

# Oxygen-3 User Guide



Model	Oxygen-3
Revision	Rev 1.9
Firmware	Rev 5.0

3066 Beta Avenue | Burnaby, B.C. | V5G 4K4  
Sales: 1.877.985.2878 \ 604.294.4465  
Support: 1.844.462.9773 \ 778.462.9773  
[support@cypress.bc.ca](mailto:support@cypress.bc.ca)

## Revision Control

Description	Revision	Date
Release Update	1.1	04-Mar-2015
Minor Update	1.2	23-Sep-2015
Update for firmware rev. 4.3	1.3	29-Sep-2015
Update for firmware rev. 4.4 - 4.5	1.4	18-Dec-2015
Update for firmware rev. 4.6 - 4.7	1.5	09-Jun-2016
Update for firmware rev. 4.8	1.6	11-Aug-2016
Added Chapter on WLAN	1.7	21-Sept-2016
Update for firmware rev. 4.9	1.8	09-Jan-2017
Update for firmware rev. 5.0	1.9	10-July-2017

## Contents

Revision Control .....	2
Contents .....	2
1 Legal Notices .....	6
1.1 Regulatory Restrictions .....	6
1.2 Electromagnetic Interference (EMI) – United States FCC Information.....	7
1.3 Electromagnetic Interference (EMI) – Canada Information .....	7
1.4 Li-Ion Battery.....	7
2 Specifications .....	8
2.1 Package Contents.....	8
2.2 General.....	8
2.3 Cellular Wireless .....	8
2.4 WLAN (Optional) .....	8
2.5 Ports .....	9
2.6 Processor and Memory .....	9
2.7 Power .....	9
2.7.1 Integrated Battery Operation .....	9
2.7.2 Power over Ethernet.....	10
2.8 Environmental.....	10
2.9 Physical Dimensions and Weight .....	10
2.10 Antennas .....	11

2.10.1	Cellular Antenna Specifications: .....	11
2.10.2	WLAN (Wi-Fi) Antenna Specifications:.....	11
3	Hardware Setup and Installation .....	12
3.1	Inserting the SIM card.....	12
3.2	Connector Overview .....	13
3.3	Installing the Antennas .....	13
3.4	Supplying the Oxygen-3 Wireless Gateway with Power .....	13
3.5	RS-232 Serial Port Installation.....	14
3.6	Physical Installation.....	14
4	Basic Operation.....	15
4.1	Power Up.....	15
4.2	LEDs.....	15
4.3	Logging into the Oxygen-3 Wireless Gateway .....	17
4.4	Changing and Saving the Configuration.....	17
4.5	Quick Start Configuration.....	18
5	Using the Web Interface .....	19
5.1	LAN Port page .....	19
5.1.1	Router Mode.....	19
5.1.2	Pass-Through Mode .....	20
5.1.2.1	Pass-Through Mode with static LAN Port IP Addresses.....	20
5.1.2.2	Pass-Through Mode with fully automatic IP assignment .....	22
5.1.1	VLAN Configuration.....	23
5.1.2	LAN Port Speed .....	24
5.1.3	Secondary IP Address.....	25
5.1.4	DNS Support.....	26
5.1.5	Customer Premise Equipment (CPE) Monitoring.....	27
5.2	WWAN Page.....	27
5.2.1	WWAN Connection Settings .....	27
5.2.2	PIN protected Accounts .....	28
5.2.3	Network Technology and WCDMA/LTE Band Selection .....	28
5.2.3.1	Band Selection from the Command Line .....	28
5.2.4	WWAN Connection Timeouts.....	29
5.2.5	Bandwidth Throttling.....	30
5.2.6	Routing Traffic Priority.....	30

5.2.7	Cellular Network Watchdog.....	31
5.3	WLAN Page (Optional - Only if Oxygen-3 Wireless Gateway supports WLAN) .....	32
5.3.1	WLAN Radio Configuration .....	32
5.3.2	WLAN Security Configuration .....	33
5.3.2.1	WLAN Radius Authentication.....	33
5.3.3	WLAN Network Settings.....	34
5.3.3.1	WLAN bridged to LAN Port, Router Mode .....	34
5.3.3.2	WLAN bridged to LAN Port, Pass-through Mode .....	35
5.3.3.3	No LAN/WLAN Bridging, Router Mode .....	36
5.3.3.4	No LAN/WLAN Bridging, Pass-Through Mode .....	37
5.4	Captive Portal.....	38
5.5	Access Control Page.....	41
5.6	Routing and SNAT/DNAT Page.....	42
5.6.1	Static Routes .....	42
5.6.2	SNAT/DNAT Setup.....	42
5.7	IPsec VPN Page.....	44
5.7.1	Dead Peer Detection .....	45
5.7.2	NAT Traversal .....	45
5.7.3	Secondary IPsec Peer .....	46
5.8	General Routing Encapsulation Tunnel Settings.....	47
5.9	Dynamic DNS.....	48
5.10	Name and Password .....	48
5.10.1	Hostname .....	48
5.10.2	Radius Authentication.....	49
5.10.3	Date and Time .....	49
5.11	Advanced Settings.....	51
5.11.1	Flash Upgrade .....	51
5.11.1.1	Upgrading using the HTTP Protocol .....	51
5.11.1.2	Upgrading using the TFTP Protocol.....	52
5.11.1.3	Upgrading from the Command Line Interface (TFTP, FTP) .....	52
5.11.2	Automatic Background Ping.....	54
5.11.3	Transparent TCP Proxy.....	54
5.11.4	Automatic Reversal to Failsafe Configuration.....	56

5.11.5	Manual Failsafe Configuration and Activation.....	56
5.11.6	Configuration Download .....	57
5.12	Event Logging .....	57
5.13	Traffic Counter .....	58
5.14	Cypress Cloud Manager .....	59
5.14.1	Basic Setup .....	60
5.14.2	CCM Server IP and Port Setup.....	61
5.15	SNMP Settings.....	61
5.15.1	Cypress Vendor MIB.....	61
5.15.2	SNMP Polling.....	62
5.15.3	SNMP Traps.....	62
6	Using the Command Line .....	64
6.1	Accessing the Command Line Interface .....	64
6.2	Changing Configuration (cfgtool).....	65
6.2.1	Overview .....	65
6.2.2	Determining and Configuring Parameter Names and Values .....	67
6.2.3	Examples .....	68
6.3	Packet Tracing (tcpdump) .....	70
6.4	Wireless Network Information (rssimon) .....	71
6.5	Ping.....	72
6.6	HPing.....	73
6.7	iPerf.....	74
6.8	Arp Cache.....	75
7	Using the RS-232 Serial Port .....	76
8	Understanding the Signal Quality Indicator (SQI).....	77
9	Troubleshooting.....	80
Contact	.....	81

# 1 Legal Notices

Due to the nature of wireless communication, the reception or transmission of data can never be guaranteed. Data may be delayed, corrupted or never received. Data transfer problems are rare with well-constructed and configured wireless networks used in conjunction with devices such as the Oxygen-3 Wireless Gateway.

Cypress Solutions Inc. accepts no responsibility for damages of any kind, including but not limited to personal injury, death, or loss of property due to the delay or loss of data resulting from the use of the Oxygen-3 Wireless Gateway.

## 1.1 Regulatory Restrictions

**CAUTION:** Any modifications to the Oxygen-3 Wireless Gateway not expressly authorized by Cypress Solutions Inc. may cause its regulatory approval status to become invalidated, thereby voiding your authority to use the product.

The Oxygen-3 Wireless Gateway contains a wireless device approved under FCC CFR 47 part 2.1091 and Industry Canada RSS-102 rules for operation as a mobile or fixed device. Maximum allowed antenna gain, including cable loss, is as follows:

### Oxygen-3

- 6.5 dBi in Cellular band
- 3.0 dBi in PCS band
- 3.0 dBi in LTE Band 2
- 6.0 dBi in LTE Band 4
- 6.5 dBi in LTE Band 5
- 9.0 dBi in LTE Band 13
- 9.0 dBi in LTE Band 17
- 3.0 dBi in LTE Band 25

### Oxygen-3 Plus

- 6.0 dBi in Cellular band
- 6.0 dBi in PCS band
- 6.0 dBi in LTE Band 1
- 6.0 dBi in LTE Band 2
- 6.0 dBi in LTE Band 3
- 6.0 dBi in LTE Band 4
- 6.0 dBi in LTE Band 5
- 9.0 dBi in LTE Band 7
- 6.0 dBi in LTE Band 8
- 6.0 dBi in LTE Band 12
- 6.0 dBi in LTE Band 13
- 6.0 dBi in LTE Band 20
- 6.0 dBi in LTE Band 25
- 6.0 dBi in LTE Band 26
- 1.0 dBi in LTE Band 30
- 9.0 dBi in LTE Band 41

Separation distance of at least 20 centimetres (eight inches) must be maintained from all persons at all times and during all modes of operation. The antenna used must not be co-located or operated in conjunction with any other antenna or transmitter. These rules are in place to prevent any possible hazard due to personal exposure to electromagnetic radiation.

## 1.2 Electromagnetic Interference (EMI) – United States FCC Information

This equipment has been tested and found to comply with limits for a class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. However, there is no guarantee that harmful interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

## 1.3 Electromagnetic Interference (EMI) – Canada Information

This digital apparatus does not exceed the class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled, “Digital Apparatus,” ICES-003 of the Department of Communications.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe B prescrites dans la norme sur le matériel brouilleur: “Appareils Numériques,” NMB-003 édictée par le Ministre des Communications.

## 1.4 Li-Ion Battery



The Oxygen-3 Wireless Gateway contains a rechargeable and non-removable Li-Ion battery. The Li-Ion battery should last for the life of the product and replacement can only be done at the factory. If, for any reason, the Li-Ion battery pack is being discarded, it must be disposed of in accordance with regulations for battery recycling in the region the device is being operated in.



**Li-ion**

The Li-Ion battery contained within the Oxygen-3 Wireless Gateway complies with UN/DOT 38.3 UN Transportation testing for Lithium Batteries.

## 2 Specifications

### 2.1 Package Contents

The Oxygen-3 Wireless Gateway ships with the following items:

- Oxygen-3 Wireless Gateway
- Rubberized mounting bracket
- Cat5e cable
- Cellular antennas (2)
- Power adaptor, 90-250VAC to 12VDC

### 2.2 General

- Input Voltage: 9-16 VDC with transient (spike) protection, 12-volt nominal
- Locking power connector
- Built-in 15Wh Li-Ion backup battery
- Current consumption: 300-400 mA @ 12V during regular operation, up to 1A when simultaneously charging the built-in battery
- Power over Ethernet (PoE PD – fully 802.3af compliant)

### 2.3 Cellular Wireless

	Oxygen-3	Oxygen-3 Plus
LTE	Category 3 (100 MBps)	Category 6 (300 MBps)
LTE Bands	2, 4, 5, 13, 17, 25	1, 2, 3, 4, 5, 7, 8, 12, 13, 20, 25, 26, 29, 30, 41
	not all bands are available with all carriers	
WCDMA	HSDPA (cat. 14), HSUPA (cat. 6), DC-HSPA (cat. 24)	
WCDMA Bands	I, II, IV, V, VIII	I, II, III, IV, V, VIII
GSM/GPRS/EDGE	Supported for 2G fallback when available	not supported

- On-board logic for always-on, always-connected operation
- Embedded radio design

### 2.4 WLAN (Optional)

- 2.4 GHz / 5 GHz dual band support
- Wi-Fi 802.11 b/g/n supported (Max. 150 Mbps)
- Access Point mode supporting up to 40 clients (stations)
- Independent WLAN network or bridged to LAN port
- Cellular to WLAN pass-through supported

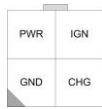


## 2.5 Ports

- 1x Fast Ethernet Auto MDI/MDIX (RJ45)
- 1x RS232 Serial Port (Molex P/N 0430-25-0400)
- USB 2.0 device support (Micro USB)
- 2x SMA Cellular RF Antenna ports: MIMO, Diversity
- 1x SMA Wi-Fi RF Antenna port (optional)
- Power Connector (Molex P/N: 39-30-1040)

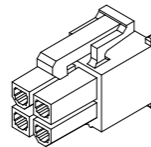
**Note:** The USB Port is not used unless Oxygen-3 Wireless Gateway is ordered for USB Mode of operation.

Power connector pin-out (mating connector P/N: Molex 39-01-2040):



(backside of Oxygen-3)

PWR Power  
GND Ground  
CHG Currently not used  
IGN Currently not used



Serial Port connector pin-out (mating connector P/N: Molex 430-25-0400):



(backside of Oxygen-3)

1, 2: GND  
3: TxD (outgoing data)  
4: RxD (incoming data)



## 2.6 Processor and Memory

	Oxygen 3	Oxygen-3 Plus
Processor	800 MHz Super Scalar ARM Cortex A8	1 GHz Super Scalar ARM Cortex A8
RAM	256 MB RAM	256 MB RAM
Flash	128 MB Flash	512 MB Flash
Firmware Upgrade	Dual Flash image technology avoids firmware corruption	Dual Flash image technology avoids firmware corruption

## 2.7 Power

### 2.7.1 Integrated Battery Operation

The Oxygen-3 Wireless Gateway has an integrated battery that can provide for 6-8 hours of power under normal operating conditions. Transitioning from AC or PoE power to running on battery is non-disruptive, with cellular connectivity and customer applications unaffected. This provides the following benefits:

- Initial placement and positioning of the unit to achieve the best RF conditions can be performed free of cabling restraints.
- The Oxygen-3 Wireless Gateway can be configured to send alerts via SNMP when the transition to battery power occurs, providing for immediate notification of AC power issues at a location. The Oxygen-3 Wireless Gateway can subsequently be queried for battery life, and further alerts can be sent based on remaining battery life.

### 2.7.2 Power over Ethernet

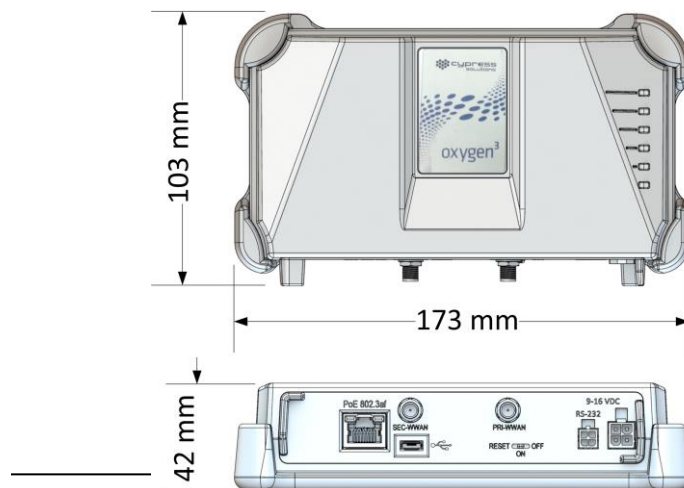
The Oxygen-3 Wireless Gateway's Ethernet port supports Power over Ethernet (PoE) and is fully 802.3af-compliant. The Oxygen-3 Wireless Gateway will act as a PoE PD ('Powered Device'), meaning that it will draw power from a PoE power source. This allows for flexibility in the installation process, specifically if the unit is located in an area where AC power may not be available.

## 2.8 Environmental

- Environmental MIL-STD-810G
  - Clause 501.5: Procedure II – High Temp (+75°C operational test)
  - Clause 502.5: Procedure II - Low Temp (-35°C operational test)
  - Clause 503.5: Procedure I-C - Thermal Shock (+75°C to -35°C operational test)
  - Clause 507.5: Procedure II - Humidity 95% RH operational test
- MIL-STD-810F:
  - Method 514.5C - Random Vibration freq. range 5-500 Hz, 0.008 g<sup>2</sup>/hz spectral density
  - Method 516-I - Shock - 40g, 11ms, Saw-tooth pulse shape, 3 axis operational test

## 2.9 Physical Dimensions and Weight

Dimensions	173 mm x 103 mm x 42 mm (L x W x H)
Weight	455 grams



## 2.10 Antennas

### 2.10.1 Cellular Antenna Specifications:

Frequencies	700/2100      694-960/1710-2170 MHz
Gain	3dBi peak
VSWR	2:1 max over range
Impedance	50 Ohm nominal
Maximum Power	5 Watt
Operating Temperature	-40°C to +85°C
Connector	SMA Plug (Male)



### 2.10.2 WLAN (Wi-Fi) Antenna Specifications:

Frequencies	Dual band: 2.4 – 2.5 GHz, 4.9 GHz – 5.825 GHz
Gain	2/4 dBi average
Radiation Pattern	Omni
Polarization	Linear Vertical
Impedance	50 Ohm nominal
Maximum Power	3 Watt
Operating Temperature	-30°C to +75°C
Connector	RP SMA



## 3 Hardware Setup and Installation

### 3.1 Inserting the SIM card



#### *Step 1 - Remove Mounting Bracket*

To gain access to the SIM card holder, first remove the black mounting bracket by bending the corner clasps on the connector side of the Oxygen-3 Wireless Gateway outwards.



#### *Step 2 – Remove SIM card cover*

Place the Oxygen-3 Wireless Gateway on a clean work surface with the bottom side up. Lift and remove the small cover door and place it aside.



#### *Step 3 - Insert SIM Card*

Slide the black SIM card holder lid towards the back to the unlock position; lift the SIM card holder door until it is flipped open.



Ensure the contact area of the SIM card is visible and that the chamfer corner (angled corner) of the SIM card is located as shown.



Close the black SIM card holder.

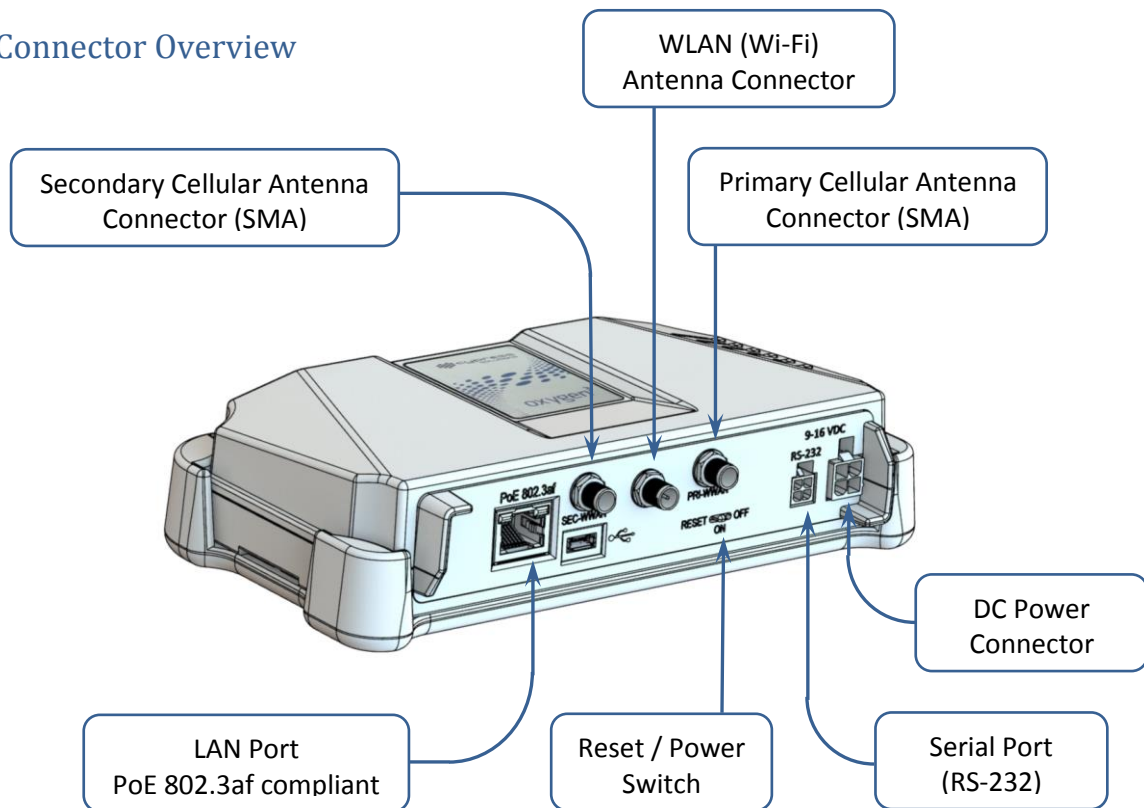
Press and slide the black SIM card holder lid forward until the lid locks into place.



#### *Step 4 - Reassemble Cover*

Place the cover door back onto the device.  
(Optional re-assembly of mounting bracket not shown)

### 3.2 Connector Overview



### 3.3 Installing the Antennas

Connect both antennas to the primary and secondary cellular SMA ports on the Oxygen-3 Wireless Gateway. These ports are labeled PRI-RF and SEC-RF. The antennas can be attached by turning the antenna thumb wheel in a clockwise direction until they are snug.



Do not tighten the antenna using any means other than normal thumb pressure. Turning the antennas independent of the thumb wheel may result in damage to the SMA jacks.

### 3.4 Supplying the Oxygen-3 Wireless Gateway with Power

The Oxygen-3 Wireless Gateway can run off three different power sources:

- The built-in battery (temporary only – the battery can typically supply power for 6-8 hours).
- DC power via the Molex locking power connector.
- PoE power via the Ethernet port from an 802.3af compliant power source.

Depending on your installation conditions, connect the supplied power adapter to the Oxygen-3 Wireless Gateway's power connector or connect to a PoE power source using an Ethernet cable.

### 3.5 RS-232 Serial Port Installation

The Oxygen-3 Wireless Gateway offers optional RS-232 connectivity. If your Gateway is equipped with a serial port, a serial cable can be used to connect the Oxygen-3 Wireless Gateway to the serial port of another device. Refer to section 2.5 for information regarding the pin-out of the Oxygen-3 Wireless Gateway's serial port.



Cypress Solutions offers a serial cable that provides direct connectivity with a Cisco® console port.

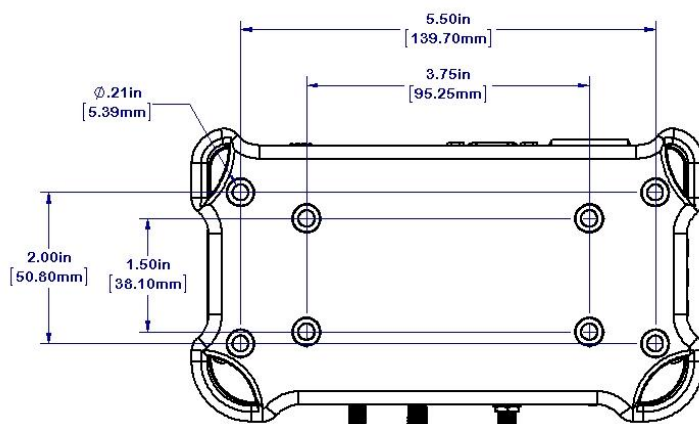
(Cypress P/N: 5115.2002)

### 3.6 Physical Installation

The Oxygen-3 Wireless Gateway ships with a rubberized mounting bracket attached. This bracket can be removed by bending the rubber clasps at the corners outwards.

The mounting bracket has eight holes to mount it securely to a flat surface. Cypress Solutions recommends using at least two mount points in diagonally opposite corners.

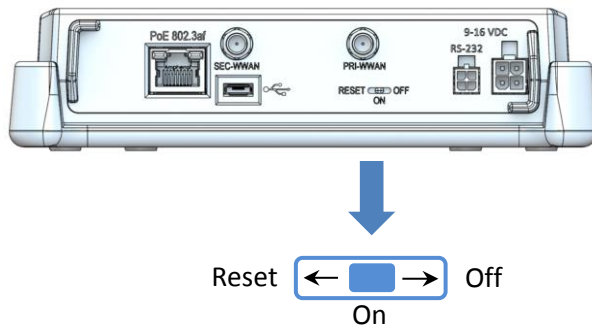
Use the drawing below for dimensions:



After the mounting bracket has been firmly installed, the Oxygen-3 Wireless Gateway can be inserted by bending the corner clasps outwards and slipping in the Oxygen-3 Wireless Gateway.

## 4 Basic Operation

### 4.1 Power Up



The Oxygen-3 Wireless Gateway has a small 3-way switch on the back panel which serves as a power and reset switch.

- When set to the 'Off' position, the Oxygen-3 Wireless Gateway is permanently off with only the integrated Real Time Clock (RTC) still being powered.
- When set to the 'On' position, the Oxygen-3 Wireless Gateway will power-up immediately when DC power or PoE power are applied. It will remain on and will continue to run off the built-in battery if DC power or PoE power are removed.
- Moving the switch to the temporary 'Reset' position will cause the Oxygen-3 Wireless Gateway to power-up using battery power, even if no DC or PoE power are applied. The switch is spring-loaded and will not remain in the 'Reset' position, but will automatically move back to the 'On' position.

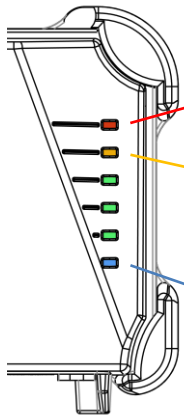
If moving the switch to the 'Reset' position fails to power-up the Oxygen-3 Wireless Gateway, then the built-in battery is likely fully discharged.

The reset switch is also used to revert the Oxygen-3 Wireless Gateway back to factory default configuration. See Section 7 for more information.

### 4.2 LEDs

The Oxygen-3 Wireless Gateway has six LEDs on its top panel:

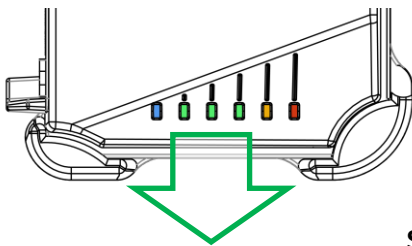
- 1x Power LED (blue)
- 3x Signal Strength LEDs (green)
- 1x Network Technology Indicator LED (orange)
- 1x Online Status LED (red)



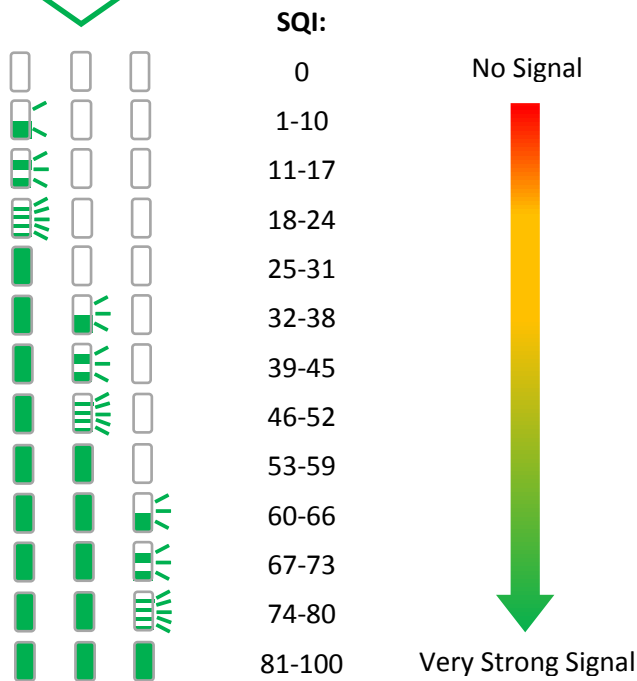
Online Status	On:	Online
	Rapid Flashing:	Attempting to Connect
	Flashing:	Disconnected
Network Type	On:	4G (LTE)
	Flashing:	3G (WCDMA)
	Off:	2G
Power	On:	Unit is turned on
	*Flashing:	Unit using battery power
	*Rapid Flashing:	Battery below 20%
	Off:	Unit is powered off

\*Oxygen-3 Plus only

The three signal quality LEDs will light up and/or flash in a distinct pattern to provide a granular reading of the current signal strength:



- Off
- On
- Slow Flashing
- Regular Flashing
- Rapid Flashing



Refer to Section 7 for more information on how to interpret the Signal Quality Index (SQI) value.



### 4.3 Logging into the Oxygen-3 Wireless Gateway

The Oxygen-3 Wireless Gateway can be configured via a web configuration interface. The primary method to access the configuration interface is by plugging a standard Ethernet cable into the LAN port of the Oxygen-3 Wireless Gateway.

By default, the Oxygen-3 Wireless Gateway will act as a DHCP server and provide the IP address **169.254.0.2/24** to a connected computer.

If your computer is not setup to obtain an IP address via DHCP, then you must configure your computer's LAN interface manually as follows:

IP Address: 169.254.0.2 - Network Mask: 255.255.255.0 - Gateway: 169.254.0.1

After plugging into the LAN port, the Oxygen-3 Wireless Gateway's web interface can be accessed at:

<http://169.254.0.1>

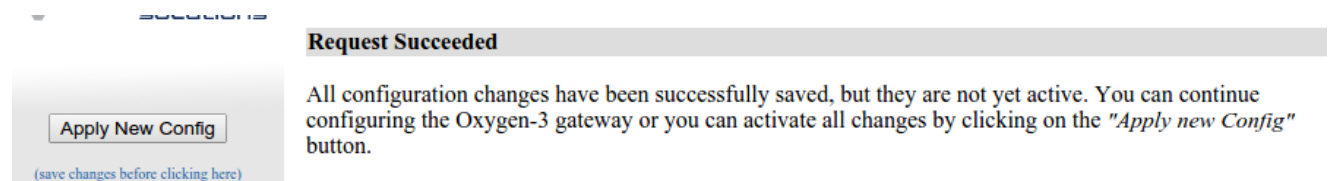
When logging into the web interface, the Oxygen-3 Wireless Gateway will show its status and overview screen. To access any of the configuration pages, a login and password are required. The default login and password for the Oxygen wireless gateway are:

Login: admin  
Password: cypress

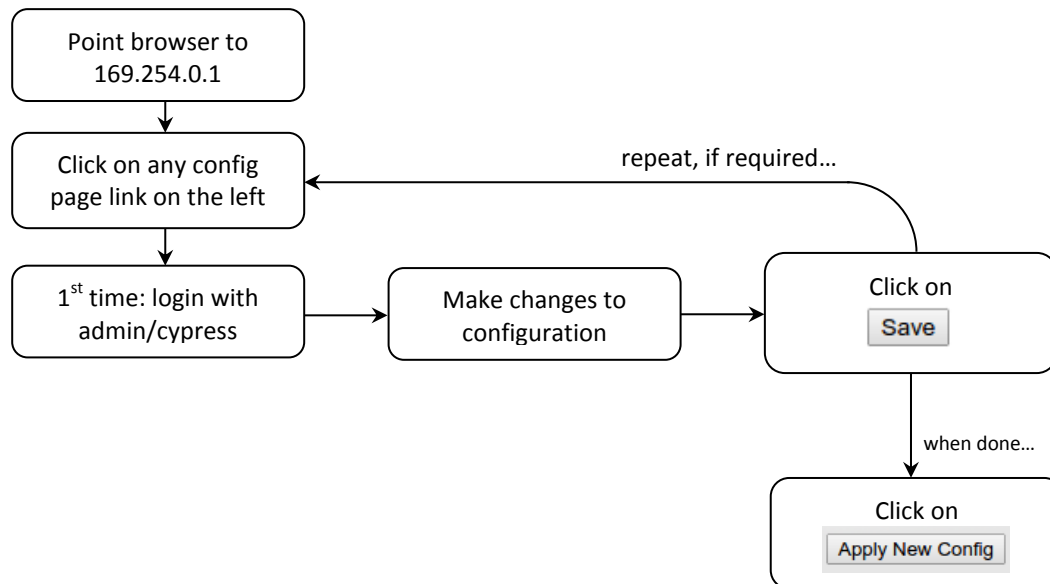
### 4.4 Changing and Saving the Configuration

The Oxygen-3 Wireless Gateway's web interface is designed so that configuration changes can be made and temporarily saved on any of the configuration pages without having to wait for the device to apply those changes.

Once all desired configuration changes have been made, they can be permanently saved and applied by clicking on the 'Apply New Config' at the top left corner of the web interface:



A typical configuration session looks as follows:



**Note:**

Clicking on 'Save' only saves configuration changes temporarily and will not yet apply them. Without clicking on 'Apply New Config' at the end of the configuration session, all changes will be lost after a reboot.

## 4.5 Quick Start Configuration

The Oxygen-3 Wireless Gateway ships with its default configuration set to 'Automatic Pass-Through.' After inserting a SIM (see Section 3.1), only one more step is required to obtain basic connectivity:

- Click on the 'WWAN' link on the left side of the Oxygen-3 Wireless Gateways web interface.
- Enter the APN as required by your carrier.

### WWAN Setup:

Access Point Name (APN):  
(required)

User Name:

- Click on 'Save', then click on 'Apply New Config.'

The Oxygen-3 Wireless Gateway should now successfully connect to the wireless network and the 'Online' LED should light up red after a short time (refer to section 4.2 for more information).

If your computer is setup to obtain its IP address via DHCP, it should renew its DHCP lease and obtain an IP address provided by your wireless carrier. For more information on the default 'Automatic Pass-Through' mode, refer to Section 5.1.2.2.

## 5 Using the Web Interface

### 5.1 LAN Port page

#### 5.1.1 Router Mode

The Oxygen-3 Wireless Gateway can operate in two fundamental **Modes of Operation**: 'Router Mode' and 'Pass-Through Mode'. To select the desired Mode of Operation, go to the 'LAN Port' configuration page within the web configuration interface.

##### LAN Setup:

Mode of Operation:

(see description above)

LAN Port IP Address and Mask:

(not required when using automatic Pass-Through)

Enable DHCP Server on LAN Port:

(required for automatic Pass-Through mode)

In Router Mode, the Oxygen-3 Wireless Gateway will obtain an IP address from the wireless carrier. Additional devices can connect via the LAN port by using network address translation (NAT) and/or IPsec tunneling.

##### LAN Setup:

Mode of Operation:

(see description above)

LAN Port IP Address and Mask:

(not required when using automatic Pass-Through)

Enable DHCP Server on LAN Port:

(required for automatic Pass-Through mode)

DHCP IP Range Start:

(lowest IP address assigned - Router mode only)

DHCP IP Range End:

(highest IP address assigned - Router mode only)

DHCP Lease Time:

(consider using 2m when in pass-through mode)

Enable NAT on LAN Port:

(not possible in Pass-Through modes)

NAT Scope:

(which source IPs should be NAT'ed)

Link-down Time when IP Changes:

(Pass-Through: to prompt DHCP client to re-acquire IP Address)

LAN Port Speed:

Router, use with NAT and/or IPsec

10.1.1.1 / 24

10.1.1.10

10.1.1.10

1h

LAN network only

3

Negotiate Automatically

IP addresses can be statically assigned to connected devices or they can be automatically assigned using DHCP. If using DHCP, the **Enable DHCP Server on LAN Port** checkbox must be checked, and a range of valid addresses must be specified in the **DHCP IP Range Start** and **DHCP IP Range End** fields.

If IPsec is required by the application, it is mandatory that the Mode of Operation be set to Router Mode. IPsec will not operate in Pass-Through Mode.

Network Address Translation (NAT) can be turned on or off by selecting or deselecting the **Enable NAT on LAN Port** checkbox.

If IPsec is *NOT* being used, enabling NAT will translate all source IP addresses for traffic outbound on the cellular interface (wwan0) to the IP address assigned by the carrier network when the modem is connected to the network successfully. Inbound traffic to the Oxygen-3 Wireless Gateway from the cellular network will not be passed to the LAN network unless an *established* session was previously initiated by a LAN-connected device.

If IPsec is being used, enabling NAT will translate all source IP addresses for outbound traffic on the cellular interface (wwan0) to the IP address assigned by the carrier network when the modem is connected to the network successfully, unless the destination IP address of the packet matches the destination private network of a defined IPsec tunnel. This is commonly referred to as Split Tunneling.

**Link-down Time when IP Changes** is not applicable in this mode.

## 5.1.2 Pass-Through Mode

In Pass-Through Mode, the IP address assigned by your carrier will be passed on to another device connected to the Oxygen-3 Wireless Gateway on the Ethernet port.

Since the connected device will assume the IP address assigned by your carrier, that IP address is no longer available for any of the Oxygen's interfaces: neither the internal cellular interface nor the Oxygen-3 Wireless Gateway's LAN interface.

However, it is required for the LAN interface to have an IP address and network mask so that it forms a valid IP network. This includes the IP address provided by your carrier which has been assigned to the connected device.

Even though in this mode packets generally just pass through the Oxygen-3 Wireless Gateway, you can still access this gateway over the cellular WWAN interface for configuration and monitoring by setting up access rules on the 'Access Control' screen. This allows for all inbound traffic to "pass-through" the Oxygen-3 Wireless Gateway to the connected Ethernet device, except for traffic on specified management ports. This is also referred to as "pin-hole" management.

### 5.1.2.1 Pass-Through Mode with static LAN Port IP Addresses

In this mode, the Oxygen-3 Wireless Gateway's LAN port will assume a static IP address and network mask.

The IP address of the connected device (which must be the IP address provided by your cellular carrier) can either be configured statically on the connected device, or the Oxygen-3 Wireless Gateway can assign this address to the connected device using DHCP.

In both cases, the IP address and network mask of the LAN port can be arbitrarily chosen, however the IP network created by the LAN address and mask must include the IP address of the connected device.

### Example 1:

If the wireless carrier assigns a static IP address to your SIM of *74.198.154.37*, this address would be configured on the connected device. Then, an arbitrary network mask and IP address for the Oxygen-3 Wireless Gateway's LAN port would need to be identified. In this case, using an IP subnet calculator and smallest possible mask, the Oxygen's LAN port can be configured for *74.198.154.38*, with a 30-bit subnet mask.

**Subnet Calculator**

Network Class: A  B  C

IP Address: 74.198.154.37

Subnet Mask: 255.255.255.252

Subnet Bits: 22

Maximum Subnets: 4194304

Host Address Range: 74.198.154.37 - 74.198.154.38

Subnet ID: 74.198.154.36

Subnet Bitmap: 0nnnnnnn.ssssssss.ssssssss.sssssshh

First Octet Range: 1 - 126

Hex IP Address: 4A.C6.9A.25

Wildcard Mask: 0.0.0.3

Mask Bits: 30

Hosts per Subnet: 2

Broadcast Address: 74.198.154.39

### LAN Setup:

#### Mode of Operation:

(see description above)

#### LAN Port IP Address and Mask:

(not required when using automatic Pass-Through)

#### Enable DHCP Server on LAN Port:

(required for automatic Pass-Through mode)

#### DHCP IP Range Start:

(lowest IP address assigned - Router mode only)

#### DHCP IP Range End:

(highest IP address assigned - Router mode only)

#### Enable NAT on LAN Port:

(not possible in Pass-Through modes)

#### Link-down Time when IP Changes:

(Pass-Through: to prompt DHCP client to re-acquire IP Address)

#### LAN Port Speed:

Pass-Through, static LAN IP

74.198.154.38 / 30

3

Negotiate Automatically

In the above example, the Oxygen-3 Wireless Gateway's LAN port is configured as *74.198.154.38/30*, while the connected device is configured with the real wireless carrier IP of *74.198.154.37/30*.

Since the IP address of the connected device is configured manually, the **Enable DHCP Server on LAN Port** option can be left unchecked.

### Example 2:

Using a custom APN, your wireless carrier assigns a dynamic IP address, however it is known that this IP address will always be part of the *22.33.44.0/24* network. The custom APN is also set up in a way so that the address *22.33.44.1* will never be assigned.

This makes it possible to configure the Oxygen-3 Wireless Gateway's LAN port statically and use DHCP to assign the carrier-provided IP address to the connected device.

In this case the Oxygen-3 Wireless Gateway's LAN port IP address and network mask would be set to *22.33.44.1/24* and DHCP would be enabled. Since the Oxygen-3 Wireless Gateway will always assign the carrier-provided IP address to the connected device, it is not required to enter anything in the ***DHCP IP Range Start and DHCP IP Range End*** fields.

#### 5.1.2.2 Pass-Through Mode with fully automatic IP assignment

This option will automatically assign the correct carrier-provided IP address to the connected device and will also configure the Oxygen-3 Wireless Gateway's LAN interface using a suitable IP address and subnet.

This option requires that DHCP be enabled on the Oxygen-3 Wireless Gateway in order to function correctly.

The connected device must also be set to use DHCP to obtain an IP address, mask, and gateway from the Oxygen-3 Wireless Gateway in order for this mode to work correctly.

Upon connecting to the cellular network, the Oxygen-3 Wireless Gateway receives an IP address from the carrier. The Gateway will then, based on received IP address, determine the smallest possible subnet mask and IP address for its Ethernet port.

The connected device running DHCP will receive the IP address provided by the carrier as well as a matching network mask and gateway IP address from the Oxygen-3 Wireless Gateway.

#### **Note:**

If your wireless carrier assigns dynamic IP addresses, the IP address received by the Oxygen-3 Wireless Gateway may change upon each connection attempt. However, the DHCP protocol, which is used by the connected device to obtain the IP address, contains no method for the DHCP host (the Oxygen-3 Wireless Gateway) to inform the client (the connected device) that an IP address change has occurred.

Instead, the Oxygen-3 Wireless Gateway will turn off the carrier ('bringing the link down') on the local Ethernet segment for a configurable amount of time to encourage the connected device to release its current IP address and obtain a new one.

For most connected devices, the default link-down time of three seconds is sufficient, however some devices may require a longer time which can be configured using the ***Link-down Time when IP Changes*** option.

A small number of devices may not react to a link-down event at all - some Cisco routers with pre 15.x IOS firmware are known to behave this way. Unfortunately, those devices will never reliably work with dynamic IP addresses in Pass-Through mode.

Since the Oxygen-3 Wireless Gateway will always assign the carrier-provided IP address to the connected device, it is not required to enter anything in the ***DHCP IP Range Start and DHCP IP Range End*** fields.

### 5.1.1 VLAN Configuration

#### **Terminology Alert:**

There are a number terms to describe untagged Ethernet frames, all of which essentially refer to the same thing. For the purposes of this document we will refer to them as 'untagged' frames:

- untagged traffic
- native VLAN traffic
- traffic for the PVID
- access VLAN traffic

With its default configuration the Oxygen-3 sends and receives untagged Ethernet frames on its Ethernet port.

The Oxygen-3 can be configured to support up to four (4) additional VLANs. These four additional VLANs are distinguished from the untagged VLAN by the use of tags (also referred to as VLAN tags, VLAN headers, DOT1Q tags/headers).

- The Oxygen-3 supports IEEE 802.1Q VLAN tags (it does not support ISL)
- The Oxygen-3 does not provide inter-VLAN routing for the traffic on the Ethernet port; if inter-VLAN routing is required for a given location another device will have to perform that function

To enable and configure VLAN functionality, click on the "[click here]" link on the main "LAN Port" configuration page.

#### **LAN Setup:**

Mode of Operation:  
(see description above)

Router, use with NAT and/or IPsec ▾

LAN Port IP Address and Mask:  
(not required when using automatic Pass-Through)

10.1.1.1 /24

VLAN Configuration:

[\[click here\]](#)

Enable DHCP Server on LAN Port:

The "VLAN Settings" page that appears consists of five sections. To enable VLAN functionality, tick the "Enable VLAN Trunking on the LAN Port:" box in the top section. If you do not tick this box, all other settings on this page are ignored.

#### **VLAN Settings:**

Enable VLAN Trunking on LAN Port:

Enable Hybrid Mode:

(Simultaneous support for tagged and untagged traffic)

The other setting in the top section, "Enable Hybrid Mode" enables or disables the Oxygen-3's Ethernet interface from sending or receiving traffic without a VLAN tag. Allowing untagged frames when the Ethernet interface is also sending and receiving tagged frames can, in some situations, lead to security issues; consider your network environment when changing this option. If "Enable Hybrid Mode" is not selected, the IP address settings on the main "LAN Port" configuration page (IP address, DHCP, NAT, and secondary IP address) will be ignored since these relate to untagged traffic.

The remaining four sections are nearly identical; each allows you to configure the options for one additional VLAN.

---

Enable VLAN Network #1:	<input checked="" type="checkbox"/>
VLAN IP Address and Mask:	<input type="text" value="10.1.2.1"/> / <input type="text" value="24"/>
VLAN ID:	<input type="text" value="2"/>
Enable DHCP Server on VLAN:	<input checked="" type="checkbox"/>
VLAN DHCP IP Range Start:	<input type="text" value="10.1.2.100"/>
VLAN DHCP IP Range End:	<input type="text" value="10.1.2.199"/>
Enable NAT for VLAN:	<input checked="" type="checkbox"/>

---

To enable an additional VLAN, you must tick the appropriate "Enable VLAN Network..." box otherwise all the remaining settings in that section will be ignored. The IP address, network mask, DHCP Server options, and NAT have the same function as was explained in section 5.1.1

When choosing a VLAN ID, keep the following in mind:

- VLAN IDs must be unique. This should be obvious but each interface can only have one instance of a particular VLAN.
- The VLANs you configure must match the settings on the device connected to the Oxygen-3 otherwise there will not be communication for that VLAN
- VLAN 0 is reserved or not usable
- VLAN 1 is reserved. It is usually used for the untagged (native, or PVID) VLAN, so do not use it for one of the Oxygen-3's additional VLANs as this will cause a conflict.
- Some network devices (Cisco) use VLANs 1002 to 1005 for 'special' purposes; if your Oxygen-3 is connecting to a network with Cisco devices in it, avoid these VLANs
- VLAN 4095 is also reserved.

## 5.1.2 LAN Port Speed

The Oxygen-3 Wireless Gateway's **LAN Port Speed** settings can be automatically negotiated, or fixed for specific speed and duplex settings as per requirements. Settings are applied using a pull-down menu.

LAN Port Speed:	<input type="text" value="Negotiate Automatically"/>
Enable Secondary IP Address for LAN Port: <small>(static IP - useful for monitoring or configuration)</small>	<div style="border: 1px solid black; padding: 2px;"> <p>Negotiate Automatically ▾</p> <p style="background-color: #f0f0f0;">Negotiate Automatically</p> <p>100Mb/s - full duplex</p> <p>100Mb/s - half duplex</p> <p>10Mb/s - full duplex</p> <p>10Mb/s - half duplex</p> </div>

When selecting a fixed LAN Port speed, make sure it matches that of the connected device otherwise no communication is possible.

**Note:** The Oxygen-3 Plus also supports 1Gb/s Ethernet Port Speed



### 5.1.3 Secondary IP Address

The Oxygen-3 Wireless Gateway also has support for a secondary static IP address on the LAN port. This option is useful when the connected device (a Cisco router, for example) has the capability of supporting a secondary IP address on the same physical port.

Even though the Oxygen-3 Wireless Gateway supports management over the wireless network, it can be desirable to manage the Gateway via the Ethernet port. This maybe particularly true in cases where the wireless carrier provides a dynamic (and therefore changing) IP address. However, even with static carrier-provided IP addresses, using the Oxygen-3 Wireless Gateway's Ethernet port for management avoids additional data usage charges on cellular subscriptions, and can therefore be advantageous.

By default, the Oxygen-3 Wireless Gateway has a secondary IP network of 169.254.0.1/24 enabled on its LAN port:

**Enable Secondary IP Address for LAN Port:**

(static IP - useful for monitoring or configuration)



**Secondary LAN Port IP Address and Mask:**

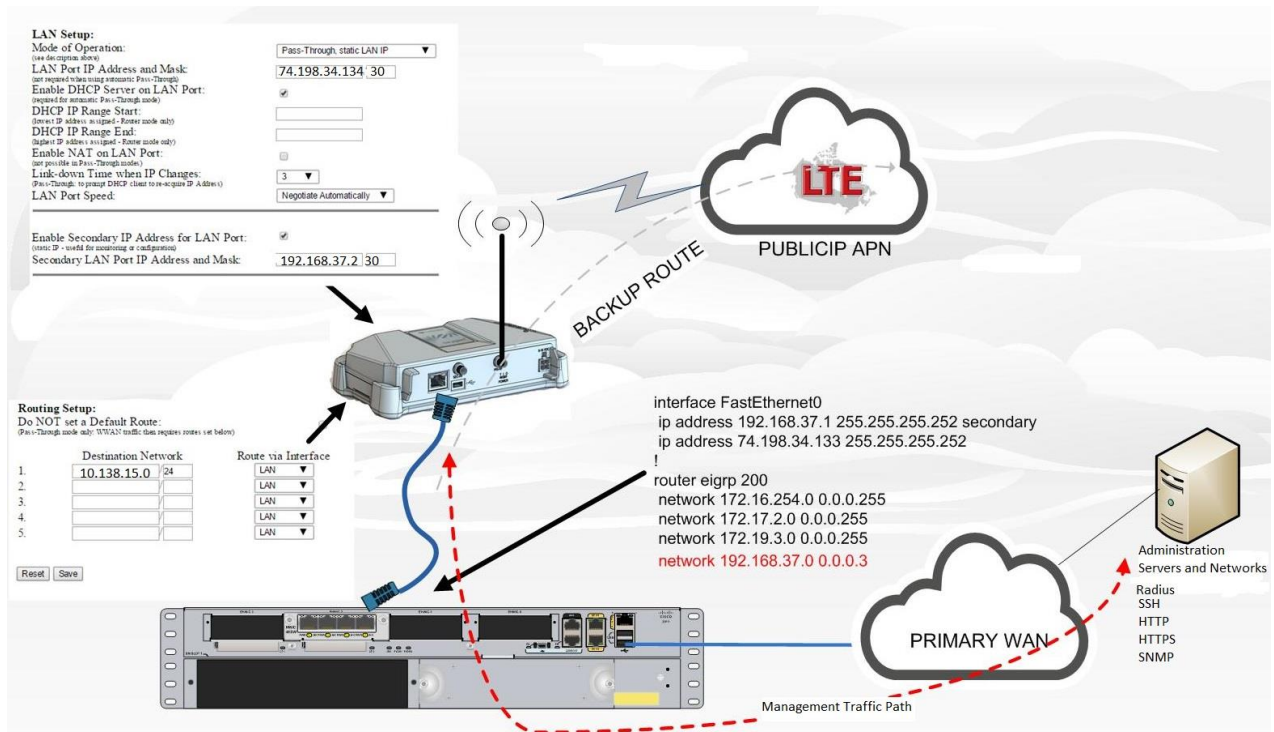
169.254.0.1 / 24

It is important to note that the Oxygen-3 Wireless Gateway's default route is the internal wireless interface. When accessing the Gateway via the Ethernet interface for management purposes, routes may have to be established to return traffic via the Ethernet port to the management server(s). This can be achieved using the Routing configuration screen.

#### **Example:**

The example below shows an Oxygen-3 Wireless Gateway configured with secondary IP implementation in a Cisco router network:

- The Oxygen-3 Wireless Gateway operates in Pass-Through mode, and has obtained a public static IP address from the cellular carrier.
- A secondary IP network has been configured on the Oxygen-3 Wireless Gateway, as well as on the cisco router. The secondary IP network has been added to the cisco routing process, advertising the subnet to distant downstream networks and routers.
- The Oxygen-3 Wireless Gateway has been configured to route all traffic from the 192.168.37.0/24 network via the Ethernet port, keeping this traffic away from the cellular network.



### 5.1.4 DNS Support

The Oxygen-3 Wireless Gateway can be set up to use up to two static DNS servers or it can be configured to use the DNS server(s) provided by your wireless carriers. Alternatively, DNS can also be disabled altogether.

DNS settings configured on the LAN Port page apply to connections originating from the Oxygen-3 Wireless Gateway and they will also be provided to any connected device that uses DHCP if enabled.

DNS Mode:

DNS IP Address #1:

(only when configured manually)

DNS IP Address #2:

#### Note:

Changes made to the DNS settings here will not automatically propagate to attached devices that use DHCP to obtain their DNS settings. It is required to either wait until the attached device renews its DHCP lease or to manually initiate a DHCP lease renewal on the attached device.

### 5.1.5 Customer Premise Equipment (CPE) Monitoring

The Oxygen-3 Wireless Gateway can monitor CPE devices connected to the Ethernet port using ICMP echo requests. The Gateway will monitor for ICMP echo replies, and consider the connected device 'up' when replies are received. If/when the device connected behind the Oxygen-3 Wireless Gateway stops responding to ICMP packets, an outbound SNMP trap can be transmitted to notify parties monitoring the equipment.

CPE monitoring works with all modes of operation. When configured for Router Mode, it is mandatory to configure the **IP Address to Monitor** field. In Pass-Through Mode, the Oxygen-3 Wireless Gateway will always monitor the IP address provided by your carrier and the **IP Address to Monitor** field can be left empty.

Enable Monitoring of CPE on LAN:   
(pings Customer Premise Equipment)

IP Address to Monitor:   
(not required in Pass-Through modes)

## 5.2 WWAN Page

### 5.2.1 WWAN Connection Settings

To successfully connect the Oxygen-3 Wireless Gateway to a cellular network of your choice, an access point name (APN) must be entered into the gateway. Your wireless carrier will provide this APN at the time your SIM card is activated.

Some carriers may also need a unique login and password in addition to the APN name in order to gain access to the wireless network, even though this has become increasingly uncommon.

**WWAN Setup:**

Access Point Name (APN):   
(required)

User Name:   
(Usually not required)

Password:   
(Usually not required)

SIM Pin:   
(Leave empty if no PIN is set)

Authentication Method:

Network Type Selection:

Use WCDMA Band(s):

Use LTE Band(s):

Less Aggressive Dialing:

Maximum Connection Time:

Idle Disconnect Timer:

In addition to providing a username and/or password, it may also be necessary to specify the authentication method as 'PAP' or 'CHAP.' Again, this has become increasingly uncommon and in almost all cases this configuration option can be left unchanged.

### 5.2.2 PIN protected Accounts

If the SIM card is protected by a PIN, enter it here. The Oxygen-3 Wireless Gateway will apply this PIN to unlock the SIM card.



The Oxygen-3 Wireless Gateway will only attempt to 'enter' the PIN once to avoid locking the SIM due to too many failed PIN entries. However, after each power-cycle, it will perform another SIM entry. If you enter the incorrect SIM, check the system log for more information.

It is not possible to *change, set or remove* a SIM PIN using the Oxygen-3 Wireless Gateway. These operations must be performed on another device, such as a phone, etc.

### 5.2.3 Network Technology and WCDMA/LTE Band Selection

In some cases, it may be necessary to restrict the Oxygen-3 Wireless Gateway's wireless module to a certain network technology (2G, 3G, 4G or a combination thereof) or to force the exclusive usage of a certain WCDMA (3G) or LTE (4G) band:

Use LTE (4G) Bands:

B2 1900 MHz	B4 1700 MHz	B5 850 MHz	B13 700 MHz	B17 700 MHz	B25 1900 MHz
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Use WCDMA (3G) Bands:

B1 2100 MHz	B2 1900 MHz	B4 1700 MHz	B5 850 MHz	B8 900 MHz
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Enable 2G Bands:



Depending on the cellular module installed in the Oxygen-3 modem, there may be more or less bands that can be selected – the module used in the example above is the MC7354.

When the Oxygen-3 Wireless Gateway is configured to use certain WCDMA or LTE band(s), the following rules apply:

- By default, all available bands will be checked which means that the best available band will be chosen
- If only certain bands are checked, then the unchecked bands will not be able to be utilized
  - LTE (4G) bands take the highest priority followed by WCDMA (3G) and finally 2G

#### 5.2.3.1 Band Selection from the Command Line

The same configuration changes described in the previous section can be made via the command line as well. Please refer to section 6.2 for more information on how to use the 'cfgtool' command:

**Use WCDMA Band(s):**

<code>cfgtool -w WWAN_3G_BAND_MASK "0x136"</code>	All Available
<code>cfgtool -w WWAN_3G_BAND_MASK "0x2"</code>	B1 (2100 MHz, IMT)
<code>cfgtool -w WWAN_3G_BAND_MASK "0x4"</code>	B2 (1900 MHz, PCS)
<code>cfgtool -w WWAN_3G_BAND_MASK "0x10"</code>	B4 (1700 MHz, AWS)
<code>cfgtool -w WWAN_3G_BAND_MASK "0x20"</code>	B5 (850MHz, Cellular)
<code>cfgtool -w WWAN_3G_BAND_MASK "0x100"</code>	B8 (900 MHz, EGSM)

**Use LTE Band(s):**

<code>cfgtool -w WWAN_LTE_BAND_MASK "0x2022034"</code>	All Available
<code>cfgtool -w WWAN_LTE_BAND_MASK "0x4"</code>	B2 (1900 MHz, PCS)
<code>cfgtool -w WWAN_LTE_BAND_MASK "0x10"</code>	B4 (1700 MHz, AWS)
<code>cfgtool -w WWAN_LTE_BAND_MASK "0x20"</code>	B5 (850MHz, Cellular)
<code>cfgtool -w WWAN_LTE_BAND_MASK "0x2000"</code>	B13 (700 MHz, Upper SMH block C)
<code>cfgtool -w WWAN_LTE_BAND_MASK "0x20000"</code>	B17 (700 MHz, Lower SMH blocks B/C)
<code>cfgtool -w WWAN_LTE_BAND_MASK "0x2000000"</code>	B25 (1900 MHz, Extended PCS)

In the above `cfgtool` commands, pay particular attention to the values after the “x” – if you add the values after the “x” then the command can include a combination of multiple bands. For example, if we want to lock the Oxygen 3 to use only the LTE band B2, we would use the following command:

```
cfgtool -w WWAN_LTE_BAND_MASK "0x4"
```

To use LTE band B2 and LTE band B5 **both** at the same time, the two values for the respective bands have to be added together and the sum needs to be used to determine the command parameter to enter:

```
cfgtool -w WWAN_LTE_BAND_MASK "0x24"
```

Note how the command above is the sum of `0x4`(LTE-B2) and `0x20`(LTE-B5).

## 5.2.4 WWAN Connection Timeouts

**Less Aggressive Dialing** is required for certain networks and is recommended on Rogers Wireless in Canada, Verizon Wireless in the United States, as well as all Jasper Control Center-based carriers. Enabling this option will increase the delay between unsuccessful connection attempts.

**Maximum Connection Time** sets the unit to automatically disconnect from the network based on a time interval. In case of network instability, this can be used to restart the connection after a certain amount of time.

Maximum Connection Time:  
Idle Disconnect Timer:

Unlimited ▾

Unlimited

1h

2h

3h

6h

12h

24h

2 days

3 days

4 days

5 days

6 days

7 days

Enabling the **Idle Disconnect Timer** forces the Oxygen-3 Wireless Gateway to disconnect after a configurable period of no bidirectional traffic was detected on the wireless interface. Since this presents another mechanism to recover from potential network problems, it is recommended to leave this option enabled.

Maximum Connection Time:

Unlimited ▾

Idle Disconnect Timer:

6h ▾

Never  
1min  
2min  
3min  
5min  
10min  
15min  
30min  
45min  
1h  
2h  
3h  
6h  
12h

### 5.2.5 Bandwidth Throttling

The Oxygen-3 Wireless Gateway supports Bandwidth Throttling on the cellular interface. This can be desirable to prevent the transmission of excessive data volumes.

**Downlink Throughput Limit:**

(in kbit/sec, leave empty for unlimited throughput)

**Uplink Throughput Limit:**

(in kbit/sec, leave empty for unlimited throughput)

Upload and download limits are configurable for both directions in kilobits per second. If no value is entered, throttling will be disabled in the respective direction (downlink and/or uplink).

### 5.2.6 Routing Traffic Priority

Prioritization of traffic is part of the larger topic of QoS (Quality of Service) and/or CoS (Class of Service). The labels QoS and CoS are usually used interchangeably; while there is a distinction between the two, it has in general been lost.

QoS/CoS adheres to the adage that "a chain is only as strong as its weakest link." For certain traffic to get 'true' prioritization, a mechanism to provide and maintain this prioritization has to exist at every point in the network. If it exists in only one location, the traffic is prioritized there but not at other points and therefore any advantage gained at that one location may be lost at another. Providing prioritization for Routing Protocol traffic on the Oxygen-3's cellular (WWAN0) interface may ensure that it reaches the cellular network but once there, there is no mechanism to ensure that it continues to get preferential treatment.

The Oxygen-3 Wireless Gateway can be configured to prioritize the transmission of routing protocol traffic on the cellular (WWAN0) interface.

The "Routing Traffic has Priority" feature is only for traffic leaving the Oxygen-3 gateway going towards the cellular network. In order for this feature to have any effect, the "Uplink Throughput Limit" must also be set. Further, the "Uplink Throughput Limit" must be set to a value that is at the lower end of the expected cellular uplink capacity; further, this expected cellular uplink capacity may change over time.

The Routing Traffic that is to receive priority handling must already have the TOS field in the header of the IP packet set to DSCP CS6 or to DSCP CS7. Most devices that participate in a routing protocol set the TOS field to DSCP CS6.

(in kbit/sec, leave empty for unlimited throughput)

**Uplink Throughput Limit:**

(in kbit/sec, leave empty for unlimited throughput)

**Routing Traffic has Priority:**

(Requires Uplink Limit to work reliably)



## 5.2.7 Cellular Network Watchdog

The Oxygen-3 Wireless Gateway has a built-in 'Network Watchdog' to monitor the availability of the cellular connection.

Usage of this watchdog is advisable; however, it is intended to be a 'mechanism of last resort.' The Oxygen-3 Wireless Gateway has many ways of detecting a cellular link failure, such as obtaining link status information from the cellular module, reacting to disconnect messages from the network, monitoring higher level traffic such as IPsec tunnels, and monitoring the cellular hardware.

### Network Watchdog Settings:

**Watchdog Ping Interval:**

(restarts WWAN connection if Pings fail)

**Primary Watchdog Ping Target:**

**Secondary Watchdog Ping Target:**

(optional - used in case Pings to primary target fail)

**Reboot Timeout:**

(optional - must be equal or greater than Ping interval)

However, there may be cases where all these methods fail and in this case the 'Network Watchdog' is supposed to provide a simple method to detect connectivity problems. It is designed to periodically ping one or two 'Ping Targets' across the wireless network. If both ping targets fail to respond, corrective action is taken:

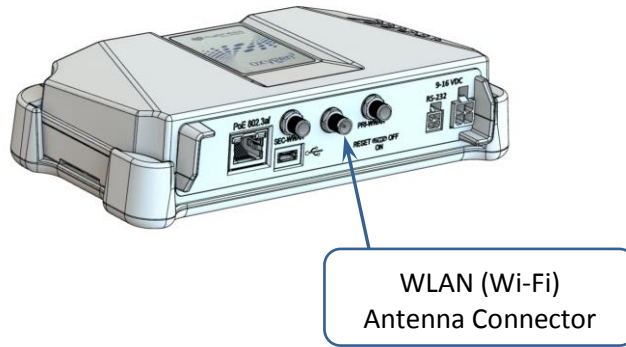
- If no ping target responds after the 'Watchdog Ping Interval' has elapsed, the cellular connection will be torn down, the cellular modem will be power-cycled and then the Oxygen-3 Wireless Gateway will attempt to re-establish a cellular connection
- If the 'Reboot Timeout' period has elapsed (must be greater than the ping interval), the Oxygen-3 Wireless Gateway will perform a complete reboot.

### Note:

- a) Since connectivity issues sometimes happen immediately after the cellular connection has been established, the first network watchdog ping will be performed within 15 minutes after a cellular connection has been established, **regardless of the configured 'Watchdog Ping Interval.'** Subsequent pings will happen after the configured 'Watchdog Ping Interval.'
- b) It is advisable to configure both a primary and a secondary ping target. If only a single ping target is configured and the ping target host goes down, all Oxygen-3 Wireless Gateways will frequently reconnect and reboot because they will (wrongly) interpret this as a cellular connection failure.

### 5.3 WLAN Page (Optional - Only if Oxygen-3 Wireless Gateway supports WLAN)

The Oxygen-3 Wireless Gateway can be ordered with WLAN (Wi-Fi) support. Whether a unit supports Wi-Fi or not can be easily determined by looking at the front panel. Only units with Wi-Fi support have an additional third antenna connector:



#### 5.3.1 WLAN Radio Configuration

The first part of the 802.11 WLAN configuration page allows the user to configure WLAN radio settings:

##### WiFi Access Point Settings:

Enable 802.11 Wi-Fi:

Delay Startup until WWAN is Connected:

WiFi SSID:

oxygen\_3-01-5b

Country Code (Regulatory Domain):  
(2-character ISO/IEC 3166-1 alpha-2 code)

CA

Stealth SSID:

(don't broadcast SSID name)

Channel:

(channels 12 and 13 are not available in North America)

- 6 (2.4 GHz)
- 1 (2.4 GHz)
- 2 (2.4 GHz)
- 3 (2.4 GHz)
- 4 (2.4 GHz)
- 5 (2.4 GHz)
- 6 (2.4 GHz)
- 7 (2.4 GHz)
- 8 (2.4 GHz)
- 9 (2.4 GHz)
- 10 (2.4 GHz)
- 11 (2.4 GHz)
- 12 (2.4 GHz)
- 13 (2.4 GHz)
- 36 (5 GHz)
- 40 (5 GHz)
- 44 (5 GHz)
- 48 (5 GHz)
- 149 (5 GHz)
- 153 (5 GHz)
- 157 (5 GHz)

- If the *'Delay Startup until WWAN is Connected'* checkbox is enabled, the Oxygen-3 Wireless Gateway won't start the internal Wi-Fi radio until a cellular (WWAN) connection has been established.
- The Oxygen-3 Wireless Gateway's WLAN radio always operates in BGN mode, supporting a maximum theoretical throughput of 150 MB/s.
- Both the 2.4GHz band and the 5GHz band are supported. (2.4GHz or 5GHz must be selected)
- The Oxygen-3 Wireless Gateway's WLAN radio has been tested to support up to 40 clients simultaneously. However, Cypress recommends no more than 20 simultaneous clients for optimum performance.



### 5.3.2 WLAN Security Configuration

The bottom part of the 802.11 WLAN configuration page allows the user to configure Wi-Fi security settings. The Oxygen-3 Wireless Gateway supports four different security options as well as MAC address whitelisting:

**WiFi Security and Authentication Settings:**

WiFi Security:

WiFi Password:

(WPA/WPA2 only)

WPA/RADIUS Server IP Address:

WPA/RADIUS Server Port:

WPA/RADIUS Password:

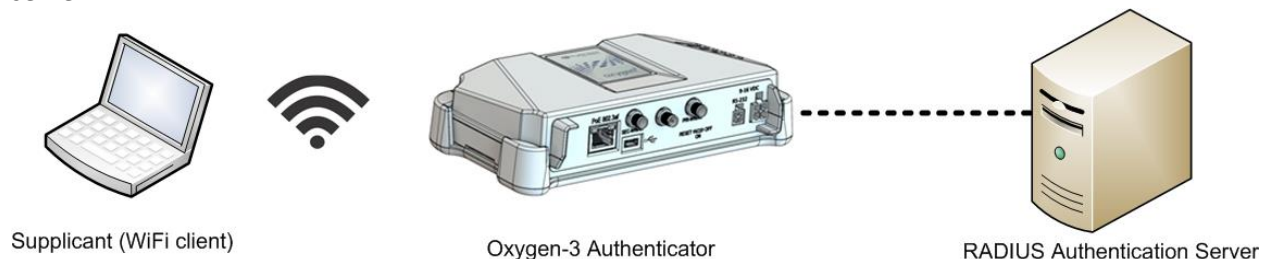
MAC-Address Whitelist:  
max 75 MAC Addresses, delimited by space

- Selecting no password (Security: *None*) is only recommended for Captive Portals.
- WPA and WPA2 security requires a local password. WPA is considered obsolete, therefore only WPA2 should be used.
- RADIUS/EAP uses an external RADIUS server to grant or deny access to the Wi-Fi network. Required RADIUS server settings are IP address and port as well as a RADIUS server password. See section 5.3.2.1 below.

MAC-Address whitelisting limits access to the WLAN network to clients with certain MAC Addresses. Because MAC Addresses can be easily spoofed, whitelisting as a security measure should only be used in combination with other security options described above.

#### 5.3.2.1 WLAN Radius Authentication

An Oxygen-3 can be configured as an 802.1x authenticator to gate WiFi authentication against a RADIUS server:



The Oxygen-3 needs to be configured with details about the RADIUS server:

**WiFi Security and Authentication Settings:**

WiFi Security:

WiFi Password:

(WPA/WPA2 only)

WPA/RADIUS Server IP Address:

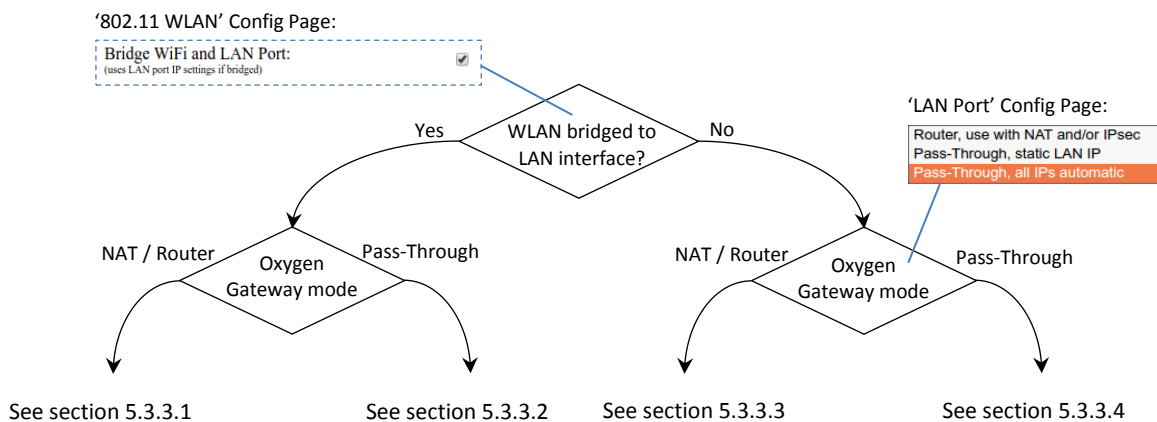
WPA/RADIUS Server Port:

WPA/RADIUS Password:

Once the three components (Supplicant / WiFi client, Oxygen-3, RADIUS server) are configured correctly, the WiFi client will be prompted for a username and password and must successfully authenticate to the RADIUS server before being allowed to connect to the Oxygen-3 WiFi network.

### 5.3.3 WLAN Network Settings

The Oxygen-3 Wireless Gateway's WLAN networking subsystem can principally be configured in four different ways, depending on whether the WLAN interface is bridged to the Ethernet LAN interface and whether the Oxygen-3 Wireless Gateway operates in pass-through mode or in router mode.



#### 5.3.3.1 WLAN bridged to LAN Port, Router Mode

Enable *'Bridge Wi-Fi and LAN Port'* on the 802.11 WLAN configuration page:

##### WiFi IP Settings:

**Bridge WiFi and LAN Port:**  
(uses LAN port IP settings if bridged)



Select *'Router, use with NAT and/or IPsec'* as the Mode of operation on the LAN Port configuration page:

##### LAN Setup:

**Mode of Operation:**  
(see description above)

Router, use with NAT and/or IPsec ▾

This mode of operation is fairly common: it allows both the LAN port and the WLAN network to operate on the same IP network. All IP settings for the bridged networks can be configured on the LAN Port configuration page:

**LAN Setup:****Mode of Operation:**

(see description above)

Router, use with NAT and/or IPsec ▾

**LAN Port IP Address and Mask:**

(not required when using automatic Pass-Through)

192.168.80.1 /24

**Enable DHCP Server on LAN Port:**

(required for automatic Pass-Through mode)

**DHCP IP Range Start:**

(lowest IP address assigned - Router mode only)

192.168.80.2

**DHCP IP Range End:**

(highest IP address assigned - Router mode only)

192.168.80.20

**DHCP Lease Time:**

(consider using 2m when in pass-through mode)

1h ▾

**Enable NAT on LAN Port:**

(not possible in Pass-Through modes)

**NAT Scope:**

(which source IPs should be NAT'ed)

LAN network only ▾

**Link-down Time when IP Changes:**

(Pass-Through: to prompt DHCP client to re-acquire IP Address)

3 ▾

**LAN Port Speed:**

Negotiate Automatically ▾

All settings (including secondary IP address settings) apply to a bridge interface consisting of the LAN port and the Wi-Fi network.

**Enable Secondary IP Address for LAN Port:**

(static IP - useful for monitoring or configuration)

**Secondary LAN Port IP Address and Mask:**

169.254.0.1 /24

### 5.3.3.2 WLAN bridged to LAN Port, Pass-through Mode

Enable 'Bridge Wi-Fi and LAN Port' on the 802.11 WLAN configuration page:

**WiFi IP Settings:****Bridge WiFi and LAN Port:**

(uses LAN port IP settings if bridged)

Select 'Pass-Through' as the Mode of operation on the LAN Port configuration page. Pass-Through allows for static IP address settings or for automatically assigned IP addresses. Select the mode that is appropriate for your application. Refer to Section 5.1.2 for more information.

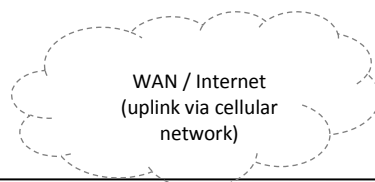
**LAN Setup:****Mode of Operation:**

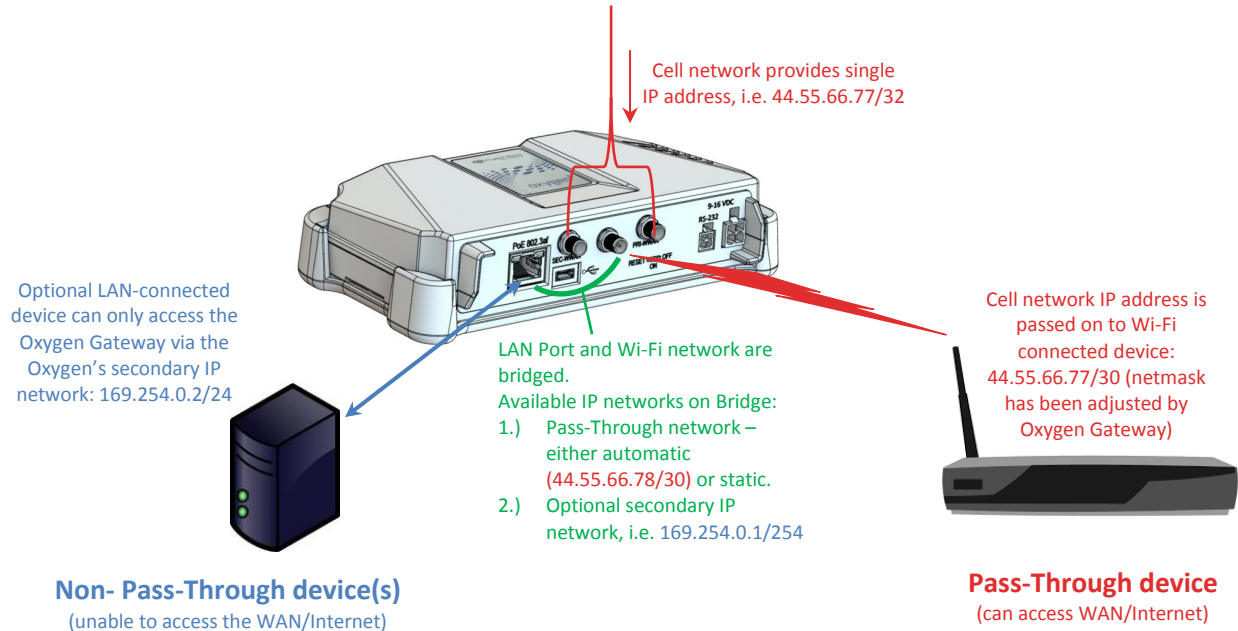
(see description above)

Pass-Through, all IPs automatic ▾

All pass-through network settings (including a secondary IP address) can be configured on the LAN Port configuration page, as described in Section 5.3.3.1 above.

In pass-through mode, the IP address assigned by the cellular network will be passed on to a device that is attached to the Oxygen-3 Wireless Gateway. Since the cellular network only provides a single IP address, **only one attached device can operate in pass-through mode**. This device can be either on the LAN port or it can be connected to the Oxygen-3 Wireless Gateway's Wi-Fi network (shown in the example below).





### 5.3.3.3 No LAN/WLAN Bridging, Router Mode

Disable 'Bridge Wi-Fi and LAN Port' on the 802.11 WLAN configuration page:

#### WiFi IP Settings:

Bridge WiFi and LAN Port:

(uses LAN port IP settings if bridged)

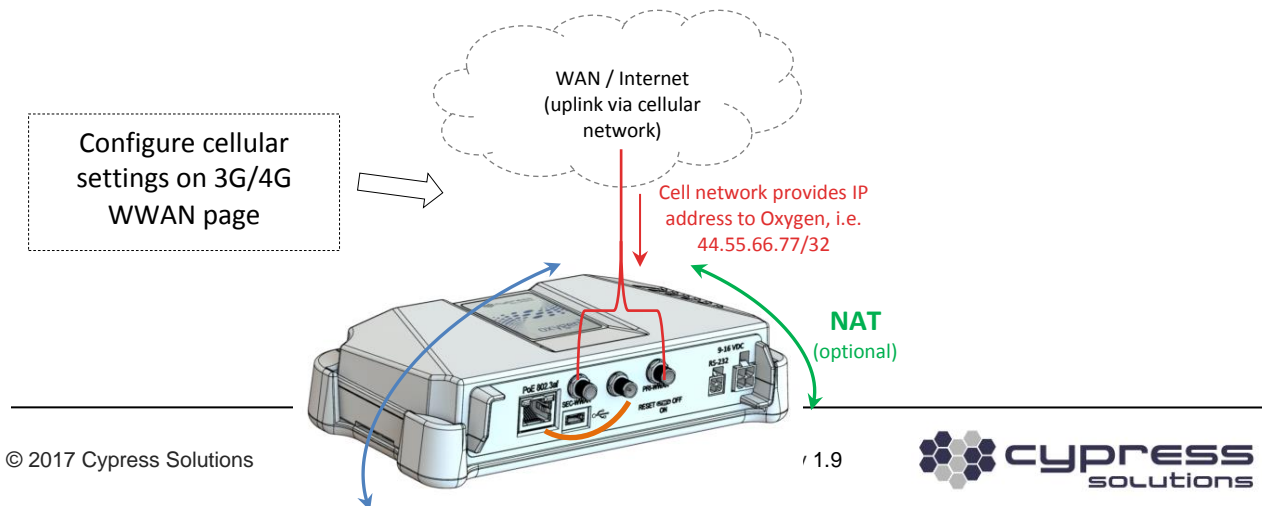
Select 'Router, use with NAT and/or IPsec' as the Mode of operation on the LAN Port configuration page:

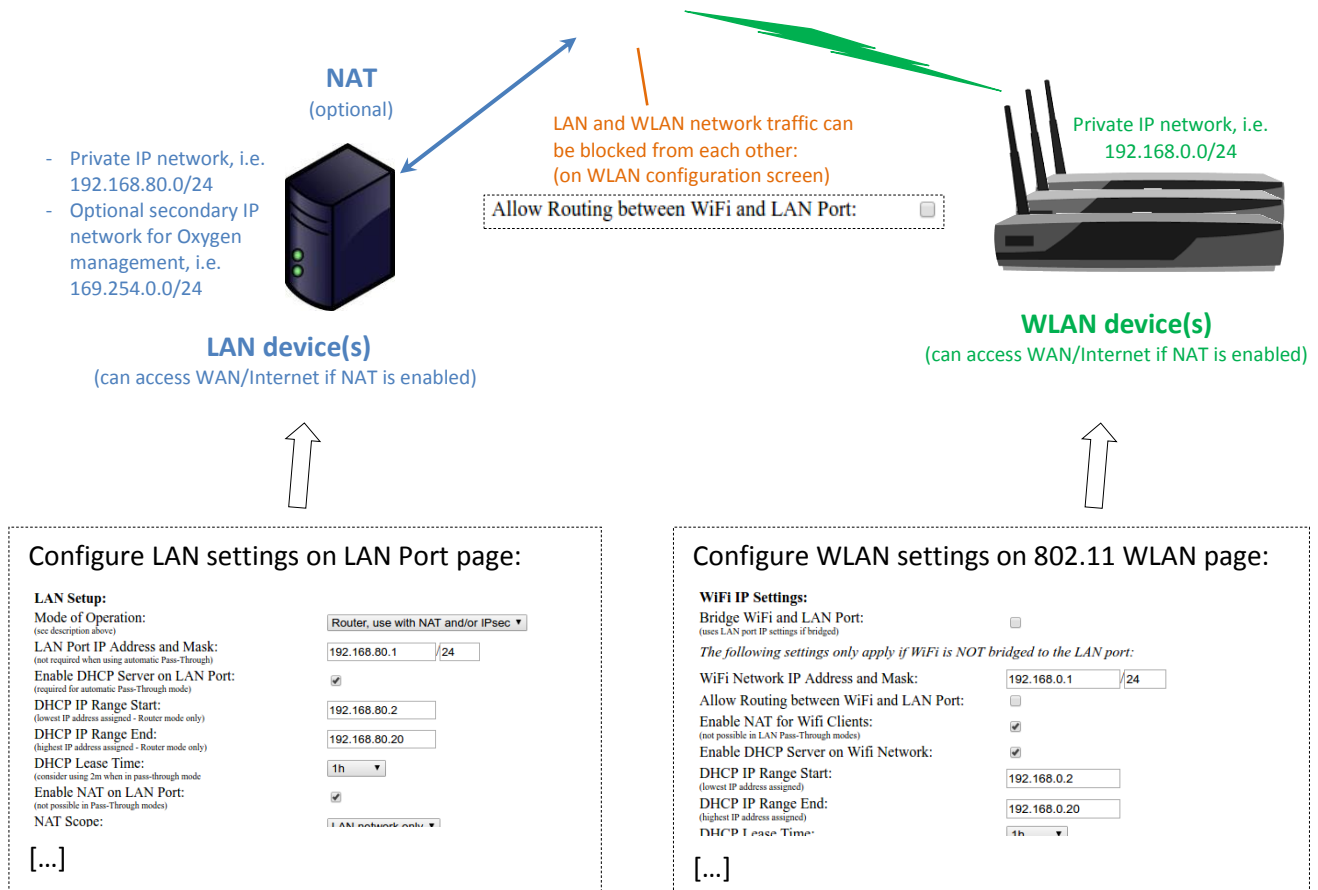
#### LAN Setup:

Mode of Operation:

(see description above)

In this mode, both the LAN port and the WLAN network operate independently. Network Address Translation (NAT) can be enabled for each of these two networks, enabling devices on each respective interface to connect to the WAN/Internet.





#### 5.3.3.4 No LAN/WLAN Bridging, Pass-Through Mode

Disable 'Bridge Wi-Fi and LAN Port' on the 802.11 WLAN configuration page:

##### WiFi IP Settings:

Bridge WiFi and LAN Port:   
(uses LAN port IP settings if bridged)

Select 'Pass-Through' as the Mode of operation on the LAN Port configuration page. Pass-Through allows for static IP address settings or for automatically assigned IP addresses. Select the mode that is appropriate for your application. Refer to Section 5.1.2 for more information.

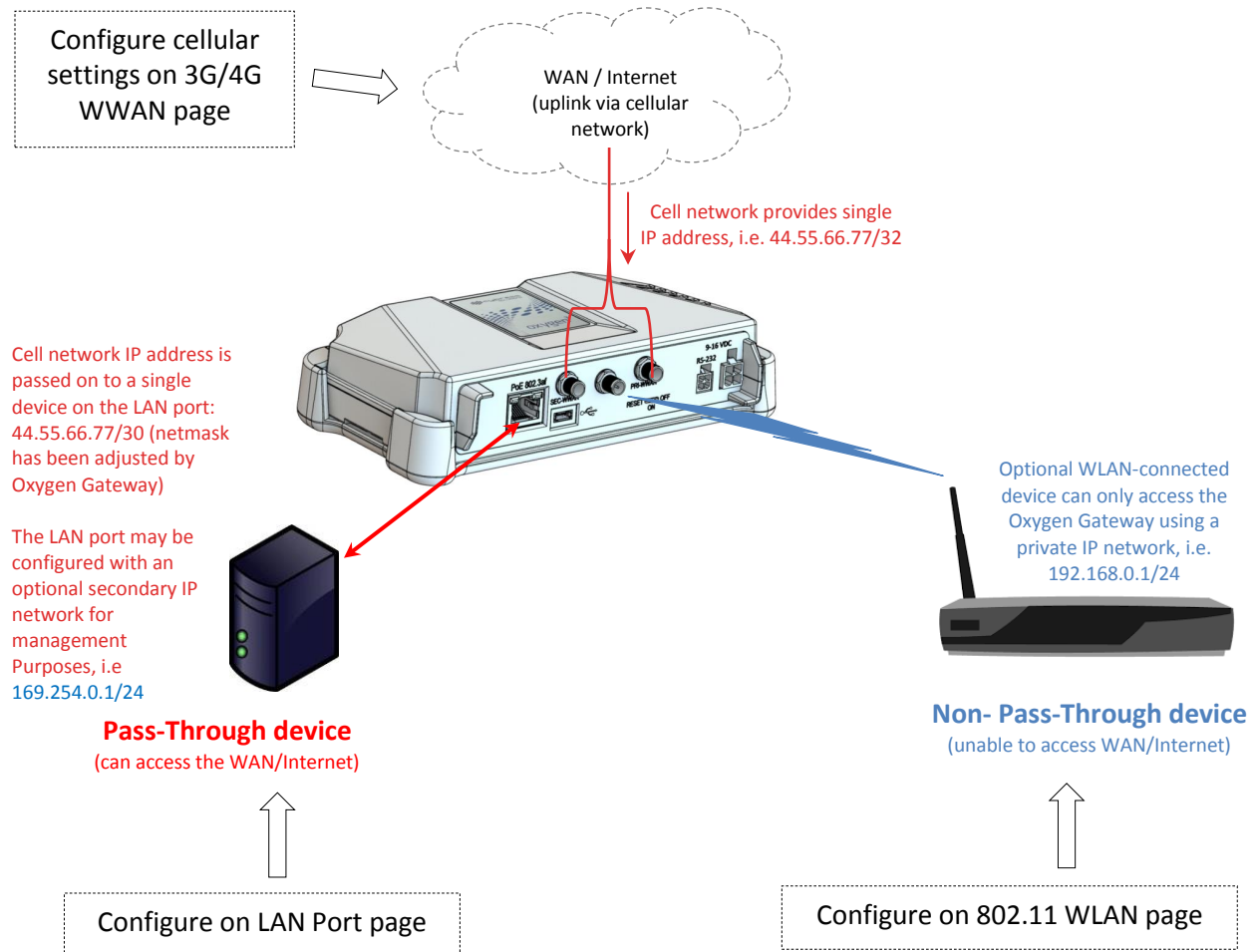
##### LAN Setup:

Mode of Operation:  (see description above)

All pass-through network settings (including a secondary IP address) can be configured on the LAN Port configuration page, as described in Section 5.3.3.1 above.

In this mode, the IP address assigned by the cellular network will be passed on to a device that is attached to the **LAN port** of the Oxygen-3 Wireless Gateway. Because the cellular network only provides a single IP address, **only one attached device can operate in pass-through mode**.

Devices that are connected to the Oxygen-3 Wireless Gateway's Wi-Fi network can only obtain a private IP address. They will only be able to access the Oxygen-3 Wireless Gateway, but not the WAN/Internet. For this reason, it is uncommon for the Oxygen-3 Wireless Gateway to be configured in this mode.



## 5.4 Captive Portal

The Oxygen-3 Wireless Gateway can be configured to work with a variety of external Captive Portal providers to act as a Wi-Fi hotspot.

The Captive Portal configuration screen can only be accessed through the *802.11 WLAN* configuration page and it is only available when WLAN is enabled and the unit is **not** operating in pass-through mode.

### WiFi Access Point Settings:

Enable 802.11 WiFi:

**LAN Setup:****Mode of Operation:**

(see description above)

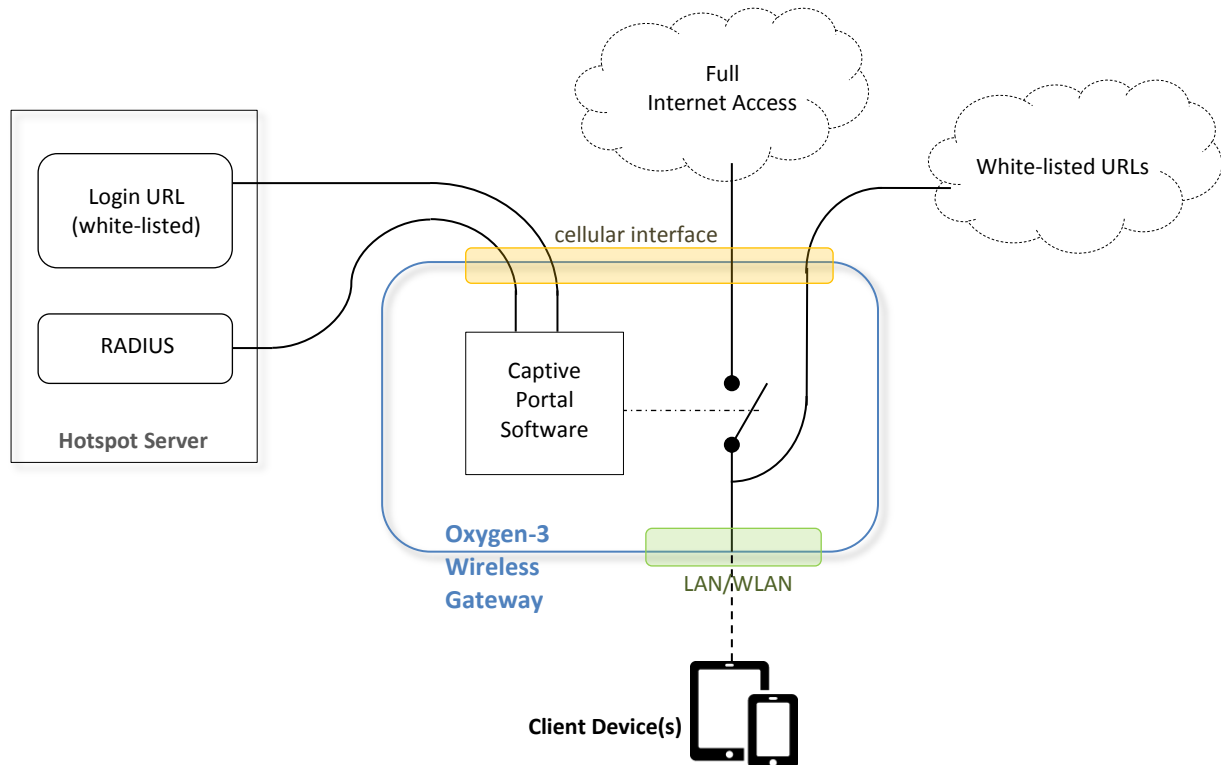
Router, use with NAT and/or IPsec ▾

If these conditions are met, click on the link at the bottom of the *802.11 WLAN* configuration page to access the Captive Portal configuration page:

**Captive Portal / Hotspot**

The [Captive Portal / Hotspot](#) feature of the Oxygen-3 gateway allows you configure the Oxygen-3 as a WiFi Hotspot using an external Captive Portal provider.

A functioning captive portal configuration requires access to external servers to provide a login page and Radius authentication. The illustration below shows the various components of such a setup:



Enter the required values for your Captive Portal provider:

**Captive Portal Settings:**

Enable Captive Portal:	<input checked="" type="checkbox"/>
RADIUS Server IP Address:	<input type="text" value="34.45.56.67"/>
Secondary RADIUS Server IP Address: <small>(optional - for backup purposes)</small>	<input type="text"/>
Authentication Port:	<input type="text" value="1812"/>
Accounting Port:	<input type="text" value="1813"/>
RADIUS Password: <small>(max. 64 characters)</small>	<input type="password" value="*****"/>
Authentication Server URL:	<input type="text" value="https://www.hotspotdudes.com/login.html"/>
UAM Port:	<input type="text" value="3990"/>
UAM Secret: <small>(max. 64 characters)</small>	<input type="text"/>
<b>Static Whitelist:</b> <small>max 75 IP, network or domain entries, delimited by space or carriage return.</small> <small>Domain names will get resolved at startup</small>	<input type="text" value="www.cypress.bc.ca&lt;br/&gt;www.hotspotdudes.com"/>
<b>Dynamic Whitelist:</b> <small>max 75 IP, network or domain entries, delimited by space or carriage return.</small> <small>Domain names will get resolved dynamically and wildcard domains are allowed</small>	<input type="text" value="www.facebook.com"/>
NAS/Gateway ID:	<input type="text" value="sample_ids"/>

*The following settings are optional and may be overwritten by values provided by the RADIUS server:*

Session Timeout (mins): <small>(max 9999 minutes, 0 to disable)</small>	<input type="text" value="60"/>
Idle Timeout (mins): <small>(max 9999 minutes, 0 to disable)</small>	<input type="text" value="10"/>
Max. Download Bandwith (kbps): <small>(max 99,999 kbps, 0 to disable)</small>	<input type="text" value="1024"/>
Max. Upload Bandwith (kbps): <small>(max 99,999 kbps, 0 to disable)</small>	<input type="text" value="512"/>

RADIUS Server IP Address, Secondary IP, Ports	The IP address and ports of the RADIUS server that is used to authenticate the hotspot clients. When using an external hotspot service, the service provider will provide these settings.
Authentication Server URL	Hotspot clients will be redirected to this URL for login. The URL is typically provided by the hotspot service provider and must be part of the static or dynamic whitelist.
UAM Port and Secret	UAM (Universal Access Method) describes a standardized method of a web form to obtain client access. The captive portal service provider will provide the required values.
Whitelists	The Oxygen-3 Wireless Gateway supports up to a total of 150 whitelisted URLs. Client devices can access these URLs without prior authentication. Dynamic whitelist entries will be resolved each time a client attempts to access them, while static whitelist entries will only get resolved once at startup. Therefore, the dynamic whitelist should be used for URLs that have changing IP addresses, for example due to the usage of content delivery networks, load balancers, etc.
NAS/Gateway ID	Typically, a location-specific ID that is used by the hotspot service provider to identify the Oxygen-3 Wireless Gateway.
Timeout and Bandwidth limits	Enter default client session timeouts and bandwidth values here. Settings provided by the RADIUS server will override any values entered here.



## 5.5 Access Control Page

The Oxygen-3 Wireless Gateway offers granular access control depending on what interface is used to access the unit for administrative or monitoring purposes.



Use caution when configuring Access Control rules. For example, disabling all Web access will make it impossible to further access the Oxygen-3 Wireless Gateway using a web browser. It may be necessary to revert to factory default settings to re-gain access.

The default Access Control settings are shown below:

### Access Setup:

	LAN (pri. IP)		LAN (sec. IP)		WLAN (not bridged)		WWAN Interface		IPsec Tunnel	
	Enable	Port	Enable	Port	Enable	Port	Enable	Port	Enable	Port
Web Access:	<input checked="" type="checkbox"/>	80	<input checked="" type="checkbox"/>	80	<input type="checkbox"/>	801	<input type="checkbox"/>	801	<input checked="" type="checkbox"/>	80
Secure Web Acs:	<input checked="" type="checkbox"/>	443	<input checked="" type="checkbox"/>	443	<input type="checkbox"/>	4431	<input type="checkbox"/>	4431	<input checked="" type="checkbox"/>	443
SSH Access:	<input checked="" type="checkbox"/>	22	<input checked="" type="checkbox"/>	22	<input type="checkbox"/>	221	<input type="checkbox"/>	221	<input checked="" type="checkbox"/>	22
Telnet Access:	<input type="checkbox"/>	23	<input type="checkbox"/>	23	<input type="checkbox"/>	231	<input type="checkbox"/>	231	<input type="checkbox"/>	23
SNMP Access:	<input checked="" type="checkbox"/>	161	<input checked="" type="checkbox"/>	161	<input type="checkbox"/>	1611	<input type="checkbox"/>	1611	<input checked="" type="checkbox"/>	161

As can be seen above, there are five administrative services available on the Oxygen-3 Wireless Gateway:

Web/HTTP – HTTPS – SSH – Telnet - SNMP

Each one of these services can be accessed in four different ways. Each combination of service and access method can be turned on or off and a specific access port can be selected.

By default, access via the WWAN interface, as well as Telnet access, is turned off for security reasons.

### Note:

The default access ports on the WWAN interface are set to non-standard ports. This is to avoid conflicts with services running on the connected device when operating on Pass-Through mode. In Pass-Through mode all incoming WWAN traffic will be forwarded (“passed through”) to the connected device, except for traffic which is designated here to be management traffic.

For example, if the WWAN SSH access port were to be set to the default port 22, then the Oxygen-3 Wireless Gateway would intercept all regular port 22 SSH traffic and thereby prevent it from reaching the connected device. Therefore, it is advisable to use non-standard ports for access via the WWAN interface.

The Oxygen-3 Wireless Gateway also allows for white-listing up to eight specific networks for exclusive access by these networks:

**Restrict Access to specific Networks:**

1. Allowed Source Network:	<input type="text"/>	<input type="checkbox"/>
2. Allowed Source Network:	<input type="text"/>	<input type="checkbox"/>
3. Allowed Source Network:	<input type="text"/>	<input type="checkbox"/>
4. Allowed Source Network:	<input type="text"/>	<input type="checkbox"/>
5. Allowed Source Network:	<input type="text"/>	<input type="checkbox"/>
6. Allowed Source Network:	<input type="text"/>	<input type="checkbox"/>
7. Allowed Source Network:	<input type="text"/>	<input type="checkbox"/>
8. Allowed Source Network:	<input type="text"/>	<input type="checkbox"/>

If the configuration fields above are left empty, then access is granted to all source networks.

## 5.6 Routing and SNAT/DNAT Page

### 5.6.1 Static Routes

The Oxygen-3 Wireless Gateway attempts to automatically establish its own IP routes, using the WWAN interface as the default route. In Pass-Through mode, the default route can be changed manually.

In all modes of operation, it is possible to define additional static routes for up to five destination networks. Each of these routes can either point to the interface in general or to a particular gateway IP address.

It is not required to add routing table entries for SNMP traps, remote syslog servers, NTP servers or the Cypress Cloud Manager server. These routes are automatically established depending on the settings of their corresponding configuration screens.

**Routing Setup:**

Do NOT set a Default Route:

(works in pass-through mode only: WWAN traffic then requires routes set below)

	Destination Network	Route via	Gateway
1.	<input type="text"/>	LAN ▼	<input type="text"/>
2.	<input type="text"/>	LAN ▼	<input type="text"/>
3.	<input type="text"/>	LAN ▼	<input type="text"/>
4.	<input type="text"/>	LAN ▼	<input type="text"/>
5.	<input type="text"/>	LAN ▼	<input type="text"/>

### 5.6.2 SNAT/DNAT Setup

Up to five static source or destination NAT translations can be configured by entering the appropriate settings on this screen.

**SNAT/DNAT Setup:**

	Type	Flow	Out Intf.	In Intf.	Proto.	Source Match	Destination Match	Change-to Address
1.	Off	Local	Any	Any	Any			
2.	Off	Local	Any	Any	Any			
3.	Off	Local	Any	Any	Any			
4.	Off	Local	Any	Any	Any			
5.	Off	Local	Any	Any	Any			

**Type**
 Off  
 Off  
 DNAT  
 SNAT

Select DNAT to change the destination address of incoming packets or SNAT to change the source address of incoming packets.

**Flow**
 Local  
 Local  
 Through

Select whether the affected packets pass through the Oxygen-3 Wireless Gateway or terminate/originate locally on the Gateway. If in doubt, select “Through” as this is the more likely scenario.

<b>Out Intf.</b>	<b>In Intf.</b>
<input type="radio"/> Any	<input type="radio"/> Any
<input checked="" type="radio"/> Any	
<input type="radio"/> WWAN	
<input type="radio"/> ETH	
<input type="radio"/> WLAN	

Selecting an incoming or outgoing interface restricts the application of a SNAT/DNAT rule to packets on the selected interface.

*Note:* For DNAT rules, only the incoming interface is relevant and for SNAT rules on the outgoing interface is relevant.

**Proto.**
 Any  
 Any  
 UDP  
 TCP  
 ICMP  
 ESP  
 AH

It is possible to restrict the application of a SNAT/DNAT rule to packets that carry UDP, TCP, ICMP, ESP or AH traffic by selecting the appropriate value here.

‘Source Match’ and ‘Destination Match’ strings are optional and should have the following format:

```
[ip] [/netmask] [:port[-port_range_end]]
```

For example:

```
33.44.55.0/24
10.30.0.0/16:1024-2048
:5556
```

Match packets to/from the 33.44.55.0/24 network, regardless of port.  
 Match packets to/from the 10.30.0.0/16 networks if their source/destination port is within the range of 1024 to 2048  
 match all packets with source/destination port 5556.

The ‘Change-to Address’ is mandatory and should follow the following syntax:

```
[ip] [:port[-port_range_end]]
```

## 5.7 IPsec VPN Page

The Oxygen-3 Wireless Gateway has support for IPsec. The following IPsec features are supported:

- Primary ISAKMP peer, with the ability to automatically fail over to a backup peer.
- Up to five simultaneous IPsec tunnels (five remote encrypted subnets, five IPsec security associations).
- Tunnel Mode only (Transport Mode is not supported).
- Support for 3DES, AES-128, AES-192, AES-256 encryption protocols.
- Support MD5, SHA1, SHA-256, SHA-384, SHA-512 hashes.
- Support for DH Groups 1, 2, 5, 14, 15, 16, 17, 18 (768 bits to 8192 bits).
- Support for Main Mode and Aggressive Mode.
- Support for NAT Traversal.
- Split tunneling.
- Dead Peer Detection (DPD).
- Debugging facility for trouble-shooting IPsec connections.

To enable IPsec, the basic mode of operation (on the LAN Port page) must be set to *Router Mode*.

### LAN Setup:

#### Mode of Operation:

(see description above)

#### LAN Port IP Address and Mask:

(not required when using automatic Pass-Through)

#### Enable DHCP Server on LAN Port:

(required for automatic Pass-Through mode)

Router, use with NAT and/or IPsec ▼
Router, use with NAT and/or IPsec
Pass-Through, static LAN IP
Pass-Through, all IPs automatic



Once *Router Mode* has been selected and the configuration has been saved, IPsec can now be configured by selecting the corresponding link on the left side of the screen.

### Note:

The Oxygen-3 Wireless Gateway will always act as the 'IPsec initiator' and it will immediately try to establish an ISAKMP security association. However, IPsec (Phase 2) security associations will only be created 'on demand,' once there is data to be transmitted.

Fill in the appropriate IPsec parameters for the customer application. If the Oxygen-3 Wireless Gateway and the remote end fail to establish an IPsec tunnel, enable the **Enable Additional Debug Information in Syslog** option below and check the system log for possible failure reasons.

### Extra Logging / Debug Options:

#### Enable Additional Debug Information in Syslog:

(Don't leave this enabled on a production machine!)



Do not leave the "Extra Logging / Debug Options" feature enabled for an extended period of time. The logging is quite verbose and will not only fill the system log with large amounts of debug log, but over time will cause older log entries to be discarded.

**IPsec VPN Setup:**

Enable IPsec VPN Tunneling:

(No encryption without IPsec)

IPsec VPN Host IP:

(Routable IP of the tunnel peer)

Enable Alternate IPsec VPN Host IP:

(Requires Alternate IPsec VPN Host IP)

Alternate IPsec VPN Host IP:

(If primary host is unavailable)

VPN Host ID:

(If different from host IP - otherwise leave empty)

Primary Destination Private Network:

(Typically non-routable, e.g. 192.168.20.3/24)

Destination Private Network #2:

Destination Private Network #3:

Destination Private Network #4:

Destination Private Network #5:

Local Private Network:

(Leave empty to use LAN port IP address)

VPN Client ID:

(If different from own IP - otherwise leave empty)**Please note that DH Groups of 1024 bits or less are no longer considered secure against state-sponsored attacks - they can possibly be broken in less than a minute.**

Phase 1 Encryption / Hash / DH-Group:

(Also called IKE, ISAKMP or Main Mode settings)  

Phase 1 Key Timeout (hours):

(Should be less than peer's key timeout value)

Phase 2 Encryption / Hash / DH-Group:

(Also called IPsec SA or Quick Mode settings)  

Phase 2 Key Timeout (hours):

(Should be less than peer's key timeout value)

Use Less Secure Aggressive Mode:

(Not recommended!)

IPsec Pre-shared Key (PSK):

(Will be stored unencrypted in the unit!)

Confirm PSK here:

### 5.7.1 Dead Peer Detection

Cypress Solutions always recommends the use of IPsec Dead Peer Detection (DPD) in wireless networks. Failure to enable this feature on **both** ends of an IPsec connection can result in inoperable IPsec tunnels due to the dynamic nature of cellular wireless connections.

**IPsec Dead Peer Detection (DPD):**

DPD Timer:

(Seconds between DPD packets)

DPD Max. Retries:

(sent every 15 sec after first DPD failure)

### 5.7.2 NAT Traversal

The Oxygen-3 Wireless Gateway supports the use of IPsec NAT Traversal (NAT-T). This should be enabled if the Oxygen-3 Wireless Gateway is running on an APN performing NAT, or if a NAT is expected prior to packets reaching the designated IPsec peer. NAT-T keepalive can be set at selected intervals to ensure NAT Translations do not expire on the NAT boundary for the IPsec connection.

**NAT Traversal (NAT-T):**

Enable IPsec NAT Traversal:

(Caution: NAT-T is frequent source of problems!)

Off ▼

NAT-T Keepalive Time:

(Seconds between keep-alive packets to keep NAT active)

20 ▼

**Note:**

NAT-Traversal is not always guaranteed to work and debugging NAT-Traversal related problems could be difficult. Some routers have special 'IPsec pass-through' modes which are meant to be enabled if IPsec packets are passing through. However, depending how these IPsec pass-through modes are implemented, they can prevent the proper functioning of an IPsec NAT-T tunnel.

### 5.7.3 Secondary IPsec Peer

The Oxygen-3 Wireless Gateway supports connections to an optional secondary IPsec host.

IPsec VPN Host IP:

(Routeable IP of the tunnel peer)

Enable Alternate IPsec VPN Host IP:

(Requires Alternate IPsec VPN Host IP)

Alternate IPsec VPN Host IP:

(If primary host is unavailable)

This support is intended for customers with High Availability (HA) requirements (for example, when multiple datacenters are in use). This feature allows for automatic failover in the event of an IPsec host outage.

If both a primary and an alternate IPsec host are configured, the Oxygen-3 Wireless Gateway will use both IPsec hosts alternately. Generally, it will attempt to connect to the primary host first. If this fails, or more generally, if the IPsec tunnel to the primary host fails, it will attempt to connect to the secondary host. Should this connection fail, it will then again switch back to the primary IPsec host and attempt to establish a connection here.

This means, that technically no preference is given to either host, except that the Oxygen-3 Wireless Gateway will attempt to connect to the primary host first, after power-up. However, it is to be expected that the IPsec tunnel will eventually get interrupted, even if only for a moment, when the cellular network forces a WWAN disconnect/reconnect (the frequency of this depends on your wireless carrier and typically ranges from once a day to once every few weeks). At this point, the Oxygen-3 Wireless Gateway will switch over to the secondary host and it will then attempt to maintain this connection for as long as possible. It will **not** monitor the link to the primary host, but rather, possibly attempt to reconnect to the primary host.

**Note:**

To reliably detect IPsec tunnel failures, it is strongly recommended to properly configure Dead Peer Detection (DPD).

## 5.8 General Routing Encapsulation Tunnel Settings

The Oxygen-3 Wireless Gateway supports General Routing Encapsulation (GRE). To enable this feature, click on 'GRE Tunnel' under 'Network Config'.

### GRE Tunnel Configuration

Please enter your GRE Tunnel configuration here. Leave the *Enable GRE Tunnel* box unchecked if you do not want to use GRE. GRE can only be used if this Oxygen-3 gateway is set to 'Router' mode.

#### GRE Tunnel Setup:

Enable GRE Tunnel:



GRE Tunnel Peer IP:

(Public IP of the tunnel peer)

GRE Tunnel Network:



GRE Tunnel Inside Peer IP:

GRE Tunnel MTU:

Destination Private Network #1:



(Typically non-routable, e.g. 192.168.20.3/24)

Destination Private Network #2:



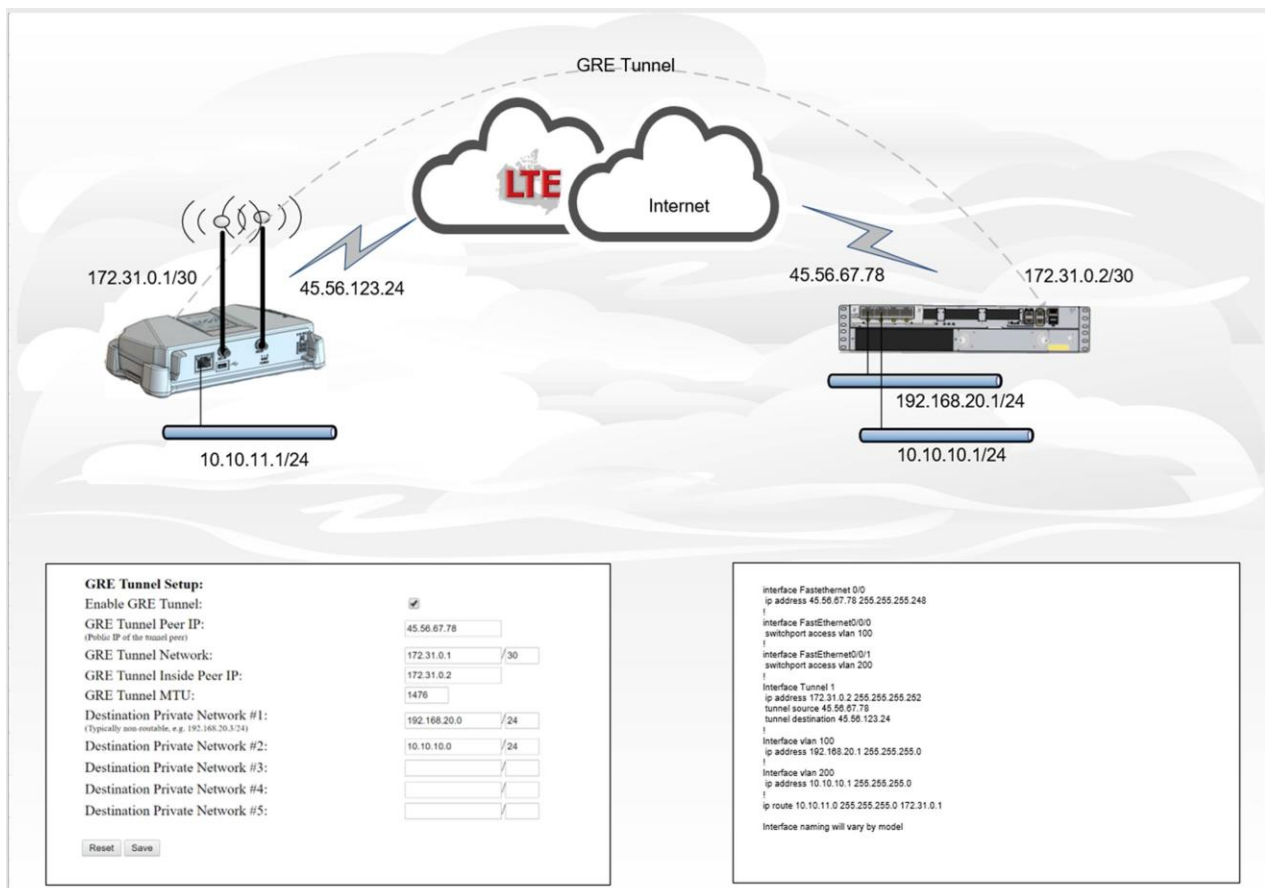
Destination Private Network #3:



Destination Private Network #4:



Destination Private Network #5:

## 5.9 Dynamic DNS

When using carrier-supplied dynamic IP addresses, dynamic DNS can be employed to determine the current IP address of the Oxygen-3 Wireless Gateway. Currently, there is support for the following dynamic DNS providers:

- changeip.com
- dyndns.org
- no-ip.com
- zoneedit.com

A third party dynamic DNS provider is the quickest way to setup this feature and most of the providers noted above will offer a free account for a limited number of hostnames.

### Dynamic DNS Setup:

Use Dynamic DNS Provider:

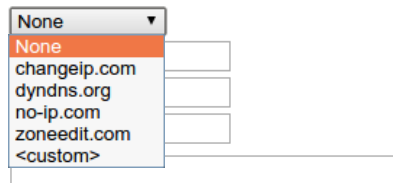
DDNS Domain Name:

DDNS User Name:

DDNS Password:

DDNS Update URL:

(only required for custom DDNS service)



The screenshot shows a web form for Dynamic DNS Setup. A dropdown menu is open, displaying the following options: 'None' (highlighted in orange), 'changeip.com', 'dyndns.org', 'no-ip.com', 'zoneedit.com', and '<custom>'. To the right of the dropdown are four empty text input fields, corresponding to the labels 'DDNS Domain Name:', 'DDNS User Name:', 'DDNS Password:', and 'DDNS Update URL:'. Below the 'DDNS Update URL:' label is a smaller text input field with the note '(only required for custom DDNS service)'.

Aside from the above commercial providers, the Oxygen-3 Wireless Gateway also supports custom, (possibly 'in-house') dynamic DNS services. When using a custom provider, please specify the updated URL. The URL will be called in the following fashion:

```
http://<user_name>:<password>@<update_URL>?hostname=<domain_name>&myip=<ip_address>
```

The Oxygen-3 Wireless Gateway will expect a reply that starts with the strings 'good' or 'nochg' as an indication that the update was either successfully completed or that no change in IP address has been detected.

## 5.10 Name and Password

### 5.10.1 Hostname

By configuring each Oxygen-3 Wireless Gateway with a unique hostname, Oxygen-3 Wireless Gateway units can be easily distinguished. Each SNMP trap generated by the Gateway will contain the hostname selected here.



Additionally, location and contact information can be configured and these values can be queried using SNMP:

Oxygen-3 Gateway Hostname: (up to 64 characters)	<input type="text" value="internal-oxygen-3"/>
Location: (up to 64 characters)	<input type="text" value="Cypress Office"/>
Contact: (up to 64 characters)	<input type="text" value="Technical writer dude"/>

### 5.10.2 Radius Authentication

Authentication for accessing the Oxygen-3 Wireless Gateway can be achieved by either using a local password or by configuring the gateway to use a RADIUS server. When using the local password, only one password for the user 'admin' can be set.

When using RADIUS, multiple accounts can be setup with unique passwords and controlled by the server, however, they will all have the same rights as the local 'admin' user.

When using RADIUS, it is advisable to enable 'local password fallback' in combination with a strong local password. Without 'local password fallback' the Oxygen-3 Wireless Gateway will be inaccessible if it loses connectivity to the RADIUS server and the only way to re-gain access will be to revert to the factory default configuration.

Authentication Method:	<input type="text" value="Local Password"/>
RADIUS Server IP Address:	<input type="text"/>
RADIUS Server Port:	<input type="text" value="1812"/>
Server reachable via:	<input type="text" value="LAN (primary IP)"/> GW: <input type="text"/>
RADIUS Password:	<input type="text"/>

By default, **Server reachable via** is configured for 'LAN interface,' indicating that the Oxygen-3 Wireless Gateway expects the Radius server to be reachable via the LAN interface. If this is true, the default setting might work – if not, it may be required to enter a specific gateway IP address as well.

Either way, it is not required to enter any additional static routes on the Routing screen. The Oxygen-3 Wireless Gateway will automatically set the required routes depending on the settings chosen here.

### 5.10.3 Date and Time

The Oxygen-3 Wireless Gateway contains a Real-Time Clock (RTC) which will maintain accurate time even when the Oxygen-3 Wireless Gateway is powered off. However, the RTC must be adjusted initially and some drift can be expected over time.

For initial time adjustment of the RTC and to set the Oxygen-3 Wireless Gateway's system clock, the time can be set manually, or it can be synchronized with the host PC.

The current time on the Oxygen-3 gateway is:  
**Tuesday November 25 20:25:25 2014**

The current time on your computer is:  
**Tuesday November 25 20:25:27 2014**

Press the following button to set the date and time on the Oxygen-3 gateway to that of your computer:

Alternatively, date and time on the Oxygen-3 gateway can be set manually here:

Year:  Month:  Date:   
 Hour:  Minute:

Setting the time manually does not account for the inevitable RTC drift over time. It is therefore recommended to configure an NTP server from which the Oxygen-3 Wireless Gateway will obtain the precise time whenever it connects to the WWAN network. When this happens, the Oxygen-3 Wireless Gateway will also update its internal Real-Time Clock.

#### System Time:

Obtain System Time from:   
 Remote NTP Server:   
(If used as time source)  
 Server reachable via:  GW:   
 Timezone Adjustment:   
(In hours relative to UTC)  
 Adjust for Daylight Saving Time:

#### Local NTP Server:

Enable Local NTP Server on LAN/WLAN:   
 Local NTP Server Stratum:   
(Range: 1 to 16, default: 10)

#### System Time:

Obtain System Time from:

When the **Adjust for Daylight Saving Time** option is enabled, the Oxygen-3 Wireless Gateway will automatically account for daylight saving time when required.

By default, **Server reachable via** is configured for 'WWAN interface', indicating that the Oxygen-3 Wireless Gateway expects the NTP server to be reachable via the default route pointing to the WWAN interface. If the server is reachable via the LAN interface, change the setting accordingly and enter a

specific gateway IP address if required. In this case, it is not required to enter any additional static routes on the **Routing** screen. The Oxygen-3 Wireless Gateway will automatically set the required routes depending on the settings chosen here.

## 5.11 Advanced Settings

### 5.11.1 Flash Upgrade

Cypress Solutions regularly provides new firmware images for the Oxygen-3 Wireless Gateway to address and add new features or address other issues. These images are provided in the form of a single compressed binary file, which includes an internal checksum as well as version and product information. This prevents possible upgrade file corruption or accidental use of an incompatible upgrade file.

**Note:**

The Oxygen-3 modem supports all firmware images, opposed to the Oxygen-3 Plus which supports firmware 5.x and above. The Oxygen-3 Plus will not allow downgrades to 4.x firmware.

Upgrading is a two-step process:

1. The Oxygen-3 Wireless Gateway will download the new firmware image. The download process can be interrupted with no ill effect. It is possible to upgrade the Oxygen-3 Wireless Gateway 'over the air,' meaning that the firmware image file can be downloaded over the WWAN connection.
2. After the firmware image passes all integrity checks, the actual upgrade will begin. The Oxygen-3 Wireless Gateway's LED will flash in a distinctive pattern to illustrate that the upgrade process has begun.

The Oxygen-3 Wireless Gateway uses two flash images in parallel, one being the active one and the other one being the spare. During the upgrade process, the spare image will be overwritten. Once the write process is complete and verified, the previous spare image will be made the active one and the previous active one will become the spare one.

If the upgrade process gets interrupted for any reason, the existing working image will have remained untouched and the Oxygen-3 Wireless Gateway will remain operational.

By default, all configuration data will be retained during the upgrade process. The same applies to the system log, which will **NOT** get cleared.

There are three different ways to upgrade the firmware of an Oxygen-3 Wireless Gateway: using the HTTP, TFTP or FTP protocol:

#### 5.11.1.1 Upgrading using the HTTP Protocol

There are three different ways to upgrade the firmware of an Oxygen-3 Wireless Gateway. The first is via HTTP, and does not require any server setup. You can select a firmware file from your local hard drive and begin the upgrade process immediately by clicking on the 'Start HTTP Upgrade' button.

#### HTTP Flash Upgrade:

Filename:  Oxygen-3-4.1.0-RC4.bin

Ignore Firmware Version Information:   
(Allows downgrading)

Revert to Factory Configuration:   
(Warning: you will lose your current configuration)

The **Ignore Firmware Version Information** option allows for downgrading to older firmware versions, however, when doing so, Cypress Solutions Inc. does not guarantee that all configuration settings will be retained.

Enabling the **Revert to Factory Configuration** option will cause the Oxygen-3 Wireless Gateway to **NOT** save any configuration data. After the firmware upgrade, the Oxygen-3 Wireless Gateway will restart with factory default configuration. Enabling this option does **NOT** affect the system log. The system log will still be retained across firmware upgrades, even if this option is checked.

#### 5.11.1.2 Upgrading using the TFTP Protocol

Using TFTP is convenient when you have a TFTP server available on the local area network. It is inadvisable to use TFTP over wireless as the higher latency usually found over a wireless link will slow down the transfer of the firmware image file.

To start a TFTP upgrade, enter the TFTP server address and firmware image filename and click on the 'Start TFTP Upgrade' button.

#### TFTP Flash Upgrade:

TFTP Server IP Address:

Filename:

Ignore Firmware Version Information:   
(Allows downgrading)

Revert to Factory Configuration:   
(Warning: you will lose your current configuration)

**Note:** When you click the Upgrade button below, the Oxygen-3 gateway will stop responding while it downloads and programs the new image. Do not interrupt this process!

Refer to Section 5.11.1.1 above for information on the **Ignore Firmware Version Information** and the **Revert to Factory Configuration** options.

#### 5.11.1.3 Upgrading from the Command Line Interface (TFTP, FTP)

Firmware upgrades can also be performed from the Oxygen-3 Wireless Gateway's command line interface, making this a suitable option for scripting, etc. Both the TFTP and the FTP protocol are supported, with FTP being the preferred option when transferring the firmware image across the wireless interface.

- **Step 1:**  
Log into the Oxygen-3 Wireless Gateway using SSH or Telnet – refer to Section 6.1 for more information.
- **Step 2:**  
Use the `netflash` command as follows:

```
TFTP: netflash <tftp server IP> <firmware image name>
FTP: netflash -f <ftp server IP> <firmware image name>
```

In case of FTP, the Oxygen-3 Wireless Gateway will prompt for a username and password to log into the FTP server:

```
Oxygen-3:~ # netflash -f 172.16.100.2 Oxygen-3-4.1.0-RC4.bin

netflash: netflash: saving current config
netflash: login to remote host 172.16.100.2
Name (172.16.100.2:admin): anonymous
Password:
netflash: ftping file "Oxygen-3-4.1.0-RC4.bin" from 172.16.100.2
4614K
netflash: got "Oxygen-3-4.1.0-RC4.bin", length=5350473
netflash: image is compressed, decompressed length=50331648

netflash: currently using flash partition #2, writing new image to partition #1

netflash: flashing root filesystem, kill is forced

[...]
```

The 'netflash' upgrade tool supports additional command line options:

```
usage: netflash [-fhiStvz?] [-I ip-address] [net-server] file-name

-f      use FTP as load protocol
-h      print help
-i      ignore any version information
-I      originate TFTP request from this address
-S      don't preserve existing configuration
-t      check the image and then throw it away
-v      display version number
```

- The '-i' option is the equivalent to the **Ignore Firmware Version Information** option described in Section 5.11.1.1 above.
- The '-S' option is the equivalent to the **Revert to Factory Configuration** option described in Section 5.11.1.1 above.

### 5.11.2 Automatic Background Ping

To maintain wireless stability for latency sensitive applications, the Oxygen-3 Wireless Gateway offers the ability to generate continuous traffic over the wireless connection. This will prevent the WWAN connection from going idle, thereby preventing the modem from falling into an idle state.

Background pinging will generate additional traffic, and it permanently allocates resources on the wireless network. Use this feature with caution and make sure to consult with your wireless carrier before activating this feature.

#### Automatic Background Pinging:

Enable Background Pinging:	<input type="checkbox"/>
Ping this Host:	<input type="text" value="www.example.com"/>
Ping Interval: <small>(in seconds, from 1 to 3600)</small>	<input type="text" value="5"/>
Ping Protocol:	<input type="text" value="ICMP (regular Pings)"/>
Ping Payload Size: <small>(from 0 to 1024 bytes)</small>	<input type="text" value="0"/>
Destination Port: <small>(UDP Pings only)</small>	<input type="text" value="0"/>

There are three different kinds of pings that can be used to maintain the wireless link:

1. ICMP pings are regular pings. These are the least likely to be filtered and most likely to receive a reply from the destination host. ICMP pings generate the most traffic, using a minimum of 56 bytes per round trip ping, and more if additional payload data is specified.
2. UDP pings consist of a single outbound UDP packet, with no inbound reply. These packets are 28 bytes. If the sole purpose of background pings is to prevent the wireless link from going dormant, then it may not be necessary to elicit a reply, making UDP pings a viable option.
3. Raw pings are IP packets with no additional payload included. There will be no reply, and with the smallest packet size being 20 bytes, no additional load will be placed on the network. However, there is the risk that the wireless carrier will filter these packets as invalid.

### 5.11.3 Transparent TCP Proxy

To enable the Transparent TCP Proxy feature, the basic mode of operation (on the LAN Port page) must be set to Router Mode.

**LAN Setup:**

Mode of Operation:  
(see description above)

LAN Port IP Address and Mask:  
(not required when using automatic Pass-Through)

Enable DHCP Server on LAN Port:  
(required for automatic Pass-Through mode)

Router, use with NAT and/or IPsec ▼
Router, use with NAT and/or IPsec
Pass-Through, static LAN IP
Pass-Through, all IPs automatic

Once Router Mode has been selected, this setting must be saved and now the Proxy can be configured.

Typically, the Oxygen-3 Wireless Gateway acts as a router, passing data between two TCP endpoints. The Oxygen-3 Wireless Gateway does not modify or interfere with the data stream. However, when configured to use the Transparent TCP proxy, the Gateway will listen for the TCP streams identified on the configuration page:

**Transparent Proxy Setup:**

Enable	Port	Source IP	Destination IP	Allow Multiple Conn.
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>

When the transparent Proxy is enabled, the Oxygen-3 Wireless Gateway will intercept those connections, terminate them locally and establish a new connection from the Gateway to the original endpoint, spoofing the original source IP address.

This means there are now two TCP connections:

- One from the connected device to the Oxygen-3 Wireless Gateway.
- Another one from the Oxygen-3 Wireless Gateway across the wireless network to the remote endpoint.

The Oxygen-3 Wireless Gateway will forward data transparently in both directions. By having control over the TCP connection across the wireless network, the Oxygen-3 Wireless Gateway can now set TCP parameters such as keepalive and retry counters and timers. This can be used to avoid problems with connected devices that have their TCP parameters set too tight for the slightly higher delay on wireless networks.

The TCP proxy supports IP address only; it is not possible to enter Hostnames in the configuration fields above.

**TCP Parameter:**

TCP Keepalive Timer:  
(From 10 to 600 seconds)

TCP Retry Counter:  
(Max. no. of retries, from 2 to 20)

TCP Retry Timer:

(Time between retries, from 5 to 60 seconds)

### 5.11.4 Automatic Reversal to Failsafe Configuration

The Oxygen-3 Wireless Gateway can automatically revert to a previous configuration, which has been declared 'safe.' This feature is useful when performing configuration changes remotely.

In case of a misconfiguration, the Oxygen-3 Wireless Gateway will then revert to a 'known good' configuration after a short period, typically between one minute and one hour.

To activate the automatic scheduled reversal to a failsafe configuration, select the time period after which to revert the configuration and then press the 'Set & Schedule Failsafe Config' button:

Schedule Automatic Failsafe Activation in:

This will start a timer after which the configuration will revert to the current state. To interrupt this timer (in case of a successful configuration change that does not need to be reverted), press the 'Clear Failsafe Activation' button:

**This Oxygen-3 gateway will revert to failsafe configuration in 14:48 min.**

Click on the button below to disable the failsafe timer.

If this button is not pressed, the Oxygen-3 Wireless Gateway will apply the failsafe configuration after the indicated time period and then reboot automatically.

### 5.11.5 Manual Failsafe Configuration and Activation

The Oxygen-3 Wireless Gateway failsafe configuration can also be set and activated manually. The currently running configuration (which should be a configuration that's known to be good) can be declared the 'Failsafe Configuration' by clicking on the 'Set Failsafe Config' button:

To manually revert to this configuration at a later time, move the power switch to the reset position and keep it there.

- Immediately, all LEDs, except the blue power LED will go off. Keep the power switch in the reset position.
- After about five seconds, one of the green signal LEDs will light up. Keep the power switch in the reset position.



- After about 10 seconds, two of the green signal LEDs and the orange Network Technology LED will light up. Now release the power switch.

The Oxygen-3 Wireless Gateway will now reboot and restart with the failsafe configuration activated. If no failsafe configuration has ever been defined, the factory default configuration will be used instead.

The Oxygen-3 Wireless Gateway also supports the ability to schedule a failsafe configuration. This allows an added degree of safety when setting configuration parameters that may result in the device rendering itself unreachable. The settings to schedule a failsafe configuration can be found below the 'Create Failsafe Config' screen.

When a failsafe configuration is scheduled, a timer will display in the 'Clear Scheduled Failsafe Activation' that counts down to zero. Once the timer has reached zero, the failsafe configuration will activate and the Oxygen-3 Wireless Gateway will reboot.

### 5.11.6 Configuration Download

When clicking on the 'Config File' web configuration page, the Oxygen-3 Wireless Gateway will create a configuration tarball on the fly and present it as a downloadable link on that page.

Similarly, an existing configuration tarball can be uploaded to the unit using 'Choose file' and 'Upload' buttons on the same page.

This allows for easy provisioning of a large number of Oxygen-3 Wireless Gateways with the same configuration.

After uploading a configuration tarball, it is necessary to reboot the Oxygen-3 Wireless Gateway for the new configuration to become active.

**Note:**

Some browsers (Chrome, for example) seem to have problems when attempting to download the configuration tarball over HTTPS. If you encounter this problem, try a different browser (Firefox typically works) or access the Oxygen-3 Wireless Gateway using HTTP.

## 5.12 Event Logging

The Oxygen-3 Wireless Gateway maintains a system log that can provide useful information for trouble-shooting purposes. The system log will remain on the Oxygen-3 Wireless Gateway even if the device is rebooted, is powered off or if the firmware gets upgraded.

The system log can be viewed by clicking on the 'System Log' link under 'Diagnostics' on the web interface, or by entering the following from the command line interface (refer to Section 6.1 on how to access the command line interface):

```
cat /var/log/messages
```

When viewing the system log from the command line interface, the full log with all entries will always be shown. When viewing the system log through the web interface, it is possible to filter out less important message by changing the setting for 'System Log – Level of Detail.'

The Oxygen-3 Wireless Gateway will also periodically log wireless radio statistics. This feature can be turned on or off here, and the log frequency can be adjusted:

#### System Log Setup:

System Log - Level of Detail:	<input type="text" value="7 - Absolutely Everything"/>
Show Last Entry on Top: <small>(reverse order)</small>	<input type="checkbox"/>
Enable Wireless Stats Logging:	<input checked="" type="checkbox"/>
Radio Statistics Log Interval:	<input type="text" value="3min"/>

Events are captured in two files, with the older one being overwritten in a circular fashion once they reach a certain size.

Log events can also be forward to a remote syslog server. To enable this feature, check the **Enable Remote Logging** option and specify the IP address of the server.

#### Log to Remote Server:

Enable Remote Logging:	<input checked="" type="checkbox"/>
Remote Server - Level of Detail:	<input type="text" value="6 - Everything but Debug"/>
Set Facility to:	<input type="text" value="Local Use 5"/>
Remote Server IP Address: <small>(Domain names can be used if DNS is enabled)</small>	<input type="text"/>
Server reachable via:	<input type="text" value="LAN (primary IP)"/> GW: <input type="text"/>

Under normal circumstances, the Oxygen-3 Wireless Gateway will only generate a syslog entry containing radio statistics at the interval specified above. However, additional features such as IPsec will generate additional entries, as well as any unusual event. As a result, syslog data can reach considerable volume and it is advisable to transmit this over the LAN interface.

Depending on where the syslog server resides, it may be necessary to enter a specific gateway IP address to allow the Oxygen Gateway to set the correct route. This can be done as part of the **Server reachable via** option.

It is not required to specify an additional static route on the **Routing** screen.

## 5.13 Traffic Counter

For applications that are sensitive to mobile traffic usage, the Oxygen-3 Wireless Gateway features two data counters to monitor data volume on the wireless WWAN interface:

- A per-session counter will monitor the usage on the WWAN interface in bytes for the duration that the gateway remains connected to the cellular network. This counter will automatically be

reset once the Oxygen-3 Wireless Gateway disconnects from the cellular network. The current byte counter value can be viewed on the main web interface overview screen or via SNMP. It is not possible to reset this counter manually.

- A persistent data volume byte counter will retain its value even when the wireless link is disconnected, the Oxygen-3 Wireless Gateway is rebooted, or remains powered off for an extended duration, or has its firmware upgraded.

This counter can reset manually by clicking on the 'Clear Counter Now' button, or it can be configured to automatically reset on a scheduled day of the month to synchronize the counter with the wireless carrier's billing cycle.

#### Byte Counter Settings:

Enable Monthly Counter Reset:



Counter Reset Date:

(Day of Month)

12 ▾

On the SNMP configuration screen, you can also enable automatic warnings when data usage has exceeded a predefined threshold. This warning will be sent via an SNMP trap to the IP specified.

## 5.14 Cypress Cloud Manager

All Oxygen-3 Wireless Gateways have the ability to be managed remotely, thereby simplifying management of large fleets. For this purpose, Cypress Solutions offers **Cypress Cloud Manager (CCM)** as a configuration and management platform. Cypress Cloud Manager (CCM) is part of Cypress's suite of cloud-based services called **Cypress Cloud Services (CCS)**.

Cypress offers CCM as a cloud-based service as well as an installable package for installation on a private network. This manual only covers client side configuration options.

Communication between the Oxygen-3 Wireless Gateway and the CCM server is always initiated by the Oxygen-3 Wireless Gateway. This allows management even when the Oxygen-3 Wireless Gateway uses a dynamic IP address or in cases where the wireless carrier deploys Network Address Translation (NAT). This implies that there is a time delay between scheduling a configuration change or firmware upgrade server-side, and the time when these actions are executed on the Oxygen Gateway-3 Wireless Gateway.

### All CCM traffic is fully SSL encrypted

#### Note:

By default, CCM functionality is turned on. The Oxygen-3 Wireless Gateway will attempt to contact Cypress Solution's CCM server. This allows Cypress support staff to access the unit remotely for troubleshooting and support purposes. If you do not wish to permit access, please disable CCM.

### 5.14.1 Basic Setup

Cypress Cloud Manager support can be enabled permanently or during a configurable maintenance window. Restricting CCM to a certain period of time (typically during the night) can be useful to avoid daytime interruptions to a live network.

CCM communication (a “CCM check-in”) is always initiated by the Oxygen-3 Wireless Gateway and happens at a configurable interval. Without limiting CCM functionality to a specific ‘maintenance window,’ the network administrator will only have limited control over the precise timing when CCM-initiated actions are executed.

Enable CCM support:    
 Daily Maintenance Window:    
 Restrict to Day(s):           
 Repeat Check-in Period:    
(after going online or after start of maintenance window)

Always On  
Disabled  
Always On  
During Maintenance Window below

6 hours  
(no repeat check-ins)  
5 min  
10 min  
15 min  
30 min  
60 min  
2 hours  
3 hours  
4 hours  
6 hours  
9 hours  
12 hours  
24 hours

CCM check-ins are performed according to the following rules:

- If, within the configured maintenance window, the Oxygen-3 Wireless Gateway will perform an initial CCM check-in 30 – 60 seconds after establishing a connection to the cellular (WWAN) network.
- Subsequent check-ins will happen periodically, per the configured **Repeat Check-in Period**.
- If a subsequent check-in is outside a configured maintenance window, it will be delayed until the next maintenance window.

More frequent check-ins result in a more responsive network; however, they also cause additional management traffic. Each check-in generates about 3 kbyte traffic.

The optional field for **Network Name** can be used to give groups of Oxygen-3 Wireless Gateways a logical group name such as “Sales Offices” or “NW Region”. This name will show up server-side on the CCM management console and makes it possible to categorize a fleet of Oxygen Gateways.

Network Name:    
(optional: allows grouping by network in CCM)



Cypress advises against enabling the **Allow firmware downgrades via CCM** option.

There can be absolutely no guarantee that existing configuration will work after a firmware downgrade, therefore, there is a high likelihood that the Oxygen-3 Wireless Gateway will lose cellular connectivity after a downgrade. Doing this remotely is not recommended.

**In cases where a firmware downgrade via CCM must be performed, this must be lab-tested beforehand!**

### 5.14.2 CCM Server IP and Port Setup

The Oxygen-3 Wireless Gateway's default server URL and port settings can be used to connect to Cypress Solution's CCM installation. Alternatively, the Oxygen-3 Wireless Gateway can be configured to communicate with a custom CCM server.

CCM Server URL:	<input type="text" value="ccm.cypress.bc.ca"/>
CCM Server Port:	<input type="text" value="11651"/>
Server reachable via:	<input type="text" value="WWAN Interface"/> GW: <input type="text"/>
Allow untrusted Server Certificates:	<input checked="" type="checkbox"/>

By default, **Server reachable via** is configured for 'WWAN interface,' indicating that the Oxygen-3 Wireless Gateway expects the CCM server to be reachable via the default route pointing to the WWAN interface. If the server is reachable via the LAN interface, change the setting accordingly and enter a specific gateway IP address if required. In this case, it is not required to enter any additional static routes on the **Routing** screen. The Oxygen-3 Wireless Gateway will automatically set the required routes depending on the settings chosen here.

## 5.15 SNMP Settings

The Oxygen-3 Wireless Gateway offers the benefit of in-depth SNMP monitoring as well as event-triggered SNMP traps. Metrics such as signal, noise, band, frequency and many others are available to monitor via industry-standard third-party SNMP monitoring applications.

The Oxygen-3 Wireless Gateway's SNMP implementation supports SNMPv2 and can be enabled by checking the **Enable SNMP** option on the SNMP configuration page.

### 5.15.1 Cypress Vendor MIB

Cypress Solutions provides a 'Vendor-MIB,' which allows the SNMP monitoring station to make use of the many customized monitoring options provided by the Oxygen-3 Wireless Gateway. This MIB needs to be installed on the SNMP monitoring station prior to querying the Oxygen-3 Wireless Gateway.

The MIB can be downloaded from the SNMP page of the Oxygen-3 Wireless Gateway's web interface by clicking on the link at the top of the page.

### 5.15.2 SNMP Polling

The Oxygen-3 Wireless Gateway can be monitored via SNMP 'GET' request, commonly referred to as 'polling.' The Oxygen-3 Wireless Gateway will only reply to polls if the configured **SNMP Read Community String** matches that of the SNMP monitoring station.

#### SNMP Setup:

Enable SNMP:	<input checked="" type="checkbox"/>
SNMP Read Community String: <small>(Leave empty to disable SNMP GET messages)</small>	<input type="text" value="public"/>
SNMP Read/Write Community String: <small>(Leave empty to disable SNMP SET messages)</small>	<input type="text" value="private"/>
Only Reply to IP Addr. or Network(s): <small>(leave empty for all)</small>	<input type="text"/> <input type="text"/> <input type="text"/>

In addition to querying the Oxygen-3 Wireless Gateway using 'GET' requests, there are a number of actions that can be initiated via SNMP 'SET' requests:

- Resetting the Oxygen-3 Wireless Gateway.
- Reverting to Factory Default configuration.
- Reverting to the Failsafe configuration (see section 0 for more information).

The Oxygen Gateway will only perform the requested action if the configured **SNMP Read/Write Community String** matches that of the SNMP monitoring station.

For additional security, up to three IP networks can be white-listed. Only SNMP requests originating from these networks will be answered. If no white-listed networks are defined, then requests from all sources will be answered.

### 5.15.3 SNMP Traps

The Oxygen-3 Wireless Gateways can be configured to send a number of event-driven or periodic traps. This feature can prove useful in cases where the wireless carrier only provides a private IP address and inbound access is restricted.

To enable traps, configure an **SNMP Trap Community String** and enter the IP address of the SNMP trap receiver (**SNMP Host IP Address**). Depending on the network topology, it may be necessary to adjust the settings for **'Send Traps via Interface / Gateway'** and enter a Gateway IP address to all the Oxygen-3 Wireless Gateways to setup proper routing rules. It is not required to add additional static routes on the **Routing** screen.

Again, the Community string configured here should match the community string of the trap receiver, however, it is important to realize that traps will be sent out regardless of whether there is a match. In case of a mismatch, the receiver will simply discard the incoming trap packet.

By default, the Oxygen-3 Wireless Gateway will send traps using the IANA-registered Cypress Solutions Enterprise ID of '28954'. For backwards compatibility with older Agilink or GNCL branded installations, this can be changed by adjusting the setting for **Use Vendor ID**.

All traps contain a 'hostname' field as described in section 5.10.1. This can be used to easily identify incoming traps at the SNMP management station, even if these traps originate from Oxygen-3 Wireless Gateways with dynamic IP addresses.

The following traps are available:

Trap	Type	Description
WWAN Status	periodic	Contains up-to-date wireless network information, such as signal quality, network type information, channel, band, data counters and more. The trap interval can be configured from one minute to two hours.
Modem Status	periodic	Contains static wireless account and equipment information, such as IMEI, IMSI, ICCID and more. The trap interval can be configured from 30 minutes to 24 hours.
RSSI Alert	event-driven	Triggered by poor signal quality. Threshold values for sending the alert trap as well as the 'alert cleared' trap can be defined below.
Interface up/down	event-driven	Triggered by LAN interface link-down/up events.
CPE up/down	event-driven	Triggered by absence (and re-occurrence) of ping replies from a connected CPE device. CPE monitoring needs to be enabled and configured on the LAN Port configuration screen (see section 5.1.5).
High Traffic Alert	event-driven	Triggered if a configurable traffic counter threshold is exceeded. Repeat alerts will be sent at 110%, 120%, 130%, etc. of configured threshold. See Section 5.13 for more information on the traffic counter.
Battery Power Alert	event-driven	Triggered by a loss (or re-occurrence) of external power sources (DC Power or PoE) and subsequent seamless switchover to the built-in battery as the primary power source.
Low Battery Alert	event-driven	Triggered by the internal battery being discharged to a level of approximately 20% or less.



Precise information on what OIDs are contained in each trap can be found in the Cypress Solutions Vendor MIB

**SNMP Trap Setup:**

SNMP Trap Community String: <small>(Leave empty to disable all traps)</small>	<input type="text" value="private"/>
Send Traps to Host at IP Address:	<input type="text" value="169.254.0.2"/>
Send Traps via Interface / Gateway:	LAN (sec. IP preferred) ▼ GW: <input type="text"/>
Use Vendor ID: <small>(for backwards compatibility - non-Cypress vendor IDs will eventually be dropped)</small>	GNCI (ID 35033) ▼
WWAN Status Trap Interval:	3min ▼
Modem Status Trap Interval:	12h ▼
Send SQI Alert Trap below: <small>(SQI = Signal Quality Index)</small>	20% ▼
Clear SQI Alert above:	32% ▼
Send Interface Up/Down Traps:	<input type="checkbox"/>
Send Pingable CPE Device Up/Down Traps: <small>(enable and configure CPE device IP on LAN screen)</small>	<input type="checkbox"/>
Send High-Traffic Alert at: <small>("0" to turn off - see Traffic Counter Page)</small>	<input type="text" value="0"/> GB ▼
Alert when Running off Battery:	<input type="checkbox"/>
Repeat Battery Alert:	Never Repeat ▼
Alert when Battery is below 20%:	<input type="checkbox"/>
Repeat Low Battery Alert:	Never Repeat ▼

## 6 Using the Command Line

### 6.1 Accessing the Command Line Interface

The Oxygen-3 Wireless Gateway's command line interface (CLI) can be accessed via SSH (recommended) or via Telnet (not recommended for security reasons).

Depending on your chosen access method and access path, make sure that access is enabled on the 'Access Control' page of the Oxygen-3 Wireless Gateway's web interface. Refer to Section 5.3 for more information.

By default, only SSH access on the LAN port and via an IPsec tunnel is enabled:

**Access Setup:**

	LAN (pri. IP)		LAN (sec. IP)		WWAN Interface		IPsec Tunnel	
	Enable	Port	Enable	Port	Enable	Port	Enable	Port
Web Access:	<input checked="" type="checkbox"/>	<input type="text" value="80"/>	<input checked="" type="checkbox"/>	<input type="text" value="80"/>	<input type="checkbox"/>	<input type="text" value="801"/>	<input checked="" type="checkbox"/>	<input type="text" value="80"/>
Secure Web Acs:	<input checked="" type="checkbox"/>	<input type="text" value="443"/>	<input checked="" type="checkbox"/>	<input type="text" value="443"/>	<input type="checkbox"/>	<input type="text" value="4431"/>	<input checked="" type="checkbox"/>	<input type="text" value="443"/>
SSH Access:	<input checked="" type="checkbox"/>	<input type="text" value="22"/>	<input checked="" type="checkbox"/>	<input type="text" value="22"/>	<input type="checkbox"/>	<input type="text" value="221"/>	<input checked="" type="checkbox"/>	<input type="text" value="22"/>
Telnet Access:	<input type="checkbox"/>	<input type="text" value="23"/>	<input type="checkbox"/>	<input type="text" value="23"/>	<input type="checkbox"/>	<input type="text" value="231"/>	<input type="checkbox"/>	<input type="text" value="23"/>
SNMP Access:	<input checked="" type="checkbox"/>	<input type="text" value="161"/>	<input checked="" type="checkbox"/>	<input type="text" value="161"/>	<input type="checkbox"/>	<input type="text" value="1611"/>	<input checked="" type="checkbox"/>	<input type="text" value="161"/>

**Note:**

Access via the WWAN interface, even if enabled on the 'Access Control' page, will not work if your wireless carrier provides a private IP address. Access may also be restricted if your wireless account uses a custom APN.



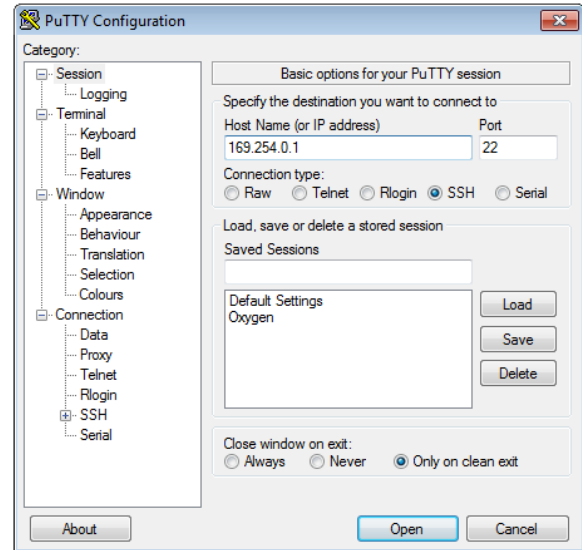
On a Windows computer, the freely downloadable PuTTY SSH client can be used to access the Oxygen-3 Wireless Gateway's command line. Linux and Mac OS X come with built-in SSH clients. The screenshot to the right shows how to establish an SSH session using PuTTY.

In this example, the Oxygen-3 Wireless Gateway is reachable at its default IP address of 169.254.0.1 using the default port 22.

After establishing a connection to the Oxygen-3 Wireless Gateway, you will be prompted for a username and password. The default username and password are:

**Username: admin**  
**Password: cypress**

The Oxygen-3 Wireless Gateway will present a standard Linux command prompt with following diagnostic tools available:

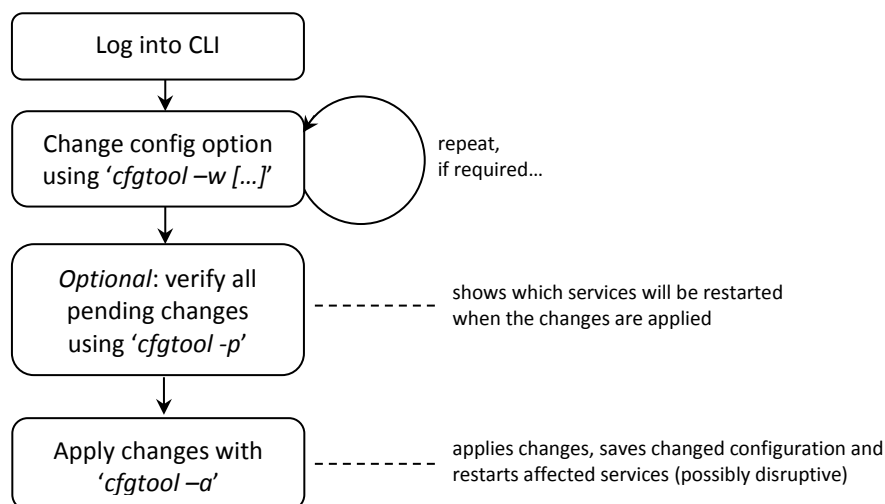


## 6.2 Changing Configuration (cfgtool)

To change the Oxygen-3 Wireless Gateway's configuration from the CLI, use the '**cfgtool**' utility.

### 6.2.1 Overview

When using **cfgtool**, follow the same workflow as outlined in Section 4.4 for the Web-GUI:



'*cfgtool*' commands have the following syntax:

```
cfgtool [options] [m] [name] [value]
```

Command	Option	Long Option (alternate)	Description
apply	-a	--apply	Apply all pending configuration changes (may cause a WWAN disconnect or other service interruptions).
help	-h	--help	Print the <i>cfgtool</i> help screen along with examples.
info	-i	--info	Show meta information for selected configuration parameter(s).
pending	-p	--pending	Shows currently pending config changes.
read	-r	--read	Shows current configuration for selected configuration parameter(s).
write	-w	--write	Write a new configuration value to a specific configuration parameter.
revert	-x	--revert	Revert selected configuration parameter value(s).
failsafe	-f	--failsafe	Set failsafe timer to [m] minutes

Argument	Description
[m]	<p>Only used in combination with the <code>failsafe</code> option:</p> <ul style="list-style-type: none"> <li>• If set to a value greater than '0,' it specifies the number of minutes after which the failsafe timer will expire and the configuration will be reverted to the failsafe config.</li> <li>• A value of '0' will disable the failsafe timer and the current configuration will be kept <b>without</b> reverting to a previously saved failsafe configuration.</li> <li>• If this Argument is omitted, the current state of the failsafe timer will be displayed.</li> </ul>
[name]	<p>Used in combination with the <code>info</code>, <code>read</code>, <code>write</code> and <code>revert</code> options:</p> <ul style="list-style-type: none"> <li>• Name, or part of the name, of one or more configuration parameters. This argument is case-insensitive.</li> <li>• Optional argument for <code>info</code>, <code>read</code> and <code>revert</code>. It is permissible to provide a partial name, which will then be used as a wildcard to match multiple configuration parameters. If this argument is omitted, the selected command will be applied to the entire configuration.</li> <li>• Mandatory argument for <code>write</code>, in which case, this argument must not be ambiguous.</li> </ul>
[value]	<p>Only used in combination with the <code>write</code> option:</p> <ul style="list-style-type: none"> <li>• The new value to be written to the specified configuration parameter.</li> </ul>



**Best Practice Recommendation:** Use the *apply* command only once at the end of a configuration session. This results in minimal disruptions and allows the Oxygen-3 Wireless Gateway to re-configure in the most efficient manner.

## 6.2.2 Determining and Configuring Parameter Names and Values

The command `cfgtool -i` will provide a complete list of all available configuration parameter names along with their type and range of allowable values:

```
Oxygen-3:~ # cfgtool -i
```

Name	Type	Range
GATEWAY_MODE	integer	0 - 2
ETH_IP	IP/maskbits (CIDR)	
LAN_ENABLE_DHCP	integer	0 - 1
DHCP_RANGE_START	IP address (A.B.C.D)	
DHCP_RANGE_END	IP address (A.B.C.D)	
LAN_ENABLE_NAT	integer	0 - 1
LAN_LINKDOWN_TIME	integer	1 - 120
DNS_MODE	integer	0 - 2
DNS_IP1	IP address (A.B.C.D)	
DNS_IP2	IP address (A.B.C.D)	
ETH_PORT_SPEED	integer	0 - 4
SEC_ETH_IP_ENA	integer	0 - 1
SEC_ETH_IP	IP/maskbits (CIDR)	
WWAN_APN1	string (generic)	
WWAN_AUTH_USER1	string (generic)	
WWAN_AUTH_PASS1	string (generic)	
[...]		

Each of these parameters is tied to an entry field in the Web-GUI. For the most part, parameter names and values are self-explanatory. Values that correspond to drop-down menus in the Web-GUI can be determined as follows:

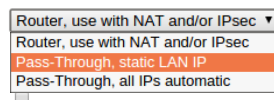
The first element of a drop-down menu parameter will have numeric value of '0' (zero). Subsequent menu elements increment upward. For example, the configuration value `GATEWAY_MODE` enumerates in the following manner:

### LAN Setup:

Mode of Operation:  
(see description above)

LAN Port IP Address and Mask:  
(not required when using automatic Pass-Through)

Enable DHCP Server on LAN Port:  
(required for automatic Pass-Through mode)



Value '0' - Router, use with NAT and/or IPsec

Value '1' - Pass-Through, static LAN IP

Value '2' - Pass-Through, all IPs automatic

As an example, if the Oxygen-3 Wireless Gateway's **Mode of Operation** is to be set to 'Router,' the following command needs to be issued from the CLI:

```
cfgtool -w gateway_mode 0
```

(this needs to be followed by `cfgtool -a` after all desired config changes have been performed).



Please note that the primary method to change the Oxygen-3 Wireless Gateway's configuration is the web-based GUI. The Web-GUI includes various checks to prevent inconsistent configuration from being applied. '*cfgtool*' lacks some of these checks and it is therefore important to test any changes that are carried out using '*cfgtool*' before deploying them to a larger number of Oxygen-3 Wireless Gateways.

### 6.2.3 Examples

#### 1. `cfgtool --read ipsec`

Displays the current configuration for all config parameters that have 'IPSEC' in their name. Note that parameters that have changed (without the changes having yet been applied) are marked with an (\*). This applies to the `IPSEC_HOST` parameter below:

Output:

```
Name ('*' = changed)      Current Config
=====
IPSEC_ENABLE              0
IPSEC_HOST (*)            10.20.30.40
IPSEC_HOST_ID             [not set]
IPSEC_HOST_ALT_ENABLE    0
IPSEC_HOST_ALT            [not set]
IPSEC_REM_NET1           [not set]
[...]
```

#### 2. `cfgtool --write ipsec_enable 1`

Set the 'IPSEC\_ENABLE' configuration parameter to '1,' which turns on IPsec VPN tunneling. Make sure all other IPsec parameters have been set before applying this config change. Unlike the Web-GUI, this tool will not do any dependency checking between individual IPsec parameters.

Output:

```
Config value successfully modified.
```

#### 3. `cfgtool --pending`

Show all pending config changes and which services will be restarted when these changes are activated (applied).

Output:

```
Name                      Change
```

```

=====
IPSEC_ENABLE          0 -> 1
IPSEC_HOST            [not set] -> 10.20.30.40

```

The following services will be restarted when changes are applied:

```

* WWAN (Cellular Connection)
* Captive Portal
* Access Rules
* IPsec VPN Tunnel
* Transparent TCP Proxy

```

#### 4. `cfgtool -x ipsec_enable`

Cancel any pending config change for the 'IPSEC\_ENABLE' configuration parameter and revert to the previous (and currently still active) value.

#### Output:

```

Name                  Change / Reversal
=====
IPSEC_ENABLE          1 -> 0

```

#### 5. `cfgtool -a`

Activate (apply) all pending config changes immediately. This may cause interruptions in connectivity depending on which services need to be restarted. (`cfgtool -p` shows which services will be restarted).

#### Output:

```

Applying all pending config changes now...

```

#### 6. `cfgtool -a -w wwan_web_acs_ena 1`

This combines the 'write' option and the 'apply' option into a single command. This should only be done when a single configuration parameter needs to be changed. This particular command enables access to the Web-GUI via the WWAN interface and activates the change immediately.

#### Output:

```

Config value successfully modified
Applying all pending config changes now...

```

#### 7. `cfgtool -f 3`

Set the current configuration as the failsafe configuration and schedule a reversal to this configuration after three minutes.

**Output:**

```
Saving current config as failsafe config...
Will revert to failsafe config in 3 minute(s).
```

**8. `cfgtool -f`**

Query the current state of the failsafe timer.

**Output:**

```
Failsafe timer active, time remaining: 2:52 min.
```

**9. `cfgtool -f 0`**

Disable the failsafe timer and keep the current configuration **without** reverting to a previously saved failsafe configuration.

**Output:**

```
Disabling failsafe timer with 2:47 min remaining.
```

## 6.3 Packet Tracing (`tcpdump`)

The Oxygen-3 Wireless Gateway contains a Linux based packet tracing facility called `tcpdump`. This is executed from the command line of the Oxygen-3 Wireless Gateway.

`tcpdump` is a convenient troubleshooting tool, as it allows for the near real-time display of traffic traversing the Oxygen-3 Wireless Gateway. This is particularly useful when attempting to identify issues that are related to customer configuration problems, downstream firewall issues, or needing verification of traffic in and out of the Oxygen-3 Wireless Gateway.

A help facility is available by typing `tcpdump --help`. Further information on `tcpdump` can be obtained from the Linux manual pages for `tcpdump`.

```
Oxygen-3:~ # tcpdump --help
tcpdump version 3.9.2
libpcap version 0.9.2
Usage: tcpdump [-aAdDeflLnNOpqRStuUvxX] [-c count] [ -C file_size ]
        [ -E algo:secret ] [ -F file ] [ -i interface ] [ -M secret ]
        [ -r file ] [ -s snaplen ] [ -T type ] [ -w file ]
        [ -W filecount ] [ -y datalinktype ] [ -Z user ]
        [ expression ]
```

Some common ways of using `tcpdump`:

```
tcpdump -n -i wwan0 host <IP address>
```

This will output all packets that traverse the wireless WWAN interface and that have *<IP address>* as either their source or destination address. The *-n* operand is used to NOT resolve IP addresses to host names. A concrete example with sample output is shown below:

```
Oxygen-3:~ # tcpdump -n -i wwan0 host 216.133.237.18
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wwan0, link-type EN10MB (Ethernet), capture size 96 bytes
13:14:50.302447 IP 216.133.237.18.500 > 74.198.34.133.500: UDP, length 92
13:14:50.314989 IP 74.198.34.133.500 > 216.133.237.18.500: UDP, length 92
```

The results of the above *tcpdump* packet trace confirm that there is UDP port 500 traffic being exchanged between the IP addresses shown. The packets are time stamped with the current time, according to the Oxygen-3 Wireless Gateway.

The following command captures all data on the wireless WWAN interface and gives a more verbose output, including packet payload:

```
Oxygen-3:~ # tcpdump -xvnNs 1500 -i wwan0
tcpdump: listening on wwan0, link-type EN10MB (Ethernet), capture size 1500 bytes
19:50:17.466056 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto: ICMP (1),
length: 84) 173.182.151.71 > 8.8.8.8: ICMP echo request, id 50950, seq 0, length 64
 0x0000: 4500 0054 0000 4000 4001 0d9c adb6 6f47
 0x0010: 0808 0808 0800 22eb c706 0000 f7c9 1644
 0x0020: 0000 0000 0000 0000 0000 0000 0000 0000
 0x0030: 0000 0000 0000 0000 0000 0000 0000 0000
 0x0040: 0000 0000 0000 0000 0000 0000 0000 0000
 0x0050: 0000 0000
19:50:18.297935 IP (tos 0x0, ttl 46, id 0, offset 0, flags [none], proto: ICMP (1),
length: 84) 8.8.8.8 > 173.182.151.71: ICMP echo reply, id 50950, seq 0, length 64
 0x0000: 4500 0054 0000 0000 2e01 5f9c 0808 0808
 0x0010: adb6 6f47 0000 2aeb c706 0000 f7c9 1644
 0x0020: 0000 0000 0000 0000 0000 0000 0000 0000
 0x0030: 0000 0000 0000 0000 0000 0000 0000 0000
 0x0040: 0000 0000 0000 0000 0000 0000 0000 0000
 0x0050: 0000 0000
```

Pressing the key combination *<ctrl>-c* stops *tcpdump*.

## 6.4 Wireless Network Information (rssiimon)

The Oxygen-3 Wireless Gateway provides a simple command line tool to obtain real-time wireless network status information in one-second intervals. It can be started by entering the following from the command line:

```
rssiimon
```

This is particularly useful when troubleshooting, as well as when trying to determine a location with optimal RF conditions during initial placement of the unit.

Since *rssimon* displays the *Cell ID*, it is also very useful when using directional antennas. This provides a level of certainty should the unit be required to connect to a particular cell site using a directional antenna.

In the example below, *rssimon* has been issued from the command line. There is a pause of one second between the output of each line.

```
Oxygen-3:~ # rssimon
Airprime MC7354, SQI: 56%, RSSI: -82 dBm, RSCP: -92 dBm, , , , , Chan: 1057, , Band: B5 (850MHz, Cellular), ,
RAT: HSDPA, no roam, Temperature: 46, , , Cell-ID: 62428922, , LAC: 11101, MCC: 402, MNC: 240
Airprime MC7354, SQI: 54%, RSSI: -82 dBm, RSCP: -93 dBm, , , , , Chan: 1057, , Band: B5 (850MHz, Cellular), ,
RAT: HSDPA, no roam, Temperature: 46, , , Cell-ID: 62428922, , LAC: 11101, MCC: 402, MNC: 240
Airprime MC7354, SQI: 54%, RSSI: -84 dBm, RSCP: -93 dBm, , , , , Chan: 557, , Band: B2 (1900 MHz, PCS), , RAT:
HSDPA, no roam, Temperature: 46, , , Cell-ID: 62428922, , LAC: 11101, MCC: 402, MNC: 240
Airprime MC7354, SQI: 54%, RSSI: -84 dBm, RSCP: -93 dBm, , , , , Chan: 557, , Band: B2 (1900 MHz, PCS), , RAT:
HSDPA, no roam, Temperature: 46, , , Cell-ID: 62428922, , LAC: 11101, MCC: 402, MNC: 240
Airprime MC7354, SQI: 54%, RSSI: -84 dBm, RSCP: -93 dBm, , , , , Chan: 557, , Band: B2 (1900 MHz, PCS), , RAT:
HSDPA, no roam, Temperature: 46, , , Cell-ID: 62428922, , LAC: 11101, MCC: 402, MNC: 240
Airprime MC7354, SQI: 64%, RSSI: -84 dBm, RSCP: -88 dBm, , , , , Chan: 557, , Band: B2 (1900 MHz, PCS), , RAT:
HSDPA, no roam, Temperature: 46, , , Cell-ID: 62428922, , LAC: 11101, MCC: 402, MNC: 240
Airprime MC7354, SQI: 64%, RSSI: -83 dBm, RSCP: -88 dBm, , , , , Chan: 1057, , Band: B5 (850MHz, Cellular), ,
RAT: HSDPA, no roam, Temperature: 46, , , Cell-ID: 62428922, , LAC: 11101, MCC: 402, MNC: 240
Airprime MC7354, SQI: 64%, RSSI: -83 dBm, RSCP: -88 dBm, , , , , Chan: 1057, , Band: B5 (850MHz, Cellular), ,
RAT: HSDPA, no roam, Temperature: 46, , , Cell-ID: 62428922, , LAC: 11101, MCC: 302, MNC: 220
```

The example shows that the Oxygen-3 Wireless Gateway is on the 3G WCDMA network and switches from the 850MHz band (channel 1057) to the 1900MHz band (channel 557) and then back. Signal quality is average, the Cell-ID is 62428922 and it is NOT roaming.

Since the unit can run on battery, *rssimon* can be issued while the Oxygen-3 Wireless Gateway is being moved around within a customer premise without any need for device to be connected to an external power source. The immediate output can provide quick insight as to be best RF location within the premises.

Pressing the key combination <ctrl>-c stops *rssimon*.

In cases where *rssimon* is being called from a script, it may be desirable to only output a certain number of lines and then stop automatically. *rssimon* provides the *-c* command line switch for that. The following example provides three lines of *rssimon* output:

```
Oxygen-3:~ # rssimon -c 3
Airprime MC7354, SQI: 56%, RSSI: -84 dBm, RSCP: -92 dBm, , , , , Chan: 537, , Band: B2 (1900 MHz, PCS), , RAT:
HSDPA, no roam, Temperature: 46, , , Cell-ID: 72428922, , LAC: 11101, MCC: 302, MNC: 220
Airprime MC7354, SQI: 56%, RSSI: -84 dBm, RSCP: -92 dBm, , , , , Chan: 537, , Band: B2 (1900 MHz, PCS), , RAT:
HSDPA, no roam, Temperature: 46, , , Cell-ID: 72428922, , LAC: 11101, MCC: 302, MNC: 220
Airprime MC7354, SQI: 56%, RSSI: -84 dBm, RSCP: -92 dBm, , , , , Chan: 537, , Band: B2 (1900 MHz, PCS), , RAT:
HSDPA, no roam, Temperature: 46, , , Cell-ID: 72428922, , LAC: 11101, MCC: 302, MNC: 220
Oxygen-3:~ #
```

## 6.5 Ping

Ping is a standard tool to test whether a certain destination can be reached. Ping can be issued from the command line with the syntax *ping <host> -I <source ip>*. The *-I* operand is optional.

Example



```
Oxygen-3:~ # ping 172.16.100.1 -I 192.168.49.1
PING 172.16.100.1 (172.16.100.1) from 192.168.49.1: 56 data bytes
64 bytes from 172.16.100.1: seq=0 ttl=255 time=202.728 ms
64 bytes from 172.16.100.1: seq=1 ttl=255 time=181.549 ms
64 bytes from 172.16.100.1: seq=2 ttl=255 time=181.030 ms
64 bytes from 172.16.100.1: seq=3 ttl=255 time=194.946 ms
64 bytes from 172.16.100.1: seq=4 ttl=255 time=226.075 ms
```

## 6.6 HPing

Hping can be used for more specific testing. There is a vast amount of options for transmitting IP, ICMP, UDP packets with numerous payload options. This can be used for testing and diagnosis of various network conditions. Some of these conditions could be troubleshooting MTU issues, TCP port specific issues with firewalls, or the need to send non ICMP based pings due to APN or firewall restrictions. The full set of commands and options are listed below. This list can be obtained at command line by issuing the *hping -h* command as shown below:

```
Oxygen-3:~ # hping -h
usage: hping host [options]
  -h --help          show this help
  -v --version       show version
  -c --count         packet count
  -i --interval     wait (uX for X microseconds, for example -i u1000)
                   --fast          alias for -i u10000 (10 packets for second)
                   --faster        alias for -i u1000 (100 packets for second)
                   --flood         sent packets as fast as possible. Don't show replies.
  -n --numeric      numeric output
  -q --quiet         quiet
```

[... remaining output omitted ...]

The following example shows the *hping* command being used to send a TCP RST (Reset) packet on TCP port 9000 to destination address 74.198.22.216 for trouble shooting purposes.

```
Oxygen-3:~ # hping -p 9000 -R 74.198.22.216
HPING 74.198.22.216 (wwan0 74.198.22.216): R set, 40 headers + 0 data bytes
```

The packet was examined on the outbound *wwan0* interface using *TCPdump* at the same time.

```
Oxygen-3:~ # tcpdump -i wwan0 host 74.198.22.216
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wwan0, link-type EN10MB (Ethernet), capture size 96 bytes

10:05:00.677311 IP 74.198.34.133.1700 > 74.198.22.216.9000: R 1840941308:1840941308(0) win 512
10:05:01.681095 IP 74.198.34.133.12tp > 74.198.22.216.9000: R 1343821945:1343821945(0) win 512
10:05:02.681400 IP 74.198.34.133.1702 > 74.198.22.216.9000: R 400207156:400207156(0) win 512R
```

In another example below, *hping* is being used to transmit a UDP packet on port 1611 with a UDP size of 1410 bytes, with the do not fragment bit set to IP address 74.198.22.216.

```
Oxygen-3:~ # hping -2 -p 1611 -d 1410 -y 74.198.22.216
HPING 74.198.22.216 (wwan0 74.198.22.216): udp mode set, 28 headers + 1410 data bytes
^C
--- 74.198.22.216 hping statistic ---
```

```
4 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

The packets were examined on the outbound `wwan0` interface using `TCPdump` at the same time.

```
10:13:44.103214 IP 74.198.34.133.1072 > 74.198.22.216.1611: UDP, length 1410
10:13:45.104221 IP 74.198.34.133.1073 > 74.198.22.216.1611: UDP, length 1410
10:13:46.105381 IP 74.198.34.133.1074 > 74.198.22.216.1611: UDP, length 1410
10:13:47.106510 IP 74.198.34.133.1075 > 74.198.22.216.1611: UDP, length 1410
```

## 6.7 iPerf

iPerf is a tool that can be used to measure the speed of a network connection. It is particularly useful in diagnosing speed issues during the design phase of networks, or as a measurement tool to verify speed availability for customers requiring certain minimum speed requirements. iPerf must run with a peer on the network. In most cases, this is a peer on a landline egress from the carrier, either Internet based, or with custom landline access.

iPerf on the Oxygen-3 Wireless Gateway can run in client mode or server mode, such that both uplink and downlink directions can be tested for speed. iPerf has command line options, which can be displayed by using the `iperf -h` help facility. These options are shown below:

```
Oxygen-3:~ # iperf -h
Usage: iperf [-s|-c host] [options]
       iperf [-h|--help] [-v|--version]

Client/Server:
  -f, --format [kmKM]      format to report: Kbits, Mbits, KBytes, MBytes
  -i, --interval #        seconds between periodic bandwidth reports
  -l, --len #[KM]         length of buffer to read or write (default 8 KB)
  -m, --print_mss         print TCP maximum segment size (MTU - TCP/IP header)

[... remaining output omitted ...]
```

In the example below, the Oxygen-3 Wireless Gateway is being used as an iPerf client (`-c` operand) connecting to an iPerf server at `169.254.0.2`, using TCP port `5001` (default), with a bandwidth report every 10 seconds, and using three TCP threads (connections) concurrently.

The results show that the aggregate measured bandwidth of the three simultaneous connections is `94.6 Mbit/sec`, which is expected given that the test was performed across the LAN interface.

```
Oxygen-3:~ # iperf -c 169.254.0.2 -t 60 -i 10 -P 3
-----
Client connecting to 169.254.0.2, TCP port 5001
TCP window size: 64.0 KByte (default)
-----
[ 8] local 169.254.0.1 port 54672 connected with 169.254.0.2 port 5001
[ 5] local 169.254.0.1 port 54670 connected with 169.254.0.2 port 5001
[ 7] local 169.254.0.1 port 54671 connected with 169.254.0.2 port 5001
[ ID] Interval      Transfer    Bandwidth
[ 8]  0.0-10.0 sec  40.1 MBytes  33.7 Mbits/sec
[ 7]  0.0-10.0 sec  34.6 MBytes  29.0 Mbits/sec
[ 5]  0.0-10.0 sec  40.0 MBytes  33.6 Mbits/sec
[SUM] 0.0-10.0 sec   115 MBytes  96.3 Mbits/sec
[ 8] 10.0-20.0 sec  34.9 MBytes  29.3 Mbits/sec
[ 5] 10.0-20.0 sec  41.9 MBytes  35.1 Mbits/sec
```

```

[ 7] 10.0-20.0 sec 35.1 MBytes 29.5 Mbits/sec
[SUM] 10.0-20.0 sec 112 MBytes 93.8 Mbits/sec
[ 5] 20.0-30.0 sec 44.6 MBytes 37.4 Mbits/sec
[ 7] 20.0-30.0 sec 44.5 MBytes 37.3 Mbits/sec
[ 8] 20.0-30.0 sec 23.8 MBytes 19.9 Mbits/sec
[SUM] 20.0-30.0 sec 113 MBytes 94.7 Mbits/sec
[ 7] 30.0-40.0 sec 38.1 MBytes 32.0 Mbits/sec
[ 8] 30.0-40.0 sec 25.4 MBytes 21.3 Mbits/sec
[ 5] 30.0-40.0 sec 48.6 MBytes 40.8 Mbits/sec
[SUM] 30.0-40.0 sec 112 MBytes 94.1 Mbits/sec
[ 5] 40.0-50.0 sec 39.9 MBytes 33.4 Mbits/sec
[ 8] 40.0-50.0 sec 23.3 MBytes 19.5 Mbits/sec
[ 7] 40.0-50.0 sec 49.5 MBytes 41.5 Mbits/sec
[SUM] 40.0-50.0 sec 113 MBytes 94.5 Mbits/sec
[ 7] 50.0-60.0 sec 50.9 MBytes 42.7 Mbits/sec
[ 8] 50.0-60.0 sec 28.9 MBytes 24.2 Mbits/sec
[ 8] 0.0-60.0 sec 176 MBytes 24.6 Mbits/sec
[ 5] 50.0-60.0 sec 32.1 MBytes 26.9 Mbits/sec
[SUM] 50.0-60.0 sec 112 MBytes 93.8 Mbits/sec
[ 5] 0.0-60.0 sec 247 MBytes 34.5 Mbits/sec
[ 7] 0.0-60.0 sec 253 MBytes 35.4 Mbits/sec
[SUM] 0.0-60.0 sec 677 MBytes 94.6 Mbits/sec
Oxygen-3:~ #

```

Below is another test with the Oxygen-3 Wireless Gateway operating in server mode:

```

Oxygen-3:~ # iperf -s
-----
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
-----
[ 9] local 169.254.0.1 port 5001 connected with 169.254.0.2 port 36125
[ 7] local 169.254.0.1 port 5001 connected with 169.254.0.2 port 36123
[ 8] local 169.254.0.1 port 5001 connected with 169.254.0.2 port 36124
[ ID] Interval      Transfer    Bandwidth
[ 7] 0.0-60.1 sec    225 MBytes 31.4 Mbits/sec
[ 9] 0.0-60.1 sec    225 MBytes 31.4 Mbits/sec
[ 8] 0.0-60.1 sec    225 MBytes 31.4 Mbits/sec
[SUM] 0.0-60.1 sec 674 MBytes 94.1 Mbits/sec

```

## 6.8 Arp Cache

The Arp Cache contains a list of MAC-Addresses currently known to the Oxygen-3 Wireless Gateway. It can be viewed using the command line. This is useful when diagnosing if devices connected behind the Oxygen-3 Wireless Gateway are online. The list can be obtained by issuing the following command:

```
cat /proc/net/arp
```

```

Oxygen-3:~ # cat /proc/net/arp
IP address      HW type    Flags       HW address    Mask        Device
169.254.0.2     0x1       0x2        00:20:f3:1e:02:25  *          eth0
Oxygen-3:~ #

```

The output will display IP addresses tied to MAC-Addresses. If you see multiple IP addresses associated to a single MAC-address, that MAC-address is likely a router or switch.

## 7 Using the RS-232 Serial Port

The Oxygen-3 Wireless Gateway's serial port allows a connection to another device for administration purposes. There are two options for gaining access to the serial port:

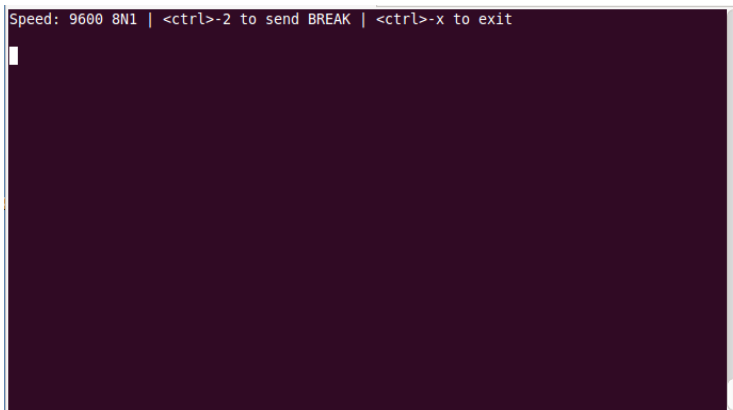
- 1) The Oxygen-3 Wireless Gateway has built-in terminal software that can be accessed from the command line by entering:

```
oxycom <baud rate>
```

For example:

```
oxycom 9600
```

This starts the Gateway's terminal software and establishes a connection via the serial port:



Press <ctrl> - 2 to send a break signal (for example to enter ROMMON mode on a Cisco® router)  
Press <ctrl> - x to exit from the terminal software

- 2) Pointing an SSH client to the Oxygen-3 Wireless Gateway's IP address, using the default port 11622, or whatever has been configured using the GUI. \* user name has to be 'admin' - no password required.

To enable this feature, click on 'Advanced -> Serial Console Passthrough' in the web GUI.

There are two optional parameters:

- 'force' to force termination of an already existing session
- <baudrate> : '2400|4800|9600|19200|38400|57600|115200', to select the serial port speed. If this parameter is omitted, the configured default baud rate setting will be used

For Example:

```
ssh -l admin -p 11622 <Oxygen-IP> force 115200
```

When using PuTTY or secureCRT, optional parameters can be entered as 'Remote command' in the options dialog.

If an 'oxycom'-user and another user that uses the new direct-ssh method compete for access to the serial port, then the user that specifies the 'force' parameter gets it!

#### Serial Console Pass-Through Options:

Enable Serial Console Pass-Through:

Serial Console Pass-Through Port:

Default Baud Rate:  ▼  
(can be overridden by SSH command parameter)

Idle Timeout:  ▼

Serial Console Access Whitelist:  
max. 30 CIDR IP Networks, delimited by space

To do so, the following preconditions must be met:

- The Oxygen-3 Wireless Gateway must have the serial port option installed.
- The Oxygen-3 Wireless Gateway must be connected to another device (typically a DTE) via a serial port cable. Refer to Section 2.5 for the pin-out of the Gateway's serial port and to section 3.5 for available cables.
- The Oxygen-3 Wireless Gateway does not support any handshaking and by default the Gateway's serial port is set to 8 data bits, no parity and 1 stop bit (8N1).
- The baud rate of the connected device must be known.

## 8 Understanding the Signal Quality Indicator (SQI)

The Oxygen-3 Wireless Gateway uses an internal Signal Quality Indicator (SQI) to display the current wireless signal quality.

The reason being, that in modern 3G and 4G networks the traditionally used RSSI indicator is no longer the best measure for signal quality. Instead, the indicators below should be used:

2G (GSM/GPRS/EDGE)	RSSI
3G (WCDMA/UMTS/HSPA)	RSCP
4G (LTE)	RSRP

However, this makes it harder for the end user to obtain a good sense of the current signal conditions. Signal strength values have different meanings, depending on network technology.

To provide a normalized value independent of the currently active network technology, the Oxygen-3 Wireless Gateway then uses the following formulas to translate the current RSSI, RSCP or RSRP value to an SQI value ranging from 0 to 100%.

- 2G:  $SQI = (RSSI + 105) * 2.5$
- 3G:  $SQI = (RSCP + 120) * 2$
- 4G:  $SQI = (RSRP + 133) * 1.587$

This leads to the following scale:

SQI lower than 20%	Very poor signal quality
SQI between 20% and 40%	Minimally acceptable signal quality
SQI between 40% and 80%	Average signal quality
SQI above 80%	Good signal quality

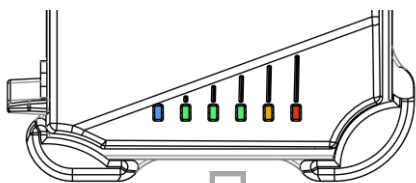
**Note:**

The SQI value only reflects current signal strength, but not current signal noise. Noise is represented by the  $E_c/I_o$  value (WCDMA) or the RSRQ value (LTE). The precise influence of the noise value on network performance is often hard to predict, other than in very general terms. When encountering a situation with high noise values, it is advisable to perform additional longer-term tests (for example ping tests and throughput test) to determine network performance.

## Reverting to Factory Default Configuration

The Oxygen-3 Wireless Gateway can be reset to factory default configuration by moving the reset/power switch to the 'Reset' position for a certain amount of time. A similar procedure is used to revert to the failsafe configuration, which is also explained here. See Section 4 how to locate the reset/power switch.

Move the reset/power switch to the 'Reset' position and hold it there. Observe the Oxygen-3 Wireless Gateway's LED patterns:



The Oxygen-3 Wireless Gateway will resume normal operation.

For the first five seconds after moving the switch to the 'Reset Position,' all LEDs except the blue power LED will be off. If the switch is released now, nothing will happen and the Oxygen-3 Wireless Gateway will resume normal operation.

For the next five seconds, the LED pattern to the left will be visible. If the switch is released now, the Oxygen-3 Wireless Gateway will reset **without any config changes**.

For the next five seconds, the LED pattern to the left will be visible. If the switch is released now, the Oxygen-3 Wireless Gateway will reboot and revert to **failsafe configuration**.

For the next five seconds, the LED pattern to the left will be visible. If the switch is released now, the Oxygen-3 Wireless Gateway will reboot and revert to **factory default configuration**.

## 9 Troubleshooting

Problem	Answer
<p>The Oxygen-3 Wireless Gateway is not powering on.</p>	<ul style="list-style-type: none"> <li>• Check that the power connector is firmly seated in the Oxygen-3 Wireless Gateway and that the switch is in the 'on' position.</li> <li>• If running off the built-in battery, consider that the battery may be discharged.</li> </ul>
<p>It is not possible to access the web interface.</p>	<p>Follow the guide to connect to the device as outlined in Section 4.3. If you are still unsuccessful, conduct the following tests:</p> <ul style="list-style-type: none"> <li>• Restart the Oxygen-3 Wireless Gateway by removing power, and adding it again.</li> <li>• Make sure that the Power LED is solid blue, and the Online LED is either solid or flashing red.</li> <li>• Ensure the computer you are connecting from is configured to obtain its IP address via DHCP.</li> <li>• Ensure you are connected via Ethernet cable to the device, and that both your link and activity lights are lit.</li> <li>• Open your network configuration and note the Oxygen-3 Wireless Gateway.</li> <li>• Attempt to access the gateway in your web browser.</li> <li>• Perform a reset to factory default configuration on the Oxygen-3 Wireless Gateway as outlined in Section 0.</li> </ul>
<p>The modem powers on, and appears to be connecting to the network, but never completes the connection attempt.</p>	<p>It is most likely that your SIM card is not activated, or the APN is set incorrectly on the Oxygen-3 Wireless Gateway.</p> <ul style="list-style-type: none"> <li>• Check the Gateway's system log to obtain additional information.</li> <li>• Contact your carrier to obtain information on your account, including activation state and APN.</li> </ul>
<p>After the modem connects to the wireless network, it is no longer possible to access the web interface.</p>	<p>When the Oxygen-3 Wireless Gateway operates in Pass-Through mode, it adjusts the IP on the Ethernet port to resemble what IP address the carrier assigns.</p> <ul style="list-style-type: none"> <li>• To find the new Ethernet IP address, open your network settings, note the Gateway and attempt to access it via your web browser.</li> <li>• Alternatively, you can configure a secondary IP address on the Oxygen-3 Wireless Gateway's LAN port (default: 169.254.0.1) and attempt to reach the Gateway at that IP address.</li> </ul>



## Contact

**Phone:****Sales**

Toll Free: 1-877-985-2878

Local: 1-604-294-4465

Toll Free: 1-844-462-9773

Local: 1-778-372-4603

**Email:**[support@cypress.bc.ca](mailto:support@cypress.bc.ca)

Emailing [support@cypress.bc.ca](mailto:support@cypress.bc.ca) will automatically generate a support ticket with Cypress Solutions.

**Mailing Address:**

Cypress Solutions Inc.

3066 Beta Avenue

Burnaby, BC

V5G 4K4

Canada

© Cypress Solutions Inc.