



NetPoint Pro

Broadband Wireless Networking Solutions

NetPoint Pro n2S5S (Software version 4.0)

SYSTEM MANUAL



This document contains information that is proprietary to Netronics Technologies Inc.

No part of this publication may be reproduced, modified, or distributed without prior written authorization of Netronics Technologies Inc.

This document is provided as is, without warranty of any kind.

Statement of Conditions

The information contained in this document is subject to change without notice.

Netronics shall not be liable for errors contained herein or for incidental or consequential damage in connection with the furnishing, performance, or use of this document or equipment supplied with it.

Information to User

Any changes or modifications of equipment not expressly approved by the manufacturer could void the user's authority to operate the equipment and the warranty for such equipment.

Copyright © 2011 by Netronics. All rights reserved.

READ THIS FIRST!

Important Safety Instructions



Caution

Read and save these instructions. Heed all warnings. Follow all instructions.



Caution

Do not defeat the safety purpose of the grounding. Only use attachments/accessories specified by the manufacturer.



Caution

Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way. For example, if the power-supply cord or plug is damaged, liquid has been spilled on the apparatus, objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, it does not operate normally, or has been dropped.



Warning

This apparatus must be connected to earth ground.



Warning

Do not open the unit. There is a risk of electric shock inside.



Caution

You are cautioned that any change or modification not expressly approved in this manual could void your authority to operate this equipment.



Caution

There are no user-serviceable parts inside. All service must be performed by qualified personnel.



Caution

The Netronics NetPoint Pro products can be installed in wet, outdoor locations. Make sure closure caps are installed and all cable connections are securely fastened and waterproofed.



Caution

The Netronics NPP 6x2.4 G2 and NPP 6x2.4 n2C can only be used with approved antennas.

Table of Contents

Introduction	6
Key Product Features	6
Organization of this Document	7
Basic Configuration	8
Connect and Access the Unit	8
Connecting to the unit using a Web Browser	9
Web Interface.....	11
Device Configuration.....	12
General Configuration.....	12
IP Configuration Information.....	14
Software Versions.....	15
Wireless Configuration	16
Dot11Radio Setup	16
Service Optimization.....	18
Advanced	19
WME	20
Access	23
SSID Configuration	23
SSID Privacy.....	25
Radius	27
Radius Configuration.....	27
Radius Authentication and Accounting	28
Mesh	30
General Mesh Configuration	32
Connectivity test and Stand-alone Configuration	33
Route	35
Filter.....	36
Site Survey.....	37
Statistics.....	39
Associated Stations.....	39
Air Occupancy.....	41
Appendix A: List of Acronyms	42

Chapter 1

Introduction

Welcome to NetPoint Pro!

At Netronics we supply customized, carrier-class, outdoor Wi-Fi network systems to commercial and municipal service providers worldwide. Our NetPoint Pro family of outdoor Wi-Fi access point products delivers the world-class performance, coverage, and economics that service provider demand. By utilizing our advanced xRF™ adaptive beamforming smart antenna technology and an innovative cellular-style mesh architecture, our Wi-Fi solutions can dramatically reduce the number of access points required to deliver wide-area, fully-mobile wireless broadband services to customers.

Netronics NetPoint Pro n2S5S unit is the key enabler for the wireless solution, which relies on the strengths of innovative xRF™ architecture. This architecture provides the coverage, capacity, and scalability required to deliver next-generation services and overcome the limitations of existing metro Wi-Fi solutions.

The Netronics cellular-style mesh architecture is a highly scalable topology which provides unprecedented flexibility to service providers deploying Wi-Fi networks.

Key Product Features

- Robust cellular-style mesh architecture
- Tx and Rx Beamforming
- Separate access & backhaul radios delivering unmatched bandwidth
- xRF smart antenna engine for unmatched coverage and capacity enhancements
- Advanced automatic mesh
- Support for all standard security scheme

Organization of this Document

The Netronics NetPoint Pro n2S5S System Manual offers information and instructions for quickly configuring the NetPoint Pro n2S5S. The instructions and information are presented in one volume as follows:

Introduction	Contains introductory information about the NetPoint Pro n2S5S.
Basic Configuration	Describes the basic configuration for the NetPoint Pro n2S5S.
Wireless Configuration	Describes the procedures for implementing and configuring the wireless network.
Access	Describes how to allow clients to receive broadcast messages from various access points within the advertised SSID range.
Radius	Describes how to configure the accounting and authorization features.
Mesh	Describes how to set up a Mesh configuration.
Site Survey	Describes how to sample the air by site-survey and pick the best channel available.
Statistics	Describes the various statistics that are available to control the network.

Chapter 2

Basic Configuration

The following section describes how to set up the environment, Access the Unit Configuration and an overview of the Web interface.

The topics include:

- Connect and Access the unit
- Connecting to the unit using a web browser
- Overview of the Web Interface

Connect and Access the Unit

Initial configuration of the NetPoint Pro n2S5S unit is done using a standard, straight-through Ethernet cable. The cable is connected from the RJ-45 port of a laptop or a PC to the unit's RJ-45 port.

The IP address must first be defined to communicate with the unit. The default setting for the unit is to obtain the IP address from a DHCP Server with no VLAN tagging. If a DHCP Server is not available, the default IP address is set to 192.168.0.1.

When the IP address is to be obtained automatically from a DHCP server, the computer or network that is connected to the unit must contain a DHCP Server. The network must be configured with VLAN tagging disabled, or uses VLAN 0.

Once connected, the DHCP server will assign an IP address to the unit. Using the DHCP Server software, this IP address can be displayed. With this IP address, the configuration of the unit can be performed by using Telnet or a web browser.

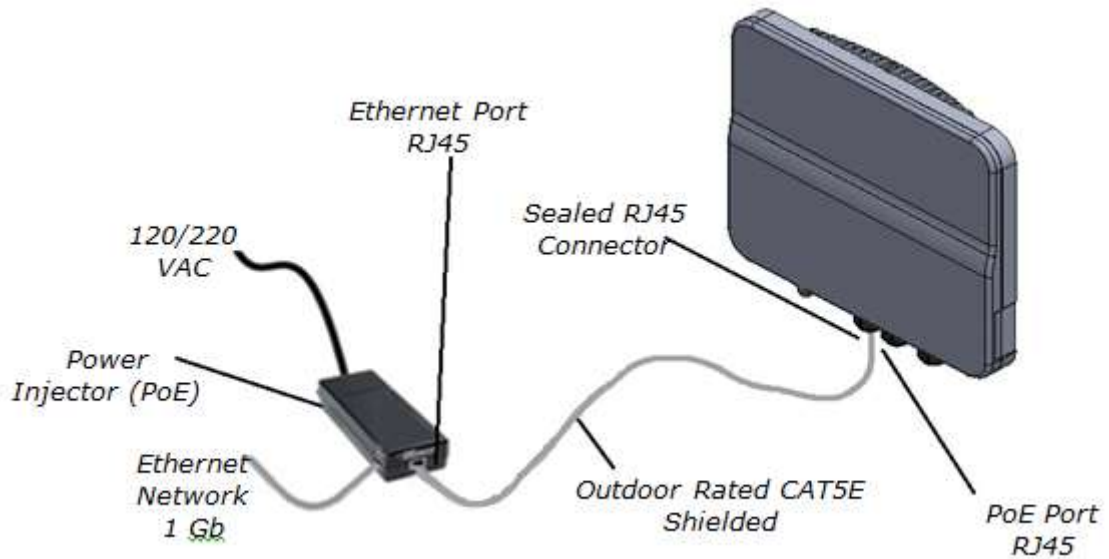


Figure 1: Connect and Access the NetPoint Pro n2S5S

Connecting to the unit using a Web Browser

Once the cable is connected, you can access the unit with a web browser. The following web browsers are supported:

- Internet Explorer 8
- Mozilla Firefox 3.6
- Google Chrome

➤ To log into the unit:

1. Power the unit and make sure the STAT led at the back of the Access Point is Green.
2. Open the web browser and enter the unit's IP address in the browser URL line. (Default IP: 192.168.0.1)
3. Once connected to the unit, a window will open requesting a User name and Password.
4. Type the User name and Password. The default values are as follows:
 - User name: super
 - Password: super
5. Once Authenticated, the initial configuration window opens.

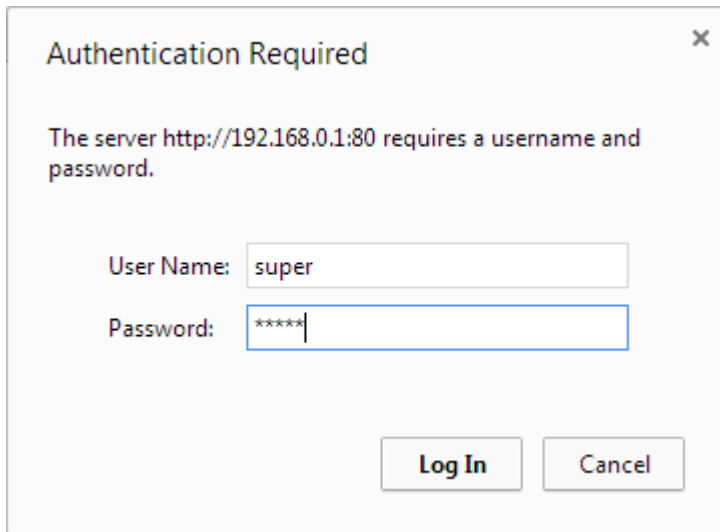


Figure 2: Google Chrome

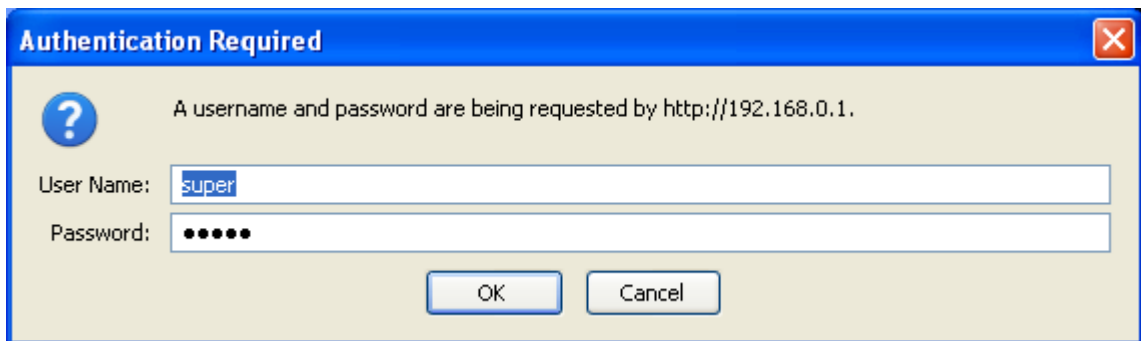


Figure 3: Mozilla Firefox



Figure 4: Initial Web Interface Window

Web Interface overview

The Web interface is divided into categories; each category has several associated configuration sub-category configurations. The available categories are listed below with a brief explanation:

- **Device**
Configure and receive basic Device information, Configure device IP and DHCP Mode and Upgrade the AP Firmware.
- **Wireless**
Configure the Wireless radios parameters, WME and SSID Attachment.
- **Access**
Configure the SSIDs and their Privacy parameters.
- **Radius**
Configure the Radius authentication and accounting servers.
- **Mesh**
Configure the Mesh, view the mesh routes and also configure the Connectivity Test and Stand-Alone features.
- **Site Survey**
Perform a Site Survey on the selected interface to grade channels according to air sampling.
- **Statistics**
Receive information of stations connected and their statistics, also, Sample the air in real-time to view it's status.

Chapter 3

Device Configuration

The following section describes how to configure general device parameters such as hostname and time, how to set an IP Address and import firmware to the device.

The topics include:

- General Configuration
- IP Configuration Information
- Software Versions

General Configuration










DEVICE > General 	
Model:	NetPoint Pro n2S5S
Host name:	 <input type="text" value="ap"/>
Date (MM/DD/YYYY):	 06 ▾ / 05 ▾ / 2014 ▾
Time (HH:MM):	 04 ▾ : 06 ▾
GMT:	 4 ▾
NTP:	 <input type="checkbox"/> Enable
Up time:	 0 days 0 hours 19 minutes 27 seconds
Temperature:	 40
Software version:	 4.0.0.0
Hardware version:	 8000-0-000
Serial number:	 NPPS1S900017
MAC Address:	 80:86:98:08:3d:12

Figure 5: Initial Screen - Information

The initial screen contains the following information:

Model	The unit model number.
Host name	The name used to identify the network.
Date	The internal date set in the unit. The format is MM/DD/YYYY.
Time	The internal time set in the unit. The format is HH:MM.
GMT	The number of hours that the current time is offset from GMT.
NTP	Network Time Protocol – an internet time protocol used to synchronize computer clocks to a centralized clock (based on the stratum level).
NTP Address	The NTP server and its IP address. Only visible if NTP is enabled.
NTP Interval	The time (in seconds) between NTP synchronizations. Only visible if NTP is enabled. The default is 1200 seconds.
Up time	Time since the last reboot.
Temperature	The unit's internal temperature.
Software Version	The version number of the currently operating software.
Hardware Version	The version number of the hardware.
Serial Number	The serial number of the unit.
MAC Address	The unit's MAC address.



When opening a service request, you will need to provide the following information:

- Model
- Serial number
- Hardware version
- Software version

IP Configuration Information

The unit can operate using either a static IP, or a dynamic IP received from a DHCP server.

DEVICE > IP

Configuration Type:	?	DHCP ▾
IP Address:	?	192.168.0.1
Net Mask:	?	255.255.255.0
Management VLAN:	?	0
Default Gateway:	?	0.0.0.0

Apply changes
Save Configuration

Figure 6: IP Screen - Information

The Information screen contains the following information:

Configuration Type	Indicates whether the IP is configured manually or received from a DHCP server
IP Address	The IP address of the Management VLAN
Net Mask	The subnet mask of the Management VLAN
Management VLAN	Configures the Ethernet Management VLAN ID. The physical Ethernet interface is a VLAN trunk. Note that VLAN ID 0 disables VLAN tagging.
Default Gateway	IP address of the default gateway



Setting the VLAN tag will cause the unit to lose communications, unless you are connected with a VLAN switch.

Software Versions

The unit maintains two software versions in two separate SW banks. In the event that there is an issue with an upgrade, the previous version can always be reloaded.

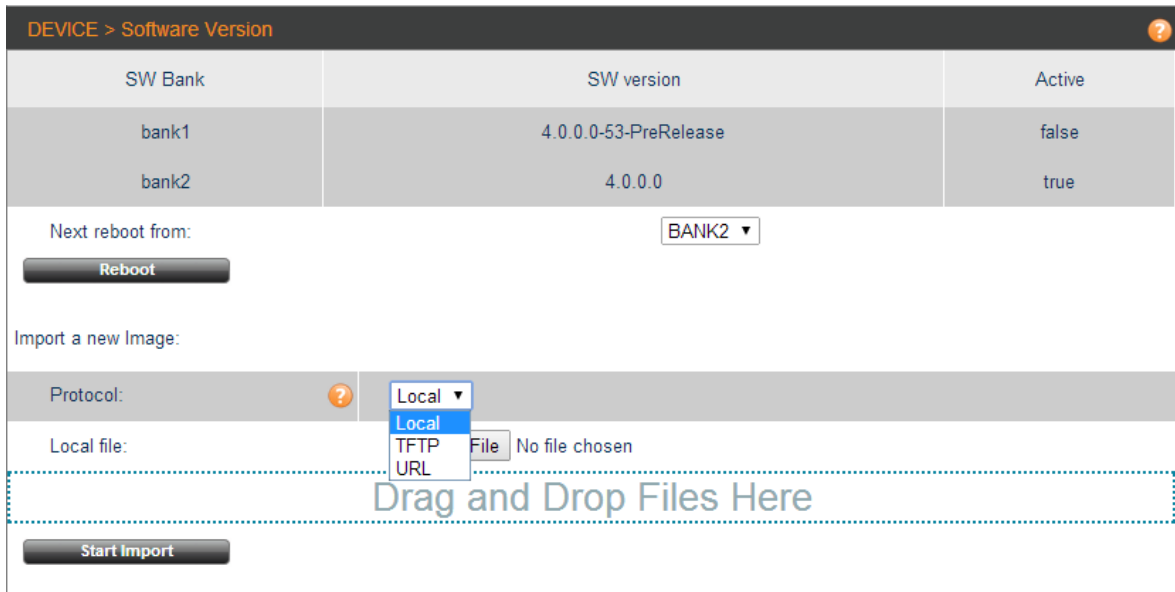


Figure 7: Software Version screen

The Software Version upgrade screen contains the following options:

- Local** Import the image by Drag & Drop or choosing a local file.
- TFTP** Using a TFTP Server on the network.
- URL** Using a Web Server on the network.

Wireless Configuration

The following section describes how to set up the wireless configuration on the device. There are several different parameters that must be set.

The topics include:

- Dot11Radio Setup
- Service Optimization
- Advanced Configuration
- Wireless Multimedia Enhancements (WME)

Dot11Radio Setup

Both of the radio interfaces are Wi-Fi, the first interface Dot11radio0 is 2.4 GHz and can act as access only, the second interface Dot11Radio1 is 5 GHz and can be configured to be Access OR Backhaul (Mesh mode). Also here you attach an existing SSID to the desired radio interface.

WIRELESS > DOT11RADIO 0	
Radio index:	0
Type:	2.4GHz
Status:	Up
Mode:	Auto
Channel:	4
Beacon Period (msec):	100
TX Power Attenuation:	2
Service:	Access
Distance (meters):	300
Max Associated Stations:	250
Auto Sensitivity:	auto
Manual Sensitivity:	-77
ERP Mode:	Disable

Attach SSIDs to Interface 0	
SSID name	Active
AP2.4	<input checked="" type="checkbox"/>
AP5	<input type="checkbox"/>

Figure 8: Radio Interface Screen

The Radio Interface screen contains the following information:

Radio Index	Radio interface number. The first interface (Dot11radio0) is used for 2.4 GHz communication, the second interface (Dot11radio 1) is used for 5GHz communication.
Type	The Wi-Fi Protocol xRF is the Netronics standard, with patented beam-forming technology.
Status	The current interface status; up (active) or down (inactive)
Mode	Actual available modes are dependent on the radio interface type, available configuration are: 802.11a / 802.11an / 802.11an HT40 / 802.11b / 802.11g / 802.11bgn / 802.11bgn HT40
Channel	Configures the Wi-Fi channel used on the specified radio interface. The actual frequencies available are dependent on the radio interface (802.11an or 802.11b/g/n), and the region for which the unit was manufactured.
Beacon Period	Configures the time period (in msec) between beacon transmissions

Service Optimization

WIRELESS > DOT11RADIO 0	
Radio index:	0
Type:	2.4GHz
Status:	Up
Mode:	Auto
Channel:	4
Beacon Period (msec):	100
TX Power Attenuation:	2
Service:	Access
Distance (meters):	300
Max Associated Stations:	250
Auto Sensitivity:	auto
Manual Sensitivity:	-77
ERP Mode:	Disable

Figure 9: Service Optimization screen

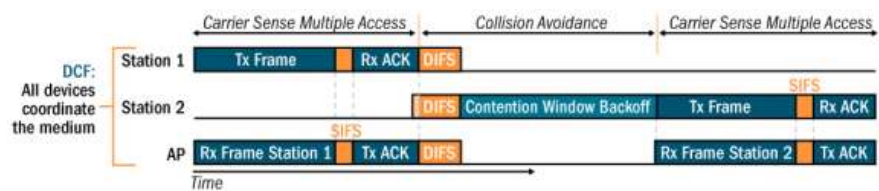
The Service Optimization parameters contain the following information:

Tx Power Attenuation

Configures the transmission power attenuation. It decreases the transmitted power by the specified dB value.

Distance

Defines the distance (in meters) between the gateway and the node units for the 802.11an backhaul radio interface. For 802.11b/g/n access radio interface, this command defines the distance between the node unit and the client



After receiving a data frame, the receiving station will send an ACK frame to the sending station if no errors are found.

If the sending station does not receive an ACK frame within a predetermined time, the sending station will resend the frame.

Distance changes the ACK timeout

Auto/Manual Sensitivity

Configures the noise-floor level in dBm for the specified radio interface. Any signal below this level is considered to be noise, and will not be recognized.



Stations with lower sensitivity level cannot associate; manual sensitivity decreases the coverage radius, and improved the service for the associated stations.

Advanced

WIRELESS > DOT11RADIO 0	
Radio index:	0
Type:	2.4GHz
Status:	Up
Mode:	Auto
Channel:	4
Beacon Period (msec):	100
TX Power Attenuation:	2
Service:	Access
Distance (meters):	300
Max Associated Stations:	250
Auto Sensitivity:	auto
Manual Sensitivity:	-77
ERP Mode:	Disable

Figure 10: Advanced screen

The Advanced parameters contain the following information:

Service	Configures the Service type of the Interface, Access for wireless access or Backhaul for Mesh Topology
Max Associated Stations	Configures the maximum number of users on a specific interface. The default value is 250.
ERP Mode	ERP Protection allows ERP (802.11g), HR-DSSS (802.11b) and legacy DSSS devices to co-exist within the same BSS. Protected mode can be provided by RTS / CTS interface.



ERP mode is used to reduce collisions when there are both b- and g- clients.

Wireless Multimedia Enhancements

Wireless Multimedia Enhancements (WME) is a method to improve Quality of Service (QoS) for wireless communications. It complies with IEEE 802.11e; the QoS extension for 802.11 networks. WME is responsible for assigning the priority level to data packets. The priority is based on packet categories. WME defines all packets into one of the following Access Categories (AC):

- Voice – Highest priority.
- Video – High priority for video traffic, which is the higher than any other data traffic.
- Best Effort – Medium priority for traffic from legacy devices or traffic from applications or devices that lack QoS capabilities.
- Background – Lowest priority for low priority traffic such as file downloads and printing jobs.

Each AC is configured separately. The default values defined in the NetPoint Pro units prioritize the AC as indicated above. Prioritization is based on time parameters that define the time duration for transmission opportunities (TXOP) and the time allowed transmitting (TXOP Limit). The parameters are as follows:

- Short Inter-Frame Space (SIFS) – Time period used in determining the minimum time between transmission opportunities (TXOP).
- Arbitrary Inter-Frame Space (AIFS) – Time period for the slot that is used in determining the minimum time between transmission opportunities (TXOP). Higher priority categories are set to a lower number of time slots.
- Contention Window (CW) – Time range that is used to determine the time between transmission opportunities (TXOP). During the initial transmission, CW is determined based on the set value of CW_{min} , which is the exponent form of the minimum CW. After each collision CW is doubled to a maximum value that is determined by the value set for CW_{max} , which is the exponent form of the maximum CW. Higher priority categories are set to lower CW values.

CW is also referred to Random Backoff Wait. The time contributed by the CW in determining the TXOP duration time, window of time up to the CW time. If the exponent form of CW is 4, then the CW is 15 microseconds, and the TXOP duration can be from the minimum TXOP to the minimum TXOP plus 15 microseconds.

- Transmission Opportunity (TXOP) Limit – Time period permitted for transmission. If transmission is not successful within this time, transmission of the packet is attempted again after waiting the TXOP duration. Higher priority categories are set to high TXOP Limits.

Wireless > WME 0

WME Mode on Interface 0 :

Interface 0 AP WME params

Category ?	CWMin ?	CWMax ?	AIFS ?	TXOP ?
besteffort	<input type="text" value="4"/>	<input type="text" value="6"/>	<input type="text" value="3"/>	<input type="text" value="0"/>
background	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="7"/>	<input type="text" value="0"/>
video	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="1"/>	<input type="text" value="3008"/>
voice	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="1"/>	<input type="text" value="1504"/>

Interface 0 BSS WME params

Category ?	CWMin ?	CWMax ?	AIFS ?	TXOP ?
besteffort	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="3"/>	<input type="text" value="0"/>
background	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="7"/>	<input type="text" value="0"/>
video	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="2"/>	<input type="text" value="3008"/>
voice	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="2"/>	<input type="text" value="1504"/>

Figure 11: Wireless WME screen

WME Mode

Enable/Disable the WME functionality.

Interface AP BSS

The WME configuration for both the access point and the associated clients.

AP

Access point side.

BSS

Client with WME support. Most newer clients support WME.

Category

The WME category. These are:

- Best effort
- Background
- Video
- Voice

CWMin

Contention window minimum value.

CWMax

Contention window maximum value.



If CSMA/CA fails, the transmission will wait an additional time defined by the range of Contention Window. Services with smaller Contention Windows have more transmission opportunities than services with larger Contention Windows.

AIFS	After sending a frame, the transmitter will wait a period of time, defined by the designated number of time slots.
TXOP	A TXOP is a bounded time interval during which a station can send as many frames as possible.

Chapter 5

Access

The Access features allow clients to receive broadcast messages from various access points within their advertised SSID range.

This section contains the following topics:

- SSID Configuration
- SSID Privacy

SSID Configuration

ACCESS > SSID

Add a new SSID :

Index	Name ?	Privacy ?	Vlan ?	Type ?	Fixed Rate ?
3	<input type="text"/>	NONE	0	BSSID	AUTO

Add

Manage SSIDs :

Index	Name ?	Privacy ?	Vlan ?	Type ?	Fixed Rate ?	Remove
1	AP2.4	NONE	0	BSSID	AUTO	<input type="checkbox"/>
2	AP5	NONE	0	BSSID	AUTO	<input type="checkbox"/>

Apply changes

Save Configuration

Figure 12: SSID Configuration screen

The SSID Configuration screen contains the following fields

Index	The SSID Index. There is a maximum of up to 7 indexes.
Name	The SSID Name; maximum 32 characters.
Privacy	The SSID Privacy policy.
VLAN	The SSID VLAN ID. One VLAN can be configured per SSID.



When providing multiple services on different VLANs, the VLAN Trunk mode should be activated on the mesh interface.

Type	There are two states for this field: Hidden – Transmits only the MAC Address BSSID – Transmits the SSID string in the beacon.
Fixed Rate	Configures the fixed transmission rate on the specified interface
Remove	Deletes the SSD from the configuration.

SSID Privacy

ACCESS > SSID Privacy

Index	Name	Privacy	Click to Expand
1	AP2.4	off	
2	AP5	off	
3	WEP	wep	
Key Type		Key value [Hex]	
40 ▾		<input type="text" value="11:22:33:44:55"/>	
104 ▾		<input type="text" value="11:22:33:44:55:66:77:88:99:00:11:12:13"/>	
40 ▾		<input type="text" value="00:00:00:00:00"/>	
40 ▾		<input type="text" value="00:00:00:00:00"/>	
4	WPA	wpa	
Key Management		Protocol	Passphrase
PSK ▾		WPA2 ▾	<input type="text" value="12341234"/>
		Data Encryption	
		AES ▾	
5	EAP	wpa	
Key Management		Protocol	Passphrase
EAP ▾		WPA2 ▾	<input type="text" value="12345678"/>
		Data Encryption	
		AES ▾	

Figure 13: SSID Privacy screen

The SSID Privacy screen contains the following fields:

Index	The SSID Privacy Index. There is a maximum of up to 7 indexes.
Name	The SSID Name; maximum 32 characters.
Privacy	The SSID Privacy type. The options are: <ul style="list-style-type: none">• None• WEP• WPA
Click to Expand	Click to view privacy details
Key Type	The key type. The options are: <ul style="list-style-type: none">• 40 bit• 104 bit
Key Value	The Key value. The options for the number of characters in the key is: <ul style="list-style-type: none">• For a 40-bit key (10*4 bits (HEX)• For a 104-bit key (26*4 bits (HEX)
Key Management	Defines the key management type. The options are: <ul style="list-style-type: none">• EAP – Extended Authorization Protocol• PSK – Pre-Shared Key
Protocol	Defines the WPA Protocol type. The options are: <ul style="list-style-type: none">• WPA1 – Supports WPA 1 only• WPA2 – Supports wpa1 and WPA2• WPA2 only – Supports WPA2 only
Passphrase	Defines the passcode that must be used during the key handshake process for WPA encryption. The value is case-sensitive, and can be between 8 and 63 characters.
Data encryption	Defines the data encryption type: <ul style="list-style-type: none">• AES – Advanced Encryption Standard (AES/CCMP)

Chapter 6

Radius

This section describes the information that must be used to configure the Radius server. This tool is used for accounting and user authentication.

The topics include:

- Radius Configuration
- Radius Authentication and Accounting

Radius Configuration

RADIUS > RADIUS Configuration		
Retry primary Interval :	?	<input type="text" value="900"/>
Interim-Interval :	?	<input type="text" value="0"/>
Max retries :	?	<input type="text" value="3"/>
Retry time :	?	<input type="text" value="0"/>

Figure 14: Radius Configuration screen

The Radius Configuration screen contains the following fields

Retry Primary Interval	After switching to the secondary Radius server, this interval configures the time, in seconds, that the unit waits before retrying the primary Radius server again (the default value is 900 seconds).
Interim Interval	Defines the frequency that the unit sends accounting updates to the Radius server.
Max Retries	Defines the Max number of attempts to retransmit a RADIUS message.
Retry Time	Defines the Max number of attempts to retransmit a RADIUS message.

Radius Authentication and Accounting

This command is used to configure the parameters required to communicate with the primary and the secondary Radius servers. For each server the authentication and accounting parameters can be configured to permit access to the Radius servers.

The accounting services monitors and records the number of packets transmitted and received by each authenticated client.

The WPA-EAP security must be configured before implementing the Radius server.

RADIUS > RADIUS Authentication

Add a new RADIUS Authentication entry :

SSID	Priority	Host	Key	Port
EAP ▼	1 ▼	<input type="text"/>	<input type="text"/>	1812

Add

Manage RADIUS Authentication :

SSID Index	SSID Name	Priority	Host	Key	Port	Remove
------------	-----------	----------	------	-----	------	--------

RADIUS > RADIUS Accounting

Add a new RADIUS Accounting entry:

SSID	Priority	Host	Key	Port
EAP ▼	1 ▼	<input type="text"/>	<input type="text"/>	1813

Add

Manage RADIUS Accounting :

SSID Index	SSID Name	Priority	Host	Key	Port	Remove
------------	-----------	----------	------	-----	------	--------

Figure 15: Radius Authentication and Accounting screen

The Radius Authentication and Accounting screen contains the following fields:

SSID	An existing SSID number.
Priority	Defines the priority of the Radius Servers: 1 – Configures the parameters to communicate with the primary Radius Server. 2 - Configures the parameters to communicate with the secondary Radius Server.
Host	IP address of the authentication or accounting Radius server.
Key	Defines the key used for Radius server security. The value is case sensitive and can be from 5 to 63 characters.
Port	Number of the authentication or accounting port on the Radius server: 1-65535. This parameter is optional. The default value for authentication port is 1812. The default value for accounting port is 1813.

Chapter 7

Mesh

An outdoor Wi-Fi mesh network is a tree-structured network that connects wireless clients to the core network (i.e. the wired internet service provider) via Wi-Fi base stations that are configured as mesh nodes and mesh gateways. A mesh gateway is defined as a base station that is connected by wire directly to the local core network and a mesh node is defined as a base station that is connected indirectly to the core network, via other mesh node or via a mesh gateway. The figure below illustrates a sample mesh network.

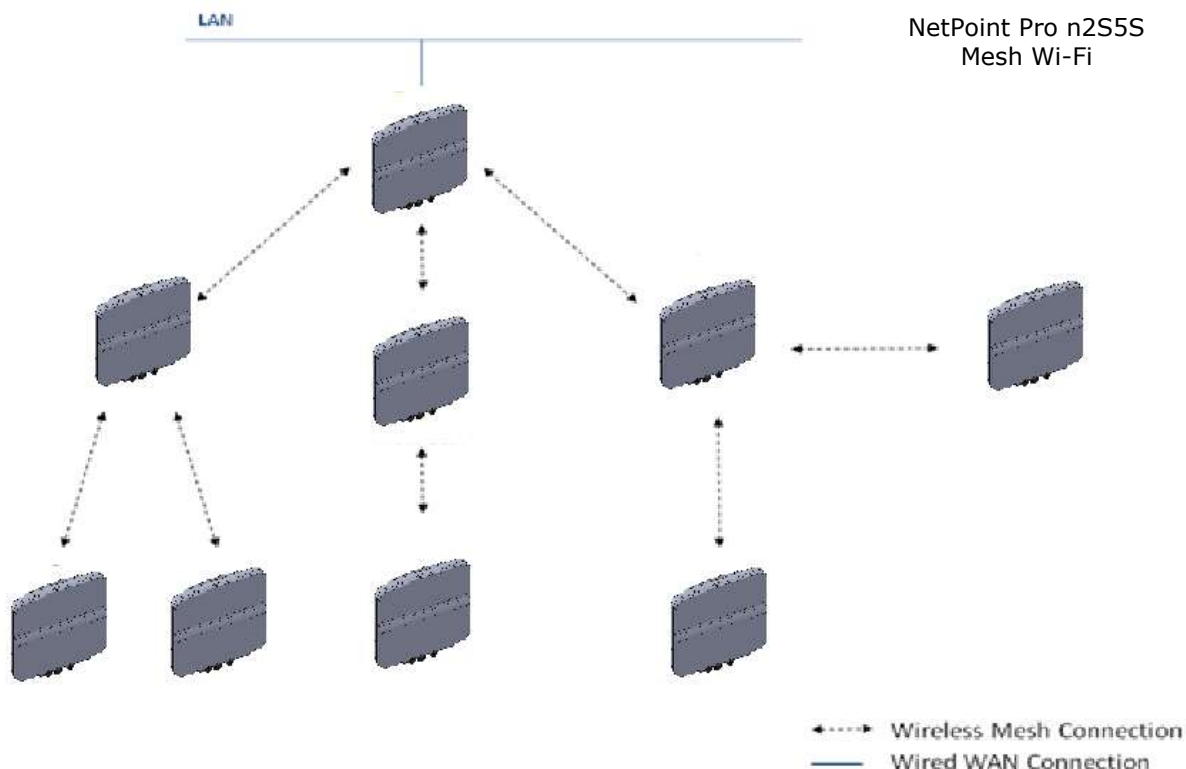


Figure 16: Typical NetPoint Pro Mesh Cluster

A node’s position in a mesh network is defined in terms of how many steps it is away from the mesh gateway. For instance, in the figure above, nodes A and C are first hop nodes and node B is a second-hop node. A Wi-Fi base station communicates using two radio interfaces. The access interface provides clients access to the base station and the mesh interface provides mesh backhaul communication between the base stations. For example, in the figure above, the Wi-Fi phone communicates with node B using the access interface, and node B communicates with node A using the mesh interface.

Base stations communicate over specific Wi-Fi channels by sending Wi-Fi data packets. A connection’s transmission capacities are expressed in terms of bandwidth and throughput. Bandwidth is the overall capacity of a connection. Throughput is the amount of capacity that remains after the overhead is accounted for (i.e. traffic which is used for traffic control or security purposes). Base-stations utilize 2.4 GHz channels for unlicensed client access, 5.8 GHz channels for unlicensed mesh backhaul.

NetPoint Pro mesh is a layer 2 transparent solution to higher layer protocols, including IP. As a result, layer 3 applications such as VPNs are not affected by handoff and continue to operate seamlessly. Mesh is implemented using 802.11a channels, maximizing the efficiency and throughput of the 802.11b/g access channels.

This section contains the following topics:

- General Mesh Configuration
- Route
- Filter
- Static Links

General Mesh Configuration

















MESH > General		
Network ID:		<input type="text" value="123456789"/>
Unit Mode:		<input type="text" value="node"/>
Connectivity test mode:		<input type="text" value="disabled"/>
Connection status to the net:		normal
Connectivity test target host:		<input type="text" value="none"/> <input checked="" type="checkbox"/> Disable target host
Connectivity test target host 2:		<input type="text" value="none"/> <input checked="" type="checkbox"/> Disable target host 2
Connectivity ping retry:		<input type="text" value="10"/>
Connectivity timeout:		<input type="text" value="1"/>
Connectivity interval:		<input type="text" value="10"/>
Connectivity ping fail interval:		<input type="text" value="1"/>
Advertising Status:		<input type="text" value="enabled"/>
Trunk:		<input type="text" value="enabled"/>
Gateway MAC Address:		00:00:00:00:00:00
MESH Stand Alone:		<input type="text" value="disable"/>
MESH Stand Alone Status:		inactive
MESH Stand Alone Passphrase:		<input type="text" value="00000000"/>

Figure 17: General Mesh Configuration

The Mesh General screen contains the following fields:

- Network ID** The name of the Mesh Network.
Defines the mesh network-id associated with the mesh network. All units in a single mesh network must have the same specified network id. The value is case sensitive and can be from 8 to 16 characters.
- Unit Mode** Configures the gateway as either a Node or Gateway.
- Advertising Status** Configures the unit as a candidate for the next hop in the mesh network. It defines whether the unit can be used to establish a connection to get access to the Mesh-Gateway.
- Trunk** Enables the Mesh VLAN Trunk mode.
- Gateway MAC Address** The MAC address of the gateway.

Connectivity test and Stand-alone Configuration

MESH > General		
Network ID:	<input type="text" value="123456789"/>	
Unit Mode:	<input type="text" value="node"/>	
Connectivity test mode:	<input type="text" value="disabled"/>	
Connection status to the net:	normal	
Connectivity test target host:	<input type="text" value="none"/>	<input checked="" type="checkbox"/> Disable target host
Connectivity test target host 2:	<input type="text" value="none"/>	<input checked="" type="checkbox"/> Disable target host 2
Connectivity ping retry:	<input type="text" value="10"/>	
Connectivity timeout:	<input type="text" value="1"/>	
Connectivity interval:	<input type="text" value="10"/>	
Connectivity ping fail interval:	<input type="text" value="1"/>	
Advertising Status:	<input type="text" value="enabled"/>	
Trunk:	<input type="text" value="enabled"/>	
Gateway MAC Address:	00:00:00:00:00:00	
MESH Stand Alone:	<input type="text" value="disable"/>	
MESH Stand Alone Status:	inactive	
MESH Stand Alone Passphrase:	<input type="text" value="00000000"/>	

Figure 18: Connectivity test and Stand-alone Configuration

The Mesh Connectivity test and Stand-Alone contains the following fields:

- Connectivity Test Mode** Configures the mesh-gateway connectivity test. This test is typically used to check Internet connectivity. This test is only applied when the unit is defined as the Mesh-Gateway. The test performs a ping command every 10 seconds. A failure occurs after 10 ping commands fail consecutively. If the connectivity test fails, the mesh mode will automatically switch to node mode. When the connection is restored, the gateway will return to mesh mode automatically.
- Connectivity Test Target Host** Specify the IP of the first Target to be pinged.
- Connectivity Test Target Host 2** Specify the IP of the Second target to be pinged.
- Connectivity ping retry** Configure how many pings will be sent before the state will change to LostAndBecameNode.
- Connectivity timeout** Configure how many seconds should pass from last ping to determine a ping fail (timeout).

Connectivity interval	Configure how much time (sec) should pass between each successful ping.
Connectivity ping fail interval	Configure how much time (sec) should pass between each unsuccessful ping.
MESH Stand Alone	When stand-alone mode is active, the device acknowledges that it does not have communications with the gateway and disables access to the clients.
MESH Stand Alone Status	Displays the current stand-alone status.
MESH Stand Alone Passphrase	Configures the mesh stand-alone SSID pre shared key
Connection status to the net	Display the connectivity status.

Route

Gateway mesh routing table

Bridging traffic for:

Name	Address	RSSI	Rate
Street	172.16.1.111	-35	N/A

Alternative next hop:

Name	Address	RSSI	Rate
------	---------	------	------

Next hop:

Name	Address	RSSI	Rate
------	---------	------	------

Node mesh routing table

Bridging traffic for:

Name	Address	RSSI	Rate
------	---------	------	------

Alternative next hop:

Name	Address	RSSI	Rate
------	---------	------	------

Next hop:

Name	Address	RSSI	Rate
Office	172.16.1.114	-30	54

Figure 19: Mesh Route Table

The Routing Tables screen contains the following fields:

- Bridging Traffic for** Nodes that are connected to the unit.
- Alternative Next Hop** Optional next hop for a gateway. This can be another node or a gateway.
- Next Hop** The mode next hop. This can be another node or a gateway

Filter

Mesh > Filter

Filter List status: Enable

Add a new MAC Address filter:

Deny

Manage MAC Address filters :

MAC address ?	Type ?	Remove
00:14:06:a5:5b:ff	Deny	<input type="checkbox"/>
00:14:06:bb:a4:53	Deny	<input type="checkbox"/>

Figure 20: Mesh Filter List

The Mesh Filter screen contains the following fields:

Filter List Status	Enables the Next Hop filter. This is only applicable for mesh nodes.
Add a new MAC Address	Permits or denies connection to the specified MAC addresses.

Chapter 8

Site Survey

The Site Survey tool is used to determine the best channel to use. The grades that appear on the Site Survey screen are based on Noise Floor and Load.



The screenshot shows the 'SITESURVEY > DOT11RADIO 0' interface. It features a 'Start Site Survey' button and a table with four columns: Channel, Load, Noise Floor, and Grade. The table lists 13 channels, with channel 13 highlighted in green, indicating it is the selected or best channel.

Channel	Load	Noise Floor	Grade
1	35	-97	66
2	70	-96	34
3	70	-96	34
4	45	-96	56
5	53	-94	49
6	61	-95	42
7	58	-96	45
8	59	-96	44
9	26	-97	74
10	31	-97	69
11	68	-97	36
12	42	-97	59
13	16	-95	82

Figure 21: Site Survey screen

The Site Survey screen contains the following fields

Start Site Survey

Starts the Start-Survey on the Corresponding Interface (2.4 GHz or 5 GHz)

Load

Represents the Air Utilization on the channel for both Wi-Fi and non-Wi-Fi devices.

On the Wi-Fi, the wide channel bandwidth is 22 MHz and the channel separation is 5 MHz, therefore every channel effects two channels below and above.

When choosing a channel you need to take into consideration the channels grades below and above.

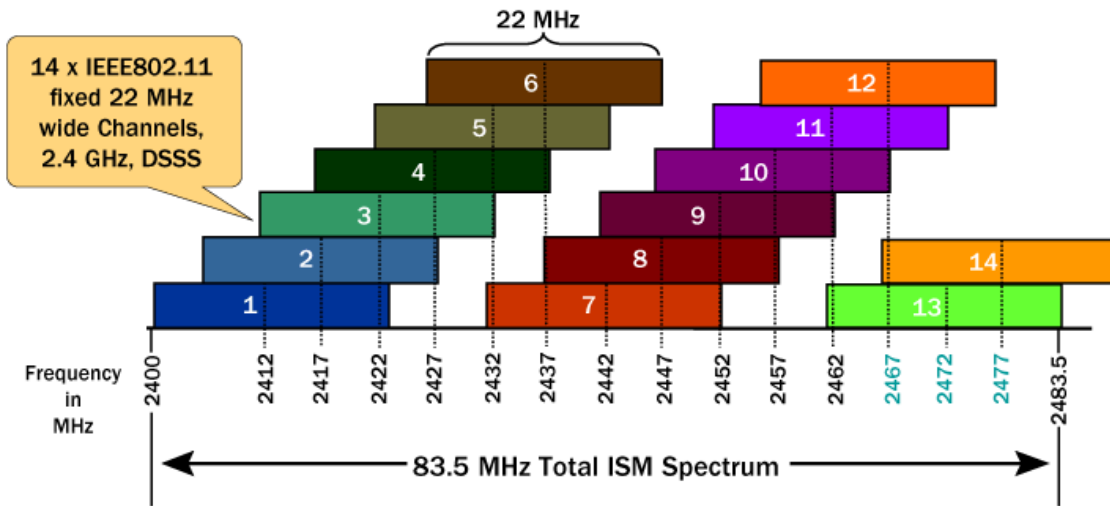


Figure 22: Channel Separation

Noise Floor

The sensitivity level represents the noise level which determines whether or not the client can associate with the base station. Clients with a higher sensitivity level are able to associate.

For example, a client with a sensitivity of -89 dBm, can associate with a client that has a sensitivity level of -88 dBm. It cannot associate with a client whose sensitivity is -90 dBm.

Grade

The Final Grade for the channel after calculating Noise Floor and Load.

Chapter 9

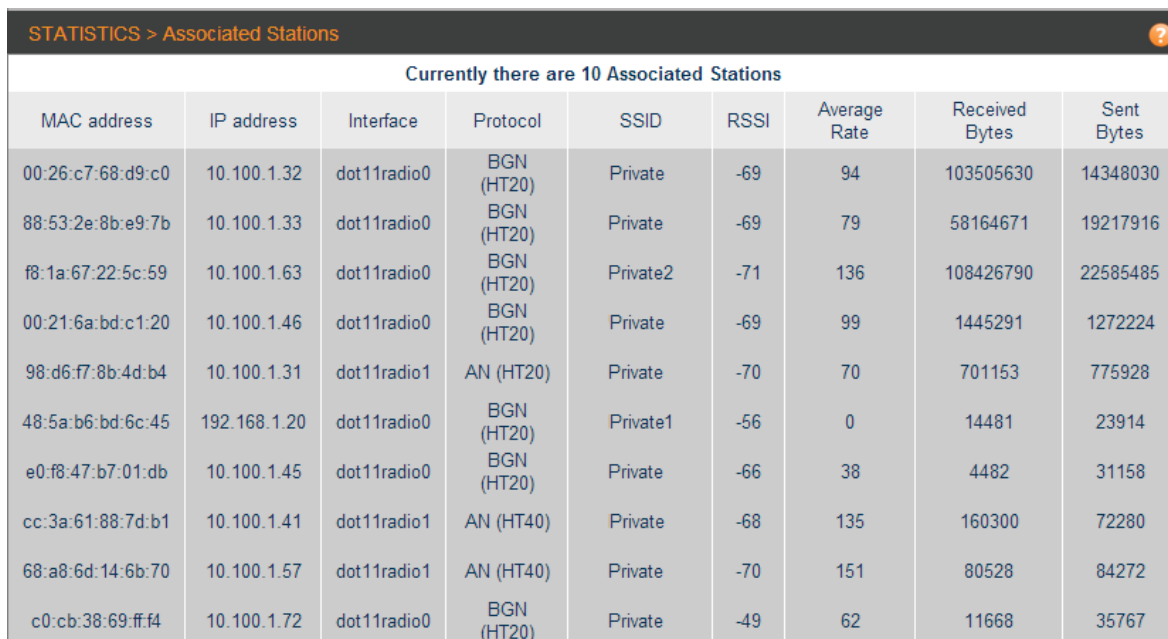
Statistics

The Statistics display information on a real-time basis to allow proper control and decision-making.

This section contains the following topics:

- Associated Stations
- Air Occupancy

Associated Stations



STATISTICS > Associated Stations

Currently there are 10 Associated Stations

MAC address	IP address	Interface	Protocol	SSID	RSSI	Average Rate	Received Bytes	Sent Bytes
00:26:c7:68:d9:c0	10.100.1.32	dot11radio0	BGN (HT20)	Private	-69	94	103505630	14348030
88:53:2e:8b:e9:7b	10.100.1.33	dot11radio0	BGN (HT20)	Private	-69	79	58164671	19217916
f8:1a:67:22:5c:59	10.100.1.63	dot11radio0	BGN (HT20)	Private2	-71	136	108426790	22585485
00:21:6a:bd:c1:20	10.100.1.46	dot11radio0	BGN (HT20)	Private	-69	99	1445291	1272224
98:d6:f7:8b:4d:b4	10.100.1.31	dot11radio1	AN (HT20)	Private	-70	70	701153	775928
48:5a:b6:bd:6c:45	192.168.1.20	dot11radio0	BGN (HT20)	Private1	-56	0	14481	23914
e0:f8:47:b7:01:db	10.100.1.45	dot11radio0	BGN (HT20)	Private	-66	38	4482	31158
cc:3a:61:88:7d:b1	10.100.1.41	dot11radio1	AN (HT40)	Private	-68	135	160300	72280
68:a8:6d:14:6b:70	10.100.1.57	dot11radio1	AN (HT40)	Private	-70	151	80528	84272
c0:cb:38:69:ff:f4	10.100.1.72	dot11radio0	BGN (HT20)	Private	-49	62	11668	35767

Figure 23: Associated Station screen

The Associated Stations screen contains the following fields:

- MAC Address** The client MAC Address.
- IP Address** The Client IP Address.

Interface	The unit physical interface the client is associated with.
Protocol	The Wi-Fi protocol used between the client and the AP (depends on what Protocol the client supports)
SSID	The SSID the client is associated with.
RSSI	The client signal received in the base station
Average Rate	The client average rate (modulation)
Received Bytes	The number of bytes downloaded by the client.
Sent Bytes	The number of bytes that were uploaded by the client.

Appendix A

List of Acronyms

Acronym	Explanation
802.11	A family of specifications related to wireless networking, including: 802.11a, 802.11b, 802.11g and 802.11n.
AP	Access Point. The hub of a wireless network. Wireless clients connect to the access point, and traffic between two clients must travel through the access point. Access points are often abbreviated to AP.
BSSID	Broadcast Service Set Identifier
CPE	Customer Premises Equipment
DHCP	Dynamic Host Configuration Protocol. A protocol which enables a server to automatically assign an IP address to clients so that the clients do not have to configure the IP addresses manually.
EAP	Extensible Authentication Protocol. A standard form of generic messaging used in 802.1X.
ESSID	Extended Service Set Identifier
SSID	Service Set Identifier, a set of characters that give a unique name to a WLAN.
VLAN	Virtual Local Access Network
WEP	Wired Equivalent Privacy. An encryption system created to prevent eavesdropping on wireless network traffic.
WNC	Wireless Network Controller of the Netronics NetPoint Pro solution.
WPA	Wi-Fi Protected Access. A modern encryption

system created to prevent eavesdropping on wireless network traffic. It is considered more secure than WEP.

WPA-EAP

WPA-Extensible Authentication Protocol

WPA-PSK

WPA-Pre-Shared Key