
	Backup & Restore Restore to Factory Default	Administrator Name[admin] Version:V1.0.0.14_EN_NST01
Status		
Network	Backup Settings	
Wireless	Click on "Backup" to save a copy of your device's configurations to your computer.	Backup
SNMP	Restore Settings	
• Tools	First click on "Browse" to browse your computer and select the configuration file you want to upload to your de	device. Then
Maintenance	click on the "Restore" button to upload your selection and apply the settings saved in that file.	
Time	Bladeren	Restore
Logs		
Configuration		
Username & Password		
Diagnostics		
LED		

Restore to Factory Default

Click the **Restore to Factory Default** button to reset Device to factory default settings.



www.niveoprofes	ssional.com	
	Backup & Restore Restore to Factory Default	Administrator Name[admin] Version:V1.0.0.14_EN_NST01
	Click the button below to reset the device. Do NOT operate the device until it is fully restored to factory default.	Help
	Restore to Factory Default	
SNMP		
▶ Tools		
	Note: I ne device will restart automatically with default settings after reset. Settings including login password, etc will all be reset to factory defaults. So remember to use the default password for login.	
	sector accory actualization contained to be the actual passifier of highin	
Configuration		
Username & Password		

Factory Default Settings:

- **User Name:** admin
- **Password:** admin.
- > IP Address: 192.168.2. 200
- Subnet mask: 255.255.255.0

3.7.5 User Name & Password

Here you can change the user name and password for web login. The default username and password is admin/admin. We suggest that you change this password to a more secure password.

www.niveoprofe	ssional.com		
	User Name & Password		Administrator Name[admin] Version:V1.0.0.14_EN_NST01
Status			
Network	Use this section to change your login user name and password	d.	Help
Wireless	Old User Name		OK
SNMP	Old Password		UN UN
▶ Tools	New User Name		
Maintenance	New Password		
Time	Confirm New Password		
Logs			
Configuration	Note:		
Username & Password	Note: User name or password should only include 1~32 characteristics	ters: numbers, letters or underscore!	
Diagnostics			
LED			

3.7.6 Diagnostics

You can choose Ping or traceroute to test your network connection.



www.niveoprofe	ssional.com
	Troubleshoot Administrator Name[admin] Version:V1.0.0.14_EN_NSTo1
	ping Utraceroute
Wireless	Please enter a valid IP address: Apply
SNMP	
• Tools	
	~

3.7.7 LED

This section allows you to modify LED status.

www.niveoprofe	ssional.com	<u> </u>	
	LED Control		Administrator Name[admin] Version:V1.0.0.14_EN_NSTo1
Status			
Network	Turn off all LEDs	Help	
Wireless			
SNMP			
• Tools			
Maintenance			
Time			
Logs			
Configuration			
Username & Password			
Diagnostics			
D LED			



Appendix 1 Glossary

Channel

A communication channel, also known as channel, refers either to a physical transmission medium such as a wire or to a logical connection over a multiplexed medium such as a radio channel. It is used to transfer an information signal, such as a digital bit stream, from one or more transmitters to one or more receivers. If there is only one AP in the range, select any channel you like. The default is **Auto**.

If there are several APs coexisting in the same area, it is advisable that you select a different channel for each AP to operate on, minimizing the interference between neighboring APs. For example, if 3 Americanstandard APs coexist in one area, you can set their channels respectively to 1, 6 and 11 to avoid mutual interference.

SSID

Service set identifier (SSID) is used to identify a particular 802.11 wireless LAN. It is the name of a specific wireless network. To let your wireless network adapter roam among different APs, you must set all APs' SSID to the same name.

WEP

WEP (Wired Equivalent Privacy) - A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.

WPA/WPA2

The WPA protocol implements the majority of the IEEE 802.11i standard. It enhances data encryption through the Temporal Key Integrity Protocol (TKIP) which is a 128-bit per-packet key, meaning that it dynamically generates a new key for each packet. WPA also includes a message integrity check feature to prevent data packets from being hampered with. Only authorized network users can access the wireless network. The later WPA2 protocol features compliance with the full IEEE 802.11i standard and uses Advanced Encryption Standard (AES) in addition to TKIP encryption protocol to guarantee better security than is provided by WEP or WPA.



Appendix 2 Configure PC

WIN7 OS Configuration

1. Click Start > Control Panel;



2. Enter Control Panel and click Network and Internet;



3. Click Network and Sharing Center;





4. Click Change adapter settings;

🚱 🕞 🧟 🕊 Network and Inte	ernet 🔸 Network and Sharing Center 🔹 👻	Search Control Panel
Control Panel Home Change adapter settings Change advanced sharing settings	View your basic network informatio	en and set up connections See full map rork Internet
	View your active network Unidentified network Public network	Access type: No network access Connections: Uccal Area Connection

5. Right click Local Area Connection and select Properties;



6. Select Internet Protocol Version 4(TCP/IPv4) and click Properties;



Ne	working
c	onnect using:
	Intel(R) PRO/1000 MT Network Connection
	Configure
Т	his connection uses the following items:
	Install Uninstall Properties
	Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks



7. Select Use the following IP address, enter 192.168.2.X (where x can be any number between 1~253) in the

IP address bar and 255.255.255.0 in the subnet mask and then click **OK** to save the configurations.

Internet Protocol Version 4 (TCP/IPv4) Properties				
General				
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.				
Obtain an IP address automatical	у			
• Use the following IP address:				
IP address:	192.168.2.5			
Subnet mask:	255.255.255.0			
Default gateway:	192.168.2.1			
Obtain DNS server address autom	natically			
Our Section Control	resses:			
Preferred DNS server:	192.168.2.1			
Alternate DNS server:	• • •			
Validate settings upon exit	Advanced			
	OK Cancel			

Windows XP OS Configuration

1. Right click My Network Places and select Properties;



2. Right click Local and select Properties;

LAN o	r High-Speed Internet	
	h	
	Disable Status Repair	
vity, and	Bridge Connections	connection.
	Create Shortcut Delete Rename	
	Properties	

3. Select Internet Protocol(TCP/IP) and click Properties;



🛨 Local Properties 🛛 🔶 🤶	X		
General Authentication Advanced			
Connect using:			
Intel(R) PRO/1000 MT Network Con Configure	۱l		
This connection uses the following items:			
☑ 🛃 QoS Packet Scheduler			
Install Uninstall Properties	ן נ		
Description			
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.			
 Show icon in notification area when connected Notify me when this connection has limited or no connectivity 			
OK Cance			

4. Select Use the following IP address, enter 192.168.2.X (where x can be any number between 1~253) in the

IP address bar and 255.255.255.0 in the subnet mask and then click **OK** to save the configurations.

Internet Protocol Version 4 (TCP/IPv4)	Properties		
General			
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.			
Obtain an IP address automatically			
Ose the following IP address:			
IP address:	192.168.2.5		
Subnet mask:	255 . 255 . 255 . 0		
Default gateway:	192.168.2.1		
Obtain DNS server address automatically O Use the following DNS server addresses:			
Preferred DNS server:	192.168.2.1		
Alternate DNS server:	• • •		
Validate settings upon exit	Advanced		
	OK Cancel		



Appendix 3 Safety and Emission Statement

CE

CE Mark Warning

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.



FCC Statement

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) 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 B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.



Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.