

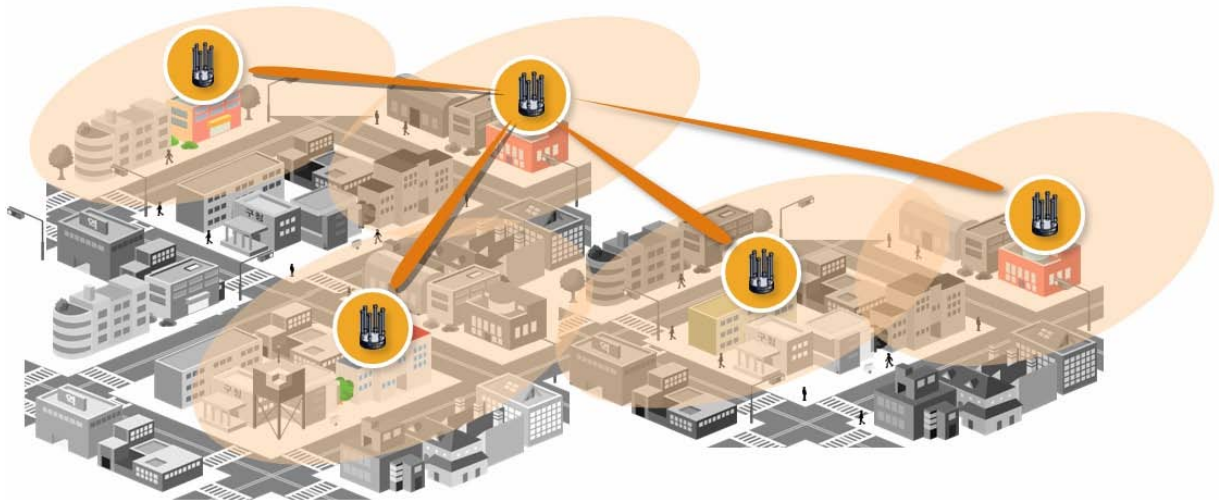


NetPoint Pro Family

Broadband Wireless Networking Solutions

NetPoint Pro 6x2.4 / 3x2.4 (G2 and G2M)

SYSTEM MANUAL



2nd Generation

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

There is a risk of personal injury or death if the NPP-6X2.4 antennas come near electric power lines. Carefully read and follow all instructions in this manual. By nature of the installation, you may be exposed to hazardous environments and high voltage. Use caution when installing the outdoor system.



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 RJ45 connectors of your Netronics NPP-6X2.4 may source DC power On pins 4,5 and 7,8. The IEEE 802.3 standards allow for pins 4,5 and 7,8 to be used for Power Over Ethernet. Some products may be incompatible with the Netronics Power Over Ethernet capability. If such problems occur, make sure that the unit is configured with the Power Over Ethernet capability set to Off (default setting). If problems persist, use Ethernet cables that have no connections to the unused pins 4,5 and 7,8.



Caution

The Netronics NPP-6X2.4 and NPP-3X2.4 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 can only be used with approved antennas.

Table of Contents

| | |
|---|-----------|
| Introduction | 7 |
| Key Product Features | 7 |
| Organization of this Document | 8 |
| Basic Configuration | 9 |
| Connect and Access the Unit | 10 |
| Connecting to the unit using a Web Browser_..... | 11 |
| Web Interface..... | 13 |
| Initial Web Interface Information..... | 15 |
| IP Configuration Information..... | 15 |
| Software Versions | 16 |
| Wireless Configuration | 17 |
| Dot11Radio Setup | 17 |
| Beacon | 19 |
| Service Optimization | 20 |
| Advanced | 22 |
| WME | 24 |
| CAC – Call Admission Control..... | 27 |
| General CAC Setup | 27 |
| MAC Classifier..... | 28 |
| VoIP Clients | 29 |
| Access | 30 |
| SSID Configuration | 30 |
| SSID Privacy | 31 |
| MAC Filter List | 33 |
| MAC Filters | 34 |
| Radius | 35 |
| Radius Configuration..... | 35 |
| Radius Authentication and Accounting | 36 |
| Mesh | 38 |
| General Mesh Configuration | 40 |
| Route | 42 |
| Filter..... | 43 |
| Static Links | 44 |
| Statistics | 45 |
| Show Associated Stations..... | 45 |
| Air Occupancy..... | 46 |
| Choosing the Best Channel – Site Survey..... | 47 |
| Wizard..... | 49 |
| Typical Scenarios | 53 |
| Basic Setup | 53 |

| | |
|--|-----------|
| Configure the Wi-Fi access channel..... | 53 |
| Software Upgrade..... | 56 |
| Establish a Mesh Network..... | 56 |
| Debug..... | 58 |
| Check the air Occupancy | 58 |
| Monitor the number of associated stations | 58 |
| Installation | 59 |
| Typical NetPoint Pro 6x2.4 | 59 |
| Typical NetPoint Pro 3x2.4 | 60 |
| Appendix A: List of Acronyms | 61 |
| Appendix B: Wiring Specifications | 63 |
| Appendix C: Quick Installation Guide..... | 64 |

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 6x2.4 and 3x2.4 units are the key enablers for the metro broadband 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 Micro/Pico/Femto topology which provides unprecedented flexibility to service providers deploying Metro Wi-Fi networks.

Key Product Features

- Robust cellular-style mesh architecture
- Separate access & backhaul radios delivering unmatched bandwidth
- xRF smart antenna engine for unmatched coverage and capacity enhancements
- Advanced automatic mesh
- Client/WDS (Wireless Distribution System) based CPE connection
- Support for all standard security scheme

Organization of this Document

The *Netronics NetPoint Pro System Manual* offers information and instructions for quickly configuring the NetPoint Pro 3x2.4 and NetPoint Pro 6x2.4. The instructions and information are presented in one volume as follows:

| | |
|-------------------------------|---|
| Introduction | Contains introductory information about the NetPoint Pro 3x2.4 and NetPoint Pro 6x2.4. |
| Basic Configuration | Describes the basic configuration for the NetPoint Pro 3x2.4 and NetPoint Pro 6x2.4. |
| Wireless Configuration | Describes the procedures for implementing and configuring the wireless network. |
| CAC | Describes the features that are available to prevent oversubscription to the 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. |
| Statistics | Describes the various statistics that are available to control the network. |
| Wizard | Describes the use of the Wizard. |
| Typical Scenarios | Describes some typical scenarios that users encounter when using the devices. |
| Debug | Provides some information solving some difficulties that may occur. |
| Installation | Shows some common installation methods. |
| Appendix A | Lists the acronyms that appear in the manual. |
| Appendix B | Details the wiring specifications. |
| Appendix C | Describes the power up and software configuration. |

Chapter 2

Basic Configuration

The following is a brief overview of the main CLI commands that are used to configure the NetPoint Pro 3x2.4 and NetPoint Pro 6x2.4. A configuration example follows the detailed list of configuration commands. These and other CLI commands are detailed in the Netronics NetPoint Pro CLI Reference Guide.

Connect and Access the Unit

Initial configuration of the NetPoint Pro 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. For more information regarding the Ethernet cable, see Appendix B: Wiring Specifications.

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.

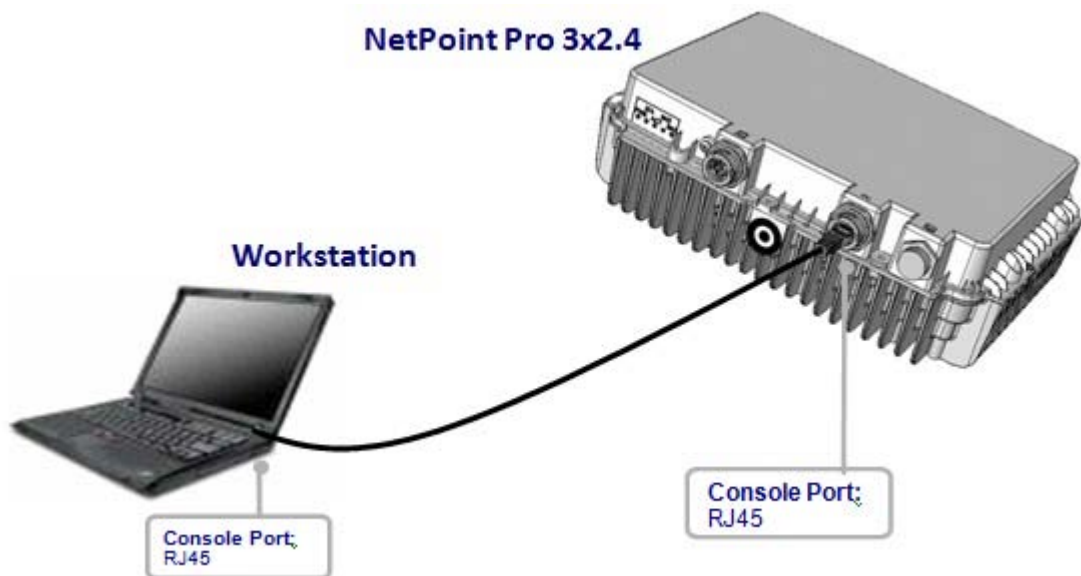


Figure 1: Connect and Access the NetPoint Pro 3x2.4

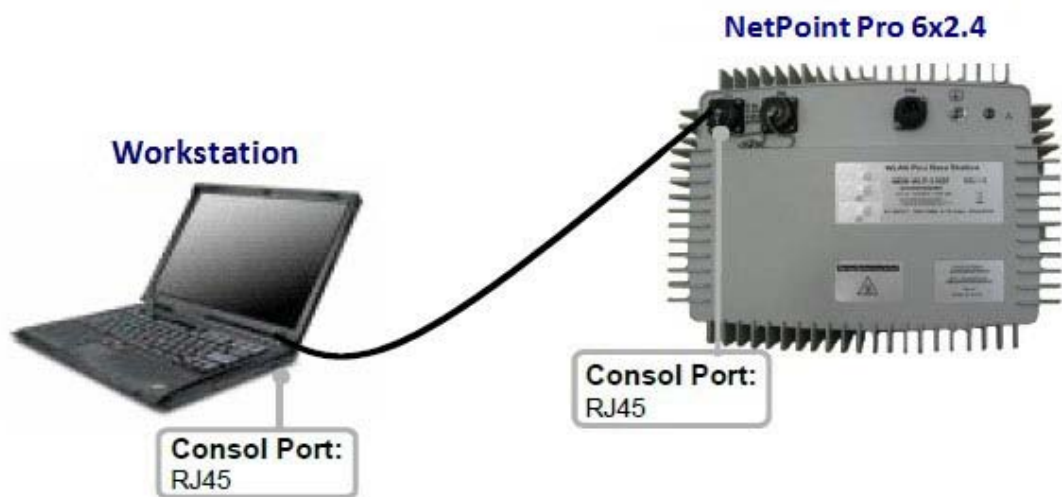


Figure 2: Connect and Access the NetPoint Pro 6x2.4

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

➤ To log into the unit:

1. Open the web browser and enter the unit's IP address in the browser URL line.
2. Once connected to the unit, a window opens requesting a User name and Password



Figure 3: Internet Explorer



Figure 4: Mozilla Firefox

3. Type the User name and Password. The default values are as follows:

- User name: super
- Password: super

4. Once authentication has been verified, the initial configuration window opens.

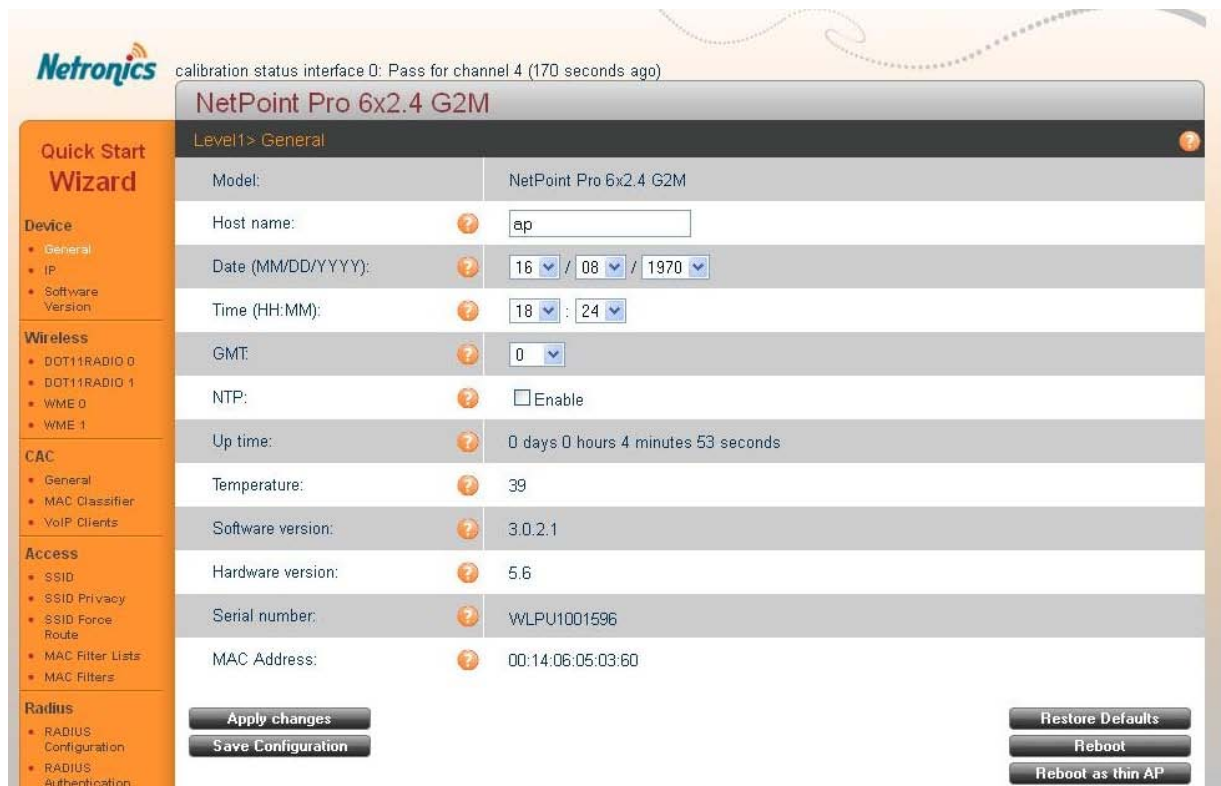


Figure 5: Initial Web Interface Window

Web Interface

The configuration web interface contains the following two main panels:

- Configuration Categories
- Configuration Details

Each category has several associated configuration sub-category configurations. Click on a category to open the available sub-categories. The available categories are as follows:

- Device
- Wireless
- CAC
- Access
- Radius
- Mesh
- Statistics

Initial Web Interface Information

| Level1 > General | |
|--------------------|-------------------------------------|
| Model: | NetPoint Pro 6x2.4 G2M |
| Host name: | <input type="text" value="ap"/> |
| Date (MM/DD/YYYY): | 16 / 08 / 1970 |
| Time (HH:MM): | 18 : 24 |
| GMT: | 0 |
| NTP: | <input type="checkbox"/> Enable |
| Up time: | 0 days 0 hours 4 minutes 53 seconds |
| Temperature: | 39 |
| Software version: | 3.0.2.1 |
| Hardware version: | 5.6 |
| Serial number: | WLPU1001596 |

Figure 6: 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. |

Note: 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.

The screenshot shows the 'Device > IP' configuration page. It features a table of configuration fields, each with a help icon (question mark in a circle) to its left. The fields are: Configuration Type (set to DHCP), IP Address (172.16.1.114), Net Mask (255.255.255.0), Management VLAN (0), and Default Gateway (172.16.1.1). Below the table are two buttons: 'Apply changes' and 'Save Configuration'.

| Field | Value |
|---------------------|---------------|
| Configuration Type: | DHCP |
| IP Address: | 172.16.1.114 |
| Net Mask: | 255.255.255.0 |
| Management VLAN: | 0 |
| Default Gateway: | 172.16.1.1 |

Buttons: Apply changes, Save Configuration

Figure 7: 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 |

Warning: 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 for safety. In the event that there is an issue with an upgrade, the previous version can always be reloaded.



Figure 8: Software Version Screen

The Software Version screen contains the following information:

- Protocol** Import the image using the selected protocol
- Address** The IP address where the file is stored
- File Name** The name of the new file on the remote server

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
- Beacon
- Service Optimization
- Advanced Configuration
- Wireless Multimedia Enhancements (WME)

Dot11Radio Setup

All of the radio interfaces are Wi-Fi, with the exception of the last one, which is the mesh interface.

| NetPoint Pro 6x2.4 G2M | | |
|------------------------|---|---|
| Level1> DOT11RADIO 0 | | |
| Radio index: |  | 0 |
| Type: |  | XRF |
| Status: |  | Up  |
| Mode: |  | mixed  |
| Channel: |  | 1  |
| Beacon Period (msec): |  | <input type="text" value="100"/> |
| Beacon Rate: |  | 1  |
| TX Power Attenuation: |  | <input type="text" value="0"/> |
| DTIM Period: |  | <input type="text" value="1"/> |
| RTS threshold (Bytes): |  | <input type="text" value="2346"/> |
| Min Rate: |  | none  |

| | | |
|--------------------------|---|----------|
| Max Rate: |  | disabled |
| Fixed Rate: |  | auto |
| Service: |  | Access |
| Distance (meters): |  | 300 |
| Max Associated Stations: |  | 250 |
| Auto Sensitivity: |  | auto |
| Manual Sensitivity: |  | -77 |
| ERP Mode: |  | Enable |
| Preamble Mode: |  | long |

Attach SSIDs to Interface 0

| SSID name | Active |
|-----------|-------------------------------------|
| AP | <input checked="" type="checkbox"/> |
| mgt | <input type="checkbox"/> |

Figure 9: Radio Interface Screen

The Radio Interface screen contains the following information:

| | |
|--------------------|--|
| Radio Index | Radio interface number. All of the interfaces are used for 2.4 GHz communication, with the exception of the last one, which is used for 5GHz communication. |
| Type | The Wi-Fi Protocol xRF, is the Netronics standard with beam-forming technology. MiniPC is a standard RF interface. |
| 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 / 802.11b / 802.11g / 802.11bg |
| Channel | Configures the Wi-Fi channel used on the specified radio interface. The actual frequencies available are dependent on the radio interface (802.11a or 802.11b/g), and the region for which the unit was manufactured. |

Beacon

Beacons are used to carry network parameters such as SSID and supported rates.

| NetPoint Pro 6x2.4 G2M | | |
|------------------------|---|-------|
| Level 1 > DOT11RADIO 0 | | |
| Radio index: | ? | 0 |
| Type: | ? | XRF |
| Status: | ? | Up |
| Mode: | ? | mixed |
| Channel: | ? | 1 |
| Beacon Period (msec): | ? | 100 |
| Beacon Rate: | ? | 1 |
| TX Power Attenuation: | ? | 0 |
| DTIM Period: | ? | 1 |
| RTS threshold (Bytes): | ? | 2346 |
| Min Rate: | ? | none |

Figure 10: Beacon

The Beacon parameters contain the following information:

| | |
|----------------------|--|
| Beacon Period | Configures the time period (in msec) between beacon transmissions |
| Beacon Rate | Configures the transmitted beacon rate for the specified radio interface |
| DTIM Period | Configures how frequently the DTIM (Delivery Traffic Indication Message) polls the client in power saving mode if data is waiting to be sent. Each beacon contains a DTIM. The DTIM period defines the number of beacons that are broadcast between sent data packets. For example, if the DTIM period is set to 4, then every fourth beacon contains a DTIM, informing the client that there is data waiting. |

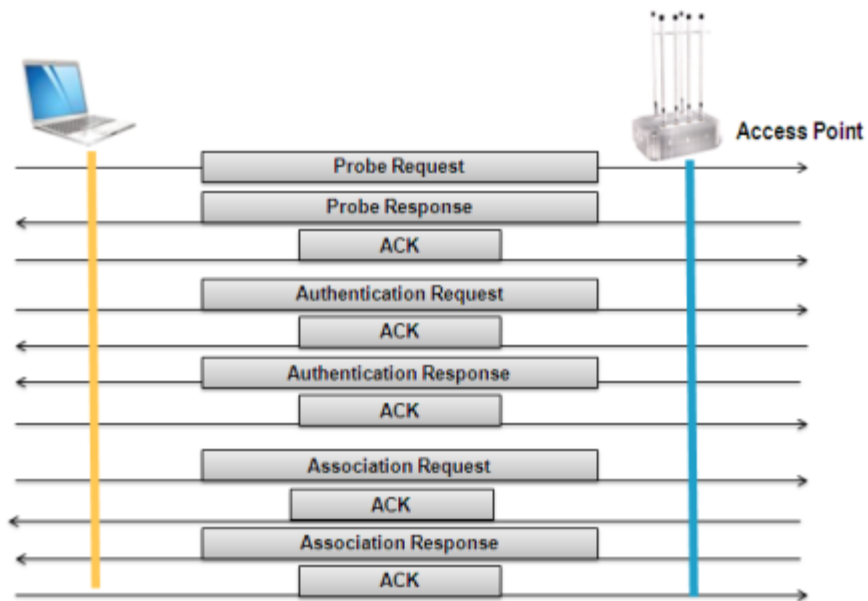


Figure 11: Beacon Association Process

Service Optimization

| Wireless > DOT11RADIO 0 | | |
|--------------------------|--|---------------------------------------|
| TX Power Attenuation: | | <input type="text" value="0"/> |
| DTIM Period: | | <input type="text" value="1"/> |
| RTS threshold (Bytes): | | <input type="text" value="2346"/> |
| Min Rate: | | <input type="text" value="none"/> |
| Max Rate: | | <input type="text" value="disabled"/> |
| Fixed Rate: | | <input type="text" value="auto"/> |
| Service: | | <input type="text" value="Access"/> |
| Distance (meters): | | <input type="text" value="300"/> |
| Max Associated Stations: | | <input type="text" value="250"/> |
| Auto Sensitivity: | | <input type="text" value="manual"/> |
| Manual Sensitivity: | | <input type="text" value="-77"/> |

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.

Max Rate

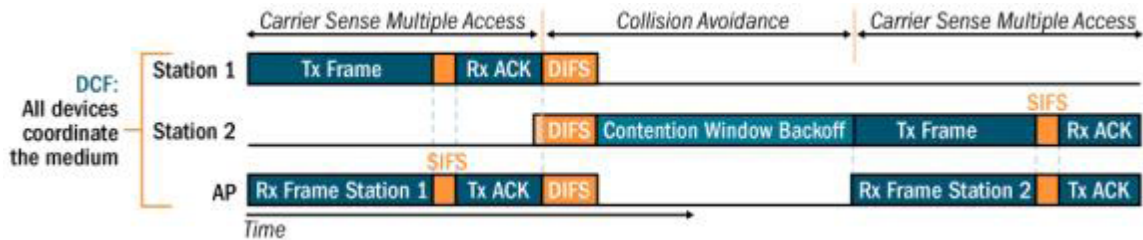
Configures the transmitted beacon rate for the specified radio interface

| Spreading Method | DSSS | | CCK | | OFDM | | | | | | | | |
|------------------|-------|-------|-------|----|------|---|------|----|--------|----|--------|----|--------|
| | DBPSK | DQPSK | DQPSK | | BPSK | | QPSK | | 16-QAM | | 64-QAM | | |
| Data Rate (Mbps) | 1 | 2 | 5.5 | 11 | 6 | 9 | 12 | 18 | 24 | 36 | 48 | 54 | |
| 802.11a | | | | | • | • | • | • | • | • | • | • | 5GHz |
| 802.11b | • | • | • | • | | | | | | | | | 2.4GHz |
| 802.11g | • | • | • | • | • | • | • | • | • | • | • | • | |

Figure 12 802.11 a/b/g Supported Rates

Distance

Defines the distance (in meters) between the gateway and the node units for the 802.11a backhaul radio interface. For 802.11b/g 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

































| NetPoint Pro 6x2.4 G2M | | |
|--------------------------|---|---|
| Level1> DOT11RADIO 0 | | |
| Radio index: |  | 0 |
| Type: |  | XRF |
| Status: |  | Up  |
| Mode: |  | mixed  |
| Channel: |  | 1  |
| Beacon Period (msec): |  | 100 |
| Beacon Rate: |  | 1  |
| TX Power Attenuation: |  | 0 |
| DTIM Period: |  | 1 |
| RTS threshold (Bytes): |  | 2346 |
| Min Rate: |  | none  |
| Max Rate: |  | disabled  |
| Fixed Rate: |  | auto  |
| Service: |  | Access  |
| Distance (meters): |  | 300 |
| Max Associated Stations: |  | 250 |
| Auto Sensitivity: |  | auto  |
| Manual Sensitivity: |  | -77  |
| ERP Mode: |  | Enable  |
| Preamble Mode: |  | long  |

Figure 12: Advanced Screen

The Advanced parameters contain the following information:

RTS Threshold Configures the RTS threshold packet size (in bytes). Packets larger than the RTS threshold will be transmitted using RTS.



RTS/CTS is used in order solve the hidden stations phenomenon in the CSMA / CA protocol. The downside of this protocol is that it reduces the bandwidth up to 70%.

Min Rate Configures the minimum transmission rate on the specified interface.

TIP

Minimum rate is used to ensure a minimum quality of service (in download). Decreases the radius and maintain high SNR. This is used mainly for VoIP networks with weak RF cards.

Fixed Rate

Configures the fixed transmission rate on the specified interface.

TIP

For fixed wireless transmission in an environment with a high amount of RF activity, it is recommended to use fixed transmission rates

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.

TIP

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

Preamble Mode

A short preamble improves the throughput performance; all 802.11b devices must support the long preamble format, but may optionally support the short preamble

**Caution**

The problem occurs when an 802.11g AP allows the use of short preamble by the stations it communicates with (also known as its BSS - Basic Service Set). The AP may also choose to allow legacy stations that do not support short preamble to associate with the BSS. If both these conditions are allowed, the legacy stations that are not short--preamble-capable will not be able to understand much of the communication in the BSS, and most importantly will not be able to receive the all-important "Protection" frames. This can result in legacy 11b stations transmitting at the same time as 11g stations, which may block both from properly sending their data.

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 print 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). For 802.11b and 802.11g the SIFS is 10 microseconds. Minimum TXOP duration is the sum of SIFS and AIFS.
- 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. For 802.11b a time slot is 20 microseconds and for 802.11g a time slot is 9 microseconds. Minimum TXOP duration is the sum of SIFS and AIFS.
- 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"/> |

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

TIP

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. |

CAC – Call Admission Control

The Call Admission Control feature is used to prevent oversubscription in the real-time media network. The feature operates by identifying the Class of Service (CoS) or by identifying the originating voice-sending device based on the MAC prefix.

This section contains the following topics:

- General CAC Setup
- MAC Classifiers
- VoIP Clients

General CAC Setup

| CAC > General | |
|-------------------------|---------|
| Enable CAC ? | false ▾ |
| Minimum VC SNR ? | 12 |
| Maximum VCs ? | 32 |
| Algorithm ? | VA1 ▾ |
| VC Ban Time (seconds) ? | 30 |

Figure 13: CAC General screen

The CAC General parameters contain the following fields

Enable CAC Enables the Call Admission Control Feature. This should be used in the event that the application does not mark the CoS bit. The CAC will identify a voice-sending device using its MAC prefix.

Minimum VC SNR Configures the CAC minimum voice call SNR threshold. For

example: if the noise level is -89 and SNR is 12, only clients with RSSI of -77 are allowed to run voice call. This guarantees a standard service level for VoIP calls.

Maximum VCs Algorithm

The maximum number of concurrent VoIP calls
Currently, only VA1 is supported

VC BAN Time (seconds)

The amount of time (in seconds) that a station is suspended, and not allowed to access the interface. This occurs when a station attempts to associate with more than the maximum number of clients.

MAC Classifier

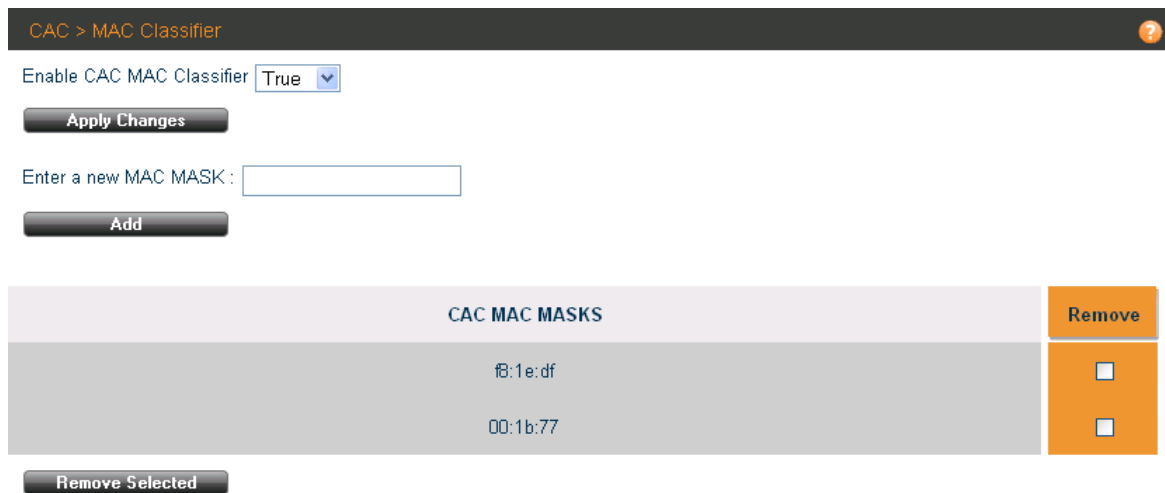


Figure 14: MAC Classifier screen

The CAC MAC Classifier parameters contain the following fields:

Enable CAC MAC Classifier

Select True to enable the CAC MAC Classifiers, or False to disable them.

Enter new MAC Mask

Enter the phone prefix for the phone vendor. Additional information regarding MAC address prefix can be found at: [http://standards .ieee.org/regauth/oui/oui.txt](http://standards.ieee.org/regauth/oui/oui.txt)

VoIP Clients

| CAC > VoIP Clients | | | | | |
|--------------------|-------|----------|-------------------|--------|----------------|
| Index | SNR ? | Active ? | MAC Address ? | RSSI ? | Session Time ? |
| 1 | 47 | FALSE | 00:1b:77:6f:07:ed | -50 | 47 |

| CAC > VoIP Clients | | | | | |
|--------------------|-------|----------|-------------------|--------|----------------|
| Index | SNR ? | Active ? | MAC Address ? | RSSI ? | Session Time ? |
| 1 | 47 | TRUE | 00:1b:77:6f:07:ed | -50 | 368 |

Figure 15: VoIP Clients

The VoIP Clients screen contains the following fields:

| | |
|--------------------|---|
| Index | The VoIP client index (Up to the maximum number of permitted VoIP calls). |
| SNR | Signal to Noise Ratio |
| Active | There are two states for this field: <ul style="list-style-type: none"> • True – The associated client does not have any active VoIP calls • False – The associated client has an active VoIP call. |
| MAC Address | The client MAC Address. |
| RSSI | The Receiver Signal Strength Indicator. Noise Level = RSSI + SNR |

Chapter 6

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
- MAC Filter List
- MAC Filters

SSID Configuration

Access > SSID

Add a new SSID :

| Index | Name ? | Privacy ? | Vlan ? | Type ? | MAC Filter List |
|-------|----------------------|-----------|--------|--------|-----------------|
| 2 | <input type="text"/> | NONE | 0 | BSSID | none |

Add

Manage SSIDs :

| Index | Name ? | Privacy ? | Vlan ? | Type ? | MAC Filter List | Remove |
|-------|--------|-----------|--------|--------|-----------------|--------------------------|
| 1 | 1100 | NONE | 0 | BSSID | none | <input type="checkbox"/> |
| 4 | mgt | WPA | 5 | HIDDEN | none | <input type="checkbox"/> |

Apply changes

Save Configuration

Figure 16: SSID Configuration screen

The SSID Configuration screen contains the following fields

| | |
|----------------|---|
| Index | The SSID Index. There is a maximum of up to 14 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. |
| MAC Filter List | Activate MAC filtering on the specific SSID |
| Remove | Deletes the SSD from the configuration. |

SSID Privacy

Access > SSID Privacy

| Index | Name | Privacy | Click to Expand |
|-----------------------|----------|--|-------------------|
| 1 | 1100 | off | |
| 2 | WEP_SSID | wep | ↑ |
| Key Type | | Key value [Hex] | |
| 40 | | 11:22:33:44:55 ✓ | |
| 104 | | 11:22:33:44:55:66:77:88:99:10:11:12:13 ✓ | |
| 40 | | 00:00:00:00:00 ✓ | |
| 40 | | 00:00:00:00:00 | |
| 3 | WPA_SSID | wpa | ↑ |
| Key Management | | Protocol | Passphrase |
| PSK | | WPA2 | 00000000 ✓ |
| | | Data Encryption | |
| | | TKIP | |
| 4 | mgt | wpa | ↑ |
| Key Management | | Protocol | Passphrase |
| EAP | | WPA2 | 12345678 |
| | | Data Encryption | |
| | | AES | |

Apply Changes
Save Configuration

Figure 17: SSID Privacy screen

The SSID Privacy screen contains the following fields:

| | |
|------------------------|--|
| Index | The SSID Privacy Index. There is a maximum of up to 14 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">• TKIP – Temporary Key Integrity Protocol• AEL – Advanced Encryption Standard (AES/CCMP) |

MAC Filter List

Access > MAC Filter Lists

Add MAC Filter list :

| Index | Name | Type |
|-------|----------------------|-------|
| 3 | <input type="text"/> | white |

Add

Manage MAC Filter lists :

| Index | Name | Type | Remove |
|-------|---------|-----------|--------------------------|
| 1 | Allowed | whiteList | <input type="checkbox"/> |
| 2 | Blocked | blackList | <input type="checkbox"/> |

Apply changes

Save Configuration

Figure 18: MAC Filter List screen

The MAC Filter List screen contains the following fields

| | |
|--------------|--|
| Index | MAC Filter index number |
| Name | MAC Filter list name |
| Type | Block or allow specific MAC addresses. The options are: White List – Only permit specified MAC Addresses to connect Black List – Do not permit specified MAC addresses to connect. |



TIP

A white list is used in deployments of fixed wireless installations for WISP, municipal Wi-Fi, safe city, etc.

MAC Filters

Access > MAC Filters

Add MAC Filter address:

| MAC Address | List Name |
|--|--|
| <input type="text" value="00:14:06:85:3B:FF"/>  | <input type="text" value="Blocked"/>  |

Manage MAC Filter addresses :

| MAC Address | List Index | List Name | Remove |
|-------------------|------------|-----------|---------------------------------------|
| 00:14:06:5a:85:9f | 2 | Blocked | <input type="button" value="Remove"/> |

Figure 19: MAC Filters screen

The MAC Filters screen contains the following fields

- | | |
|--------------------|---|
| MAC Address | The MAC address of the device |
| List Name | The list name to associate with that MAC address. |

Chapter 7

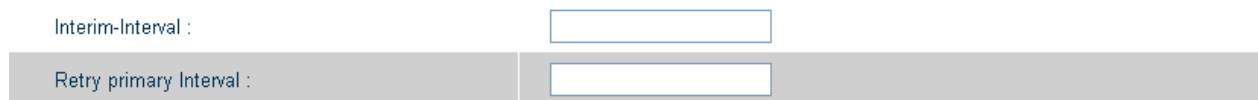
Radius

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



The screenshot shows a configuration interface with two rows. The first row has the label 'Interim-Interval :' on the left and an empty rectangular input box on the right. The second row has the label 'Retry primary Interval :' on the left and another empty rectangular input box on the right. The background of the input area is light gray.

Figure20: Radius Configuration screen

The Radius Configuration screen contains the following fields

| | |
|-------------------------------|--|
| Interim Interval | Defines the frequency that the unit sends accounting updates to the Radius server (the default value is 600 seconds). |
| 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). |

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.

Add a new RADIUS Authentication entry :

| SSID | Priority | Host | Key | Port |
|----------------------|----------|----------------------|----------------------|------|
| <input type="text"/> | 1 | <input type="text"/> | <input type="text"/> | 1812 |

Manage RADIUS Authentication :

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

Add a new RADIUS Accounting entry:

| SSID | Priority | Host | Key | Port |
|--------|----------|----------------------|----------------------|------|
| test4u | 1 | <input type="text"/> | <input type="text"/> | 1813 |

Manage RADIUS Accounting :

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

Figure 21: 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 8

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.

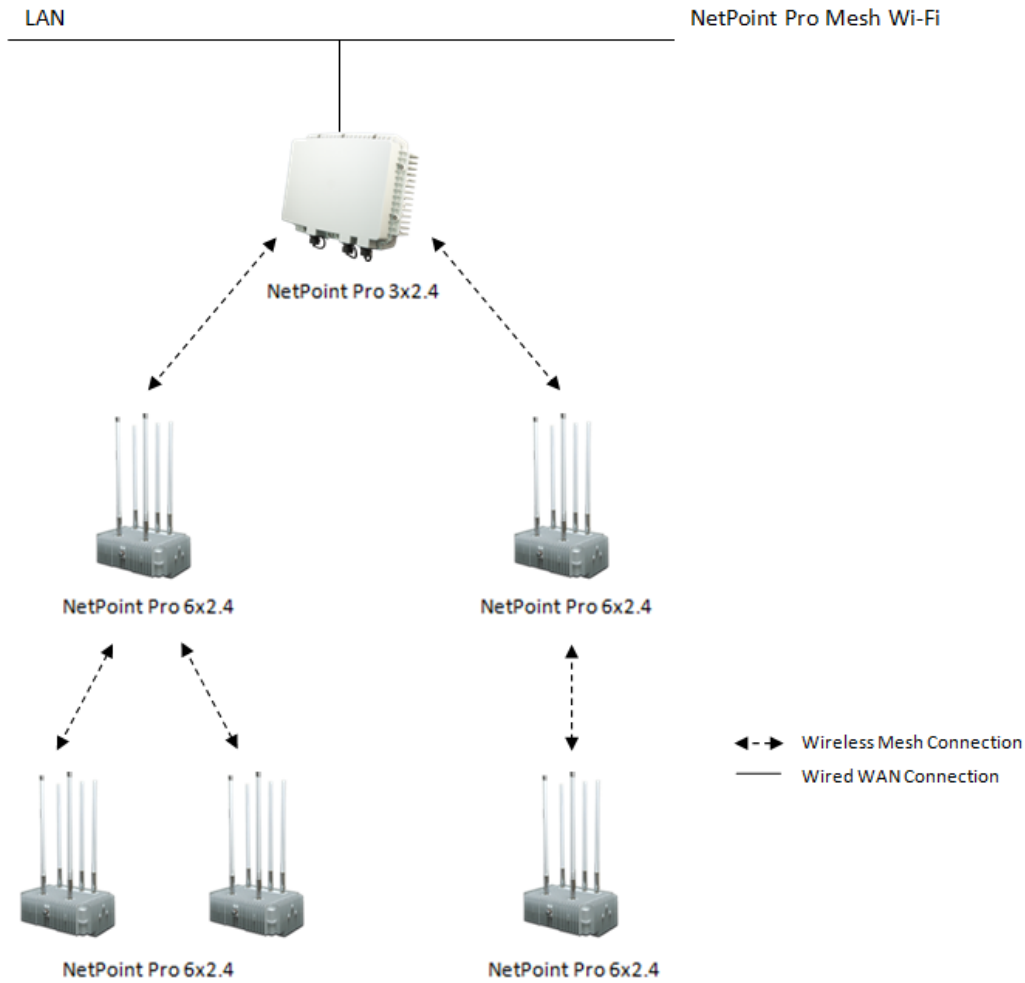


Figure 22: Typical NetPoint Pro Mesh Cluster

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="12344321"/> |
| Unit Mode: |  | <input type="text" value="gateway"/> |
| Connectivity test mode: |  | <input type="text" value="disabled"/> |
| Connection status to the net: |  | normal |
| Connectivity test target host: |  | <input type="text" value="none"/> |
| Advertising Status: |  | <input type="text" value="enabled"/> |
| Trunk: |  | <input type="text" value="disabled"/> |
| Gateway MAC Address: |  | 00:14:06:41:d3:c0 |
| MESH Stand Alone: |  | <input type="text" value="enabled"/> |
| MESH Stand Alone Status: |  | |
| MESH Stand Alone Passphrase: |  | <input type="text" value="00000000"/> |
| SECURITY : <input type="text" value="none"/> | | |

The Mesh General screen contains the following fields:

| | |
|---------------------------------------|--|
| Network ID | Defines the mesh network id associated with the unit. All units in a single mesh network have the same specified network id. A string value that defines the name of the mesh network. The value is case sensitive and can be from 8 to 16 characters. |
| Unit Mode | Configures the gateway as either a Node or a Mesh. |
| 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 status to the net | Display the connectivity status. |
| Connectivity Test Target Host | Specify the target IP address or Host name. The name can be up to 64 characters. |
| Advertising Status | Configures advertising this unit as a candidate for the next hop in the mesh network. It defines whether the unit that 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. |
| 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 |
| Security | Mesh Security - WEP (40 or 104 bit) or AES (128 bit) |

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 |

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:

| | |
|----------------------|--|
| <input type="text"/> | Deny <input type="button" value="v"/> |
|----------------------|--|

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"/> |

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. |

Static Links

Static links are available only in WDS mode and are relevant only on the access channel.

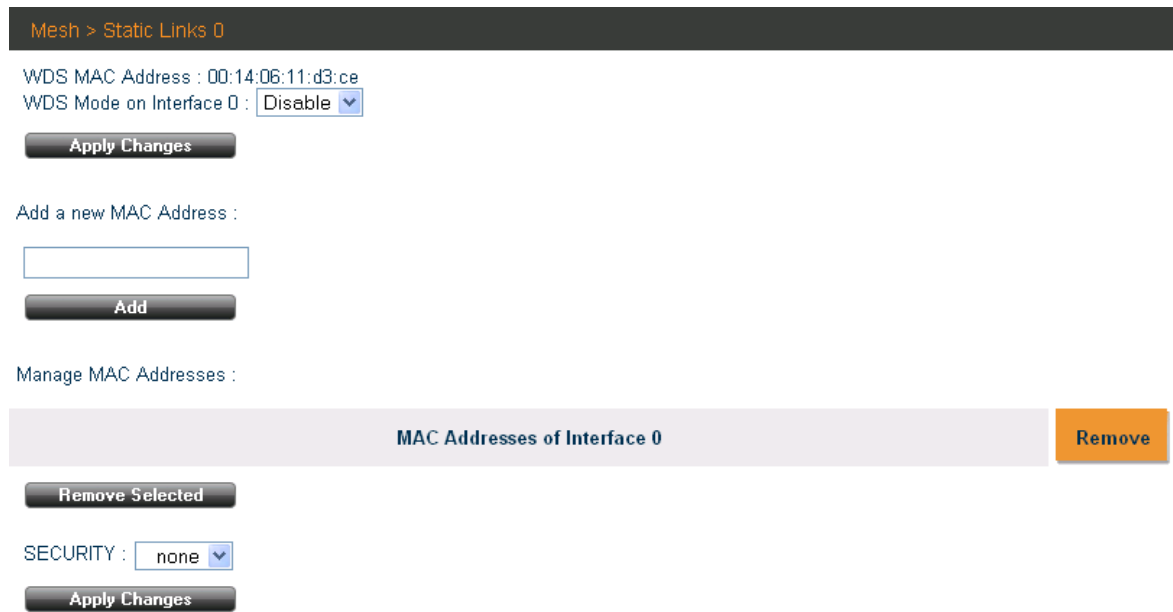


Figure 23: Static Links screen

The Static Links screen contains the following fields:

| | |
|--------------------------------|------------------------------------|
| WDS Mode on Interface 0 | Enables WDS mode. |
| Add a new MAC Address | Adds a WDS device’s MAC addresses. |
| Manage MAC Addresses | Manages WDS peer lists |
| Security | Select either none, WEP or AES |

Chapter 9

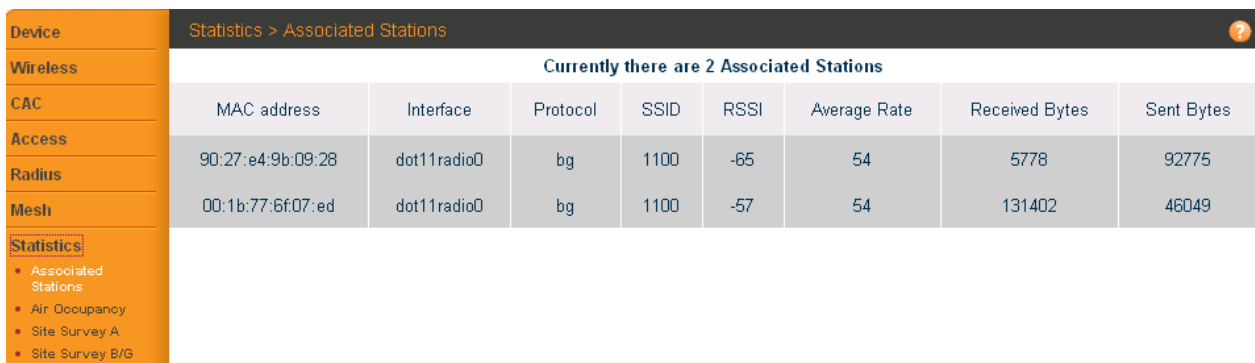
Statistics

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

This section contains the following topics:

- Show Associated Stations
- Air Occupancy
- Choosing the Best Channel – Site Survey

Show Associated Stations



| Device | | Statistics > Associated Stations | | | | | | |
|----------|-------------------|---|----------|------|------|--------------|----------------|------------|
| Wireless | | Currently there are 2 Associated Stations | | | | | | |
| CAC | MAC address | Interface | Protocol | SSID | RSSI | Average Rate | Received Bytes | Sent Bytes |
| Access | 90:27:e4:9b:09:28 | dot11radio0 | bg | 1100 | -65 | 54 | 5778 | 92775 |
| Radius | 00:1b:77:6f:07:ed | dot11radio0 | bg | 1100 | -57 | 54 | 131402 | 46049 |
| Mesh | | | | | | | | |

Statistics

- Associated Stations
- Air Occupancy
- Site Survey A
- Site Survey B/G

Figure 24: Associated Stations screen

The Associated Stations screen contains the following fields

| | |
|-----------------------|---|
| MAC Address | The client MAC Address. |
| Interface | The unit physical address associated with the client. |
| Protocol | The appropriate Wi-Fi protocol |
| SSID | The SSID associated with the client. |
| 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. |

Air Occupancy

The air utilization status

| Device | Statistics > Air Occupancy | | | | | |
|--|----------------------------|----------------|----------------|-------------------|-------------------|-------------|
| Wireless | Interface | TX Frame Ratio | RX Frame Ratio | Clear Count Ratio | Sensitivity Level | Noise Level |
| CAC | 0 | 5 | 7 | 13 | auto | -101 |
| Access | 1 | 0 | 0 | 0 | auto | -93 |
| Radius | | | | | | |
| Mesh | | | | | | |
| Statistics | | | | | | |
| <ul style="list-style-type: none"> Associated Stations Air Occupancy Site Survey A Site Survey B/G | | | | | | |

Figure 25: Air Occupancy screen

The Air Occupancy screen contains the following fields:

| | |
|--------------------------|---|
| Interface | The physical radio interface. |
| Tx Frame Ratio | Displays the Wi-Fi load associated with transmitted frames as a percentage of the maximum air occupancy. |
| Rx Frame Ratio | Displays the Wi-Fi load associated with valid received frames as a percentage of the maximum air occupancy. |
| Clear Count Ratio | Displays the current Wi-Fi load as a percentage of the maximum air occupancy. Clear count load is the summation of the loads due to RX Frames, TX Frames and noise. |
| Sensitivity Level | Displays the current interface sensitivity level. |
| Noise Level | Configures the noise floor level in dBm for the specified radio interface. |

Choosing the Best Channel – 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 sensitivity and utilization.

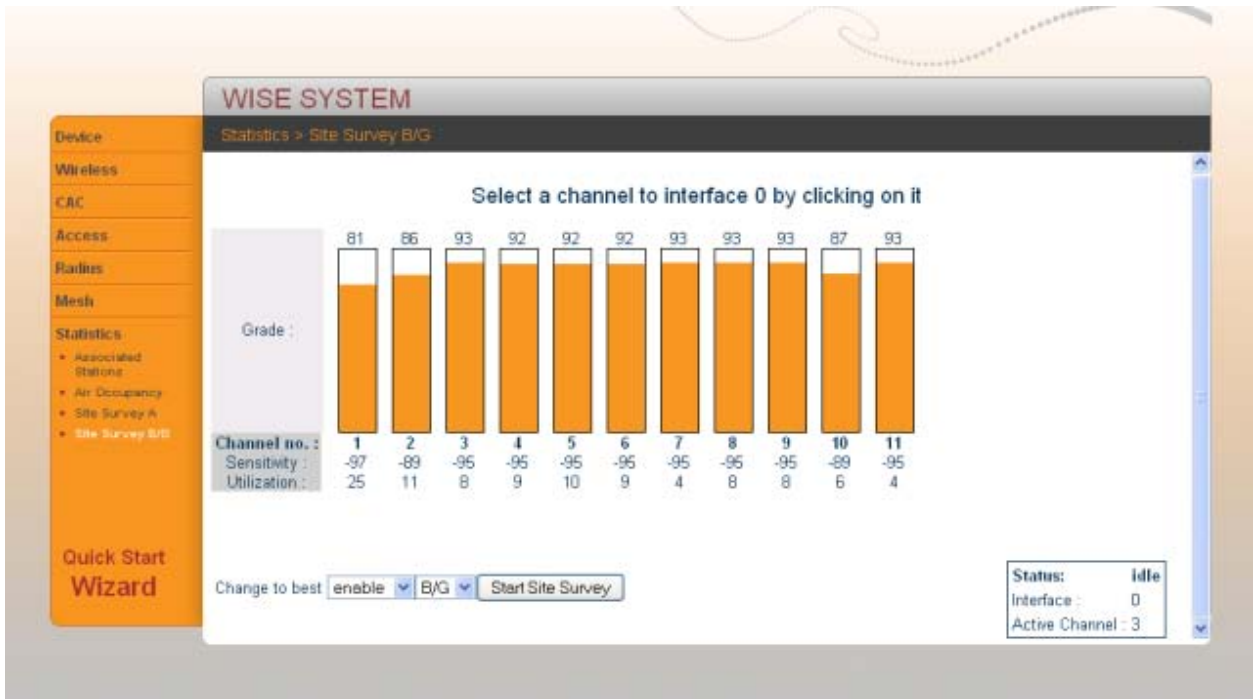


Figure 26: Site Survey screen

The Site Survey screen contains the following fields

Sensitivity

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 -88dBm. It cannot associate with a client whose sensitivity is -90 dBm.

Utilization

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 22MHz and the channel separation is 5MHz, 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.

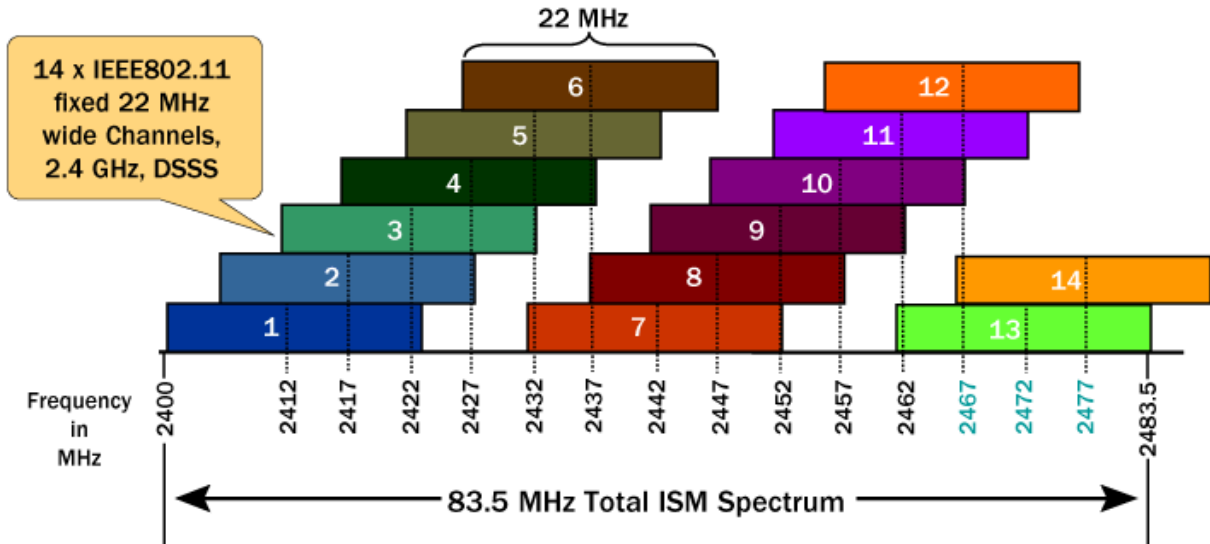


Figure 27: Channel Separation



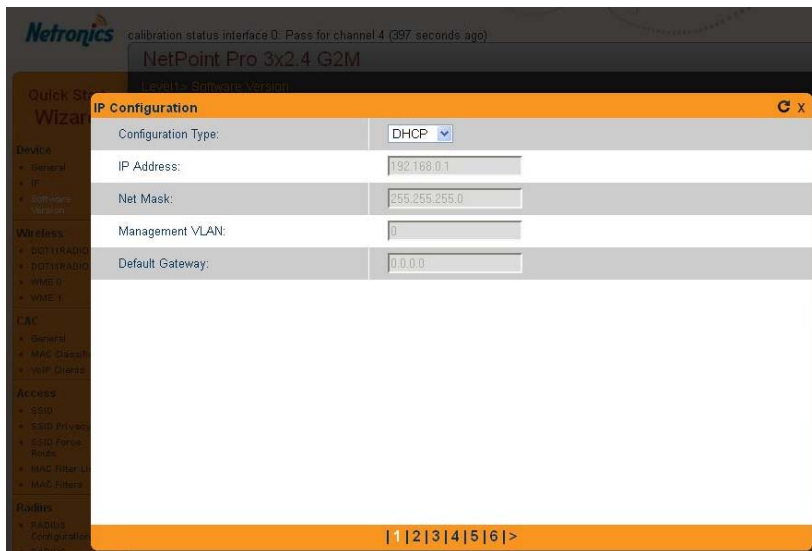
Don't forget you need 5 channels separation between radio interface 0 and radio interface 1 on the NetPoint Pro 3x2.4.

Chapter 10

Wizard

The Wizard allows you to configure the unit and begin working within two minutes.

Step 1 – IP Configuration

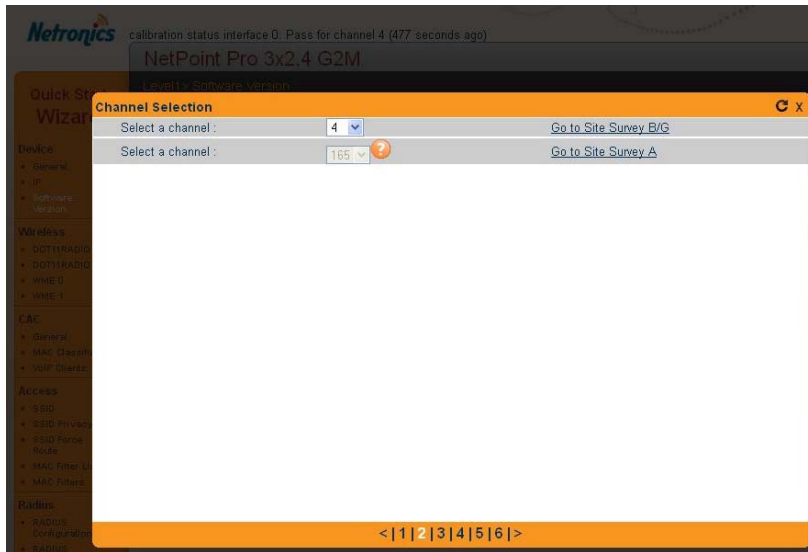


The screenshot shows the Netronics NetPoint Pro 3x2.4 G2M configuration wizard. The main window is titled "IP Configuration" and contains the following fields:

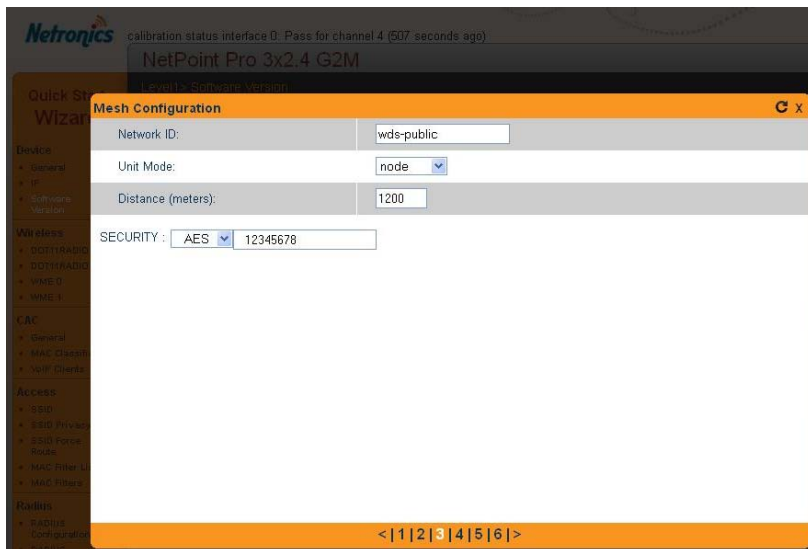
| Field | Value |
|---------------------|---------------|
| Configuration Type: | DHCP |
| IP Address: | 192.168.0.1 |
| Net Mask: | 255.255.255.0 |
| Management VLAN: | 0 |
| Default Gateway: | 0.0.0.0 |

The wizard is currently on step 1 of 6, as indicated by the progress indicator at the bottom: | 1 | 2 | 3 | 4 | 5 | 6 | >

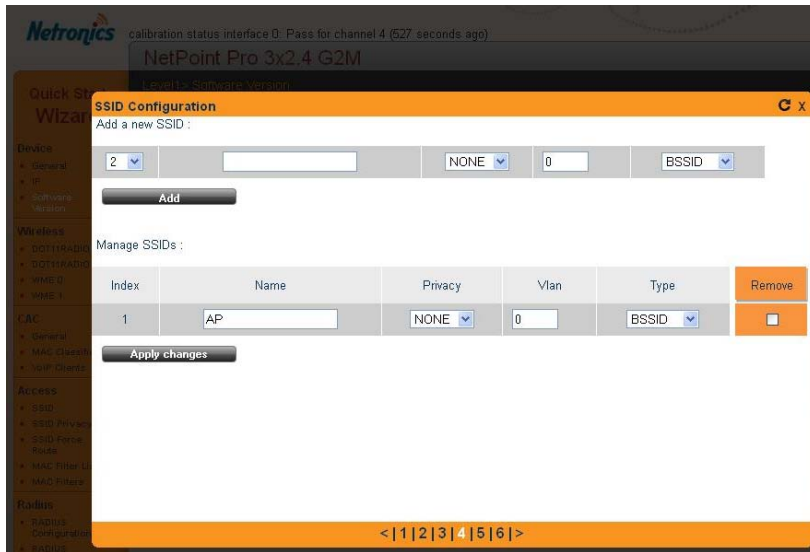
Step 2 – Channel Selection



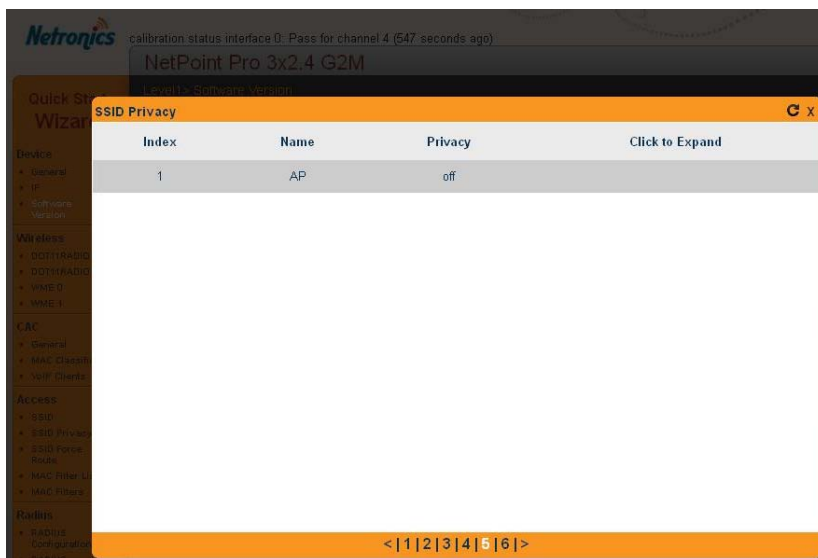
Step 3 – Mesh setup



Step 4 – Access channel (SSID's)



Step 5 – Security / Privacy



Step 6 – Attach SSID to radio interface



Chapter 11

Typical Scenarios

This section describes some common scenarios that are performed on the devices.

Basic Setup

Configure the following parameters:

- Host name
- Date
- NTP

Configure the Wi-Fi access channel

1. Go to the Access tab and configure the SSID.

The screenshot shows the configuration interface for SSIDs. On the left is a navigation menu with categories: Device, Wireless, CAC, Access (with sub-items: SSID, SSID Privacy, MAC Filter Lists, MAC Filters), Radius, Mesh, and Statistics. The main content area is titled 'Access > SSID' and contains two sections: 'Add a new SSID' and 'Manage SSIDs'.

Add a new SSID:

| Index | Name | Privacy | Vlan | Type | MAC Filter List |
|-------|------|---------|------|-------|-----------------|
| 2 | | NONE | 0 | BSSID | none |

Manage SSIDs:

| Index | Name | Privacy | Vlan | Type | MAC Filter List | Remove |
|-------|--------|---------|------|--------|-----------------|--------------------------|
| 1 | test4u | NONE | | HIDDEN | none | <input type="checkbox"/> |

- Go to the Wireless tab and configure the wireless parameters.

Wireless > DOT11RADIO 0

| | |
|------------------------|-------|
| Radio index: | 0 |
| Type: | XRF |
| Status: | Up |
| Mode: | mixed |
| Channel: | 3 |
| Beacon Period (msec): | 250 |
| Beacon Rate: | 1 |
| TX Power Attenuation: | 0 |
| DTIM Period: | 1 |
| RTS threshold (Bytes): | 2346 |
| Min Rate: | none |

- Choose the best available Wi-Fi channel.

WISE SYSTEM
Statistics > Site Survey B/G

Select a channel to interface 0 by clicking on it

| Grade | 81 | 86 | 93 | 92 | 92 | 92 | 93 | 93 | 93 | 87 | 93 |
|--------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| Channel no.: | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| Sensitivity: | -97 | -89 | -95 | -95 | -95 | -95 | -95 | -95 | -95 | -89 | -95 |
| Utilization: | 25 | 11 | 8 | 9 | 10 | 9 | 4 | 8 | 8 | 6 | 4 |

Change to best: enable B/G Start Site Survey

Status: idle
Interface: 0
Active Channel: 3

TIP

The physical installation is extremely important. You must mount the unit in a good location, in LOS to the coverage area, and select the best Wi-Fi channel.

Bad Installation



Good Installation



Software Upgrade

To upgrade the unit to a newer software version, you must first obtain the firmware from Netronics. Once you have the firmware, it should be placed in the TFTP directory.

The NetPoint Pro is a TFTP client. It connects to the TFTP server using a TFTP protocol. Make sure that the TFTP protocol uses the proper port to get through the firewall. Use UDP port 69.

1. Install a TFTP server on a PC.
2. Connect to the unit.
3. Run a software upgrade to the new version.
4. Reboot the unit.

Establish a Mesh Network

Mesh clusters have unique Mesh Network IDs. To create a Mesh cluster, it is essential that you perform a mesh design.

To establish a Mesh cluster, consider the following:

1. Maximum of 6 to 8 units in the mesh cluster.
2. Maximum 3 hops from the Gateway to the last node.
3. The distance for the OMNI mesh backhaul antenna is between 1000-2000 meters.
4. If possible, the mesh nodes should be placed in a manner that they are aware of each other.
5. Decide which one of the units is the gateway (connected to the backhaul)
6. Decide which ones of the nodes are not allowed to bridge for other nodes traffic, meaning that they will be the last nodes in the tree.

For example:



Chapter 12

Debug

Check the air Occupancy

The air occupancy is a very important parameter to estimate how much of the air is used. The Clear Count parameter show displays the percentage of the air occupancy.

The air occupancy is a critical parameter when estimating the performance on a specific channel. When the air occupancy is higher than 20%, the channel performance will deteriorate significantly due to multiple air collisions.

Monitor the number of associated stations

Monitoring the number of associated stations displays the current clients on the systems with their basic RF parameters.

Low rates consume more air time from other stations; a single station with low rate (modulation rate) can affect the entire MAC utilization of all the stations and reduce the overall performance of the network.

Chapter 13

Installation

Typical NetPoint Pro 6x2.4 Installation



Typical NetPoint Pro 3x2.4 Installation



Appendix A

List of Acronyms

| Acronym | Explanation |
|----------------|--|
| 802.11 | A family of specifications related to wireless networking, including: 802.11a, 802.11b, and 802.11g. |
| 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 |
| PMK | Pairwise Master Key |
| SSID | Service Set Identifier, a set of characters that give a unique name to a WLAN. |
| TKIP | Temporal Key Integrity Protocol |
| VLAN | Virtual Local Access Network |
| WDS | Wireless Distribution System |
| WEP | Wired Equivalent Privacy. An encryption system created to prevent eavesdropping on wireless network traffic. |

| | |
|---------|---|
| WMG | Wireless Media Gateway of the Netronics solution. |
| WNC | Wireless Network Controller of the Netronics 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 |

Appendix B

Wiring Specifications

| Console Port (DTE) | RJ-45-to-RJ-45 Straight Cable | | RJ-45 to DB-9 Terminal Adapter | Console Device |
|--------------------|-------------------------------|-----------|--------------------------------|----------------|
| | RJ-45 Pin | RJ-45 Pin | DB-9 Pin | |
| Signal | | | | Signal |
| No connection | 1 | 1 | 8 | CTS |
| No connection | 2 | 2 | 6 | DSR |
| No connection | 3 | 3 | 5 | GND |
| GND | 4 | 4 | 5 | GND |
| RxD | 5 | 5 | 3 | TxD |
| TxD | 6 | 6 | 2 | RxD |
| No connection | 7 | 7 | 4 | DTR |
| No connection | 8 | 8 | 7 | RTS |

Table 1: Console Port Signalling and Cabling with a DB-9 Adapter for the NetPoint Pro 6x2.4 Unit

Appendix C

Power Up and Software Configuration

The NetPoint Pro units are normally mounted on streetlights (poles or walls) where it is inconvenient to configure. Therefore, it is recommended that wireless communication be established to the unit prior to installation, so that the unit can later be configured and monitored remotely. To verify communications when installing the unit, the Mesh-Gateways must be installed and powered up first.

The LEDs on the unit indicate the status of communications between the unit and the network. See Table 5 for more information on the LED indicators.

The ACT LED on the Mesh-Gateway should be checked to verify that wired communications have been established. The BH LED on the Mesh-Gateway should be checked to verify that wireless communications have been established.

When powering up a Mesh-Node, the BH LED should be lit to verify that the unit's wireless communication is connected. The boot time is about 2.5 minutes. The BH LED indicator will light up after the boot is completed.

| LED | Function |
|------|---|
| PWR | Green – There is power to the unit. Unlit – There is no power to the unit. |
| STAT | Green – The operational status of the unit is normal. Red – The unit is in a failure state. Unlit – There is no power to the unit. |
| ACT | Green – When the LED is on, there is a communication connection. When the LED is flashing, traffic is flowing through the unit. Unlit – There is no communication connection. |
| BH | Green – On a Mesh-Gateway, the mesh functionality is activated. On a Mesh-Node, the unit is connected to the mesh. Unlit – On a Mesh-Gateway, the mesh functionality is not activated or no Ethernet link is available. On a Mesh-Node, the unit is not configured or failed to connect to the mesh. |

Table 2: LED Indicators