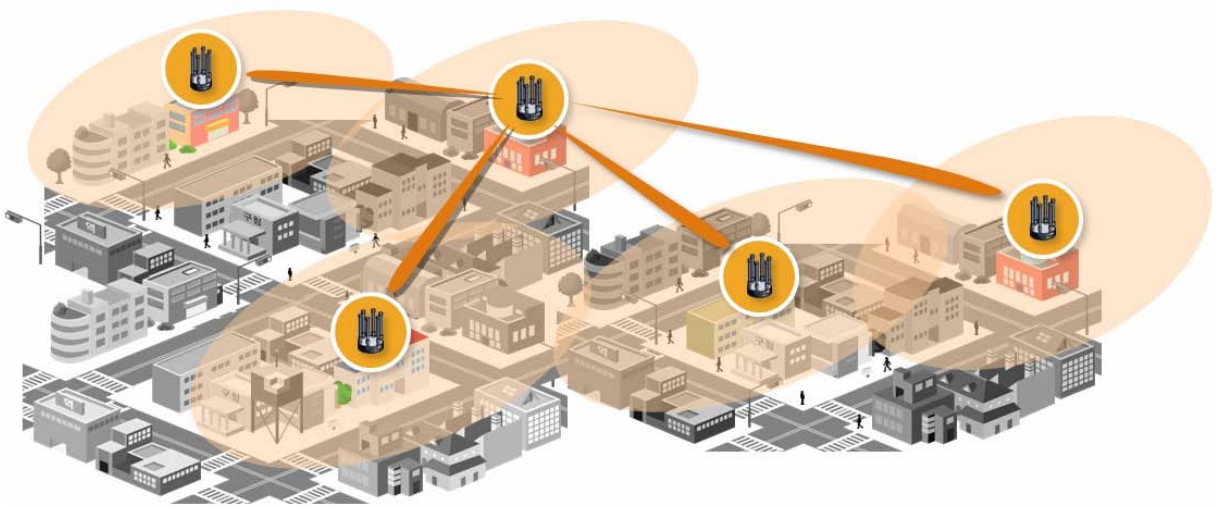
NetPoint Pro Family

Broadband Wireless Networking Solutions

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

CLI Configuration Guide



2nd Generation

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.

READ THIS FIRST!

Important Safety Instructions

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

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

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.

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.

This apparatus must be connected to earth ground.

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

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

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

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.

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.

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

Table of Contents

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
Implementing a Mesh Network	Describes the advance configuration procedures for implementing a Mesh network.
Implementing Client Access	Describes the advance configuration procedures for implementing client access.
Authentication Types	Describes the advance configuration procedures for authentication.
Upgrading the Software	Explains how to update the NetPoint Pro 3x2.4 and NetPoint Pro 6x2.4 software.
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.

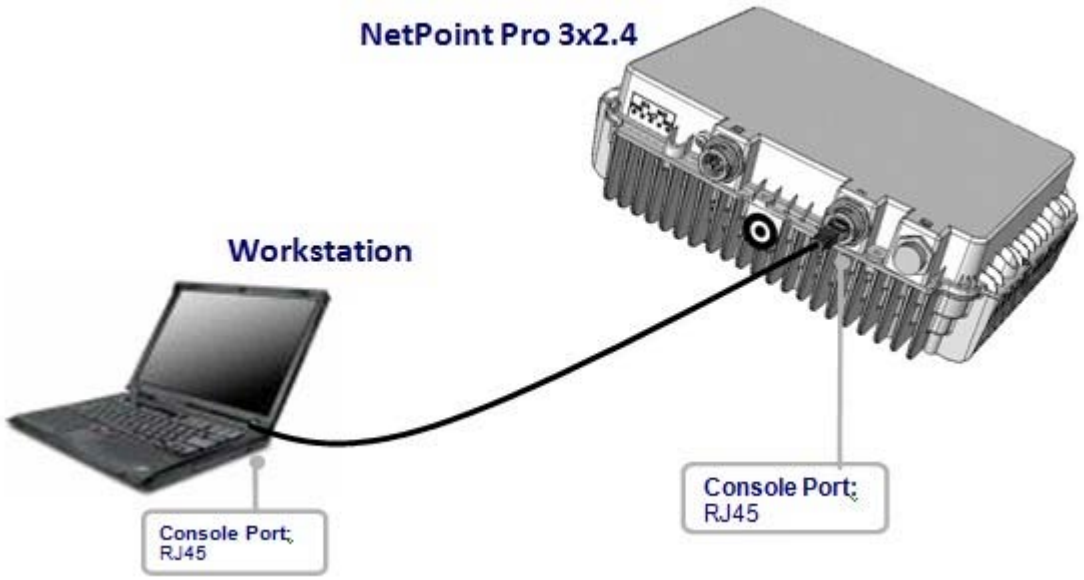


Figure 1: Connect and Access the NetPoint Pro 3x2.4

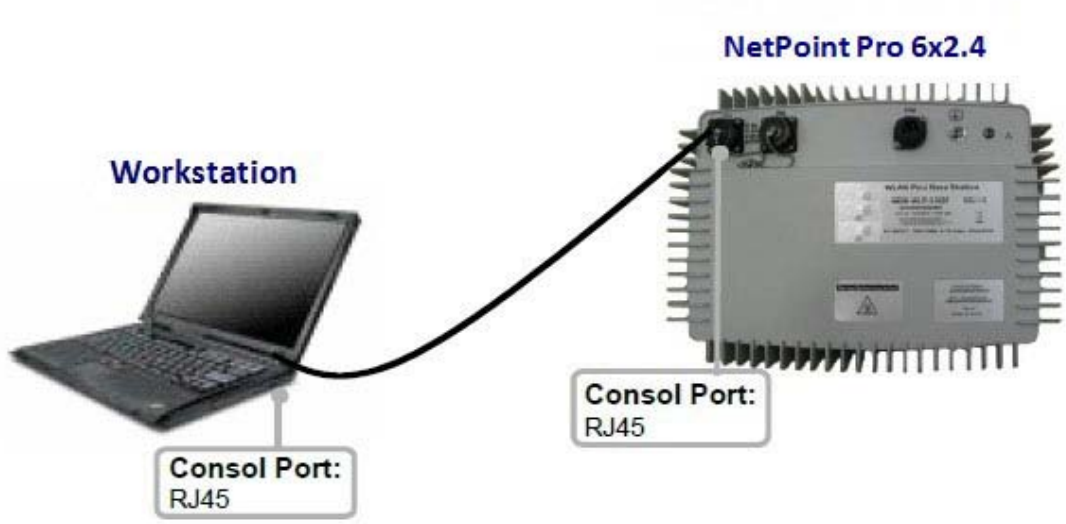


Figure 2: Connect and Access the NetPoint Pro 6x2.4

To communicate with the unit the IP address must be defined. 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 no VLAN tagging/ID in use 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 using Telnet.

Note: If the DHCP server is down, the IP address of the unit returns to the default value of 192.168.0.1 with no VLAN tagging. To connect to the unit the computer IP address must be set accordingly. (For example: IP address to 192.168.0.10 with a subnet mask of 255.255.255.0)

Once the IP address of the unit is determined, use the telnet to communicate with the unit.

- To use Telnet:

  From the Start menu:

  1. Select **All Programs > Accessories > Run**
  2. Type **Telnet <IP Address>**. Where <IP Address> is the IP address of the unit. (for example, Telnet 192,168.0.1)
  3. Click **OK**.

4. A Telnet window opens.
5. Log in using the predefined “super” user (user: super; password: super).

```
System: NetPoint Pro 6x2.4
SW Version: 3.0.1.2-39-PreRelease
User Name: super
Password:
--> User logged in successfully
ap>
```

The user name determines the authorization level and determines whether the operator can view configuration and operation parameters, or implement changes. A new user and password name should be added. However, the default name and password can be used for the initial configuration.

The default system prompt is set to **ap**.

Configuring the Management Connectivity

Configuring the management connectivity involves setting the device IP address, subnet mask, management VLAN and default gateway. These procedures are detailed in the following sections.

Assigning management IP and VLAN ID

Define the management IP address, subnet mask and the management VLAN on the same network through which you connect to the NetPoint Pro 3x2.4 and NetPoint Pro 6x2.4 unit. You can use the CLI command:

configure ip vlan {<vlan number> | none}
{<address ipaddress> [<mask ipaddress>] | dhcp}
[default gateway <gateway ipaddress>]

The default settings for the management connectivity are for the unit to obtain the IP address from a DHCP Server and there is no VLAN tagging.

Example:

To assign a management IP and VLAN, where:

Management IP Address = 192.168.30.102

Management IP Subnet Mask = 255.255.255.0

VLAN ID = 0 with no VLAN tagging
Default Gateway IP Address = 192.168.30.254

specify:

configure ip vlan none 192.168.30.102 255.255.255.0 default gateway 192.168.30.254

If the IP address is to be obtained from a DHCP server, the management IP address, subnet mask and the default gateway should not be specified.

The default gateway must be defined when specifying the management IP address.

Example:

To define that the management IP is to be obtained from a DHCP server, where:

VLAN ID = 100

specify:

configure ip vlan 100 dhcp

Configuring the Device Prompt

By default the device prompt is set to “ap”. However, configuring a unique device prompt is very useful for the operator. A unique device name allows the operator to quickly identify to what device he is logged in. The prompt can be defined using the following CLI command:

hostname <prompt string>

Configuring the Radio Frequency

The Radio interface frequency is configured by using the following CLI command:

configure interface Dot11Radio <interface number>
channel {<channel number> | default | auto}

Configuring SSID

The NetPoint Pro 3x2.4 and NetPoint Pro 6x2.4 units can support up to 16 SSIDs. Each radio interface must be configured with a minimum of one SSID that is defined as a BSSID. Each SSID has its unique privacy configuration and unique VLAN ID. VLAN-ID 0 represents no VLAN tag. Each SSID can be defined as either a Broadcast SSID (BSSID) or a hidden one.

Define the SSID parameters. This configuration stage is common to SSID to be used as primary (broadcast) or hidden. The next step in the configuration is to attach the defined SSID to the interface. To define and use an SSID use the following CLI commands:

configure ssid <index number> name <ssid string>
vlan <vlan number> privacy-method {none | wep | wpa}
type {hidden | bssid}
configure interface Dot11Radio <interface number>
ssid <index number> {add | remove}

Example:

To create a new SSID with its own VLAN-ID, and no privacy, where:

SSID Index Number = 1
SSID Name = NPP-AP

VLAN-ID = 100
Privacy Method = none
SSID Type = bssid

specify:

configure ssid 1 name NPP-AP vlan 100 privacy-method none type bssid

To attach the defined SSID to the radio interface, where:

Interface Number = 0
SSID Index Number = 1

specify:

configure interface dot11Radio 0 ssid 1 add

Configuring the Mesh Network

The Mesh network is used to support wireless backhauling and meshing between NetPoint Pro 3x2.4 and NetPoint Pro 6x2.4 units. The Mesh network supports backhauling over both the 2.4 GHz access radio and the 5 GHz backhaul radio.

Device Mode Configuration

All NetPoint Pro 3x2.4 and NetPoint Pro 6x2.4 units connected to the wired Ethernet must be configured as a Mesh-Gateway. To configure the units use the following CLI command:

configure mesh mode {gateway | node}

and specify:

configure mesh mode gateway

All units that operate as a Mesh-Node are not connected to a wired Ethernet. They are connected to the network with a wireless connection though other NetPoint Pro 3x2.4 and NetPoint Pro 6x2.4 units. To set the mesh mode accordingly, specify the following CLI command:

configure mesh mode node

Setting the Radio Service

The radio interface can be configured to support access and/or mesh services. To enable the mesh over the radio interface, the radio service must be set to support backhaul services. To configure the services supported use the following CLI command:

configure interface Dot11Radio <interface number>
service {access | backhaul}

Example:

To define the service on the radio interface, where:

Interface Number = 2

specify:

configure interface Dot11Radio 2 service backhaul

Setting the Radio Channel of the Mesh-Gateway

When configuring a mesh network, the mesh interface for all Mesh-Gateways must be assigned a channel. Mesh-Gateways that are close to each other should be assigned a different channel to minimize interference.

The channels available for each unit are set in the factory and are dependent on the region to which the unit was manufactured. To display all available channels on the radio mesh interface, use the *show interface Dot11Radio channel-list* command.

Setting the channel defines the frequency on which the mesh interface communicates. To see the list of channels and their associated frequency see Table 1.

The channel on the radio mesh interface is defined by using the following CLI command:

configure interface Dot11Radio <interface number>
channel {<channel number> | default | auto}

Example:

To define the channel on the mesh interface, where:

Interface Number = 2
Channel = 165

specify:

configure interface Dot11Radio 2 channel 165

Saving the Configuration

Once you have modified the existing configuration file, save the file for future use. To do this, issue the following CLI command:

copy running-config startup-config

NetPoint Pro 6x2.4 Configuration Example

The following example assumes that you are configuring a NetPoint Pro 6x2.4 from its default configuration using the serial port. If the NetPoint Pro 6x2.4 device is configured from the Ethernet or Dot11Radio, issuing any one of the following commands could disconnect the user:

- Changing the IP address
- Changing the SSID or WDS configuration

```
##### configure management ip  ####
ap> /configure ip vlan none 192.168.30.102 255.255.255.0
ap> /configure ip default-gateway 192.168.30.254

#### remove default bssid configuration ####
ap> /configure interface Dot11Radio 0 ssid 1 remove
ap> /configure ssid 1 remove

#### configure a new bssid ####
ap> /configure ssid 1 name MY-SSID vlan 0 privacy-method none type
bssid
ap> /configure interface Dot11Radio 0 ssid 1 add

#### mesh gateway configuration ####
ap> /configure mesh mode gateway
ap> /configure mesh network-id MyMeshNet
ap> /configure mesh privacy AES passphrase MyMeshKey

#### set channels and enable the radios ###
ap> /configure interface Dot11Radio 0 channel 1
ap> /configure interface Dot11radio 0 enable
ap> /configure interface Dot11radio 1 channel 157
ap> /configure interface Dot11radio 1 enable

#### save configuration ####
ap> /copy running-config startup-config
```

Chapter 3

Implementing a Mesh Network

Overview

The Mesh network is used to support wireless backhauling and meshing between NetPoint Pro 3x2.4 and NetPoint Pro 6x2.4 units. The Mesh network supports backhauling over both the 802.11b/g access radio and the 802.11a backhaul radio.

The mesh topology is based on a tree structure as illustrated in Figure 5. At the top of each tree is a NetPoint Pro 6x2.4 unit that is functioning as a Mesh-Gateway, which is connected to the backbone network through its wired port. All other NetPoint Pro 6x2.4 units in the tree are functioning as Mesh-Nodes. Each Mesh-Node is wirelessly connected to a NetPoint Pro 6x2.4 unit creating a backhaul mesh that leads to a Mesh-Gateway. The WMG and third party CPEs connect at the bottom of the tree. The clients communicate with the NetPoint Pro 6x2.4 units on the access radio.

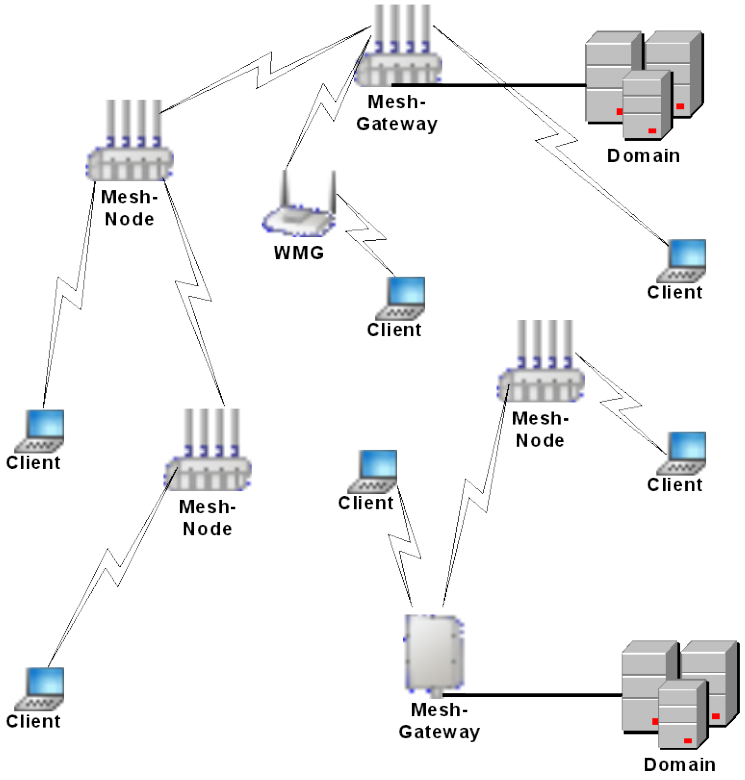


Figure 3: Mesh Network

Mesh network routing is automatic, therefore when more than one route exists, the NetPoint Pro 6x2.4 will route the traffic using the best route. In a similar way, the mesh will recover from a fault by selecting an alternate route when required.

The Mesh-Gateway is the only NetPoint Pro 6x2.4 unit connected to the wired LAN. All other NetPoint Pro 6x2.4 units are Mesh-Nodes and they depend on the mesh network for backhaul connectivity. A Mesh-Node determines various routes to the Mesh-Gateway and selects the route with the best connectivity. If you want to limit the automatic route selection made by the mesh, you can manually restrict the selection by defining and implementing a mesh filter list.

When configuring a mesh network, all Mesh-Gateways must be assigned a channel. The Mesh-Gateways that are close to each other should be assigned a different channel to minimize interference. The Mesh-Nodes scan all available channels and select the channel that offers the best connectivity to the mesh network. For more information on assigning a channel, see Radio Settings.

It is important to note that the number and quality of hops will determine the network performance. In most cases, the physical deployment of the devices is the limiting factor in route selection.

By default, the unit is configured as a Mesh-Node, were the 802.11a backhaul radio interface is defined to participate in the mesh network.

This chapter describes the options and procedures that can be used to configure the mesh network. The following lists the procedures described in this chapter:

- Device Mode Configuration
- Mesh Network Name
- Radio Interface Mesh Configuration
- Radio Settings Configuration
- Wi-Fi Protocol Time Intervals Configuration
- Antenna Diversity Configuration
- Mesh Security Configuration
- Displaying Mesh Configuration
- Displaying Mesh Routing
- Implementing Mesh Filtering
- Example of a multiple unit configuration

Device Mode Configuration

All NetPoint Pro 3x2.4 and NetPoint Pro 6x2.4 units connected to the wired Ethernet must be configured as a Mesh-Gateway. To configure the units use the following CLI command:

configure mesh mode {gateway | node}

and specify:

configure mesh mode gateway

All units that operate as a Mesh-Node are not connected to a wired Ethernet. They are connected to the network with a wireless connection though other NetPoint Pro 3x2.4 and NetPoint Pro 6x2.4 units. To set the mesh mode accordingly, specify the following CLI command:

configure mesh mode node

Mesh Network Name Configuration

All NetPoint Pro 3x2.4 and NetPoint Pro 6x2.4 units connected to the same mesh network must be configured with the same network name (ID). Configuring different networks names may be used to create a number of independent networks. By default the network ID is configured as “wds-public”. To set the network ID use the following CLI command:

configure mesh network-id <network-id>

Example:

To define a network ID, where:

Network ID = MyMeshNetwork

specify:

configure mesh network-id MyMeshNetwork

Radio Interface Mesh Configuration

The user must configure one radio interface on each unit to participate in the mesh network. By default, the 802.11a backhaul interface is defined to participate in the mesh network. Only one interface on each unit can be defined to participate at one time. All units in the mesh network must use the same type of interface to communicate with each other. To configure an interface to participate in the Mesh use the following CLI command:

configure mesh interface Dot11Radio <interface number>
wds {enable | disable}

Example:

To enable a radio interface to participate in a mesh network, where:

Interface Number = 2

specify:

configure mesh interface Dot11Radio 2 wds enable

Note: To enable the 802.11b/g access radio interface to participate in the mesh network, the service type must be properly configured for the interface. For more information, see Setting the Access Radio Service.

Radio Settings Configuration

When configuring a mesh network, all Mesh-Gateways must be assigned a channel. Mesh-Gateways that are close to each other should be assigned a different channel to minimize interference. Mesh-Nodes scan all available channels and select the channel that offers the best connectivity to the mesh network. The channel on a Mesh-Node should not be configured.

Table 1 display all channels and frequencies supported by the NetPoint Pro 3x2.4 and NetPoint Pro 6x2.4 units. The actual frequencies available are dependent on the region to which the unit was manufactured. The default setting for the gateway channel is channel 161 on the 802.11a backhaul interface, which is 5805 MHz.

Interface	Channel and Frequencies	
802.11a backhaul radio	Channel and Frequencies for IEEE 802.11a:	
	34 – 5170 MHz	34 – 5170 MHz
	36 – 5180 MHz	36 – 5180 MHz
	38 – 5190 MHz	38 – 5190 MHz
	40 – 5200 MHz	40 – 5200 MHz
	42 – 5210 MHz	42 – 5210 MHz
	44 – 5220 MHz	44 – 5220 MHz
	46 – 5230 MHz	46 – 5230 MHz
	48 – 5240 MHz	48 – 5240 MHz
	52 – 5260 MHz	52 – 5260 MHz
	56 – 5280 MHz	56 – 5280 MHz
	60 – 5300 MHz	60 – 5300 MHz
	64 – 5320 MHz	64 – 5320 MHz
	100 – 5500 MHz	100 – 5500 MHz
	104 – 5520 MHz	104 – 5520 MHz
	Default channel for 802.11a radio is 161 (5805 MHz).	
802.11b/g access radio	Channel and Frequencies IEEE 802.11b/g:	
	1– 2412 MHz	8– 2442 MHz
	2– 2417 MHz	9– 2447 MHz
	3– 2422 MHz	10– 2452 MHz
	4– 2427 MHz	11– 2457 MHz
	5– 2432 MHz	12– 2462 MHz
	6– 2437 MHz	13– 2467 MHz
	Default value for Dot11Radio 0 is channel 4 (2427 MHz). For NetPoint Pro 3x2.4, the default value for Dot11Radio 1 is channel 11 (2457 MHz).	
4.9GHz Public Safety	Channel and Frequencies for 4.9GHz Public Safety:	
	20 – 4950 MHz	20 – 4950 MHz
	30 – 4955 MHz	30 – 4955 MHz
	40 – 4960 MHz	40 – 4960 MHz
	50 – 4965 MHz	50 – 4965 MHz
	Default channel for 4.9GHz Public Safety is 20 (4950 MHz).	

Table 1: Interface Channels and Frequencies

The following radio settings can be configured or displayed:

- Display Channel List
- Configure Channels in the radio interface Channel-List
- Setting the Radio Channel of the Mesh-Gateway
- Setting the Radio Interface Service (see Setting the Access Radio Service in the Implementing Client Access chapter)

Display Channel List

The channels available for each NetPoint Pro 3x2.4 and NetPoint Pro 6x2.4 unit are set in the factory and are dependent on the region to which the unit was manufactured. Prior to defining the channel on the radio mesh interface, display all the channels available on the unit. To display the available channels use the following CLI command:

show interface Dot11Radio <interface number> **channel-list**

Example:

To display the available channels and their status, where:

Interface Number = 2

specify:

show interface Dot11Radio 2 channel-list

The following is a typical display of a channel-list:

```
ap> show interface Dot11Radio 2 channel-list
-------------------------------------------------------------------
|Interface    |Channel  |Is Allowed  |Reason  |Unallowed time  |
|-------------|---------|------------|--------|----------------|
|Dot11Radio2  |149      |true        |none    |0               |
|.............|.........|............|........|................|
|Dot11Radio2  |153      |true        |none    |0               |
|.............|.........|............|........|................|
|Dot11Radio2  |157      |true        |none    |0               |
|.............|.........|............|........|................|
|Dot11Radio2  |161      |true        |none    |0               |
|.............|.........|............|........|................|
|Dot11Radio2  |165      |true        |none    |0               |
|.............|.........|............|........|................|
ap>
```

To use a channel in the list that is disabled, use the *configure interface Dot11Radio channel-list* command to enable the channel.

Configure Channels in the Channel-List

The status of the channels in the channel-list is used to enable or limit the available channels and frequency on the radio interface. The set the status of a channel use the following CLI command:

configure interface Dot11Radio <interface number>
channel-list {un-allow | allow} {<channel number> | all}

Example 1:

To enable all the channels in the channel-list, where:

Interface Number = 2

specify:

configure interface Dot11Radio 2 channel-list allow all

Example 2:

To disable a channel in the channel-list, where:

Interface Number = 2
Channel = 149

specify:

configure interface Dot11Radio 2 channel-list un-allow 149

Setting the Radio Channel of the Mesh-Gateway

When configuring a mesh network, the mesh interface for all Mesh-Gateways must be assigned a channel. Mesh-Gateways that are close to each other should be assigned a different channel to minimize interference.

The channels available for each unit are set in the factory and are dependent on the region to which the unit was manufactured. To display all available channels on the radio mesh interface use the *show interface Dot11Radio channel-list* command.

Setting the channel defines the frequency on which the mesh interface communicates. To see the list of channels and their associated frequency see Table 1.

The channel on the radio mesh interface is defined by using the following CLI command:

configure interface Dot11Radio <interface number>
channel {<channel number> | default | auto}

Example:

To define the channel on the mesh interface, where:

Interface Number = 0
Channel = 165

specify:

configure interface Dot11Radio 2 channel 165

Setting the Radio Interface Service

To enable the 802.11b/g radio interface to participate in the mesh network, the service type must be properly configured for the interface. The radio interface service must be set to support backhaul, or mixed services. By default, the service on 802.11b/g radio interfaces is set to support access only. To configure the service see Setting the Access Radio Service in the Implementing Client Access chapter.

Configuring Mesh Peers (2.4 GHz Only)

When the mesh network uses the 802.11b/g radio interface the mesh links between the units (peers) must be configured manually. To configure a link, both peers must be configured. Each peer must specify the other peer's MAC address. To configure each peer use the following CLI command:

configure mesh interface Dot11Radio <interface number>
wds-peer <macaddress> [remove]

To display the current mesh peers associated with the unit, use the *show mesh route* command**.**

Note: Caution should be used when configuring the mesh peer links manually. Improper configuration can result with network loops.

Note: To enable the 802.11b/g access radio interface to participate in the mesh network, the service type must be properly configured for the interface. For more information, see Setting the Access Radio Service.

Example:

To define a mesh link between two peers, where:

Peer1 Radio Interface = Dot11Radio 0
Peer1 MAC Address = 00:14:06:11:00:01

Peer2 Radio Interface = Dot11Radio 1
Peer2 MAC Address = 00:14:06:11:00:02

specify on Peer1:

configure mesh interface Dot11Radio 0
wds-peer 00:14:06:11:00:02

specify on Peer2:

configure mesh interface Dot11Radio 1
wds-peer 00:14:06:11:00:01

Configuring the Wi-Fi Protocol Time Intervals

To optimize the Wi-Fi protocol time intervals for long distance usage, the distance between the Gateway and the node units must be specified. This value is then used by the units to optimize the Wi-Fi protocol time intervals.

The distance specified is based on the distance between the Gateway and the furthest node for each network.

The distance should be specified as follows:

- For a maximum distance of 1200 meters or less, specify 1200.
- For a maximum distances greater than 1200 meters, specify the actual distance.
- Specify the same value for all units in the network.

To specify the distance between units, use the following CLI command:

configure interface Dot11Radio <interface number>
distance <distance>

Mesh Security

Configuring the Mesh privacy is used to protect the connections in the mesh network. All the units in the network must be configured with the identical network name and privacy settings. The mesh network can use either of the following encryption protocols.

- **Wired Equivalent Privacy (WEP)** is a protocol that is part of the IEEE 802.11 wireless networking standard to secure wireless networks. The WEP protocol is implemented by using either a standard 64-bit WEP encryption that uses a 40 bit encryption key, or an extended 128-bit WEP encryption that uses a 104 bit encryption key.
- **Advanced Encryption Standard (AES)** is a Federal Information Processing Standard (FIPS). It uses a block cipher that has been adapted as a encryption standard. AES encryption is implemented by using password phrase that can be from 8 to 63 characters.

Mesh security is configured or removed by using one of the following CLI commands:

configure mesh privacy none
configure mesh privacy wep key {40 | 104} <key hex>
configure mesh privacy AES passphrase <passphrase string>

Example 1:

To define the WEP security, where:

WEP Key Length = 40 bit
WEP Key = 11:22:33:44:55

specify:

configure mesh privacy wep key 40 11:22:33:44:55

Example 2:

To define the AES security, where:

AES Passphrase String = secretkey

specify:

configure mesh privacy AES passphrase secretkey

Displaying Mesh Configuration

To display the current mesh configuration, use the following CLI command:

show mesh params

The mesh configuration displays the mesh timeout, mesh interface, mesh security settings and whether the unit has been defined as a Mesh-Gateway or Mesh-Node.

Displaying Mesh Routing

The mesh routing table contains the routing entry for the current next hop to get access to the Mesh-Gateway. It also displays all the alternative next hop routing entries. To display the current mesh routing table, use the following CLI command:

show mesh route

Implementing Mesh Filtering

Mesh Filtering manages the routing of the mesh network. It is used to limit the structure of the mesh network. Mesh filtering defines a list of MAC addresses that can be denied or permitted connectivity to the mesh interface. Each unit uses its mesh filtering MAC address list to determine its next hop in the mesh network. This feature can perform the following functions:

- Defines and uses a list of MAC addresses to determine which units are permitted to be the next hop.
- Defines and uses a list of MAC addresses to determine which units are not permitted to be the next hop.
- Displays the list of MAC addresses configured for mesh filtering.
- Displays the status of mesh filtering.

To implement these functions the following commands are used:

- configure mesh filter-list
- show mesh filter-list

Defining and Using a Mesh Filter

The CLI provides a mechanism to define and use mesh filtering to manage the mesh network. The configuration and implementation of mesh filters is a multi-part procedure.

- Define the filter list type
- Define and create a list of MAC addresses for mesh filtering
- Enable the mesh filtering feature

Defining the Filter List Type

The first step in implementing mesh filtering is to define the type of the mesh filter list that will be implemented. The mesh filter list can either be a list of MAC address that are denied or permitted connectivity to the mesh interface. Each unit uses its mesh filtering MAC address list to limit its next hop in the mesh network. To define the type, use the following command:

configure mesh filter-list type {permit | deny}

Defining MAC addresses for Mesh Filtering

The next step in implementing mesh filters is to add and define the MAC addresses that are used for mesh filtering. To define the MAC addresses, use the following command:

configure mesh filter-list mac <macaddress> {add | remove}

This command allows you to add or remove MAC addresses and defines the type of MAC addresses added. When defining the MAC addresses, all the MAC addresses should be defined as either permitted to be the next hop or denied to be the next hop. Do not define both types on a single unit. To display all MAC addresses currently defined for mesh filtering use the *show mesh filter-list* command.

Example 1:

To define the mesh filter list to contain MAC addresses that are permitted to be the next hop, specify:

configure mesh filter-list type permit

Example 2:

To add a MAC address to the mesh filter list, where:

MAC Address to be added = 00:14:06:11:00:00

specify:

configure mesh filter-list mac 00:14:06:11:00:00 add

Example 3:

To delete a MAC address that is currently included in the mesh filter list, where:

MAC Address to be deleted = 00:14:06:11:00:00

specify:

configure mesh filter-list mac 00:14:06:11:00:00 remove

Enabling the Mesh Filtering Feature

Once the MAC addresses have been added to the mesh filter, the mesh filtering feature must be enabled. To enable this feature, use the following command:

configure mesh filter-list {enable | disable}

Example:

To enable the mesh filtering feature, specify:

configure mesh filter-list enable

Example of a Multiple Unit Configuration

The sections above describe the tasks and commands used to configure mesh networks. This section demonstrates a complete procedure to configure a multiple unit mesh network using the commands described above.

The following figure displays a multiple unit mesh network with multiple gateways:

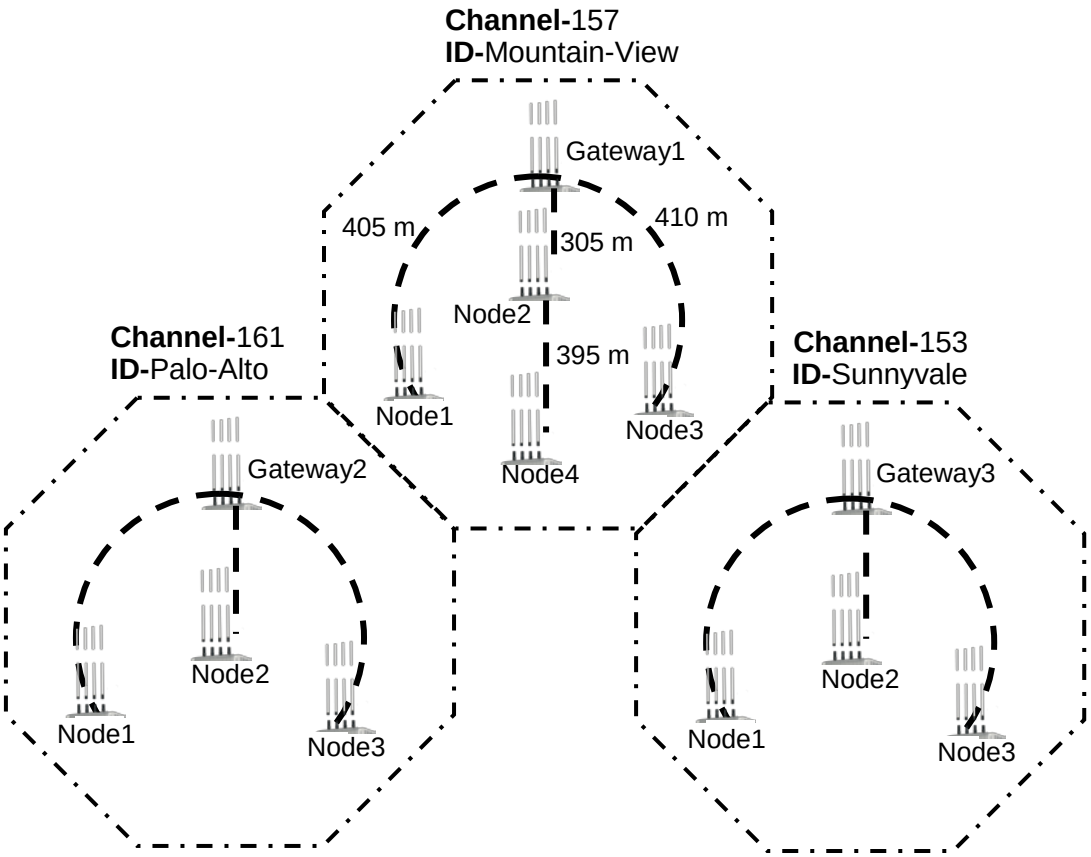


Figure 4: Multiple Gateway Mesh Network

This mesh network contains three gateways, which requires multiple Network IDs and multiple channels. To configure this mesh network, the network is first broken into three segments. Each segment contains an individual gateway, and all the NetPoint Pro 3x2.4 and NetPoint Pro 6x2.4 units associated with this gateway. Each segment is configured separately. This configuration is demonstrated below.

Configuring Mountain-View Segment

The Mountain-View segment contains a Mesh-Gateway and four Mesh-Nodes. To configure this segment the following procedures and commands are implemented for each of the devices:

- Device Prompt Configuration – *hostname*
- Device Mode Configuration – *configure mesh mode*
- Mesh Network Name Configuration – *configure mesh network-id*
- Radio Interface Mesh Configuration – *configure mesh interface*
- Display Channel List – *show interface Dot11Radio channel-list*
- Set the Radio Channel (Gateway only) – *configure interface channel*
- Wi-Fi Protocol Time Intervals – *configure interface Dot11Radio distance*
- Mesh Security Configuration – *configure mesh privacy*
- Display the Mesh Routing Table – *show mesh route*

Device Prompt Configuration

The first step in configuring the device is to change the prompt to easily identify the device you are configuring. This step is not required, but is recommended. The prompt can be defined using the following CLI command:

hostname <prompt string>

Device Mode Configuration

Each device must be configured for the mode of operation in the mesh. The device must be configured either as a Mesh-Gateway or Mesh-Node. The mode can be defined using the following CLI command:

configure mesh mode {gateway | node}

Mesh Network Name Configuration

Each device connected to the same mesh network must be configured with the same network name (ID). To set the network ID use the following CLI command:

configure mesh network-id <network-id>

Radio Interface Mesh Configuration

Each device can only have one radio interface that can participate in the mesh network. This radio interface must be defined for each device. All units in the mesh network must use the same type of interface to communicate with each other. To configure an interface to participate in the Mesh use the following CLI command:

configure mesh interface Dot11Radio <interface number> enable

Display Channel List

Prior to defining the channel and frequency that will be used for the mesh, it is recommended to display all available channels. The Channel List table will display all available channels and their current status. To display the Channel List table use the following CLI command:

show interface Dot11Radio <interface number> **channel-list**

Set the Radio Channel of the Mesh-Gateway

Each Mesh-Gateway must be assigned a channel to its radio mesh interface. Mesh-Gateways that are close to each other should be assigned a different channel to minimize interference. The channel on the mesh interface is defined by using the following CLI command:

configure interface Dot11Radio <interface number>
channel <channel number>

Configuring the Wi-Fi Protocol Time Intervals

To optimize the Wi-Fi protocol time intervals for long distance usage, the distance between the Gateway and the node units must be specified. This value is then used by the units to optimize the Wi-Fi protocol time intervals.

The distance specified should be the distance between the Gateway and the furthest node for each network. The minimum distance specified should be 1200 meters. To specify the distance between units, use the following CLI command:

configure interface Dot11Radio <interface number>
distance <distance>

Mesh Security Configuration

Configuring the Mesh privacy is used to protect the connections in the mesh network. All the units in the network must be configured with the identical network name and privacy settings. The mesh network can use either of the following encryption protocols.

- Wired Equivalent Privacy (WEP)
- Advanced Encryption Standard (AES)

Mesh security is configured or removed by using one of the following CLI commands:

configure mesh privacy none
configure mesh privacy wep key {40 | 104} <key hex>
configure mesh privacy AES passphrase <passphrase string>

Display the Mesh Routing Table

Once the configuration is complete for each segment, display the mesh routing table to confirm the configuration. To display the mesh routing table use the following CLI command:

show mesh route

Examples

The following figures are examples of the configuration for the Mountain-View Segment for each device. The bold text is the text entered by the user.

Gateway1

```
ap> hostname Gateway1
Gateway1> /configure mesh mode gateway
Changing wds root status might cause the device to become inaccessible.
It is recommended that you verify you have other means of accessing the
device (such as SSH).

Are you sure you wish to continue? (Y/N) Y

We are calibrating the system. Service is limited until process ends.
We are calibrating the system. Service is limited until process ends.
This AP is now defined as mesh gateway.

Gateway1> /configure mesh network-id Mountain-View
Gateway1> /configure mesh interface Dot11Radio 2 enable
Gateway1> show interface Dot11Radio 2 channel-list
-----------------------------------------------------------------
|Interface    |Channel  |Is Allowed  |Reason  |Unallowed time  |
|-------------|---------|------------|--------|----------------|
|Dot11Radio2  |149      |true        |none    |0               |
|.............|.........|............|........|................|
|Dot11Radio2  |153      |true        |none    |0               |
|.............|.........|............|........|................|
|Dot11Radio2  |157      |true        |none    |0               |
|.............|.........|............|........|................|
|Dot11Radio2  |161      |true        |none    |0               |
|.............|.........|............|........|................|
|Dot11Radio2  |165      |true        |none    |0               |
|.............|.........|............|........|................|
Gateway1> /configure interface Dot11Radio 2 channel 157
Gateway1> /configure interface Dot11Radio 2 distance 1200
Gateway1> /configure mesh privacy AES passphrase MountainPassword
Gateway1>
```

Node1

```
ap> hostname Node1
Node1> /configure mesh mode node
Changing wds root status might cause the device to become inaccessible.
It is recommended that you verify you have other means of accessing the
device (such as SSH).

Are you sure you wish to continue? (Y/N) Y

We are calibrating the system. Service is limited until process ends.
We are calibrating the system. Service is limited until process ends.
This AP is now defined as mesh node.

Node1> /configure mesh network-id Mountain-View
Node1> /configure mesh interface Dot11Radio 2 enable
Node1> /configure interface Dot11Radio 2 distance 1200
Node1> /configure mesh privacy AES passphrase MountainPassword
Node1>
```

Node2

```
ap> hostname Node2
Node2> /configure mesh mode node
Changing wds root status might cause the device to become inaccessible.
It is recommended that you verify you have other means of accessing the
device (such as SSH).

Are you sure you wish to continue? (Y/N) Y

We are calibrating the system. Service is limited until process ends.
We are calibrating the system. Service is limited until process ends.
This AP is now defined as mesh node.

Node2> /configure mesh network-id Mountain-View
Node2> /configure mesh interface Dot11Radio 2 enable
Node2> /configure interface Dot11Radio 2 distance 1200
Node2> /configure mesh privacy AES passphrase MountainPassword
Node2>
```

Node3

```
ap> hostname Node3
Node3> /configure mesh mode node
Changing wds root status might cause the device to become inaccessible.
It is recommended that you verify you have other means of accessing the
device (such as SSH).

Are you sure you wish to continue? (Y/N) Y

We are calibrating the system. Service is limited until process ends.
We are calibrating the system. Service is limited until process ends.
This AP is now defined as mesh node.

Node3> /configure mesh network-id Mountain-View
Node3> /configure mesh interface Dot11Radio 2 enable
Node3> /configure interface Dot11Radio 2 distance 1200
Node3> /configure mesh privacy AES passphrase MountainPassword
Node3>
```

Node4

```
ap> hostname Node4
Node4> /configure mesh mode node
Changing wds root status might cause the device to become inaccessible.
It is recommended that you verify you have other means of accessing the
device (such as SSH).

Are you sure you wish to continue? (Y/N) Y

We are calibrating the system. Service is limited until process ends.
We are calibrating the system. Service is limited until process ends.
This AP is now defined as mesh node.

Node4> /configure mesh network-id Mountain-View
Node4> /configure mesh interface Dot11Radio 2 enable
Node4> /configure interface Dot11Radio 2 distance 1200
Node4> /configure mesh privacy AES passphrase MountainPassword
Node4>
```

Once the configuration is completed, display the mesh routing table for each device to confirm the configuration.

Gateway1

```
Gateway1> show mesh route
Time: 07:28:18  Date: Mon March 26, 2007 local

Currently bridging traffic for:
name:Node1 Address:10.0.14.14 (00:14:06:41:03:20) rssi=-63
name:Node2 Address:10.0.14.13 (00:14:06:41:02:20) rssi=-60
name:Node3 Address:10.0.14.8 (00:14:06:41:02:B0) rssi=-61
Gateway1>
```

Node1

```
Node1> show mesh route
Time: 07:28:20  Date: Mon March 26, 2007 local

Next hop:
name:Gateway1 Address:10.0.14.1 (00:14:06:41:03:21) rssi=-63

Alternate next hop:
name:Node2 Address:10.0.14.13 (00:14:06:41:02:20) rssi=-72
name:Node3 Address:10.0.14.8 (00:14:06:41:02:B0) rssi=-73
name:Node4 Address:10.0.14.15 (00:14:06:41:03:22) rssi=- 67

Currently bridging traffic for:
No Peers

Node1>
```

Node2

```
ap> show mesh route
Time: 07:28:22  Date: Mon March 26, 2007 local

Next hop:
name:Gateway1 Address:10.0.14.1 (00:14:06:41:03:21) rssi=-60

Alternate next hop:
name:Node1 Address:10.0.14.14 (00:14:06:41:03:20) rssi=-66
name:Node3 Address:10.0.14.8 (00:14:06:41:02:B0) rssi=-73

Currently bridging traffic for:
name:Node4 Address:10.0.14.15 (00:14:06:41:03:22) rssi=-60
Node2>
```

Node3

```
Node3> show mesh route
Time: 07:28:24  Date: Mon March 26, 2007 local

Next hop:
name:Gateway1 Address:10.0.14.1 (00:14:06:41:03:21) rssi=-61

Alternate next hop:
name:Node1 Address:10.0.14.14 (00:14:06:41:03:20) rssi=-74
name:Node2 Address:10.0.14.13 (00:14:06:41:02:20) rssi=-66
name:Node4 Address:10.0.14.15 (00:14:06:41:03:22) rssi=- 70

Currently bridging traffic for:
No Peers

Node3>
```

Node4

```
Node4> show mesh route
Time: 07:28:26  Date: Mon March 26, 2007 local

Next hop:
name:Node2 Address:10.0.14.13 (00:14:06:41:02:20) rssi=-60


Alternate next hop:
name:Node1 Address:10.0.14.14 (00:14:06:41:03:20) rssi=-67
name:Node3 Address:10.0.14.8 (00:14:06:41:02:B0) rssi=-70

Currently bridging traffic for:
No Peers

Node4>
```

Chapter 4

Implementing Client Access

Overview

Implementation of the Client access must be performed only after implementing and configuring the Mesh network. When the Mesh network is configured on the 802.11b/g access radio, special configuration considerations must be made.

This chapter describes the options and procedures that can be used to configure the Client Access. The following lists the procedures described in this chapter:

- Configuring the Radio Settings
- Configuring Multiple SSIDs
- Deleting an SSID
- Implementing WME QoS
- Implementing Client Security
- Implementing Client Filters

Configuring the Radio Settings

When configuring client access the radio settings on the interface should be configured. The NetPoint Pro 3x2.4 and NetPoint Pro 6x2.4 units are preconfigured from the factory with default values that allow client access operation. However, for optimal performance it is recommended that the radio settings be review and optimally configured. The following access radio settings can be configured:

- Radio Channel
- Radio Sensitivity
- Radio Reception Level
- Radio Mode
- Radio Service

- Beacon Period
- DTIM Period
- RTS Threshold
- ERP Mode

Setting the Access Radio Channel

When configuring a NetPoint Pro 3x2.4 or NetPoint Pro 6x2.4 unit, the access radio interface must be assigned a communication channel to operate. The channel selected defines the frequency at which the interface communicates. When multiple access radio interfaces are used on a single unit or multiple units are close to each other, different channel should be assigned to each interface to minimize interference. The channels selected should have a minimum frequency difference of 25 MHz, which is a difference of 5 channels, between the interfaces.

Table 2 displays all access radio channels and frequencies supported by the NetPoint Pro 3x2.4 and NetPoint Pro 6x2.4 units. The actual frequencies available are dependent on the region to which the unit was manufactured. The default setting for access radio interfaces Dot11Radio 0 is channel 4.

Interface	Channel and Frequencies
Dot11Radio	Channel and Frequencies: 1– 2412 MHz 2– 2417 MHz 3– 2422 MHz 4– 2427 MHz 5– 2432 MHz 6– 2437 MHz 8– 2442 MHz 9– 2447 MHz 10– 2452 MHz 11– 2457 MHz 12– 2462 MHz 13– 2467 MHz Default value for Dot11Radio 0 is channel 4 (2427 MHz).

Table 2: Access Radio Dot11Radio Channels and Frequencies

When the access radio interface is also used for the mesh network, all units must use the same channel. When the unit has one access radio interface, this interface will also be used for CPE access. When the unit has multiple access radio interfaces, it is recommended that one interface be used for the mesh network and the other interface will be used for CPE access. The second interface that is used for CPE access should be defined with a different channel and be configured as described above.

The channel and frequency on the access radio interface is configured by using the following CLI command:

configure interface Dot11Radio <interface number>
channel {<channel number> | default | auto}}

Note: To enable the access radio interface to participate in the mesh network, the service type must be properly configured for the interface. For more information, see Setting the Access Radio Mode.

Setting the Access Radio Sensitivity

The range and capacity of the units are highly dependent upon its RX sensitivity. RX sensitivity is measured in dBm. A large negative number (as example -101dBm) is considered high sensitivity, while a smaller number (as example -90dBm) is considered low sensitivity.

A high sensitivity will result in an increased range along with higher susceptibility to noise and interference. The higher noise susceptibility will result in lower throughputs.

A low sensitivity will result in a reduced range with lower susceptibility to noise. The lower noise susceptibility will result in higher throughputs.

Clearly, when setting the device sensitivity the user has to compromise range verses capacity.

The amount of noise in the system can be monitored by the Viewer or by the following CLI command:

show spectrum-management clear-count-percent

Figure 7 displays a printout of the *spectrum-management clear-count-percent* command. In this example on the Dot11Radio 0 interface the air is currently occupied at 15% of the time. Out of these 15%, 1% was used to transmit WLAN packets and 8% of the time was used to receive packets. Note that packets are received from all WLAN devices at your current frequency. Therefore, a large amount of the RX airtime might be taken by neighboring networks. The remaining 6% (i.e. 15-8-1=6) is the amount of airtime occupied by non-WLAN signals. These 6% are what we call noise.

```
ap> show spectrum-management clear-count-percent
-------------------------------------------------------------------------------------------
|Interface    |Tx Frame Ratio |Rx Frame Ratio |Clear Count Ratio |Sensitivity Level |Noise Level |
|-------------|---------------|---------------|------------------|------------------|------------|
|Dot11Radio 0 |1              |8              |15                |auto              |-100        |
|.............|...............|...............|..................|..................|............|
|Dot11Radio 1 |3              |9              |12                |auto              |-94         |
-------------------------------------------------------------------------------------------
ap>
```

Figure 5: Spectrum-Management Clear-Count-Percent Printout

By default, the 802.11b/g channel is set to automatically adjust the interface sensitivity to the noise level in the air. Noise levels of up to 20% are considered normal. If the amount of noise exceeded this level, you should consider changing a channel or lowering the sensitivity.

The following CLI command sets the sensitivity level to automatic:

configure interface Dot11Radio <interface number>
sensitivity auto

The current sensitivity level can be monitored using:

show spectrum-management clear-count-percent

The sensitivity could also be set manually to support local optimization by an operator. The sensitivity level can be set as follows:

- For xRF radio interface: (-101) - (-77)
- For non-xRF 802.11b/g radio interface: (-96) - (-72)
- For 802.11a radio interface: (-89) - (-60)

The following CLI command sets a static sensitivity level:

configure interface Dot11Radio <interface number>
sensitivity <level number>

Setting the Access Radio Max Associated

The access radio interface can be configured to reject clients associated to the access point based on the number associated clients. By default, the radio interface maximum number of users is set to 250 associated clients. The maximum number of associated client can be set from 1 to 250. The following CLI command sets the maximum number of associated clients:

configure interface Dot11Radio <interface number>
max-assoc <maximum associated clients>

Setting the Access Radio Mode

The Wi-Fi mode of the access radio interface can be configured to operate in one of two modes:

- 802.11g Mode Only – Interface will only accept communications from devices operating in 802.11g mode.
- Mixed Mode – Interface will accept communications from devices operating in 802.11b and 802.11g modes.

By default, the access radio interface is defined for use in a mixed mode.

To define the Wi-Fi mode on the access radio interface, use the following CLI command:

configure interface Dot11Radio <interface number>
mode {a | b | g | mixed | pureg}

Setting the Access Radio Service

The access radio interface can be configured to support access and/or mesh services. To enable the mesh over the access radio interface, the access radio service must be set to support backhaul, or mixed services. By default, the access radio service is set to support access service. To configure the services supported use the following CLI command:

configure interface Dot11Radio <interface number>
service {access | backhaul}

Setting the Access Radio Beacon Period

The beacon period is the time period between beacons. This time period can be configured for each access radio interface. By default, the Radio Beacon Period is set to 250 milliseconds. This results with the specified access radio interface transmitting a beacon every 250 milliseconds. The beacon period can be set from 100msec to 1000msec. Setting the beacon period can be done using the following CLI command:

configure interface Dot11Radio <interface number>
beacon-period <period number>

Setting the Access Radio DTIM Period

The DTIM (Delivery Traffic Indication Message) period defines how frequently the DTIM informs the client in power saving mode if data is waiting to be sent. Each beacon transmitted contains a DTIM. The DTIM informs the client if data is waiting and when the next time data is available. The DTIM period defines the number of beacons that are transmitted between sending data packets.

By default, the Radio DTIM Period is set to 1. This defines that every beacon transmitted contains a DTIM informing the client whether or not data is waiting. The DTIM period can be set to a frequency from 1 to 8 beacons. Setting the DTIM period can be done using the following CLI command:

configure interface Dot11Radio <interface number>
dtim-period <period number>

Setting the Access Radio RTS Threshold

The RTS threshold defines the threshold packet size for implementing RTS (request to send). Packets larger than the RTS threshold will be transmitted using RTS. The lower the threshold the more frequently the system uses RTS.

By default, the RTS threshold is set to 2346 bytes. The RTS threshold can be set from 1 byte to 2346 bytes. Setting the RTS threshold can be done using the following CLI command:

configure interface Dot11Radio <interface number>
rts <threshold number>

Setting the Access Radio ERP Mode

The access radio interface can be configured to support ERP Mode. The ERP mode is used to reduce collisions when there are b and g clients.

By default, the ERP Mode is disabled. To enable or disable the ERM Mode, use the following CLI command:

configure interface Dot11Radio <interface number>
erp-mode {enable | disable}

Configuring Multiple SSIDs

The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple access points on a network or sub-network can use the same SSID. Configuring the same SSID across multiple APs will enable the users to roam between them seamlessly. SSID names are case sensitive and can contain up to 32 alphanumeric characters.

The NetPoint Pro 3x2.4 and NetPoint Pro 6x2.4 units can support up to 14 SSIDs. Each radio interface must be configured with a minimum of one SSID that is defined as a BSSID. Each SSID has its unique privacy configuration and unique VLAN ID. VLAN-ID 0 represents no VLAN tag and multiple SSIDs can have their VLAN ID set to 0.

Each SSID can be defined as either a Broadcast SSID (BSSID) or a hidden one. Passive scanning clients will not detect a hidden SSID, since it doesn't transmit any beacon frames. Configuring multiple BSSIDs on the same interface is known as creating a Virtual Access Point. A Virtual Access Point is a logical entity that exists within a physical access point. When a single Physical AP supports multiple Virtual APs, each Virtual AP appears to stations to be an independent Physical AP, even though only a single Physical AP is present.

Note: SSIDs, VLANs, and encryption schemes are mapped together on a one-to-one-to-one basis. One SSID can be mapped to one VLAN, and one VLAN can be mapped to one encryption scheme.

Define the SSID parameters. This configuration stage is common to SSID to be used as primary (broadcast) or hidden. In the following example, three SSID's are defined as NPP1, NPP2, and NPP-HIDDEN, each with its own VLAN-ID, and no privacy.

```
ap> /configure ssid 1 name NPP1 vlan 0 privacy-method none
type bssid
ap> /configure ssid 2 name NPP2 vlan 100 privacy-method none
type bssid
ap> /configure ssid 3 name NPP-HIDDEN vlan 200 privacy-
method none type hidden
```

The next step in the configuration is to attach the defined SSIDs to the interface:

```
ap> /configure interface dot11Radio 0 ssid 1 add
ap> /configure interface dot11Radio 1 ssid 1 add
ap> /configure interface dot11Radio 0 ssid 2 add
ap> /configure interface dot11Radio 1 ssid 2 add
ap> /configure interface dot11Radio 0 ssid 3 add
ap> /configure interface dot11Radio 1 ssid 3 add
```

Deleting an SSID

To delete an SSID, the SSID must first be removed from the interface. After the SSID is removed, then the SSID can be deleted. The following example demonstrates the deletion of SSID 3 from interface dot11Radio 0.

To remove an SSID from the interface:

ap> configure interface dot11Radio 0 ssid 3 remove

To delete an SSID:

ap> configure ssid 3 remove

Implementing WME QoS

Wireless Multimedia Enhancements (WME) is a method to improve Quality of Service (QoS) for wireless communications. It complies with IEEE 802.11e, which is 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 four 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 3x2.4 and NetPoint Pro 6x2.4 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 to transmit (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 in number of 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) – Is a range of time that is used in determining the time between transmission opportunities (TXOP). During the initial transmission, CW is determined based on the set value of *CWmin,* 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 CWmax*,* 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 CW is 15 microseconds, and the TXOP duration can be from the minimum TXOP duration to the minimum TXOP duration plus 15 microseconds.
- Transmission Opportunity (TXOP) Limit – Time period allowed to transmit. 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.

The WME feature is configured by using the following CLI commands:

- **configure interface Dot11Radio wme –** Configures the WME quality of service (QoS) parameters for each category.

  configure interface Dot11Radio <interface number>
  wme {voice | video | besteffort | background}
  [cw_min <cw min number>] [cw_max <cw max number>]
  [aifs <slots number>] [txop-limit <time limit>]
- **configure ssid privacy-method –** This command enables or disables the WME feature on the specified interface.

  configure interface Dot11Radio <interface number>
  wme-enable {true | false}

Select the Access Categories to be configured: voice, video, best effort, or background.

The *slots number* parameter defines the number of slots for the AIFS time period. The value can be set from 0 to 15 time slots.

The minimum CW is determined by the *cw min number* parameter, which is the exponent form of the minimum CW. The maximum CW is determined by the *cw max number* parameter*,* which is the exponent form of the maximum CW.

The minimum CW (CWmin) and maximum CW (CWmax) is calculated from the following equations:

$$CWmin = 2^{cw\ min\ number} - 1$$

$$CWmax = 2^{cw\ max\ number} - 1$$

The *cw min number* and *cw min number* parameters can be set from 0 to 15. This results with a CWmin and CWmax from 0 to 32767 microseconds.

The *time limit* parameter defines the time period allowed to transmit (TXOP Limit). The value can be set from 0 to 8192 microseconds.

The default values for all parameters are dependent on the AC.

For Voice:

- slots number = 2
- cw min number = 2
- CWmin = 3 microseconds
- cw max number = 3
- CWmax = 7 microseconds
- time limit = 1504 microseconds

For Video:

- slots number = 2
- cw min number = 3
- CWmin = 7 microseconds
- cw max number = 4
- CWmax = 15 microseconds
- time limit = 3008 microseconds

For Best Effort:

- slots number = 3
- cw min number = 4
- CWmin = 15 microseconds
- cw max number = 10
- CWmax = 1023 microseconds
- time limit = 0 (minimum time)

For Background:

- slots number = 7
- cw min number = 4
- CWmin = 15 microseconds

- cw max number = 10
- CWmax = 1023 microseconds
- time limit = 0 (minimum time)

Example:

To define the WME quality of service for voice, where:

Access Radio interface = 0

AIFS = 1 time slot

cw min number = 1

cw max number = 3

TXOF Limit = 3 milliseconds

specify:

```
/configure interface Dot11Radio 0 wme voice
cw_min 1 cw_max 3 aifs 1 txop-limit 3000
configure interface Dot11Radio 0 wme-enable true
```

Implementing Client Security

The SSID privacy is used to protect the connections with the clients. The privacy (encryption) scheme is configured per SSID. The access network can use either of the following encryption protocols:

- **Wired Equivalent Privacy (WEP)** is a protocol that is part of the IEEE 802.11 wireless networking standard to secure wireless networks. The WEP protocol is implemented by using either a standard 64-bit WEP encryption that uses a 40 bit encryption key, or an extended 128-bit WEP encryption that uses a 104 bit encryption key.
- **Wi-Fi Protected Access (WPA)** is a standards-based, interoperable security enhancement that strongly increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and will be forward-compatible with the upcoming IEEE 802.11i standard. It includes two new data-confidentiality protocols (TKIP and AES-CCMP).

Using WEP Security

WEP security is implemented by using either a standard 64-bit WEP encryption that uses a 40 bit encryption key, or an extended 128-bit WEP encryption that uses a 104 bit encryption key.

Client security with WEP encryption is configured or removed by using one of the following CLI commands:

- **configure ssid –** Configures a new SSID. This command can be used to define the privacy method of a new SSID.

configure ssid <index number> name <ssid string>
vlan <vlan number> privacy-method {none | wep | wpa}
type {hidden | bssid}

- **configure ssid privacy-method –** This command defines the privacy method of an existing SSID.

  configure ssid <index number>
  privacy-method {none | wep | wpa}

- **configure privacy wep ssid –** This command defines the WEP key to a specific SSID.

  configure privacy wep ssid <index number>
  index <key index> {40 | 104} <key hex>

The *index number* parameter specifies a new or existing SSID index number. Each NetPoint Pro 3x2.4 or NetPoint Pro 6x2.4 unit supports 16 SSIDs and the allowable index number is 1-16. To display all the existing SSIDs and their current security settings, use the *show privacy wpa ssids* command.

The *key index* parameter defines the WEP key index number. In this software version the index number is always set to 1.

The *{40 | 104}* parameter defines the length of the WEP encryption key to be defined.

The *key hex* parameter defines the WEP encryption key. When the key is a 40 bit key, specify a 5 octet string in hexadecimal format. When the key is a 104 bit key, specify a 13 octet string in hexadecimal format.

Example:

To define WEP security on an existing SSID, where:

SSID Index Number = 3
Key Index = 1
WEP Key Length = 40 bit
WEP Key = 11:22:33:44:55

specify:

/configure ssid 3 privacy-method wep
/configure privacy wep ssid 3 index 1 40 11:22:33:44:55

Using WPA Security

WPA implements TKIP and AES-CCMP (Temporal Key Integrity Protocol and Cipher Block Chaining Message Authentication Code Protocol) for data protection and 802.1X for authenticated key management.

WPA1 and WPA2 offer a high level of assurance for end users and network administrators that their data will remain private and that access to their networks will be restricted to authorized users.

WPA security supports two mutually exclusive management types:

- **WPA-Extensible-Authentication-Protocol (WPA-EAP):** Using WPA-EAP key management, the client and the authentication server authenticate each other using an EAP authentication method, and the client and server generate a Pairwise Master Key (PMK).
- **WPA-Pre-shared key (WPA-PSK):** Using WPA, the server generates the PMK dynamically and passes it to the NetPoint Pro 3x2.4 or NetPoint Pro 6x2.4 unit. Using WPA-PSK, however, you configure a pre-shared key on both the client and the unit, and that pre-shared key is used as the PMK.

Client security with WPA encryption is configured or removed by using one of the following CLI commands:

- **configure ssid –** Configures a new SSID. This command can be used to define the privacy method of a new SSID.

  configure ssid <ssid index> name <ssid string>
  vlan <vlan number> privacy-method {none | wep | wpa}
  type {hidden | bssid}
- **configure ssid privacy-method –** This command defines the privacy method of an existing SSID.

  configure ssid <ssid index>
  privacy-method {none | wep | wpa}
- **configure privacy wpa –** This command defines the WPA security. There are parameters that are defined to a specific SSID and there areglobal parameters that defines the wpa security for the unit.

  configure privacy wpa ssid <ssid index>
  [passphrase <passphrase string>]
  [key-mngmnt {eap | psk}]
  configure privacy wpa [gtk-interval <interval number>]
  [data-encryption {tkip | aes | both}]
  [protocol {wpa1 | wpa2 | wpa2only}]
  [preauthentication {enable | disable}]

The *ssid index* parameter specifies a new or existing SSID index number. Each NetPoint Pro 3x2.4 or NetPoint Pro 6x2.4 unit supports 16 SSIDs and the allowable index number is 1-16. to display all the existing SSIDs and their current security settings, use the *show privacy wpa ssids* command.

The *passphrase string* parameter defines the passphrase that is used during the key handshake process for WPA encryption on a specific SSID. The value is case sensitive and can be from 8 to 63 characters.

The key management defines the type of key management that is used for WPA encryption on a specific SSID. There are two types available: EAP and PSK. When set to *eap*, the WPA encryption uses the Extended Authorization Protocol method. When set to *psk*, the WPA encryption uses the Pre-Shared Key method.

The GTK (Group Temporal Key) interval used on the unit for WPA security is defined globally. It defines the time interval the unit initiates a GTK change in seconds. By default, the GTK interval is set to 3600 seconds (1 hour). The interval can be set from 30 to 42,949,672 seconds.

The type of data encryption used on the unit for WPA security is defined globally. There are two types available: TKIP and AES- CCMP. When set to *tkip*, the unit uses Temporal Key Integrity Protocol for the WPA encryption. When set to *aes*, the unit uses Advanced Encryption Standard with Cipher Block Chaining Message Authentication for the WPA encryption. By default, the data encryption type is set to TKIP.

The WPA security protocol used on the unit is defined globally. There are two types available: WPA1 and WPA2. When set to *wpa1*, the unit only supports WPA1 protocol. When set to *wpa2*, the unit supports WPA1 and WPA2 protocols. When set to *wpa2only*, the unit only supports WPA2 protocol. By default, the WPA security protocol is set to *wpa2* (supports WPA1 and WPA2).

The Preauthentication feature on the unit is set globally. When the Preauthentication feature is enabled, a WPA2 wireless client can perform an 802.1X authentication with other wireless access points while it is still connected to its current wireless access point. By default, the Preauthentication feature is disabled.

Example:

To define the WPA security on an existing SSID, where:

SSID Index Number = 3

WPA Passphrase = PasswordPhrase

WPA Key Management Type = PSK

GTK Interval = 20 hours (72000 seconds)

WPA Data Encryption Type = TKIP

WPA Protocol Type = WPA1 only

Preauthentication Feature = disabled

specify:

```
/configure ssid 3 privacy-method wpa
/configure privacy wpa ssid 3 passphrase PasswordPhrase
key-mngmnt psk
/configure privacy wpa gtk-interval 72000
/configure privacy wpa data-encryption tkip


/configure privacy wpa protocol wpa1
/configure privacy wpa preauthentication disable
```

Implementing Client Filters

Client filters are used to permit or deny client access to the unit. The filters are based on the MAC addresses of the clients. This feature can perform the following functions:

- Defines and uses a list of MAC addresses that permits access to the unit.
- Defines and uses a list of MAC addresses that denies access to the unit.
- Creates and deletes MAC filter lists.

- Exports MAC filter lists.
- Imports MAC filter lists.
- Displays the configuration of the current MAC filter lists.
- Displays the MAC filter list index for each SSID.

Defining and Using a Client Filter

The CLI provides a mechanism to define and use client filters to permit or deny client access. The configuration and implementation of client filters is a multi-part procedure.

- Create a MAC filter list
- Define the MAC addresses in the list
- Map a MAC filter list to an SSID

To implement these procedures the following commands are used:

- configure mac-filter list new
- configure mac-filter add
- configure mac-filter list add-mac
- configure mac-filter list remove-mac
- configure ssid macfilter
- show mac-filter indices
- show mac-filter list

Creating a MAC Filter List

The first step in implementing client filters is to create the MAC filter list that contains the MAC address to be filtered. Use the *configure mac-filter list new* command to create new white or black MAC filter lists. These lists can then be used to permit or deny client access to the unit.

When creating a new list, a new index number must be specified for this list. Use this index number to use, configure or delete the list. To display all MAC filter list indices use the *show mac-filter indices* command.

To create a new MAC filter list, use the following CLI command:

configure mac-filter list <index number> **new** <name string> type {white | black}

Example:

To create a new white MAC filter list, where:

MAC Filter List Index = 3
MAC Filter List Name = WhiteList2

specify:

configure mac-filter list 3 new WhiteList2 type white

A new list does not contain any MAC addresses. The addresses must be added to the list to be implemented. For more information on defining MAC filter lists, see section Defining a MAC Filter List.

Defining a MAC Filter List

The second step in implementing client filters is to define the MAC addresses contained in the MAC filter list. Only existing lists can be defined. For more information on creating a new MAC filter list, see section Creating a MAC Filter List. To define a MAC filter list, MAC addresses are added or deleted from the list.

The following commands are used to define a list:

configure mac-filter list <index number> **add-mac** <macaddr>
configure mac-filter list <index number> **remove-mac** <macaddr>

Once a MAC filter list is defined, the MAC addresses contained in the list can be displayed using the following command:

show mac-filter list <index number>

To define a MAC filter list the index number must be specified. To display all MAC filter list indices use the *show mac-filter indices* command.

Example 1:

To add a MAC address to an existing MAC filter list, where:

MAC Filter List Index = 3
MAC Address to be added = 00:14:06:11:00:00

specify:

configure mac-filter list 3 add-mac 00:14:06:11:00:00

Example 2:

To display the MAC addresses to an existing MAC filter list, where:

MAC Filter List Index = 3

specify:

show mac-filter list 3

Mapping a MAC Filter List to an SSID

The last step in implementing client filters is to map a defined MAC filter list to an existing SSID. For more information on defining a MAC filter list, see section Defining a MAC Filter List. For more information on configuring an SSID, see section Configuring the Radio Settings.

To map a MAC filter list to an SSID, use the following CLI command:

configure ssid <index number>
macfilter <mac-filter-index number>

To map a MAC filter list the index number of the list and the index number of the SSID must be specified. To display all MAC filter list indices use the *show mac-filter indices* command. When the SSID was created the index number was specified. To display all SSID indices use the *show ssid params* command.

Example:

To create map MAC filter list, where:

SSID Index Number = 9
MAC Filter List Index = 3

specify:

configure ssid 9 macfilter 3

Creating a MAC Filter List

The second step in importing and implementation MAC addresses is to create the MAC filter list that will contain the MAC address to be filtered. The name of the MAC filter list must be the same name of the imported file from the TFTP server. If the MAC filter list already exists, you can skip to the next step (see section Loading MAC Addresses).

Use the *configure mac-filter list new* command to create new white or black MAC filter lists. When creating a new list, a new index number must be specified for this list. Use this index number to use, configure or delete the list. To display all MAC filter list indices use the *show mac-filter indices* command.

To create a new MAC filter list, use the following CLI command:

configure mac-filter list <index number> **new** <name string> type {white | black}

Example:

To create a new white MAC filter list, where:

MAC Filter List Index = 3
MAC Filter List Name = WhiteList2

specify:

configure mac-filter list 3 new WhiteList2 type white

A new list does not contain any MAC addresses. The addresses can be added to the list by loading imported MAC addresses. For more information on importing MAC addresses, see section Importing MAC Addresses. For more information on loading MAC addresses, see section Loading MAC Addresses.

Chapter 5

Authentication Types

Configuring Authentication Types

In the most common 802.1X WLAN environments, the NetPoint Pro 3x2.4 and NetPoint Pro 6x2.4 units defer to the Radius server to authenticate users and to support particular EAP authentication types. The Radius server handles these functions, and provides crucial authentication and data-protection capabilities according to the requirements of the EAP authentication type in use. The Radius client runs on the NetPoint Pro 3x2.4 and NetPoint Pro 6x2.4 units and sends authentication requests to a central Radius server, which contains all user authentication and network service access information. The Radius server is normally a multi-user system running Radius server software (such as developed by Microsoft or other software vendors).

The wireless client device and Radius server on the wired LAN use 802.1x and EAP to perform mutual authentication through the NetPoint Pro 3x2.4 or NetPoint Pro 6x2.4 unit.

1. The Radius server sends an authentication challenge to the client.
2. The client uses a one-way encryption of the user-supplied password to generate a response to the challenge and sends that response to the Radius server.
3. The Radius server receives the encryption response from the client and compares the response to the information stored in its database.

When the Radius server authenticates the client, the process repeats in reverse, and the client authenticates the Radius server.

Configuring the Radius Client

Your unit must be configured to support the Radius server communication. At a minimum, you must identify the Radius server software and define the method lists for Radius authentication. Alternatively, you can define method lists for Radius authorization and accounting.

Identifying the Radius Server

Communications to the Radius server involves several components:

- IP address
- Authentication destination port
- Accounting destination port
- Key string

You should identify the Radius security server's IP address and specific UDP port numbers. The combination of the IP address and the UDP port number creates a unique identifier.

A Radius server and the access point use a shared secret text (key) string to encrypt passwords and exchange responses.

The Radius client in the unit can be configured by using the following commands:

configure radius {accounting | authentication}
ssid <ssid index> priority <priority number>
[host <address ipaddress>] [port <port number>]
key <secret string>
configure radius {accounting | authentication}
ssid <ssid index> priority <priority number> remove

Chapter 6

Upgrading the Software

The NetPoint Pro 3x2.4 and NetPoint Pro 6x2.4 units support TFTP application and HTTP web browser upgrades. New software images can be downloaded from the Netronics website. Before performing the upgrade procedure, make sure you have the appropriate files on your computer. A software upgrade can be performed by connecting to the Ethernet port or over the air connected through the access or BH radios. When a software upgrade is performed, a new image is copied to the unit's Flash (ROM memory). The Flash holds two software images. Therefore, when a new image is uploaded, the running image is not overridden. If, for any reason, the software upgrade fails, the unit can continue to function with its current image.

TFTP Software Upgrade

To upgrade software using TFTP, the user has to prepare a TFTP server with the new software image. A freeware TFTP server such as PumpKIN can be downloaded from the Internet and installed on the technician's PC.

To upgrade the software via TFTP use the following command:

```
import image from tftp <ip address> <filename>
```

TFTP Upgrade Example

```
ap>
ap> /import image from tftp <ip address> <filename>
ap> /show messages software-download
Software download started.
Verifying server and path.
TFTP path OK.
Flash erase started.
Flash erase finished.
Download started from 192.168.30.103 gapsw-1.3.5.11995-Beta-
28.02.2006@180244.img.
Download finished.
Verification started.
Verification passed.
Writing to environment.
Software download finished.
```

URL Software Upgrade

URL software upgrade may be used to load software directly from an HTML link or an FTP server.

To upgrade the software via URL use the following command:

```
import image from url <url link>
```

When uploading from an FTP site, the URL link has to be formatted as follows:

```
ftp://user:password@host:port/path and filename
```

To upgrade the software version:

a. Use the import image from tftp/url command.
b. Wait for the “Software download finished” message.
c. Reboot the system by using the “reload” command.

To observe the software upgrade progress use the following command:

```
show messages software-download
```

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	EGOed 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
Signal	RJ-45 Pin	RJ-45 Pin	DB-9 Pin	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 though 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