GO Metro Broadband Wireless

Getting Started Technical Guide for WLP

Wireless LAN Pico Base Station

Version 2.3

Document #: DO000124

Trademarks and Licensing Agreement

GO Networks Inc.
1943 Landings Drive • Mountain View, CA 94043 • USA
Tel +1.650.962.2000 • Fax +1.650.962.2010
Email support@gonetworks.com

Version 2.3

FCC Compliance Status

The following information is for FCC compliance:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits of a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment, this equipment generates, uses, and radiates radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference. However, there is no guarantee that interference will not occur.

To meet regulatory restrictions, the outdoor access point must be professionally installed.

The Part 15 radio device operates on a non-interference basis with other devices operating at this frequency when using its antennas. Any changes or modifications not expressly approved by GO Networks could void the user's authority to operate the equipment.

The antennas used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Table of Contents

Introduction

GO Networks' WLP device is a key enabler for the Metro Broadband Wireless (MBW) Solution. GO Pico Cellular WiFi architecture offers a novel topology for metro WiFi networks, 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 WiFi solutions.

The GO Networks' Pico Cellular WiFi architecture is a highly scalable Micro/Pico topology which provides unprecedented flexibility to service providers deploying Metro WiFi networks.

Key Product Features

- Robust Pico cellular WiFi solution
- Separate access & backhaul radios delivering unmatched bandwidth
- xRF™ smart antenna engine for unmatched (360^{o}) coverage and capacity enhancements
- Advanced automatic mesh
- Designed for streetlight, wall, or pole deployment
- Client/WDS based CPE connection
- Support for all standard security scheme

Organization of this Document

The GO Metro Broadband *Getting Started Guide* for the Wireless LAN Pico Base Station (WLP) offers information and instructions for quickly installing and configuring the WLP. The instructions and information are presented in one volume as follows:

Introduction	Contains introductory information about the WLP.
GO WLAN Pico Base Station	Presents a general description and overview of the WLP including content and safety procedures.
Installation Process	Describes the installation process for the WLP.
Configuring the WLP	Describes how to configure the WLP.
Upgrading the WLP Software	Explains how to update the WLP software.
Appendix A	Lists the acronyms that appear in the manual.
Appendix B	Details the wiring specifications.

GO Wireless LAN Pico Base Station (WLP)

The GO **W**ireless **L**AN **P**ico Base Station (WLP) complements the **W**ireless **L**AN **S**ector Base Station (WLS). It delivers street-level coverage and provides capacity enhancements in dense metro areas over a single 802.11b/g channel, while meshing traffic over an 802.11a radio.

The WLP Base Station delivers omni-directional (360^{o}) coverage while retaining full xRF smart antenna engine functionality for enhanced capacity and range.

WLP Package Components

The WLP package items are listed in Table 1:

DESCRIPTION	REV	QTY
Wall/Poll Mount Kit Assembly (new)	1.0	1
Connectors Kit for WLP Package	1.0	1
WLP unit	1.0	1
WLP Access Antenna 2.4GHz 7.4dBi Gain, Omni		4
802.11a 5Ghz 10dBi Omni Antenna (Backhaul)		2
Photocell Power Adapter with cable length 6 ft (180cm)		1
Antenna Support Plate		1

Table 1: WLP Package Contents

Deployments of gateway devices connected by wire to an indoor switch/router would include installation of a lightning protector. A lightning protector is not supplied as part of the standard package. It can be ordered from GO Networks as an accessory.

Specific installation may require different Power/Ethernet connections. See Cable Connections for more details.

WLP Safety Information

RF Exposure

The WLP, an outdoor access point, is compliant with the requirements set forth in CFR 47 section 1.1307, addressing RF Exposure from radio frequency devices as defined in OET Bulletin 65. The outdoor access point antennas should be installed to provide a separation distance of at least 3 feet (1 meter) from humans.

WLP Lightning Protector

A lightning protector is required when the WLP unit is installed in an outdoor location and the Ethernet cable connects to an indoor network device.

The purpose of the lightning protection is to protect people and equipment located indoors from lightning that might strike the WLP or its outdoor cables. Therefore, the lightning protector device should be installed indoors, as close as possible to the point where the cables enter the building.

The lightning protector can also be installed outdoors, as long as the cables that go from the lightning protector to the indoors are well protected from lightning between the box and the building entrance.

Verify that you have shared grounding. GO Networks offers a lightning protector that can be ordered separately.

Information de sécurité pour WLP

Exposition aux fréquences RF

Le point d'accès extérieur WLP est compatible avec la norme CFR 47 section 1.1307 concernant l'exposition aux appareils émetteurs de fréquences radio RF définis par le Bulletin 65 de l'OET. Les antennes doivent être installées à une distance minimum d'un mètre de personnes humaines.

Paratonerre pour WLP

Un paratonnerre est nécessaire lorsque le point d'accès WLP est installe à l'extérieur et lié à un network intérieur par un câble Ethernet.

La fonction du paratonnerre est de protéger les personnes et équipement situés en intérieur des éclairs qui pourraient frapper le WLP ou son câble extérieur. Par conséquent, le paratonnerre doit être installé en intérieur le plus près possible du point où le câble de liaison pénètre le bâtiment.

Le paratonnerre peut aussi être installé en extérieur à la condition que les câbles a l'intérieur du bâtiment soient protégés des éclairs entre le point d'accès et l'entrée du bâtiment

Vérifier que la prise de terre est partagée. GO Networks met a disposition à la vente un paratonnerre.

Installation Process

Installing the WLAN Pico Base Station involves the following steps:

1. Performing a Site Survey
2. Assembling and Mounting
3. Mounting the WLP unit
4. Connecting the Antennas
5. Connecting the cables
6. Powering up the unit and configuring the software
7. Performing a Post-installation Testing Procedure to verify connectivity and operation

Site Survey

Most wireless LANs include many access points installed in various locations in an overlapping radio-cell pattern. It is important to carefully identify each access point’s position and the assignment of its radio channels. Therefore, a site survey becomes an essential first step before physically deploying the GO MBW WLP Pico Cellular Base Station solution.

Installation of the access points requires a backhaul to interface the corporate network or Internet. This backhaul connection can be a mesh configuration, an Ethernet-wired connection, or a third-party solution. When using any method other then a wired connection, keep in mind the WLP has to have a good reception on its BH side so it will not limit the access-channel performance.

Conclude the site survey with a detailed plan of the MBW system deployment. The system deployment plan should include WLP mounting points and the routes for the power and backhaul cables.

Note: When mounting the WLP on a pole (or wall mount), the pole should be able to support four times the weight of the WLP, as well as the wind loading created by the WLP.

Since the mounting structure itself is a potential source of interference, the cell should be mounted with at least 4 feet of clearance between the antennas and the mounting structure.

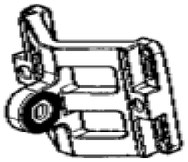
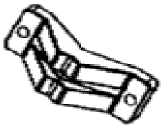
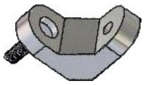
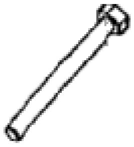
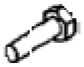
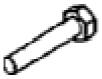
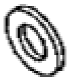
Assembling and Mounting

The universal mount is used to attach and secure the WLP to a wall, a streetlight arm, or a variety of poles.

The WLP mounting consists of the following stages and should be performed in the following order:

1. Connect the WLP unit to the brackets using the ‘L’ adaptor.
2. Secure the mounting brackets to a streetlight arm, wall, or pole.
3. Assemble the WLP unit to the bracket.
4. Ground the WLP unit.
5. Align the WLP unit.
6. Mount the Antenna to the WLP unit.

Table 2 lists the universal mount parts:

Item No.	Description	Qty	Picture
A	Wall/Poll Bracket	1	
B	Clamping Bracket	1	
C	WLP ‘L’ Adapter Wall/Poll Mount	1	
D	Hex Bolt M8x70	2	
E	Hex Bolt M8 x25	1	
F	Hex Bolt M8x40	1	
G	Flat Washer M8	3	

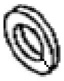
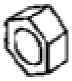
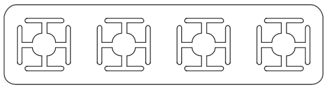
Item No.	Description	Qty	Picture
H	Spring Washer M8	4	
I	Nut M8	1	
J	Antenna Support Plate	1	

Table 2: Mounting Kit Part List

Hardware and Connectors Installation Tools

The following tools are required to mount the WLP on a pole.

Combination Wrench (13 mm)	13 mm
Level	

Table 3: Mounting Tools and Equipment

Note: All hardware and tools used for assembling and mounting the WLP are Metric.

To assemble the 'L' adaptor [C] to the WLP unit:

- Attach the 'L' adapter to the WLP using an M8 x25 hex bolt [E], a spring washer [H], and a flat washer [G], as illustrated in Figure 1.

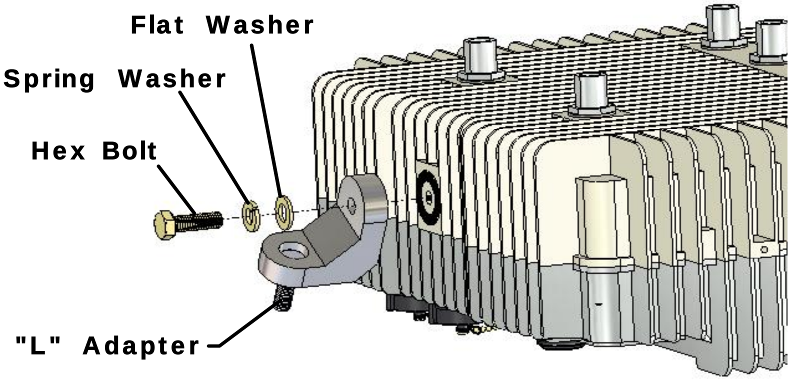


Figure 1: Mount 'L' Assembly

Mounting Brackets

To secure the mounting brackets:

1. Select an optimal mounting location on the pole. Select the highest mounting location with minimal obstacles to the antennas for optimal performance.

   NOTE: When mounting the WLP on a pole, it should be placed on a pole that can support four times the weight of the WLP, as well as the wind loading created by the WLP.

2. Installation of the mounting brackets to a streetlight arm or a pole differs according to the width of the pole, as illustrated in Figure 2.

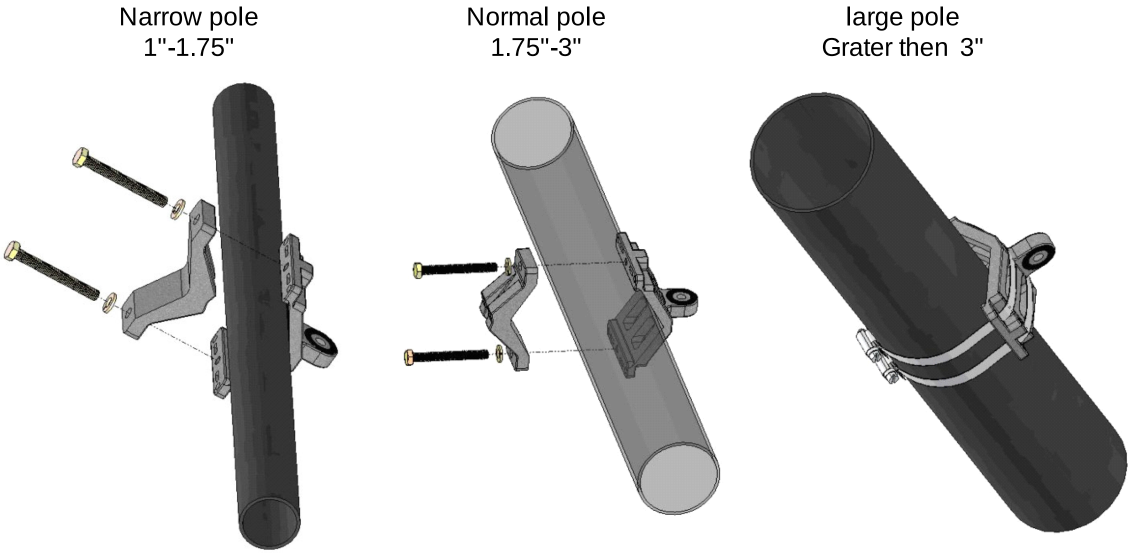


Figure 2: Pole Bracket Assembly

3. For narrow poles (1”–1.75” diameter):
   a) Place the two brackets, [A] and [B], around the pole at the approximate height where you wish to place the unit. When placing the clamping bracket [B], the small notch side should be in contact with the pole.
   b) Use two M8x70 hex bolts [D] and spring washers, insert them through both brackets and tighten them around the pole so that the two brackets are securely fastened.
4. For normal poles (1.75”–3” diameter):
   a) Place the two brackets, [A] and [B], around the pole at the approximate height where you wish to place the unit. When placing the clamping bracket [B], the large notch side should be in contact with the pole.
   b) Use two M8x70 hex bolts [D] and spring washers [H], insert them through both brackets and tighten them around the pole so that the two brackets are securely fastened.
5. For poles larger than 3” in diameter:
   a) The wall/poll bracket [A] and two 0.5" (13mm) wide stainless steel hose clamps (not supplied with mounting kit) are used. The hose clamps must be the appropriate size to fit around the pole and bracket.
   b) Open the each hose clamp by rotating the screw on the clamp counterclockwise. There may be additional resistance just before the clamp is completely open. This is normal and you should continue rotating the screws until the clamps are open.
   c) Insert the band of each clamp through both slots and over the bracket [A].
   d) Place the bracket [A] and hose clamps around the pole at the approximate height where you wish to place the unit.
   e) Close each clamp by reinserting the band under the screw and rotate the screw clockwise.
   f) Position the bracket in the appropriate location and tighten the clamps around the pole so that the bracket is securely fastened.

6. For wall mounting:

    a) Fasten the wall/poll bracket [A] to the wall using four 3/16" (5mm) bolts, as shown in Figure 3. Use the appropriate bolts and fasteners, which is dependent on the material of the wall. Wall-mounting bolts and fasteners are not supplied with the mounting kit.

    b) Place the wall/poll bracket [A] at the appropriate location where you wish to place the unit. Using the four holes at the corners of the bracket, mark the location where the fasteners need to be installed.

    c) Install the four fasteners in the wall.

    d) Insert the four bolts through the bracket and securely fasten the bracket to the wall.

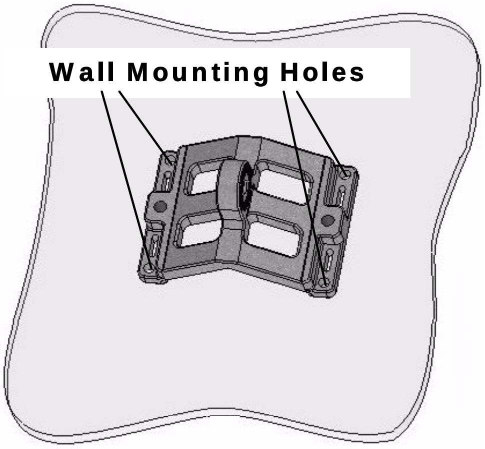


Figure 3: Bracket Wall Mounting

Mounting the WLP

To mount the WLP unit:

1. After assembling the brackets, mount the WLP unit on to the bracket as shown in Figure 4. Use a flat washer [G], a spring washer [H] and a nut [I].

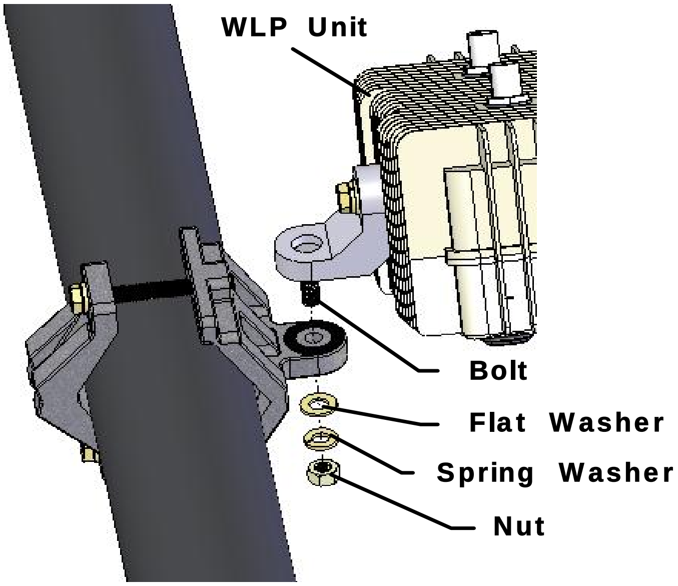


Figure 4: WLP Unit Mounting

2. Once the WLP unit is mounted, release the bolts slightly and align the WLP unit horizontally using the level, as shown in Figure 5. When the unit is perfectly aligned, firmly close all bolts, applying 120 inch-lbs of torque.

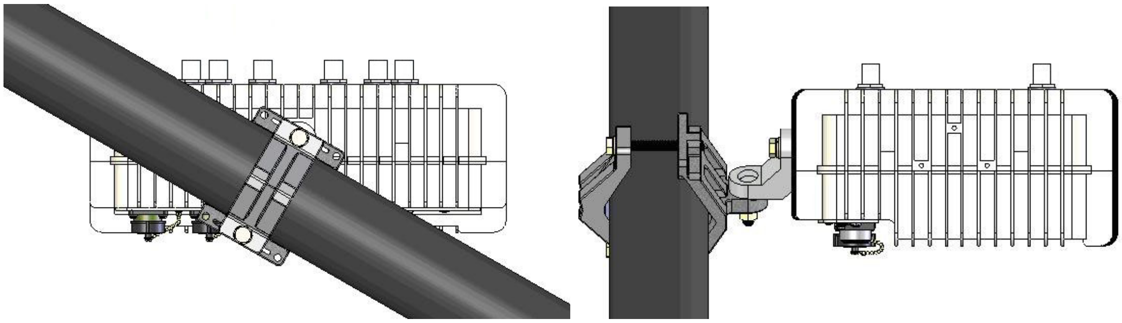


Figure 5: Aligning the WLP

Mounting the Antenna

The WLP supports six antennas. Four WiFi antennas used for user access, which operate on the 2.4 GHz band, marked A1 to A4. Two antennas are used for the mesh networking connections, which operate on the 5 GHz band, marked B1 and B2.

To mount the antennas on the WLP:

1. Attached the four 2.4 GHz band antennas to terminals A1 to A4 and screw all antennas into place by hand. Rotate each antenna at its metallic base. The antennas should rotate easily. Tighten the antenna by hand only. Do not apply excessive force by using any tool, as this may damage the unit.

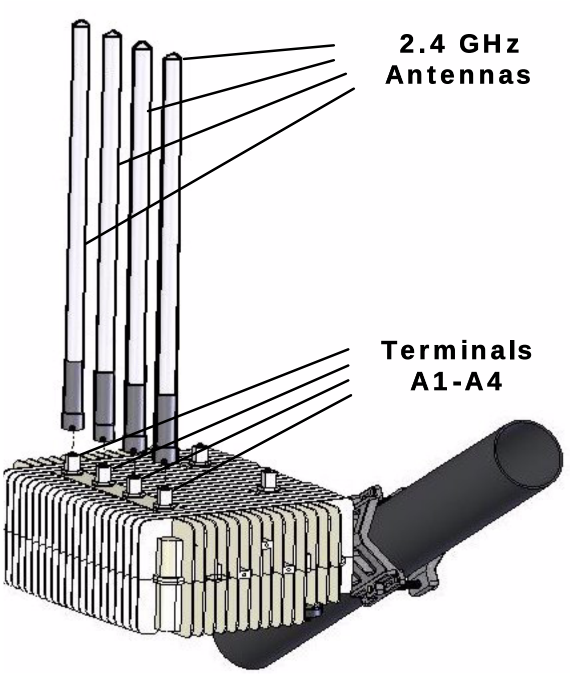


Figure 6: 2.4 GHz Band Antennas Installation

2. Insert the four 2.4 GHz band antennas into the Antenna Support Plate [J]. The antennas must be inserted evenly, so that the plate is level and all the antennas are protruding the same. Use caution not to change the alignment of the WLP.

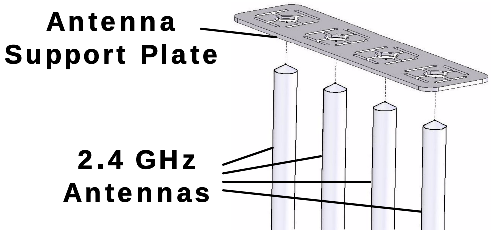


Figure 7: Antenna Support Plate Installation

3. Attached the two 5 GHz band antennas to terminals B1 and B2. Tighten the antennas by hand at it metallic base. The antennas should rotate easily. Do not apply excessive force by using any tool, as this may damage the unit.

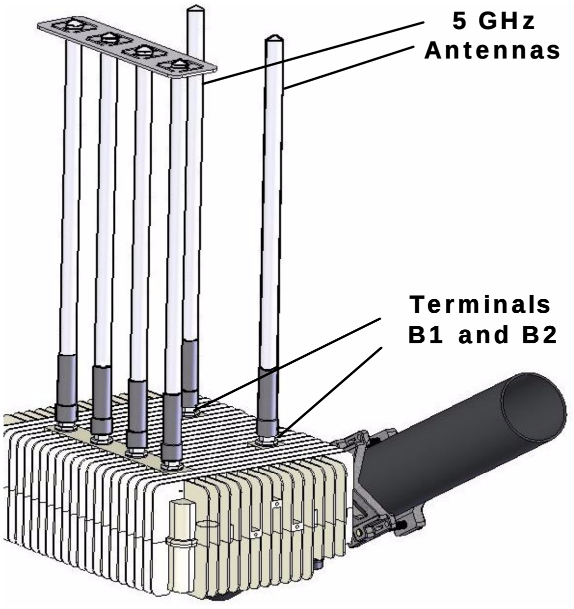


Figure 8: 5 GHz Band Antennas Installation

Cable Connections

When the WLP is properly aligned, the connecters are located at the bottom of the unit.

Cable requirements are often unique to the location and deployment topology of each installation. As a result of this limitation, the Ethernet and grounding cables are not included in the installation kit.

The following cables are required to install the WLP unit and should be connected in the following order:

- **Grounding Cable –** Provides the necessary electrical safety functions.
- **Ethernet Cable –** Required only for WLP units connected to a wired network.
- **Power Cable –** Supplies AC power to the WLP unit. The supplied AC power cable is designed to connect directly to a photocell power adapter.
- **RS-232 Console Cable –** Provides a connection from the WLP unit to a console (laptop computer) for configuration. This is only required when the WLP unit is not pre-configured. This cable is not provided with the WLP unit. It is recommended that the WLP is pre-configured prior to installation.

Table 4 lists the WLP Connectors Kit parts:

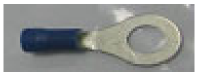
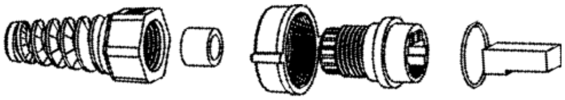
Item No.	Description	Qty	Picture
A	Solderless Ring Terminal	1	
B	Sealed RJ45 connector	1	

Table 4: Mounting Kit Part List

Cable Installation Tools

The following special tools are required to install and connect cables related to the WLP.

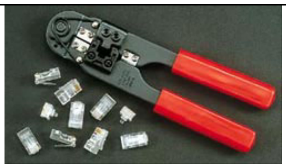
Slotted Screwdriver 1/8" (3mm) wide	
Terminal Crimp Tool	
RJ45 Crimp Tool	 HT-210A
Volt Meter	

Table 5: Cable Installation Tools and Equipment

Grounding Cable

Connect a grounding wire to the grounding screw at the bottom of the WLP unit. A 10 AWG grounding cable is required to ground the WLP unit.

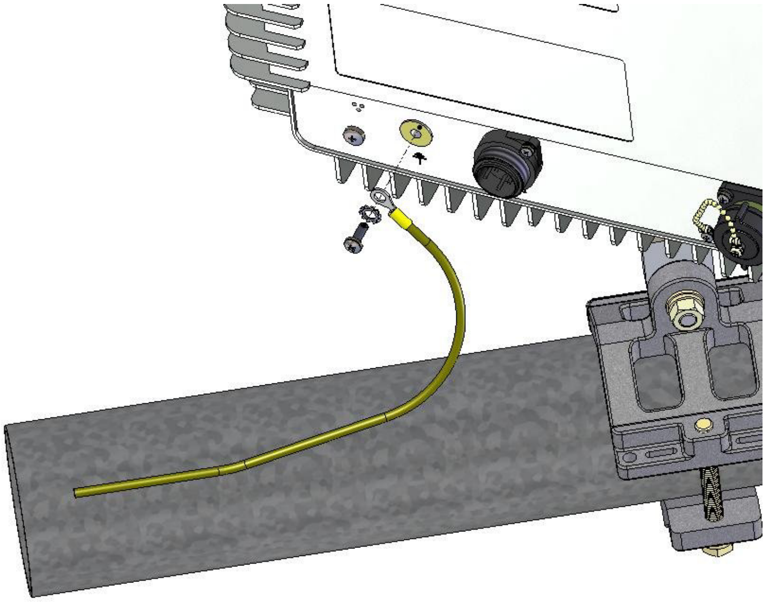


Figure 9: Grounding Connection

To ground the WLP unit:

1. Crimp the solderless ring terminal [A] contained in the WLP Connectors Kit to the grounding cable.
2. Attach the solderless ring terminal [A] to the bottom of the WLP unit using the grounding screw.
3. Connect the other end of the grounding cable to a proper ground.

Note: Connect the 10 AWG grounding cable before connecting any other cables. When removing the WLP, the grounding cable should be the last cable removed.

Noter: *Connecter la prise de terre 10 AWG avant de connecter tout autre câble. Pendant la désinstallation du WLP, la prise de terre doit être le dernier câble retiré.*

Ethernet Connection

Ethernet connection is used for wired backhaul connection or an interface to a third party wireless BH solution. Use outdoor rated CAT5 shielded cables or better. The outer diameter of the Ethernet cable should be 4.8 – 7 mm. When using CAT5 shielded cables the cable can be up to 100 meters.

Following is a diagram explaining how the Ethernet cable should be assembled prior to connecting it to the WLP unit:

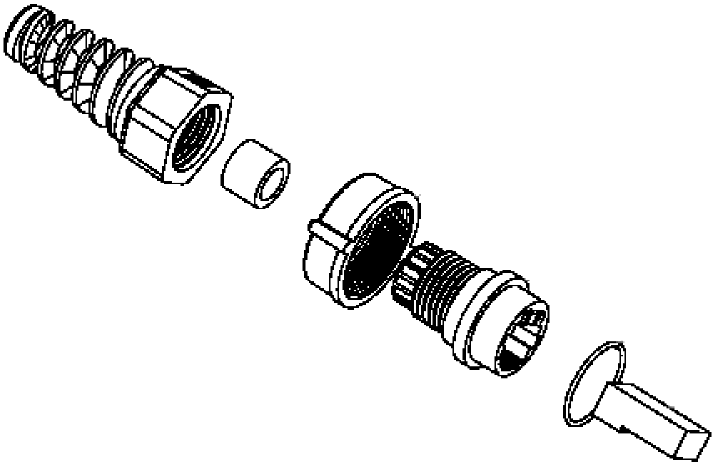


Figure 10: Ethernet Cable Connector

Power Connection

The WLP unit can be connected to an AC power source by one of several methods. It can be connected directly to a power source or by using an adapter to connect to the streetlight photocell (photo-control). The WLP unit can support input voltage of 100 to 240 VAC (50 to 60 Hz).

Note: Connect the grounding cable before connecting any other cables. When removing the WLP, the grounding cable should be the last cable removed.

Noter: *Connecter la prise de terre 10 AWG avant de connecter tout autre câble. Pendant la désinstallation du WLP, la prise de terre doit être le dernier câble retiré.*

To connect the AC power to the WLP via the streetlight photocell:

1. Check the input voltage to the streetlight photocell. The voltage must be between 100 to 240 VAC. If yes, continue with this procedure. Otherwise, use a different method for the power connection.
2. Remove the streetlight photocell. Turn the photocell counterclockwise and lift the photocell out of the socket.
3. Insert the Auxiliary Power Adapter in the socket of the photocell. Note that one prong is larger than the other two. Align the larger prong on the adapter with the larger slot in the socket. Insert the Auxiliary Power Adapter into the socket and rotate the adapter clockwise.

4. Insert the photocell into the Auxiliary Power Adapter. Align the larger prong on the photocell with the larger slot in the socket on top of the adapter. Insert the photocell into the socket and rotate the photocell clockwise.
5. Connect the Auxiliary Power Adapter cable to the power connector socket on the WLP.
6. After connecting the power, verify that the Power (PWR) LED is lit.
7. Check the photocell. Cover the photocell and verify that the streetlight operates.

Console Connection

Figure 11 illustrates the RS-232 cable connections used to connect the WLP to a console (notebook computer to configure the WLP).

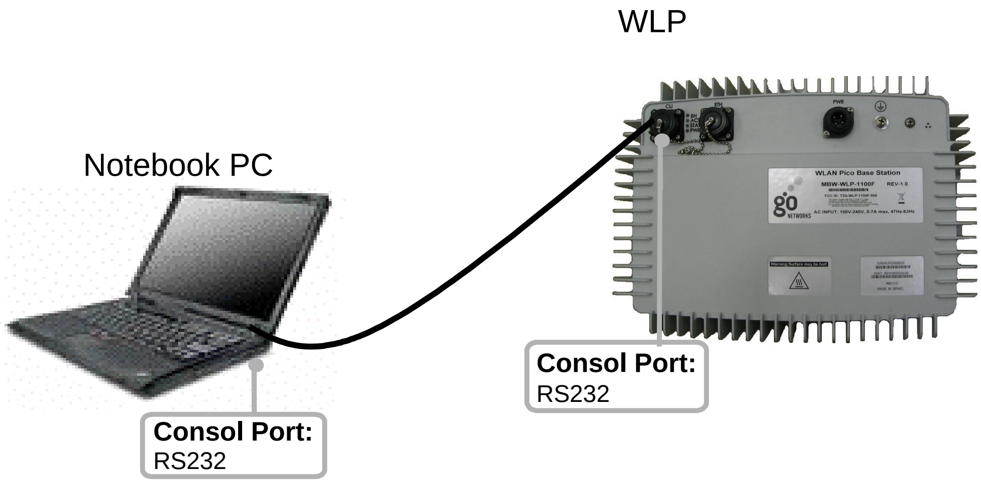


Figure 11: Connect and Access the WLP

Note: New laptops may not include an RS-232 serial port. If a serial port is not available, you may use a USB to serial converter.

Power Up and Software Configuration

The WLP unit is normally mounted on a streetlight (pole or wall) 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 from the ground. To verify communications when installing the WLP unit, the Mesh-Gateways must be installed and powered up first.

The LEDs on the WLP unit indicate the status of communications between the WLP unit and the network. See Table 6 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 WLP unit's wireless communication is connected. WLP 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 WLP unit is normal. **Red –** The WLP 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 WLP unit. **Unlit** – There is no communication connection.
BH	**Green** – On a Mesh-Gateway, the mesh functionality is activated. On a Mesh-Node, the WLP 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 WLP is not configured or failed to connect to the mesh.

Table 6: WLP LED Indicators

Configuring the WLP

Following is a brief overview of the main CLI commands that are used to configure the WLP. A configuration example follows the detailed list of configuration commands. These and other CLI commands are detailed in the *GO MBW CLI Reference Guide*.

Connect and Access the WLP

Initial configuration of the WLP is done using a serial cable. A standard RS232-interface DB-9 cable is connected to the COM port of a laptop or a PC to the WLP unit's console port. For more information regarding the serial cable, see *Appendix B, Wiring Specifications*.

Once the WLP IP address is configured, the rest of the configuration can be done using Telnet via the network.

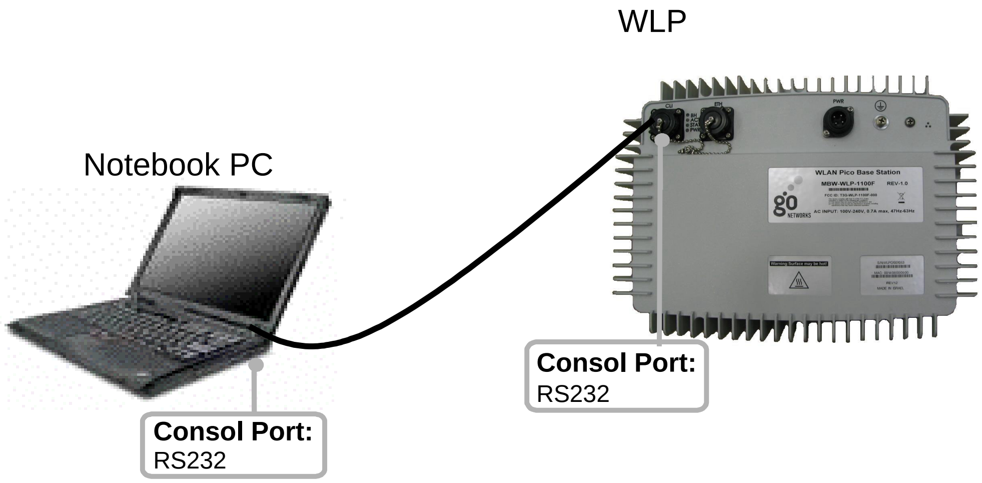


Figure 12: Connect and Access the WLP

Once the cable is connected, you can then operate a terminal program, such as HyperTerminal. The PC port should be configured as follows:

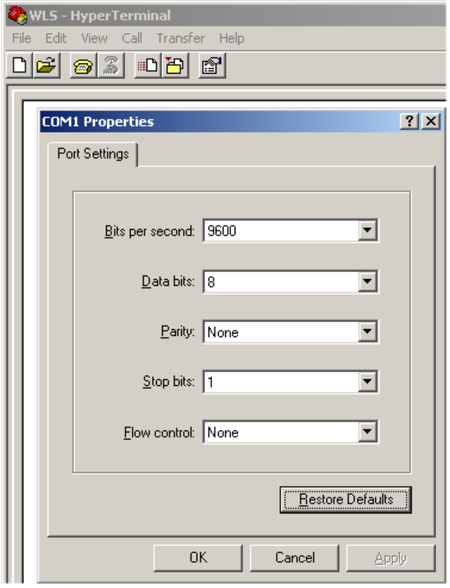
- Baud rate = 9600
- Data bits = 8
- Parity = none
- Stop bits = 1
- Flow control = None

Note: New laptops may not include an RS-232 serial port. If a serial port is not available, you may use a USB to serial converter.

To use HyperTerminal:

From the Start menu:

1. Select **All Programs > Accessories > Communications > HyperTerminal**.
2. Define a new connection.
3. Right-click and select **Properties**. Set or verify the above values.
4. Click **OK**.



Bits per second: 9600
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None

Figure 13: HyperTerminal Configuration

5. Establish the connection between the WLP and the laptop (or PC).
6. Log in using the predefined “super” user (user: super; password: super).

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 **go**.

Configuring the Management Connectivity

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

Assigning management IP and VLAN

Define the static IP address, subnet mask and the management VLAN on the same network through which you connect to the WLP. You can use the CLI command:

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

The default IP address is 192.168.0.10 with 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

specify:

```
configure ip vlan none 192.168.30.102 255.255.255.0
```

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

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
```

Default Gateway

Define the default gateway by using the Configure mode (consult with your network administrator). You can use the CLI command:

```
configure ip default-gateway {<ip ipaddress> | disable}
```

Example:

To define the default gateway, where:

Default Gateway IP Address = 192.168.30.254

specify:

```
configure ip default-gateway 192.168.30.254
```

Note: If you are using DHCP client on the first gateway, you do not need to configure the default gateway.

Configuring the Device Prompt

By default the device prompt is set to “go”. 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 WLP prompt can be defined using the following CLI command:

```
hostname set <prompt string>
```

Configuring the Radio Settings

Setting the Radio Frequency

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

```
configure interface {Dot11Radio | BHRadio} <interface number>
     channel <channel number>
```

Setting the Radio Data Rates

By default, the 802.11b/g channel is defined for use in a mixed mode. You can select a rate per channel for one of two states: g or mixed (a combination of g and b). The following CLI command syntax is used:

```
configure interface Dot11Radio <interface number>
     mode {g | mixed}
```

Setting the Radio Sensitivity

The range and capacity of the WLP device is 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/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 interface wifi-load-ratio
```

Figure 14 displays a printout of the wifi-load-radio command. In this example on the Dot11Radio 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 air time might be taken by neighboring networks. The remaining 6% (i.e. 15-8-1=6) is the amount of air time occupied by non-WLAN signals. These 6% are what we call noise.

```
go> show interface wifi-load-ratio
-------------------------------------------------------------------------------
|Interface Name      |Clear Count Ratio   |Rx Frame Count      |Tx Frame Count
|--------------------|--------------------|--------------------|---------------
|Dot11Radio0         |15                  |8                   |1
|....................|....................|....................|...............
|BHRadio0            |12                  |9                   |3
-------------------------------------------------------------------------------
go>
```

Figure 14: WiFi Load 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 15% 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 interface wifi-stats
```

The sensitivity could also be set manually to support local optimization by an operator. The sensitivity level can be set from –101dBm to –77dBm. The following CLI command sets a static sensitivity level:

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

Setting the Radio Reception Level

The Radio can be configured to reject clients that are below a defined signal level. By default, the Radio Reception Level is set to -103dBm. This results with all clients being accepted, as -103dBm is higher than the maximum sensitivity. The reception level can be set from –103dBm to -50dBm. Setting the reception level can be done using the following CLI command:

```
configure interface Dot11Radio <interface number>
     reception-level <level number>
```

Access Radio WDS Configuration

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

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

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 WLP unit 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. 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 GO-WLP1, GO-WLP2, and GO-HIDDEN, each with its own VLAN-ID, and no privacy.

```
go> /configure ssid 1 name GO-WLP1 vlan 0 privacy-method none
type bssid
go> /configure ssid 2 name GO-WLP2 vlan 100 privacy-method
none type bssid
go> /configure ssid 3 name GO-HIDDEN vlan 200 privacy-method
none type hidden
```

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

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

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:

```
go> configure interface dot11Radio 0 ssid remove 3
```

To delete an SSID:

```
go> configure ssid 3 remove
```

Configuring the Mesh Network

The WLP mesh network is based upon WDS (Wireless Distribution System) protocol. WDS is used to support wireless backhauling and meshing between WLP and CPE units. WDS supports backhauling over both the 2.4 GHz access radio and the 5 GHz backhaul radio.

The mesh topology is based on a tree structure as illustrated in Figure 15. At the top of each tree is a WLP unit that is functioning as a Mesh-Gateway, which is connected to the backbone network through its wired port. All other WLP units in the tree are functioning as Mesh-Nodes. Each Mesh-Node is wirelessly connected to a WLP 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 WLP units on the access radio.

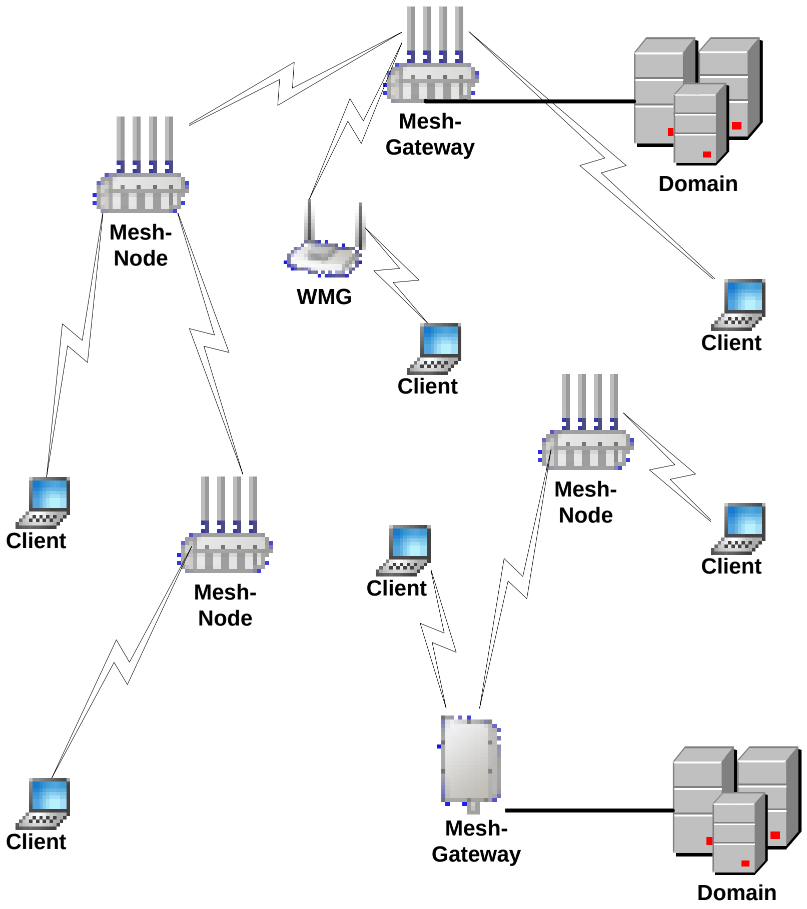


Figure 15: WDS Mesh Network

Mesh network routing is automatic, therefore when more then one route exists, the WLP 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 WLP unit connected to the wired LAN. All other WLP units are Mesh-Nodes and they depend on the WDS 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.

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. For more information on assigning a channel, see Configuring the 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 BHRadio interface is defined to participate in the mesh network.

Mesh Mode Configuration

All WLP units connected to the wired Ethernet must be configured as a Mesh-Gateway. To configure the WLP use the following CLI command:

configure mesh mode {gateway | node}

and specify:

```
configure mesh mode gateway
```

All WLP 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 WLP or WLS devices. To set the mesh mode accordingly, specify the following CLI command:

```
configure mesh mode node
```

Mesh Network Name

All WLP 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 WLP to participate in the mesh network. By default, the BHRadio interface is defined to participate in the mesh network. Only one interface on each WLP can be defined to participate at one time. All devices 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 | BHRadio} 0 enable
```

Note: To enable the Dot11Radio interface to participate in the mesh network, the service type must be properly configured for the interface. For more information, see Access Radio WDS Configuration.

Mesh Security

Configuring the Mesh privacy can protect the connections in the mesh network. All the WLP units in the network must be configured with the identical network name and privacy settings. The mesh network can use either WEP or AES encryption protocols.

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 of the WLP, 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 for the WLP, use the following CLI command:

```
show mesh route
```

Configuring WDS CPE connection

The WDS protocol can be used to connect with CPE devices. To configure the WDS connection manually, use the following CLI command:

```
configure interface {Dot11Radio | BHRadio} <interface number>
     wds-peer {add | remove} <address macaddress>
```

The MAC address is the MAC address of the CPE unit.

Note: Caution should be used when configuring the WDS connection manually. Improper configuration can result with network loops.

Example:

To connect to a CPE device manually, where:

Radio Interface = BHRadio
CPE MAC Address = 00:14:06:11:00:00

specify:

```
   configure interface BHRadio 0 wds-peer add
         00:14:06:11:00:00
```

Configuring Authentication Types

In the most common 802.1X WLAN environments, the WLP 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 WLP device 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 WLP.

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 in the WLP

Your WLP 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

WLP-to-Radius server communication 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 WLP can be configured by using the following command:

```
configure radius-server {primary | secondary}
     {authentication | accounting} <port  1 – 65535>
     host <ip address> key <secret 5 – 64 string> enable
```

Configuring Privacy Methods

The privacy (encryption) scheme is configured per ESSID.

Using WPA Key Management

WiFi 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).

WPA leverages 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 key management 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 WLP. Using WPA-PSK, however, you configure a pre-shared key on both the client and the WLP, and that pre-shared key is used as the PMK.

The WPA key management in the WLP can be configured using the following commands:

```
configure privacy wpa { <ssid integer(1-16)> [ passphrase
<passphrase string(8-63)> ] [ key-mngmnt { eap | psk } ]

configure privacy wpa gtk-interval <interval integer(30-
42949672)>

configure privacy wpa data-encryption { tkip | aes }

configure privacy wpa protocol { wpa1 | wpa2 | wpa2only }

configure privacy wpa preauthentication { enable | disable }
```

For example, configuring SSID 1 with a pass phrase of 12345678:

```
/configure privacy wpa 1 key-mngmnt psk passphrase 12345678
/configure privacy wpa protocol wpa1
/configure privacy wpa data-encryption tkip
/configure privacy wpa gtk-interval 72000
/configure privacy wpa preauthentication disable
```

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-configure startup-configure
```

WLP Configuration Example

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

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

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

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

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

#### mesh gateway configuration ####
go> /configure mesh mode gateway
go> /configure mesh network-id MyMeshNet
go> /configure mesh privacy AES passprash MyMeshKey

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

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

Upgrading the WLP Software

The WLP supports TFTP and URL software upgrades. 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 WLP 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 WLP can continue to function with its current image.

Obtaining a New Software Image

New software images can be downloaded from the GO Networks FTP site using the following connection information:

```
ftp://versions:ver2go@ftp.gonetworks.com
Username: versions
Password: ver2go
```

The software images are under the WLS directory. Note that the images are named WLS, as WLS and WLP devices are loaded with the same software 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

```
go>
go> /import image from tftp <ip address> <filename>
go> /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.

Acronym	Explanation
WLP	Wireless Base Station. Access point of the GO Networks MBW solution.
WLS	Wireless Base Station access point of the GO Networks MBW solution.
WMG	Wireless Media Gateway of the GO Networks MBW solution. GO Media dedicated CPE.
WNC	Wireless Network Controller of the GO Networks MBW solution.
WPA	WiFi 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 7: Console Port Signaling and Cabling with a DB-9 Adapter for the WLP Unit