

## Default Access Credentials

- Default IP address: **192.168.1.1**
- Default password: **admin**
- Default username (for SSH): **root**
- Default link (for settings): <https://192.168.1.1>

# Telco X1 Pro Documentation



RCM Certified

# Table of Contents

Default Access Credentials	1
<b>Hardware Specifications</b>	<b>6</b>
Electrical	6
Cat12 LTE Advanced Pro Modem	6
Physical	8
<b>1 Package Contents</b>	<b>9</b>
Important changes in TelcOS 2.3	10
<b>2 General Setup &amp; Quick Start</b>	<b>11</b>
2.0.1 Default Access Credentials	11
2.1 Firmware Upgrade	11
2.2 Quick Start	12
<b>Done!</b>	<b>14</b>
<b>3 Mobile Data - Advanced Setup</b>	<b>15</b>
3.1 Authentication	15
3.2 Band Locking	16
Lock to Frequency Bands	16
Steps	16
<b>4 Wifi - Advanced Setup</b>	<b>17</b>
4.1 Wifi Radio Configuration	17
4.1.1 General	18
4.2 Advanced Wifi Radio Configuration	19
About ACMA WiFi Regulations	20
4.3 Advanced Interface Options	21
4.3.1 General Tab	21
4.3.2 Wireless Security Tab	22
2.4.3.3 MAC Filter Tab	23
2.4.3.4 Advanced Settings	24
<b>5 Advanced - Command Line Interface</b>	<b>25</b>
5.0.1 Access the Command Line Interface	25
Example	25
5.0.2 Show all available commands	26
5.1 Signal Information	26
5.1.2 Get Signal Strength	26
<b>6 Advanced Networking</b>	<b>27</b>

6.1 Port Forwarding	27
6.1.1 Adding a Port Forward Rule	27
Steps	27
Example	28
6.2 Using WAN Port as an Extra LAN Port	29
Steps	29
6.3 WAN Failover Options	31
Steps	31
6.4 Guest WiFi Configuration Example	32
6.4.1 Wireless Configuration for the Guest Network	32
6.4.2 Network Configuration for the Guest Network	34
6.4.3 Firewall Rules for the Guest Network	37
Allow Guests to use DNS	38
Allow Guests to use DHCP	38
Conclusion	39
6.5 Bridge Mode	39
6.5.1 How to use Bridge Mode	39
6.5.2 Bridge Mode Tips	40
Band Locking	40
Access X1 Pro while in Bridge Mode	40
ssh root@192.168.1.1	40
Quit Bridge Mode	40
Button	40
SSH	40
6.6 NBN Connectivity	41
<b>7 Services</b>	<b>42</b>
7.1 Dynamic DNS (DDNS)	42
Steps	42
7.2 Automatic Recovery	43
7.2.1 Example	44
7.3 Wake on LAN	44
7.3 File Shares (SAMBA/NAS)	45
<b>8 Firmware and Backup</b>	<b>47</b>
8.1 Backup	47
8.2 Restore or Transfer Settings	47
8.3 Install New Firmware	47
8.4 Reset	47
<b>9 Tips and Recommendations</b>	<b>48</b>
9.1 Wireless Security and Performance	48
9.2 Device Security	48
9.3 Network Security	48

9.4 Network Reliability

## Telco X1 Pro

# Hardware Specifications

## Electrical

- PoE powered - guaranteed 50m range over Cat6 cable
- Antenna connectors
  - 2x Mobile data: SMA Female antenna connector
  - 2x Wifi: RP-SMA Female
  
- 2.4GHz WiFi - 802.11a/b/g/n
  - up to 300Mbps capacity
  - up 100m radius outdoor coverage area 30m indoor
  - Recommended for up to 100 clients
- 5GHz WiFi - 802.11ac
  - Up to 900Mbps capacity
  - Up to 100m radius outdoor coverage area 30m indoor
  - Recommended for up to 100 clients
  
- 1000Mbps Gigabit Ethernet: 4 LAN, 1 WAN
  - 1x WAN Port
    - Can be changed to extra LAN
  - 4x LAN Ports
  
- Cat12 LTE Advanced Pro Modem
  - Peak Download Rate: 600Mbps
  - Peak Upload Rate: 150Mbps
  - Maximum aggregated bandwidth: up to 60MHz
  - Transmit Power (max)
    - LTE Bands: +23 dBm +/- 2dB
    - UMTS Bands: +24 dBm +/- 3dB
  - Supported Frequency Bands)
    - LTE Band 1
    - LTE Band 2
    - LTE Band 3
    - LTE Band 5
    - LTE Band 7
    - LTE Band 8
    - LTE Band 9
    - LTE Band 12
    - LTE Band 13

- LTE Band 14
- LTE Band 17
- LTE Band 18
- LTE Band 19
- LTE Band 20
- LTE Band 21
- LTE Band 25
- LTE Band 26
- LTE Band 28
- LTE Band 29
- LTE Band 30
- LTE Band 32
- LTE Band 38
- LTE Band 39
- LTE Band 40
- LTE Band 41
- LTE Band 66
- UMTS Band 1
- UMTS Band 5
- UMTS Band 6
- UMTS Band 8
- UMTS Band 9
- UMTS Band 19
- 1x Nano-SIM slot
- Power consumption: < 12W

## Physical

- Height: 30mm
  - With antennas: add 145mm to height
- Width: 155mm
- Depth: 110mm
- Weight: 200g
- Material: Metal
- Operating temperature: -10° to +55° C
- Operating humidity: 10% to 90% non-condensing
- DIN Rail Installation - DIN rail mounts included
- Backplate Installation - Mounts available
- Desktop/Set top Installation

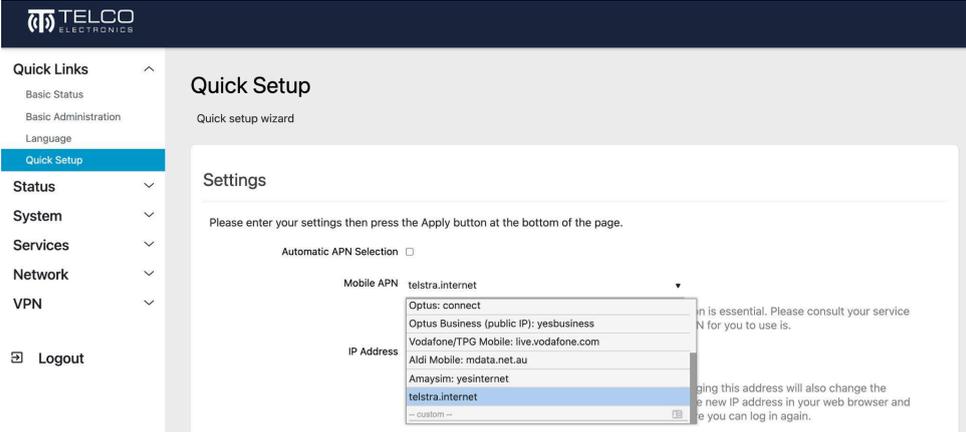
# 1 Package Contents

Please ensure your package contains everything in the following list. In the event that anything is missing or damaged, please do not hesitate to contact us at [sales@telcoantennas.com.au](mailto:sales@telcoantennas.com.au) or +61 (07) 3393 9919 M-F 9am to 5pm AEST.

1. 1x Telco X1 Pro
2. 1x Power Supply
3. 2x LTE antennas
4. 2x Wifi antennas
5. 1x Ethernet cable
6. 2x DIN rail mounts

# Important changes in TelcOS 2.3

- 1. When Changing the **APN**, please use the new **Quick Setup Wizard** located under **Quick Links > Quick Setup**. This is a workaround for a bug in the new Linux Distributed Switch Architecture which will remove a required “device” attribute from the MOBILEDATA interface configuration. This bug will be addressed in a future release.

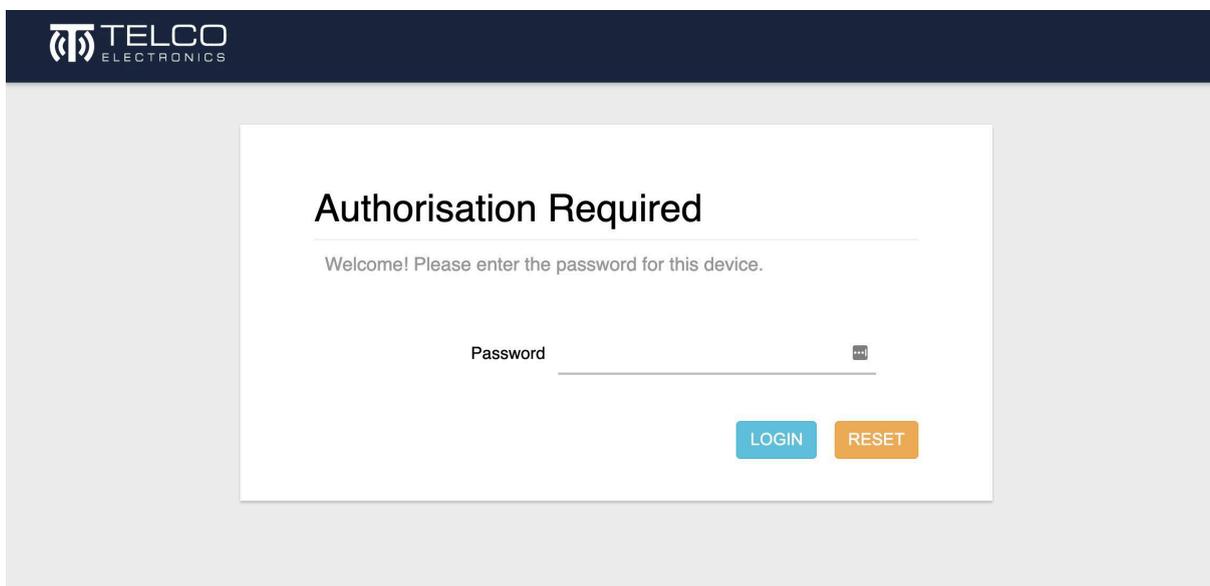


## Quick Start Procedure

# 2 General Setup & Quick Start

### 2.0.1 Default Access Credentials

- Default IP address: **192.168.1.1**
- Default Password: **admin**
- Default Username (for SSH): **root**



## 2.1 Firmware Upgrade

Please visit [www.telcoelectronics.com.au/downloads](http://www.telcoelectronics.com.au/downloads) for the latest firmware, free for life, which contains new features, enhancements and fixes.

Power cycling the device is required after a firmware upgrade.

## 2.2 Quick Start

1. Insert your SIM card and power up the device



SIM should be **facing upwards** when inserted. Push SIM tray all the way in until flush with the case (not shown)

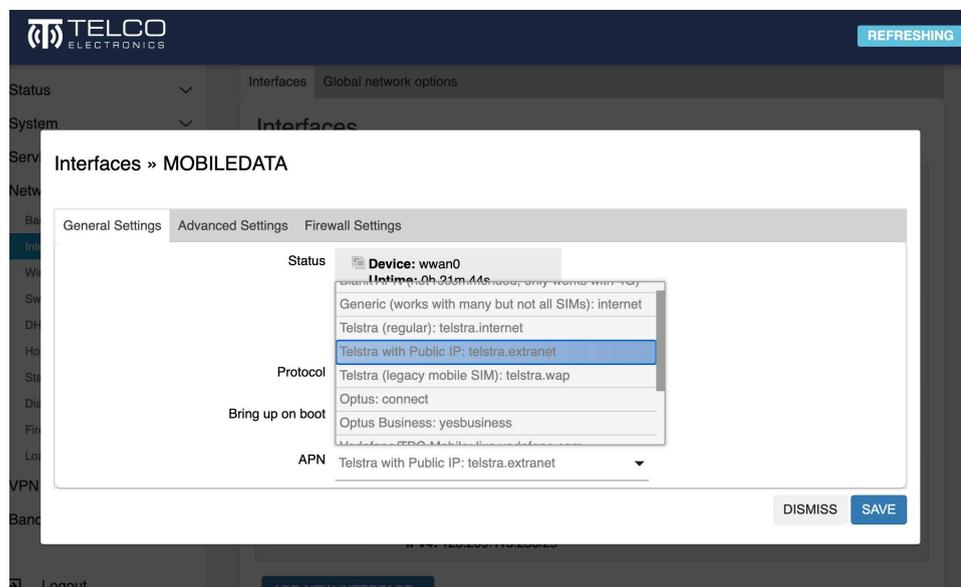
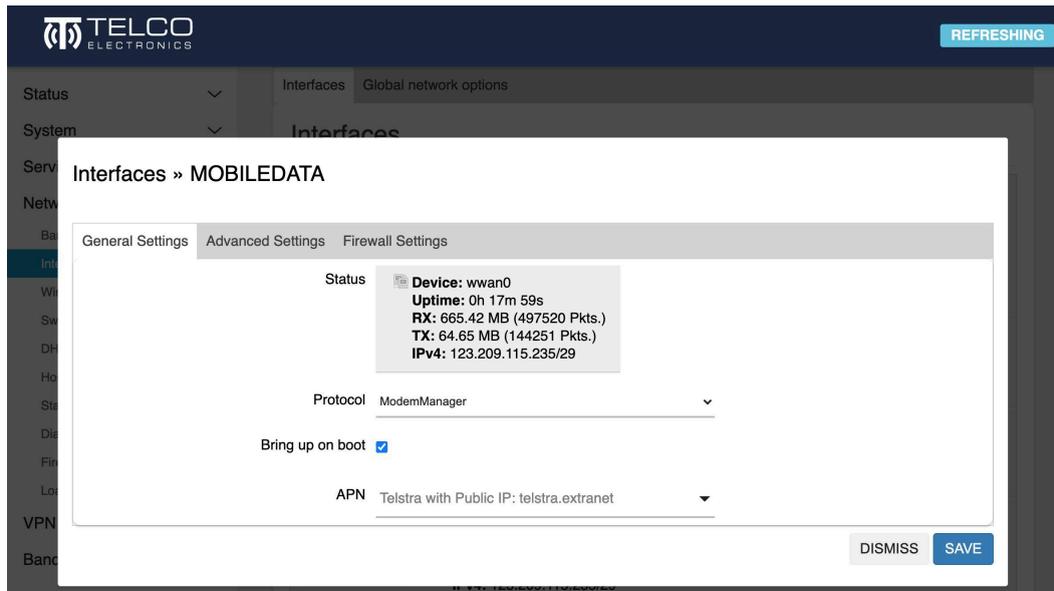
2. Connect your computer to the device via LAN port or use Wifi
3. Log in using the access credentials
4. Navigate to **Network > Interfaces > MobileData** and click **Edit**

The screenshot displays the TELCO ELECTRONICS web interface. On the left, a sidebar menu lists various system settings, with 'Interfaces' highlighted in blue and circled in red. A red arrow points from this menu item to the 'EDIT' button of the 'MOBILEDATA' interface in the main content area. The 'MOBILEDATA' interface is currently selected and shows the following configuration:

Interface	Protocol	Uptime	MAC	RX	TX	IPv4	IPv6	Actions
LAN (br-lan)	Static address	0h 18m 12s	32:15:D9:F5:48:42	65.37 MB (127530 Pkts.)	671.12 MB (498239 Pkts.)	10.36.41.1/24	fd97:e5f3:bd78::1/60	RESTART STOP EDIT DELETE
WAN (eth1)	DHCP client		46:A8:5C:62:A9:5D	0 B (0 Pkts.)	0 B (0 Pkts.)			RESTART STOP EDIT DELETE
WAN6 (eth1)	DHCPv6 client		46:A8:5C:62:A9:5D	0 B (0 Pkts.)	0 B (0 Pkts.)			RESTART STOP EDIT DELETE
MOBILEDATA (wwan0)	ModemManager	0h 17m 44s		665.37 MB (497344 Pkts.)	64.62 MB (144074 Pkts.)		123.209.115.235/29	RESTART STOP EDIT DELETE

At the bottom of the interface, there are buttons for 'ADD NEW INTERFACE...', 'SAVE & APPLY', 'SAVE', and 'RESET'.

5. Enter your APN or choose appropriately from the dropdown menu



6. Proceed to **Advanced Setup** if necessary, outlined in Section 3 of this documentation
7. Set up Wifi as required - outlined in Section 4 of this documentation
  - a. To set the Wifi Password (key): Navigate to **Network > Wireless > Edit > Wireless Security**. For details, see Section 4.3.2
8. Physically install the device as required

# Done!

The screenshot displays the 'Interfaces' section of the TELCO ELECTRONICS management interface. The left sidebar contains navigation options: Status, System, Services, Network (with sub-items: Band Locking, Interfaces, Wireless, DHCP and DNS, Hostnames, Static Routes, Diagnostics, Firewall, Load Balancing, SQM QoS), VPN, and Bandwidth Monitor. A 'Logout' button is at the bottom of the sidebar. The main content area shows a table of network interfaces with their respective protocols, statistics, and control buttons.

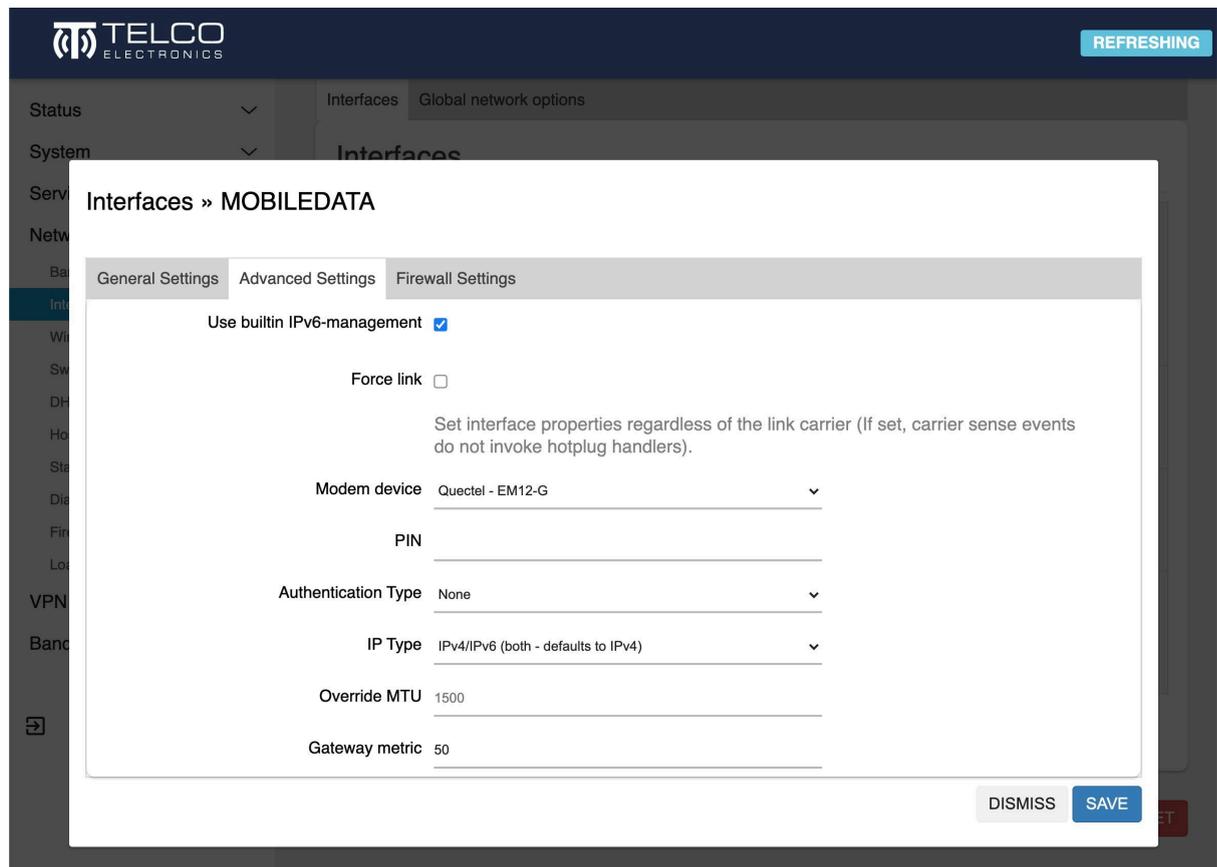
Interface	Protocol	Uptime	MAC	RX	TX	IPv4	IPv6	IPv6-PD	Actions
LAN br-lan	Static address	0h 6m 28s	2A:96:07:BC:96:CA	822.25 KB (7477 Pkts.)	3.34 MB (5625 Pkts.)	192.168.1.1/24	fd97:1e65:48fe:c::1/62	fd12:adff:1126::1/60	RESTART STOP EDIT DELETE
WAN eth1	DHCP client	0h 6m 19s	C2:4C:71:E1:16:2B	324.95 KB (2255 Pkts.)	16.03 KB (221 Pkts.)	192.168.0.186/24			RESTART STOP EDIT DELETE
WAN6 eth1	DHCPv6 client	0h 6m 19s	C2:4C:71:E1:16:2B	324.95 KB (2255 Pkts.)	16.03 KB (221 Pkts.)		fd97:1e65:48fe:0:c04c:71ff:fee1:162b/64	fd97:1e65:48fe::731/128	RESTART STOP EDIT DELETE
MOBILEDATA wwan0	ModemManager	0h 0m 15s		3.67 KB (99 Pkts.)	4.15 KB (101 Pkts.)	120.157.12.128/24			RESTART STOP EDIT DELETE

*MobileData interface up and running, along with WAN interface*

## 3 Mobile Data - Advanced Setup

### 3.1 Authentication

If your connection requires the use of extra parameters, these are located under the Advanced Setup options.



The following advanced options are revealed by navigating to the **Advanced** tab when editing the **MobileData** interface:

- PIN
- Authentication type: None, PAP/CHAP (both), PAP, CHAP
- PAP/CHAP username (requires Authentication type not set to 'None')
- PAP/CHAP password (requires Authentication type not set to 'None')
- IP connection type: IPv4/IPv6 (default to IPv4), IPv4 only, IPv6 only

**Tip:** Use of these options depend on your SIM card and mobile data plan. Please consult your mobile network operator (*e.g.* Telstra) for the details. These details are normally included with your SIM as accompanying documentation if they are required.

**Note:** Either incorrectly setting, or erroneously omitting any of these values, will result in a connection failure.

## 3.2 Band Locking

### Lock to Frequency Bands

- Menu location: **Network > Band Locking**

You may set the X1 Pro to only use a selection of 3G and 4G frequency bands.

**Important:** please check beforehand that the desired frequency bands are indeed available in your area, else you may lock to bands that are not available and thus will not connect to the mobile data network.

### Steps

1. Select the desired bands
2. Click **Lock Bands**
3. Wait a moment as the X1 Pro locks bands then restarts the mobile connection.
4. Check the **Status > Mobile Data Status** page to confirm you are on the desired bands.

**TELCO ELECTRONICS**

Status ▾  
System ▾  
Services ▾  
Network ▾  
Band Locking  
Interfaces  
Wireless  
Switch  
DHCP and DNS  
Hostnames  
Static Routes  
Diagnostics  
Firewall  
Load Balancing  
VPN ▾  
Bandwidth Monitor ▾  
Logout

### Band Locking

Select which bands you want to restrict the modem to using. Please check that the desired service is available in your area before locking.

Here you can restrict the modem to use only the specified bands. This can be used to improve performance by only using clean or strong bands, or bands with higher bandwidth. Please be aware that under some circumstances, restricting to too few bands can limit the ability of the modem to perform carrier aggregation, which can limit speed. You can view frequency band details on the [Mobile Data Status](#) page.

Note: MobileData connection will restart after changing bands.

**4G LTE Bands**  B1  B2  B3  B4  B5  B7  B8  B9  B12  B13  B14  B17  B18  
 B19  B20  B21  B25  B26  B28  B29  B30  B32  B38  B39  B40  
 B41  B66

4G LTE bands provide higher data capacity.  
Australian bands: B1, B3, B5, B7, B8, B28, B40

**3G Bands**  B1  B2  B3  B4  B5  B8  B9  B19

3G bands may have greater availability under some circumstances.  
Australian bands: B1, B5, B8

Reset to Default

## 4 Wifi - Advanced Setup

While it works great out of the box, X1 Pro offers a wide array of options that give you complete control over the dual band wireless LAN hardware. Wifi performance will decrease the further you move away from the access point and will vary depending on environmental factors such as: obstructions, interference, and the quality of the connecting devices. The X1 Pro gives you all the tools you need to maximise performance for your deployment.

Navigate to **Network > Wireless** and **Edit** the Wifi network

The screenshot shows the TELCO ELECTRONICS management interface. The left sidebar contains navigation options: Status, System, Services, Network (expanded), VPN, and Bandwidth Monitor. Under Network, options include Band Locking, Interfaces, Wireless (selected), Switch, DHCP and DNS, Hostnames, Static Routes, Diagnostics, Firewall, and Load Balancing. The main content area is titled 'Wireless Overview' and displays two radio configurations:

- radio0:** Generic 802.11bgn, Channel: 6 (2.437 GHz) | Bitrate: 144.4 Mbit/s, Signal: -37/-99 dBm. SSID: X1 Pro 2.4GHz | Mode: Master, BSSID: 8C:88:2B:00:02:AA | Encryption: None. Buttons: RESTART, SCAN, ADD, DISABLE, EDIT, REMOVE.
- radio1:** Generic 802.11acn, Channel: 36 (5.180 GHz) | Bitrate: 200 Mbit/s, Signal: -64/-106 dBm. SSID: X1 Pro 5GHz | Mode: Master, BSSID: 8C:88:2B:00:02:A8 | Encryption: None. Buttons: RESTART, SCAN, ADD, DISABLE, EDIT, REMOVE.

Below the overview is the 'Associated Stations' table:

Network	MAC-Address	Host	Signal / Noise	RX Rate / TX Rate	
Master "X1 Pro 2.4GHz" (wlan0)	[REDACTED]	nicksWorkMBP2.lan (10.36.41.121, fe80::1cc2:7343:547:a955)	-36/-99 dBm	144.4 Mbit/s, 20 MHz, MCS 15, Short GI 144.4 Mbit/s, 20 MHz, MCS 15, Short GI	DISCONNECT
Master "X1 Pro 5GHz" (wlan1)	[REDACTED]	Galaxy-A5-2017.lan (10.36.41.133, fd97:e5f3:bd78:0:a4cd:476d:ed7a:fd4e)	-61/-106 dBm	6.0 Mbit/s, 20 MHz 200.0 Mbit/s, 40 MHz, VHT-MCS 9, VHT-NSS 1, Short GI	DISCONNECT

Wireless configuration options are distinguished by **Device** options, which are changeable parameters of the wifi radio for that network, and by **Interface** options, which are changeable parameters of a particular Wifi ESSID or Mesh ID that identifies that network. X1 Pro supports multiple networks, all with different parameters\*.

### 4.1 Wifi Radio Configuration

TELCO ELECTRONICS

Wireless Network: Master "X1 Pro 5GHz" (wlan1)

General Setup | **Advanced Settings**

Status

Mode: Master | SSID: X1 Pro 5GHz  
 BSSID: 8C:98:2B:00:02:A8  
 Encryption: None  
 Channel: 36 (5.180 GHz)  
 Tx-Power: 23 dBm  
 Signal: -70 dBm | Noise: -106 dBm  
 Bitrate: 200.0 Mbit/s | Country: AU

Wireless network is enabled **DISABLE**

Operating frequency

Mode	Channel	Width
AC	36 (5180 MHz)	80 MHz

Maximum transmit power

driver default - Current power: 23 dBm

Specifies the maximum transmit power the wireless radio may use. Depending on regulatory requirements and wireless usage, the actual transmit power may be reduced by the driver.

General Setup | **Wireless Security** | MAC-Filter | Advanced Settings

Mode: Access Point

ESSID: X1 Pro 5GHz

Network: lan

Choose the network(s) you want to attach to this wireless interface or fill out the *custom* field to define a new network.

Hide ESSID:

WMM Mode:

DISMISS SAVE

#### 4.1.1 General

- **Transmit Power** - amount of power output by the radio, limited by the EIRP limit dictated by the Country Code
  - Default: auto
  - Unit: expressed as both dBm and mW
- **Channel**
  - Default: auto
  - Selectable in **Access Point** mode
- **Mode**
  - AC (5GHz radio)
  - N
  - Legacy (b/g)
- **Width**
  - 20MHz
  - 40MHz (Only possible if no overlapping channel exists. ACMA Regulation). Firmware will actively scan and check for an overlapping channel in order to comply with [ACMA regulations](#).
  - 80MHz (5GHz) ACMA Regulations Apply

## 4.2 Advanced Wifi Radio Configuration

Wireless Network: Master "X1 Pro 5GHz" (wlan1)

General Setup	Advanced Settings
Country Code	AU - Australia <span>▼</span>
Allow legacy 802.11b rates	<input checked="" type="checkbox"/>
Distance Optimization	auto <span>⊞</span> Distance to farthest network member in meters.
Fragmentation Threshold	off
RTS/CTS Threshold	off
Force 40MHz mode	<input type="checkbox"/> Always use 40MHz channels even if the secondary channel overlaps. Using this option does not comply with IEEE 802.11n-2009!
Beacon Interval	100

Advanced device options include the following:

- **Country Code** - the ISO/IEC 3166 country code which determines the frequencies and transmit power allowed to be used in that designated regulation domain. Please set this to the country you are operating the device in, in order to comply with local regulations.
  - Default: AU - Australia
- **Allow legacy 802.11b rates** - allow 802.11b devices to connect the expense of losing faster data rates. We recommend disabling this unless you explicitly need to support 802.11b devices.
  - Default: Enabled
- **Distance Optimisation** - Used by proprietary system to optimize transmission to the furthest client.
  - Default: blank
  - Unit: meters
- **Fragmentation Threshold** - specify the maximum size of a frame before it is broken into smaller frames. Useful when operating in areas with interference or long distance links. Setting to the maximum value of 2346 effectively disables this feature.
  - Default value: blank
  - Unit: 802.11 frame size (bytes, *i.e.* octets)
- **RTS/CTS Threshold** - Request To Send/Clear To Send threshold - use the 802.11 RTS/CTS protocol for frames above this size limit. Useful when operating in areas with a high concentration of other Access Points or clients, though setting the value too low adds unnecessary overhead. Setting to the maximum value of 2346 effectively disables this feature.
  - Default: blank
  - Unit: 802.11 frame size (bytes, *i.e.* octets)

- **Force 40MHz mode** - force the radio to use 40MHz channels even if the bonded channel overlaps with the primary channel. This is not compliant with 802.11n-2009, but can increase the available bandwidth, however its use must be considered against the effects of self-interference.
  - Default: Disabled
- **Beacon Interval** - Time Units between broadcasts of the 802.11 beacon (a management frame) which serves to synchronise devices connected to the AP. Setting a lower value can improve throughput at the expense of raised power usage by the clients. Setting too high a value could lower power consumption but may cause connectivity issues.
  - Default: 100
  - Unit: 802.11 Time Unit (100TU = 102.4ms)

## About ACMA WiFi Regulations

If Channel Width is set to 40MHz, the wifi driver will perform a legally required scan to check for overlapping channels. If any such channel is detected, the wifi radio will fallback to 20MHz and will be noted in the system log as such:

```
daemon.notice hostapd: wlan0: ACS-COMPLETED freq=2412 channel=1
daemon.notice hostapd: wlan0: interface state ACS->HT_SCAN
daemon.notice hostapd: 20/40 MHz operation not permitted on channel pri=1
sec=5 based on overlapping BSSes
```

## 4.3 Advanced Interface Options

The **Wireless Interface** section contains options for changing the operation of a wireless interface.

The screenshot shows the 'Advanced Settings' tab for a wireless interface. The 'Mode' is set to 'Access Point'. The 'ESSID' is 'X1 Pro 5GHz'. The 'Network' is set to 'lan'. There is a checkbox for 'Hide ESSID' which is unchecked, and a checkbox for 'WMM Mode' which is checked. Below the network selection, there is a note: 'Choose the network(s) you want to attach to this wireless interface or fill out the custom field to define a new network.'

### 4.3.1 General Tab

- **Mode** - the primary function of this interface
  - **Access Point** - a complete, standard wireless access point which broadcasts an SSID and allows clients to connect
  - **Client** - allows connecting the X1 Pro to another SSID as a client. Correct SSID and authentication credentials are required. See also: **Scan** for the recommended way of setting up a Client network
  - **802.11s** - mesh network support
  - **Ad-Hoc** - legacy mesh network support
  - **Pseudo Ad-hoc** - useful for PtP topology with no interference. Included for legacy support.
  - **Monitor** - monitor wireless traffic
  - **Access Point (WDS)** - useful for PtP relay networks, normally requiring 2 AP's.
    - *Tip: Prevent WDS throughput loss by connecting your devices to the LAN port of the X1 Pro.*
  - **Client (WDS)** - useful for PtP relay networks
- **ESSID** - Extended Service Set Identification, other devices will see this as the **SSID**.
- **Network** - the network to attach this interface to. Networks are where firewall rules and routing settings are managed.
- **Hide ESSID** - hide the broadcast of the ESSID (SSID)
  - Default: disabled
- **WMM Mode** - Toggle Wifi Multimedia Mode support
  - Default: enabled

## 4.3.2 Wireless Security Tab

**Wireless Security** options are where you will change the encryption and passwords used to secure your Wifi network.

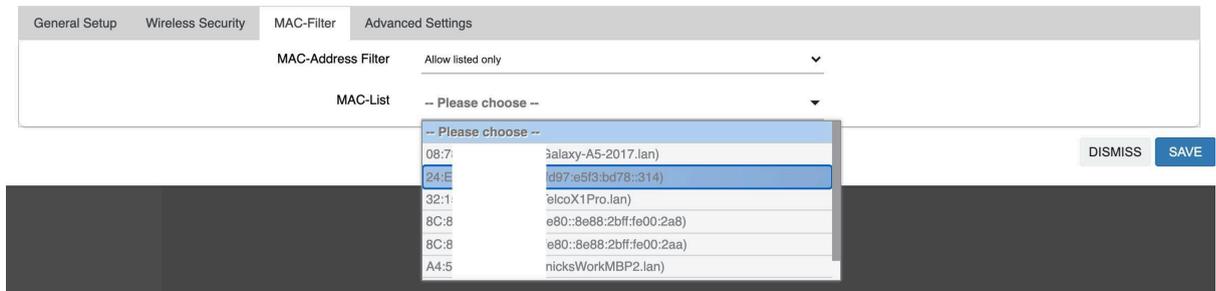
General Setup	Wireless Security	MAC-Filter	Advanced Settings
Encryption		WPA2-PSK (strong security) ▼	
Cipher		Force CCMP (AES) ▼	
Key		CorrectHorseBatteryStaple ⓘ •	
802.11r Fast Transition		<input type="checkbox"/>	
Enables fast roaming among access points that belong to the same Mobility Domain			
Enable key reinstallation (KRACK) countermeasures		<input type="checkbox"/>	
Complicates key reinstallation attacks on the client side by disabling retransmission of EAPOL-Key frames that are used to install keys. This workaround might cause interoperability issues and reduced robustness of key negotiation especially in environments with heavy traffic load.			

**Tip:** For the most secure Wifi access point use the following settings: *WPA2-PSK*, *Force CCMP (AES)*, *Enable KRACK countermeasures* and a strong password.

- **Encryption**
  - No Encryption
  - WPA2-PSK - Wifi Protected Access v2 with Pre-shared Key
    - Pre-Shared key is the password
  - WPA-PSK - Wifi Protected Access v1 with Pre-shared Key
  - WEP Open System
  - WEP Shared Key
  - WPA-PSK/WPA2-PSK - Default to WPA2, but fall back to WPA if not supported by the client. Trade-off is security for backwards compatibility.
- **Cipher**
  - Various ciphers are included for backwards compatibility and state of the art security.
- **Key**
  - The wifi password, in technical terms known as a “key”
- **Enable key reinstallation (KRACK) countermeasures**
  - Countermeasure for the WPA2 KRACK vulnerabilities disclosed in late 2017. We recommend enabling this feature.

### 2.4.3.3 MAC Filter Tab

The **MAC-Filter** tab contains settings for controlling access to the Wifi based on a MAC address blacklist or whitelist.



- **Allow listed only** - basic whitelisting policy
- **Allow all except listed** - basic blacklisting policy
- **MAC-List** - Choose from a dropdown containing connected hosts, or select *--custom--* to enter one.

### 2.4.3.4 Advanced Settings

**Advanced Settings** contain options for fine tuning Wifi parameters.

General Setup	Wireless Security	MAC-Filter	Advanced Settings
<p><b>Isolate Clients</b> <input type="checkbox"/></p> <p>Prevents client-to-client communication</p>			
<p><b>Interface name</b> wlan1</p> <p>Override default interface name</p>			
<p><b>Short Preamble</b> <input checked="" type="checkbox"/></p>			
<p><b>DTIM Interval</b> 2</p> <p>Delivery Traffic Indication Message Interval</p>			
<p><b>Time interval for rekeying GTK</b> 600</p> <p>SEC</p>			
<p><b>Disable Inactivity Polling</b> <input type="checkbox"/></p>			
<p><b>Station inactivity limit</b> 300</p> <p>SEC</p>			
<p><b>Maximum allowed Listen Interval</b> 65535</p>			
<p><b>Disassociate On Low Acknowledgement</b> <input checked="" type="checkbox"/></p> <p>Allow AP mode to disconnect STAs based on low ACK condition</p>			

- **Isolate Clients** - prevent client-to-client communication
  - Default: disabled
- **Interface name** - Override the default interface name
  - Default: blank
- **Short Preamble** - shorten the 802.11 preamble to reduce overhead
  - Default: enabled
- **DTIM Interval** - Delivery Time Indication Message Interval is used to aid power saving for wireless devices. A longer interval could save more power on mobile devices but could reduce performance in latency-sensitive applications such as VoIP.
  - Range: 1 to 255
  - Default: 2
- **Disassociate On Low Acknowledgement** - When the ACK from clients (stations) is low, disassociate, or kick the client from the AP. Recommended to leave enabled

## 5 Advanced - Command Line Interface

### 5.0.1 Access the Command Line Interface

TelcOS Melaleuca contains a BusyBox shell environment accessible via SSH featuring a writable file system, scripting support in Lua and Shell script, and ships with two powerful text editors (as of Melaleuca 1.2): vi and GNU nano.

SSH Credentials

- **Username:** root
- **Password:** the current device password, the default is **admin**

Example

```
BusyBox v1.31.1 () built-in shell (ash)

  _____  _  _____  _  _____  _  _____  _  _____  _  _____
 /_/_/  _/  /_/_/  _/  /_/_/  _/  /_/_/  _/  /_/_/  _/  /_/_/  _/  /_/_/  _/
/_/_/  _/  /_/_/  _/  /_/_/  _/  /_/_/  _/  /_/_/  _/  /_/_/  _/  /_/_/  _/
/_/_/  _/  /_/_/  _/  /_/_/  _/  /_/_/  _/  /_/_/  _/  /_/_/  _/  /_/_/  _/

-----
TelcOS Melaleuca 1.4 || www.telcoelectronics.com.au
-----

Welcome! For a list of commands run "help"
root@TelcoX1Pro:~#
```

## 5.0.2 Show all available commands

### Command

```
mmcli --help-all
```

## 5.1 Signal Information

These commands must be run from a shell on the device.

### 5.1.2 Get Signal Strength

#### Command

```
mmcli -m any --signal-get
```

#### Example Output

Current:

Network 'lte': '-65 dBm'

RSSI:

Network 'lte': '-65 dBm'

ECIO:

Network 'lte': '-2.5 dBm'

IO: '-106 dBm'

SINR (8): '9.0 dB'

RSRQ:

Network 'lte': '-16 dB'

SNR:

Network 'lte': '1.0 dB'

RSRP:

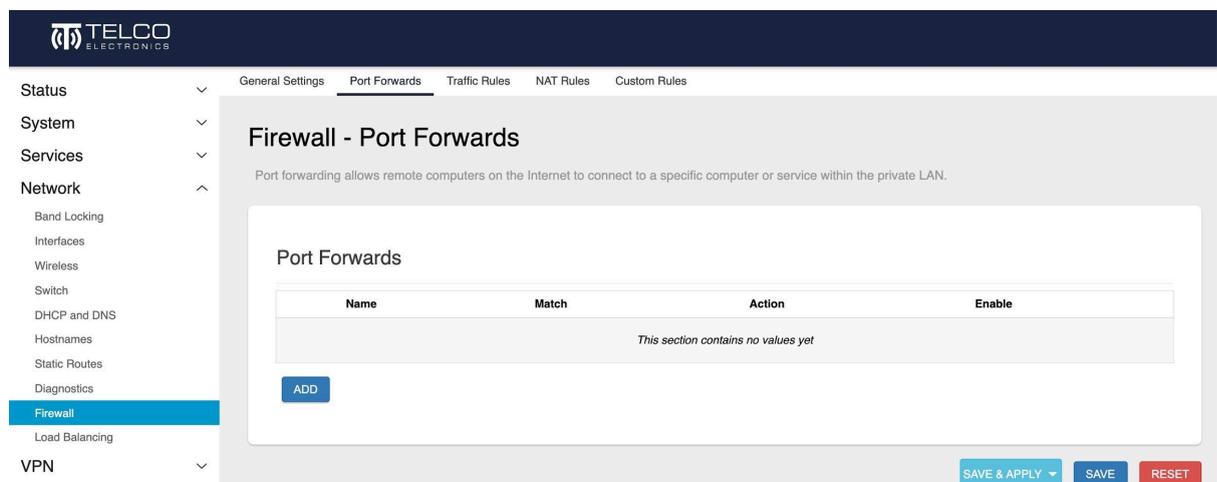
Network 'lte': '-96 dBm'

## 6 Advanced Networking

### 6.1 Port Forwarding

*Port forwarding* allows you to make a service available on the internal network available on an external network, such as the Internet. In the TelcoS Melaleuca, port forwarding is accomplished with the Port Forwards Wizard, located in the Firewall settings.

- Menu Location: **Network > Firewall > Port Forwards**



#### 6.1.1 Adding a Port Forward Rule

A port forward rule requires seven items, three of which are pre-filled:

- **External Port:** The port you will use on the WAN-side to access the forwarded port
- **Internal Port:** The port you wish to make available from the WAN
- **Internal IP Address:** The IP address of the device with the port you wish to forward
- **Name:** a label for the rule, can be anything
- **Protocol:** TCP and UDP, TCP only, UDP only
- **External Zone:** normally WAN (internet)
- **Internal Zone:** LAN

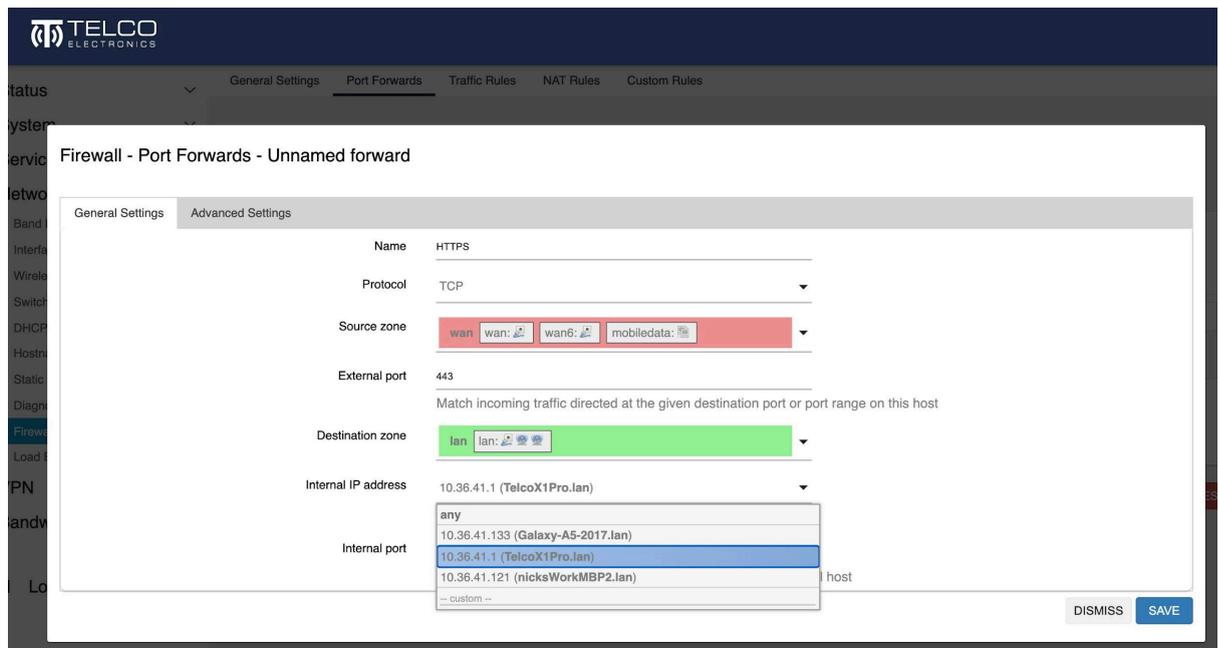
#### Steps

1. Enter a name for the rule
2. Enter the external port
3. Select the device with the to-be-forwarded port from the menu, or type in the IP address manually

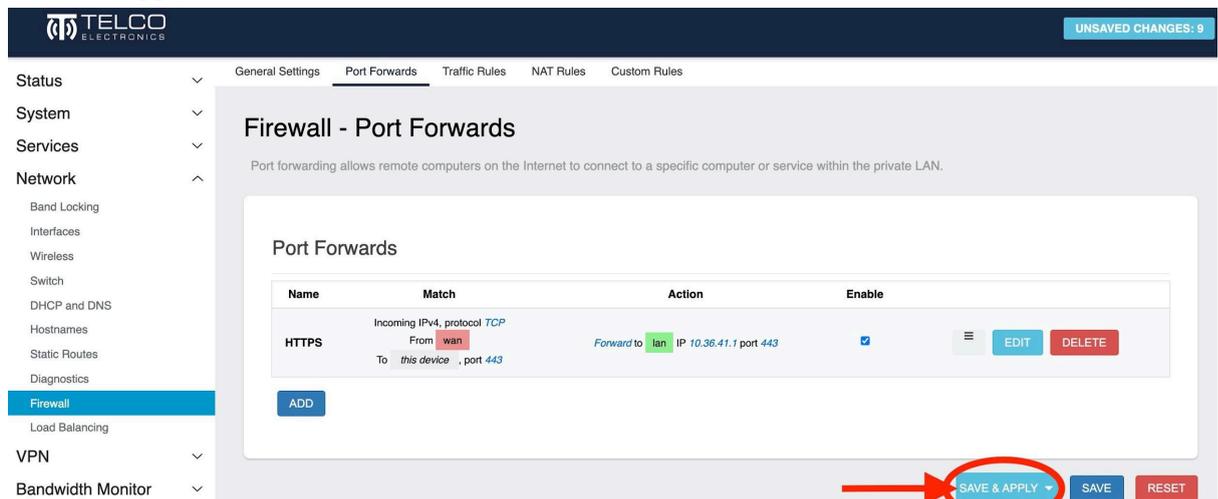
4. Enter the internal port to be forwarded
  5. Save & Apply
- Once applied, the rule is active instantly. Note, to access your newly forwarded device from the internet, you must specify the port and protocol.

### Example

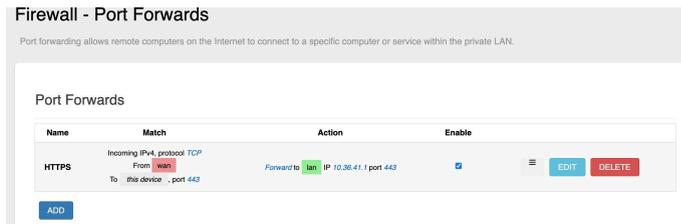
#### Entering the rule



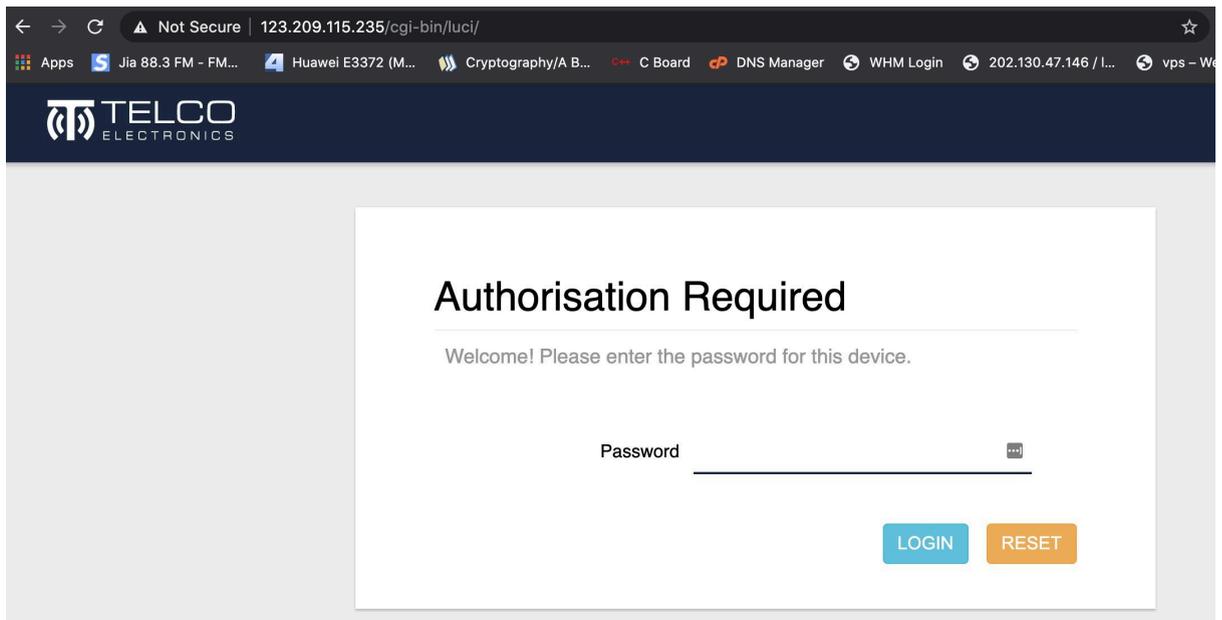
#### Save and Apply



### Active and enabled rule



### Testing the rule (note public IP address in browser)



## 6.2 Using WAN Port as an Extra LAN Port

Port functionality is configurable. By performing the following steps, both ports will function as LAN ports and any device plugged into WAN will receive an IP address and internet connectivity from the X1 Pro.

- Menu Location: **Network > Interfaces > LAN > Edit > Physical Settings**

### Steps

1. Navigate the menu to Network > Interfaces > LAN > Edit > Physical Settings
2. In the Interface drop down, add **Ethernet Adapter eth1** to the group by ticking the box next to it.
3. Apply & Save, then reboot or power cycle the X1 Pro.

*The Ethernet Adaptor eth1 has been added to the LAN group.*

Interfaces » LAN

The screenshot shows the Mikrotik WinBox interface for configuring a bridge. At the top, there are tabs for 'General Settings', 'Advanced Settings', 'Physical Settings', 'Firewall Settings', and 'DHCP Server'. The 'Physical Settings' tab is active. It contains the following options:

- Bridge interfaces** : Creates a bridge over specified interface(s)
- Enable STP** : Enables the Spanning Tree Protocol on this bridge
- Enable IGMP snooping** : Enables IGMP snooping on this bridge

Below these options is an 'Interface' dropdown menu. The current selection is 'eth1'. The dropdown list is open, showing the following items:

- Ethernet Adapter: "eth0" (lan)
- Ethernet Switch: "eth1" (wan, wan6)
- Ethernet Adapter: "wwan0" (mobiledata)
- Wireless Network: Master "X1 Pro 2.4GHz" (lan)
- Wireless Network: Master "X1 Pro 5GHz" (lan)
- custom -

At the bottom right of the settings panel, there are 'DISMISS' and 'SAVE' buttons. The 'SAVE' button is highlighted in blue.

## 6.3 WAN Failover Options

WAN failover is configurable by setting the **Gateway Metric** value on either the MobileData or WAN interface. **The interface with the lowest *gateway metric* value is used as the priority connection.** If at any time the primary connection goes down, the modem will switch over to the using the interface with the next lowest metric in a matter of seconds. Once the primary link becomes available again the modem will revert to using it.

- Menu Location: **Network > Interfaces > WAN/MobileData > Edit > Advanced Settings > Gateway Metric**
- **Default Values:**
  - MobileData: 50
  - WAN: 10

By default the MobileData interface is a backup connection, and the wired WAN, if connected, will be the primary. To swap this behaviour, simply **swap the two interfaces' gateway metric values.**

### Steps

1. Navigate the menu to **Network > Interfaces > WAN/MobileData > Advanced > Gateway Metric**
2. Edit the gateway metric value
3. Apply & Save both then reboot or power cycle the X1 Pro.

### Interfaces » MOBILEDATA

The screenshot shows the 'Advanced Settings' tab for the MobileData interface. The 'Gateway metric' field is highlighted with a red box and contains the value 50. Other settings include 'Use builtin IPv6-management' (checked), 'Force link' (unchecked), 'Modem device' (Quectel - EM12-G), 'PIN' (empty), 'Authentication Type' (None), 'IP Type' (IPv4/IPv6 (both - defaults to IPv4)), and 'Override MTU' (1500). At the bottom right, there are 'DISMISS' and 'SAVE' buttons.

## 6.4 Guest WiFi Configuration Example

This guide will set up a secure **guest wifi** network that has access to the Internet but not to the LAN or the router admin interface or command line. This same concept can be applied to public WiFi, kiosks, IoT, or any application where you want to supply wireless Internet access but do not want to allow the devices using it to access the X1 Pro configuration page, other guest devices, or any services other than HTTP and HTTPS.

You can download a configuration patch to apply to your own Telco X1 Pro [here](#). For your convenience we recommend applying it to a factory reset Telco X1 Pro, as **it will replace** the existing Wireless, Network, Firewall and DHCP configuration with factory defaults plus the items mentioned in this section. You can use the rest of this guide to familiarise yourself with the settings you may want to change after applying this patch, such as the WiFi network name, password, or other settings.

Learn how to apply the configuration patch in [Restore or Transfer Settings](#).

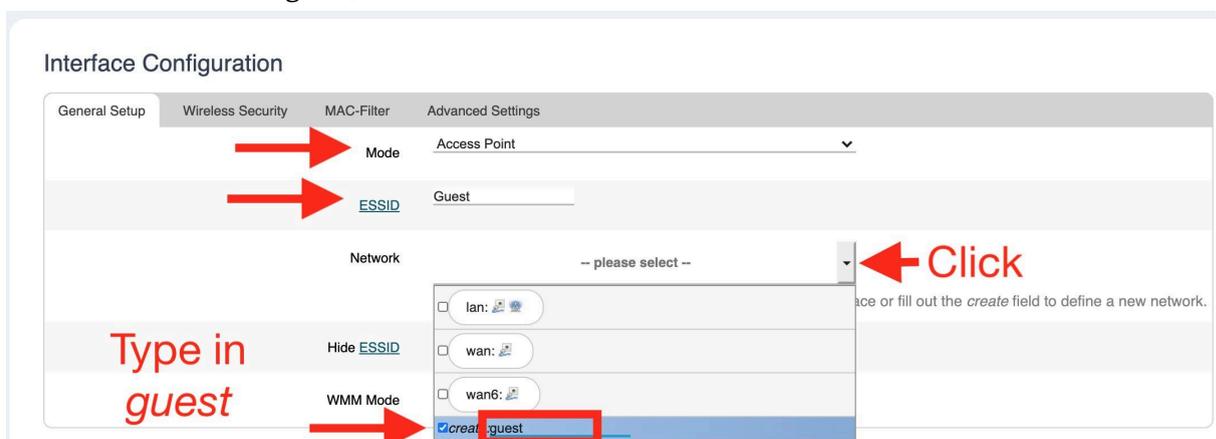
### 6.4.1 Wireless Configuration for the Guest Network

Here we will set up the Wireless SSID, Wireless Security and other WiFi options such as Client Isolation.

1. Navigate to **Network > Wireless** and click **Add**



2. Create the new WiFi network. Here we name the WiFi SSID *Guest* and create a new Interface called *guest*, at the same time.



### 3. Configure the *Guest SSID* **Wireless Security**

Here we use strong **WPA2-PSK** encryption with the **AES** cipher and **GuestWiFiPassword** as the Key/Password.

General Setup	Wireless Security	MAC-Filter	Advanced Settings
		Encryption	WPA2-PSK (strong security) <input type="text"/>
		Cipher	Force CCMP (AES) <input type="text"/>
		Key	GuestWiFiPassword <input type="password"/>
		802.11r Fast Transition	<input type="checkbox"/>
		Enables fast roaming among access points that belong to the same Mobility Domain	
		Enable key reinstallation (KRACK) countermeasures	<input type="checkbox"/>
		Complicates key reinstallation attacks on the client side by disabling retransmission of EAPOL-Key frames that are used to install keys. This workaround might cause interoperability issues and reduced robustness of key negotiation especially in environments with heavy traffic load.	

### 4. Enable **Client Isolation** if you do not want clients on the Guest wifi network to be able to access one another.

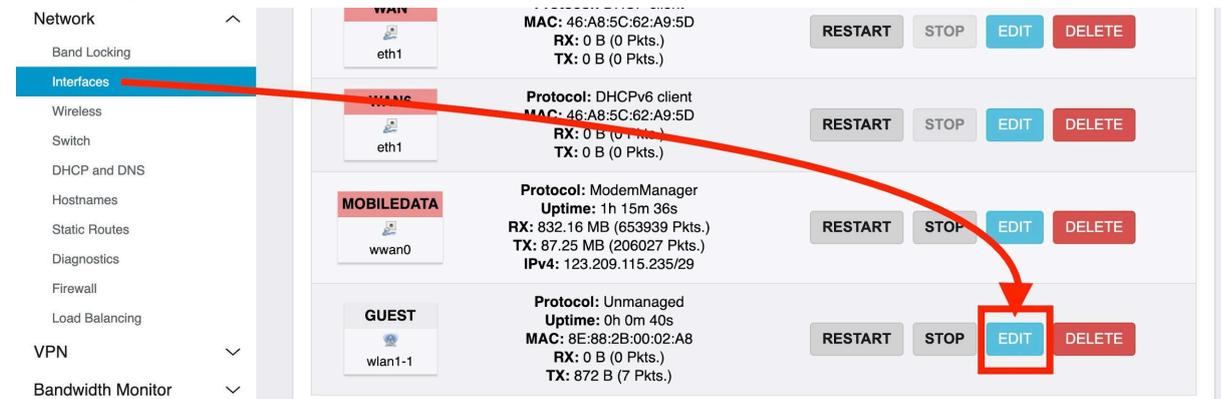
#### Interface Configuration

General Setup	Wireless Security	MAC-Filter	Advanced Settings
		Isolate Clients	<input checked="" type="checkbox"/>
		Prevents client-to-client communication	
		Interface name	<input type="text"/>
		Override default interface name	
		Short Preamble	<input checked="" type="checkbox"/>
		DTIM Interval	2 <input type="text"/>
		Delivery Traffic Indication Message Interval	
		Disassociate On Low Acknowledgement	<input checked="" type="checkbox"/>
		Allow AP mode to disconnect STAs based on low ACK condition	

## 6.4.2 Network Configuration for the Guest Network

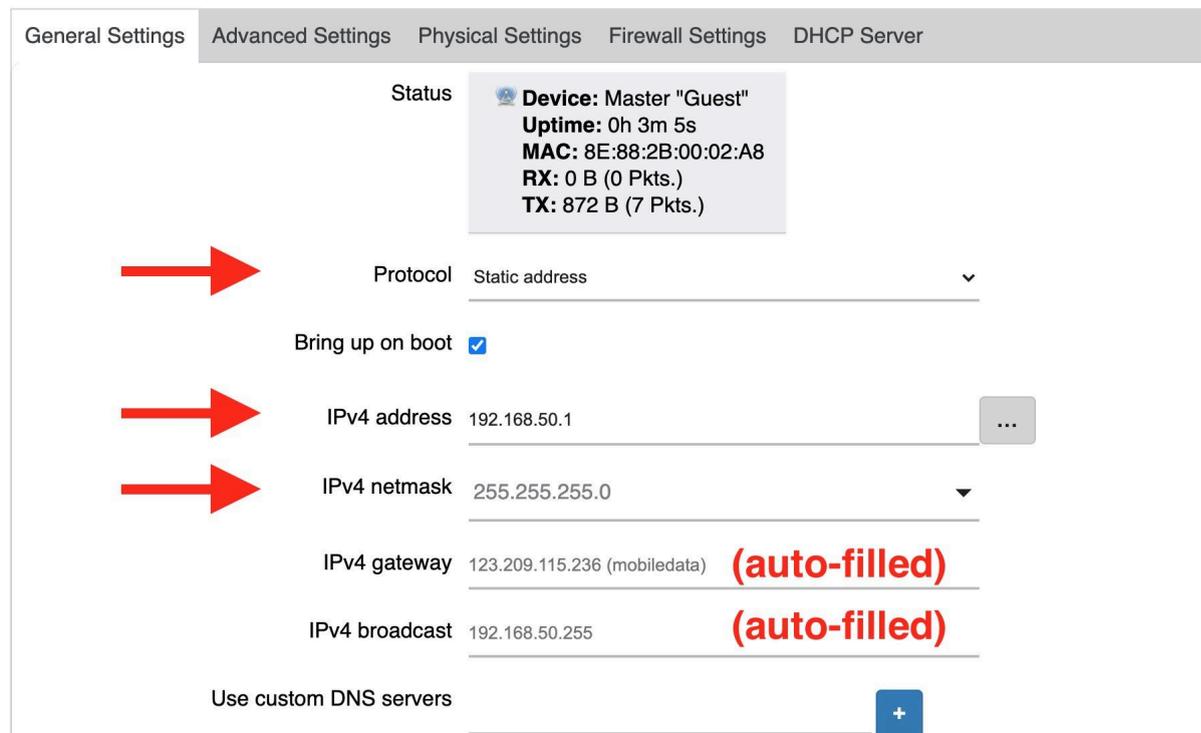
Here we will specify the IP address scope, DHCP options, and DNS settings for the Guest network. We are setting up a guest network with capacity for up to 253 active DHCP leases. You have the option of setting custom DNS servers for guests as well.

1. Navigate to **Network > Interfaces** and **Edit** the new **Guest** network.



2. Use the **Static address** protocol, and the following settings:

### Interfaces » GUEST



3. Scroll down to edit the DHCP server options. We do not expect *guests* to hang around for long so we want to make the lease time shorter than the default 12h,

so the DHCP pool does not contain a lot of stale leases. You can tweak this setting to your requirements.

#### Interfaces » GUEST

General Settings Advanced Settings Physical Settings Firewall Settings DHCP Server

General Setup Advanced Settings IPv6 Settings

Ignore interface

Disable [DHCP](#) for this interface.

Start

Lowest leased address as offset from the network address.

Limit

Maximum number of leased addresses.

Lease time

Expiry time of leased addresses, minimum is 2 minutes (2m).

DISMISS SAVE

4. Navigate to the **Firewall Settings** tab of the **Guest** Interface (at the top under Common Configuration) and assign it to the **Guest firewall zone**. If the zone does not exist, you can create it there.

#### Interfaces » GUEST

General Settings Advanced Settings Physical Settings Firewall Settings DHCP Server

Create / Assign firewall-zone

Choose the firewall zone you want to assign to this interface. Select *unspecified* to remove the interface from the associated zone or fill out the *custom* field to define a new zone and attach the interface to it.

DISMISS SAVE

#### 5. Add External DNS Servers

Go to the DHCP Server > Advanced tab and enter the following to make the hosts on this network use Google and Cloud Flare public DNS

**DHCP-Options:** 6,8.8.8.8,1.1.1.1

Interfaces » GUEST

General Settings   Advanced Settings   Physical Settings   Firewall Settings   DHCP Server

General Setup   Advanced Settings   IPv6 Settings

**Dynamic DHCP**

Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.

**Force**

Force DHCP on this network even if another server is detected.

**IPv4-Netmask** 255.255.255.0

Override the netmask sent to clients. Normally it is calculated from the subnet that is served.

**DHCP-Options** 6,8,8,8,8,1,1,1,1,1

Define additional DHCP options, for example "6,192.168.2.1,192.168.2.2" which advertises different DNS servers to clients.

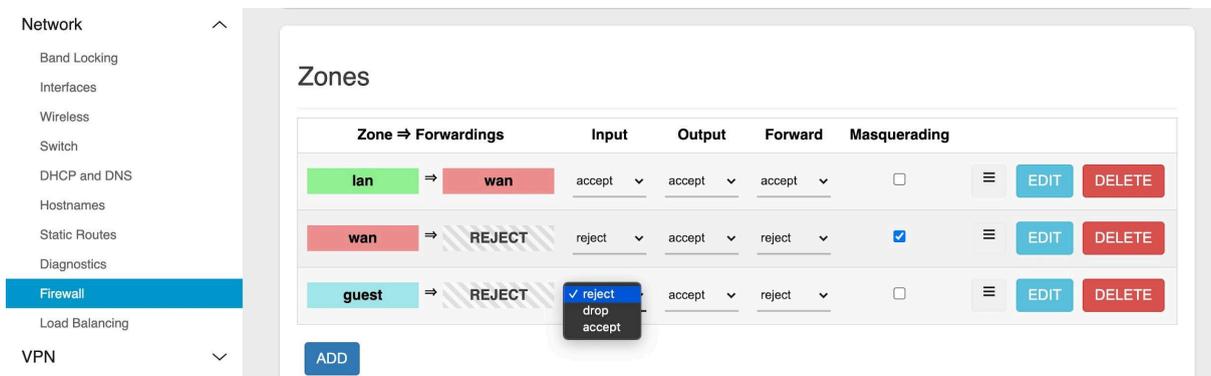
6. **Save and Apply** the Guest Interface configuration, which should now look something like this:

<p><b>GUEST</b></p>  <p>wlan1-1</p>	<p><b>Protocol:</b> Static address</p> <p><b>Uptime:</b> 0h 2m 2s</p> <p><b>MAC:</b> 8E:88:2B:00:02:A8</p> <p><b>RX:</b> 0 B (0 Pkts.)</p> <p><b>TX:</b> 1.23 KB (8 Pkts.)</p> <p><b>IPv4:</b> 192.168.50.1/24</p>	<p><b>RESTART</b>   <b>STOP</b>   <b>EDIT</b>   <b>DELETE</b></p>
--	--	---

### 6.4.3 Firewall Rules for the Guest Network

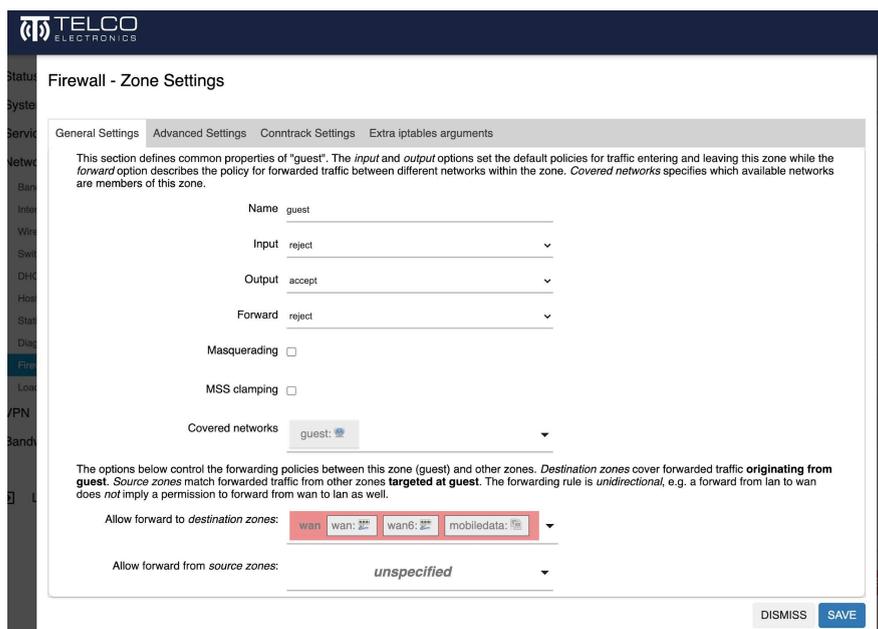
In this section we will finally specify exactly what the Guest network should and should not have access to. We want Guests to be able to access the Internet, but do not want them to be able to access the router settings, or, in our case, anything besides HTTP and HTTPS. Note that the guests also require DNS and DHCP in order to use HTTP/HTTPS, so we need to create rules to allow that traffic to reach the guests, but that is about all.

1. Navigate to **Network > Firewall**
2. Set the **Guest** firewall zone Input policy to **reject**
3. **Save and Apply**



4. **Edit** the **Guest** Firewall zone

We will now allow the Guest zone to access the WAN.



5. Set ***Allow forward to destination zones: WAN***
6. **Save and Apply**

#### Allow Guests to use DNS

1. Create a new **Traffic Rule** by navigating to **Firewall > Traffic Rules** and clicking **Add** at the bottom of the page.
2. Settings for this rule
  - a. **Name:** Guest DNS
  - b. **Protocol:** TCP + UDP
  - c. **Source Zone:** guest
  - d. **Source Port:** 53
  - e. **Destination Zone:** Device (input)
3. **Save and Apply**

#### Firewall - Traffic Rules - Unnamed rule

General Settings	Advanced Settings	Time Restrictions
Name	Guest DNS	
Protocol	TCP   UDP	
Source zone	guest <input type="text" value="guest: 🌐"/>	
Source address	-- add IP --	
Source port	53	
Destination zone	Device (input)	
Destination address	-- add IP --	
Destination port	any	
Action	accept	

DISMISS **SAVE**

#### Allow Guests to use DHCP

1. Create another Rule to allow DHCP for Guests.
2. Settings for this rule
  - a. **Name:** Guest DHCP
  - b. **Protocol:** UDP
  - c. **Source Port:** 67-68
  - d. **Destination Zone:** Device (input)

## Firewall - Traffic Rules - Guest DHCP

General Settings	Advanced Settings	Time Restrictions
Name	Guest DHCP	
Protocol	UDP	
Source zone	guest <input type="text" value="guest: 🌐"/>	
Source address	-- add IP --	
Source port	67-68	
Destination zone	Device (input)	
Destination address	-- add IP --	
Destination port	any	
Action	accept	

DISMISS **SAVE**

## Conclusion

You have now set up a secure Guest WiFi network that allows guests to securely connect to the Internet, without being able to access the router settings, or other guests on the network. This protects both the guests using your network from nefarious actors, as well as your network from said actors.

## 6.5 Bridge Mode

Bridge Mode is a special mode of operation that allows the IP address from the Mobile Data connection to be passed on to a device connected to one of the LAN ports. When Bridge Mode is activated, the X1 Pro will be inaccessible, as it is acting as a modem only. You can access the X1 Pro via SSH via the WAN port by configuring your PC to have a static IP address on the 192.168.1.1/24 subnet, such as 192.168.1.2. You should only have one device connected to the LAN when Bridge Mode is active, because this device will receive the IP address configuration settings from the mobile data network via DHCP.

### 6.5.1 How to use Bridge Mode

1. Navigate to **Network > Bridge Mode**
2. Select the correct APN for your SIM card and data plan
3. Optionally enter the PIN, Username and Password associated with the SIM
4. Confirm

5. Click Enable Bridge Mode

## 6.5.2 Bridge Mode Tips

### Band Locking

You can lock the X1 Pro to a specific set of frequency bands by performing the [Band Locking](#) *before* activating Bridge Mode. This allows you to ensure the selected bands work, and also that the required level of performance has been achieved before putting the X1 Pro into Bridge Mode.

### Access X1 Pro while in Bridge Mode

Starting in firmware version 2.1.10, The X1 Pro can be accessed via the WAN port while in bridge mode. Set your computer to have a static IP with the following settings:

- Address: 192.168.1.1
- Subnet Mask: 255.255.255.0
- Gateway: 192.168.1.1

You can now SSH into the X1 Pro

- `ssh root@192.168.1.1`

### Quit Bridge Mode

Bridge Mode can be undone by resetting the X1 Pro to factory defaults using the Reset Button or by SSHing in and running the

### Button

When the X1 Pro is fully booted, press and hold the reset button for 10 seconds, then release it. You will see the lights begin flashing, which indicates that the reset is in progress.

### SSH

SSH in to the X1 Pro via the WAN port, then run the reset command:

- `firstboot -y`
- Reboot

## 6.6 NBN Connectivity

NBN is not officially supported by the X1 Pro, but it is possible to connect the X1 Pro to NBN FTTC service with the following configuration:

1. Navigate to **Network > Interfaces > Switch**
2. Set the **VLAN** configuration as per the following image:

The screenshot shows the 'Switch' configuration page for 'switch0'. The 'Enable VLAN functionality' checkbox is checked. Below it, 'Enable mirroring of incoming packets' and 'Enable mirroring of outgoing packets' are unchecked. The 'VLANs on "switch0"' table is as follows:

VLAN ID	Description	CPU (eth0)	CPU (eth1)	LAN 1	LAN 2	LAN 3	LAN 4	WAN	
1	tagged	tagged	untagged	untagged	untagged	untagged	untagged	off	DELETE
2	untagged	untagged	off	off	off	off	off	tagged	DELETE

3. **Save and Apply** the Switch/VLAN settings
4. Navigate to **Network > Interfaces > WAN** and change the protocol from DHCP to **PPPoE**
5. Enter the credentials (PAP/CHAP username and password) to authenticate with your NBN provider's account (contact your NBN provider or check your supplied router for this information). Leave all other settings at their defaults.
6. **Save and Apply** the WAN interface changes
7. Connect the NBN ethernet cable to the WAN port then **reboot** the X1 Pro and other devices

## 7 Services

### 7.1 Dynamic DNS (DDNS)

DDNS allows a device with a dynamically changing, but public IP address to be reached via a static hostname. TelcoS Melaleuca supports a wide range of DDNS service providers including but not limited to: No-IP, DynDNS, Google, and more. TelcoS Melaleuca supports running multiple DDNS services simultaneously. Normally, a special mobile data plan is required to get a public IP address, and uses a purpose built APN, such as *Telstra.Extranet*. Consult your mobile network operator for details.

Menu Location: **Services > Dynamic DNS**

#### Steps

On the Basic Tab

1. Give your new DDNS instance a **name** and click **Add**
2. Fill out the required details as follows:
  - a. Select the **DDNS Service Provider** from the list
  - b. Click the **Change Provider** button
  - c. **Enable** the service by ticking the Enable box
  - d. Enter the Fully Qualified Domain Name (FQDN) of the **Lookup Hostname** as provided by your DDNS provider, for example: mytest.ddns.net
  - e. Enter the same FQDN in the **Domain Field**

On the Advanced Tab:

3. Change the **IP Address Source** to URL
4. Set the **Event Network** to the appropriate network, such as mobiledata for 4G or WAN for a wired connection
5. **Save and Apply**
6. **Reboot** the device for the changes to take effect.

See screenshots as follows:

#### Basic Settings

#### Details for: ddns

Configure here the details for selected Dynamic DNS service.

Basic Settings	Advanced Settings	Timer Settings	Log File Viewer
Enabled	<input checked="" type="checkbox"/>		
	If this service section is disabled it could not be started. Neither from LuCI interface nor from console		
Lookup Hostname	telcovpntest.ddns.net		
	Hostname/FQDN to validate, if IP update happen or necessary		
IP address version	<input checked="" type="radio"/> IPv4-Address <input type="radio"/> IPv6-Address		
	Defines which IP address 'IPv4/IPv6' is send to the DDNS provider		

## Advanced Settings

Configure here the details for selected Dynamic DNS service.

Basic Settings	Advanced Settings	Timer Settings	Log File Viewer
	IP address source [IPv4]	URL	<input type="text" value="URL"/> <small>Defines the source to read systems IPv4-Address from, that will be send to the DDNS provider</small>
	URL to detect [IPv4]	<a href="http://checkip.dyndns.c">http://checkip.dyndns.c</a>	<small>Defines the Web page to read systems IPv4-Address from</small>
	Event Network [IPv4]	mobiledata	<small>Network on which the ddns-updater scripts will be started</small>
	Bind Network	-- default --	<small>OPTIONAL: Network to use for communication Casual users should not change this setting</small>
	Force IP Version	<input type="checkbox"/>	<small>OPTIONAL: Force the usage of pure IPv4/IPv6 only communication.</small>
	Force TCP on DNS	<input type="checkbox"/>	<small>OPTIONAL: Force the use of TCP instead of default UDP on DNS requests.</small>
	PROXY-Server	user:password@myprc	<small>OPTIONAL: Proxy-Server for detection and updates. Format: [user:password@]proxyhost:port IPv6 address must be given in square brackets: [2001:db8::1]:8080</small>
	Log to syslog	Notice	<small>Writes log messages to syslog. Critical Errors will always be written to syslog.</small>
	Log to file	<input checked="" type="checkbox"/>	<small>Writes detailed messages to log file. File will be truncated automatically. File: "/var/log/ddns/ddns.log"</small>

## 7.2 Automatic Recovery

In the Automatic Recovery section you can configure automatic reboots triggered when the internet connection becomes unavailable or at a specified interval of time.

Menu Location: **System > Automatic Recovery**

- **Operating Mode** - Choice of
  - Reboot on Internet Connection Lost
  - Periodic Reboot (an interval of time such as 1 hour)
- **Force Reboot Delay** - After this many seconds the device will trigger a forced hard reboot if the soft reboot fails, ensuring the reboot takes place.
- **Period** - In periodic mode, it defines the reboot period. In internet mode, it defines the longest period of time without internet access before a reboot is engaged. Default unit is seconds, you can use the suffix 'm' for minutes, 'h' for hours or 'd' for days.
- **Ping Host** - The IP address or FQDN of the host to ping, normally an Internet server that is expected to always be up, such as Google DNS 8.8.8.8
- **Ping Period** - How often to ping the Ping Host.

## 7.2.1 Example

Example configuration to reboot after 5 minutes of loss of internet connectivity:

**Automatic Reboot**

Here you can configure an automatic reboot when the Internet connection has been lost for a certain amount of time, or after a certain period of time, such as daily.

**Operating mode** Reboot on internet connection lost

**Forced reboot delay** 30

When rebooting the system, the service will trigger a soft reboot. Entering a non zero value here will trigger a delayed hard reboot if the soft reboot fails. Enter a number of seconds to enable, use 0 to disable

**Period** 1h

In periodic mode, it defines the reboot period. In internet mode, it defines the longest period of time without internet access before a reboot is engaged. Default unit is seconds, you can use the suffix 'm' for minutes, 'h' for hours or 'd' for days

**Ping host** 8.8.8.8

Host address to ping

**Ping period**

How often to check internet connection. Default unit is seconds, you can use the suffix 'm' for minutes, 'h' for hours or 'd' for days

DELETE

ADD

## 7.3 Wake on LAN

Wake on LAN allows you to send a “magic packet” to a device attached to the Telco X1 Pro. The target device must support Wake on LAN functionality in its network card and BIOS. If that support is enabled on the target host, then you can send a Wake on LAN packet to it and it will power on.

**Wake on LAN**

Wake on LAN is a mechanism to remotely boot computers in the local network.

**Network interface to use** eth0

Specifies the interface the WoL packet is sent on

**Host to wake up** 00:0C:29:10:FC:99 (ubuntu.lan)

Choose the host to wake up or enter a custom MAC address to use

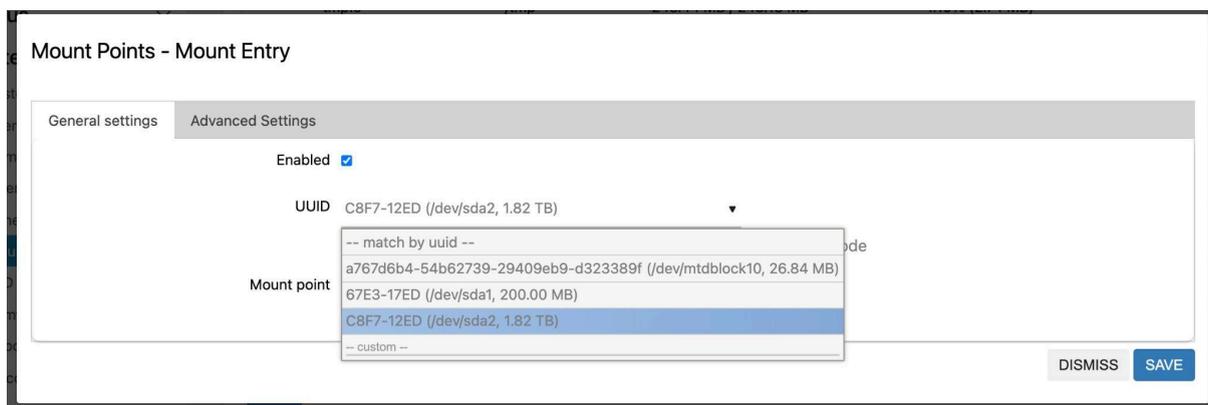
**Send to broadcast address**

WAKE UP HOST

## 7.3 File Shares (SAMBA/NAS)

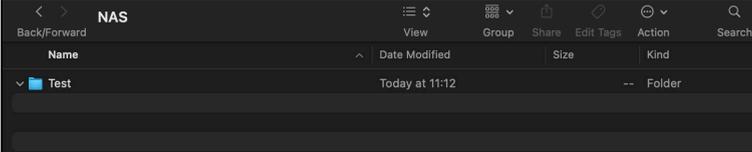
TelcoOS Melaleuca supports sharing disks with the network (NAS - network attached storage). To set up a shared disk follow the following steps:

1. Format your disk using the **FAT** or **ext4** file system
2. Plug in the disk to the USB port on the Telco X1 Pro / Telco X1 Pro 5G
3. Navigate the main menu to **System** > [Mount Points](#)
4. Add a new Mount Point using the **Add** button and selecting your disk from the dropdown menu.
  - a. Leave **Enabled** ticked



- b. Give it a mount point, such as: **/mnt/NAS**
  - c. **Save and apply**
5. Navigate the main menu to **Services** > [Network Shares](#)
6. Set the **Listen interface** to be **LAN**, or your desired interface, such as a VPN interface
7. Add a new **Shared Directory** using the **Add** button, and fill in the following properties:
  - a. **Name:** the name to display the share under, e.g. **"NAS"**
  - b. **Path:** the path used under the Mount Points. i.e. **/mnt/NAS**
  - c. **Force Root:** enable this to avoid complicated filesystem permissions if you just want everyone to be able to read/write from the disk, otherwise set up file system permissions using standard Linux practices
  - d. **Allow guests:** enabled
  - e. **Create Mask:** 0700
  - f. **Directory Mask:** 0700
8. Reboot the Telco X1 Pro / Telco X1 Pro 5G to finalise the settings

To confirm everything is working, open your network share browser on your PC or Mac and you should see your new share advertised as available. Access it using **guest** credentials.



## 8 Firmware and Backup

- Menu Location: **System** > **Firmware and Backup**

### 8.1 Backup

You can download a configuration backup on the Firmware and Backup page. This file can be used to transfer settings between Telco X1 Pro units.

### 8.2 Restore or Transfer Settings

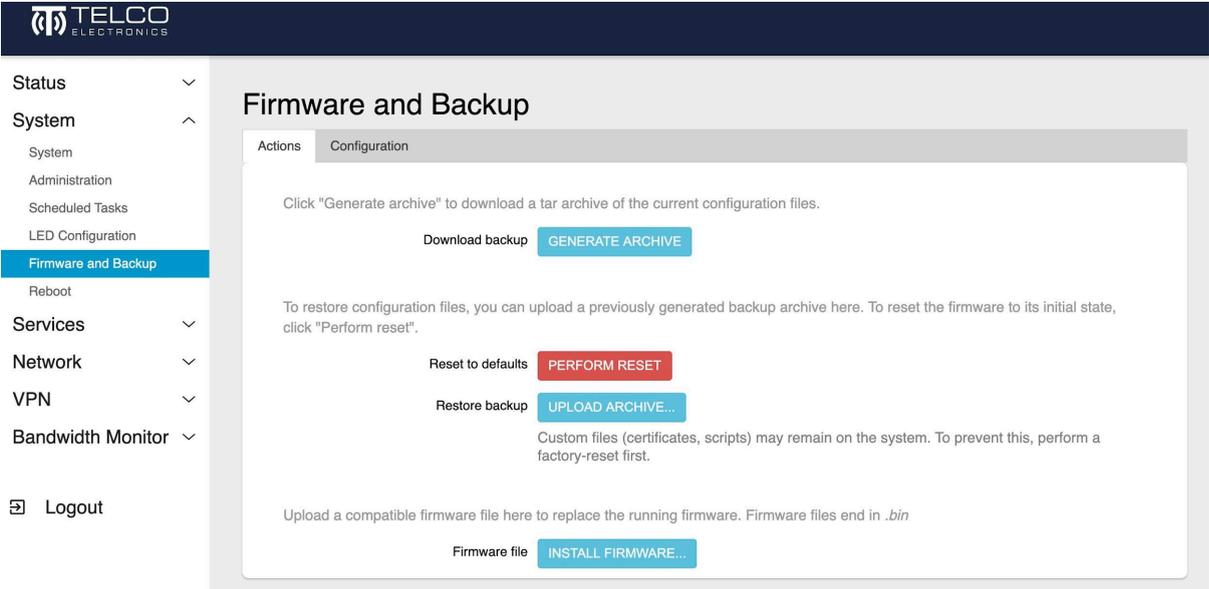
Upload a previously generated X1 Pro Backup file here. The X1 Pro will immediately reboot and apply the settings.

### 8.3 Install New Firmware

Here you can install a new or previous Telco X1 Pro firmware version. For a clean installation untick the “keep settings” box. Beware that sometimes settings between versions may conflict.

### 8.4 Reset

Restore the device to factory default settings.



The screenshot shows the 'Firmware and Backup' page in the Telco Electronics web interface. The page is divided into two tabs: 'Actions' and 'Configuration'. The 'Configuration' tab is active. The page contains the following sections:

- Download backup:** A button labeled 'GENERATE ARCHIVE' is next to the text 'Download backup'.
- Reset to defaults:** A red button labeled 'PERFORM RESET' is next to the text 'Reset to defaults'.
- Restore backup:** A blue button labeled 'UPLOAD ARCHIVE...' is next to the text 'Restore backup'.
- Upload a compatible firmware file:** A blue button labeled 'INSTALL FIRMWARE...' is next to the text 'Upload a compatible firmware file here to replace the running firmware. Firmware files end in .bin'.

The left sidebar shows the navigation menu with 'Firmware and Backup' highlighted. The top header includes the Telco Electronics logo and the page title 'Firmware and Backup'.

## 9 Tips and Recommendations

The following practices may help to improve the security and performance of your Telco Electronics device. While predominantly low risk, not all of these practices may be applicable to your network environment or deployment, *i.e.* some may even be counterproductive depending on the scenario. These practices are listed here to serve as a guide to what options you have at your disposal.

### 9.1 Wireless Security and Performance

- Enable [KRACK vulnerability](#) countermeasures
  - Location: Wireless Security tab when editing wireless network
- Use *WPA-2* encryption with the *CCMP AES* cypher and a secure key
  - Location: Wireless Security tab when editing wireless network
- Disable *Allow legacy 802.11b rates* to improve wireless performance
  - Location: Network > Wireless > Edit > Device Configuration > Advanced Settings

### 9.2 Device Security

- Use [key-based authentication](#) instead of a password to access the X1 Pro via SSH. Add your key and deselect *Password Authentication*
  - Location: Password and SSH page
- Change the default router password to something secure
  - Location: Password and SSH page

### 9.3 Network Security

- Use DNS servers that provide protection from known malicious domains
  - Location: Edit MobileData and WAN > Advanced > deselect *Use Provider's DNS Servers* and enter your preferred
- Enable *Drop Invalid Packets* in firewall
  - Location: Network > Firewall > General Settings
- Isolate wifi clients if you wish to prevent wifi hosts from communicating with one another
  - Location: Wireless Security tab when editing wireless network

### 9.4 Network Reliability

- Set up an automatic reboot if the internet connection goes down. Follow our example in the [Ping Reboot](#) section.

- Run the modem in MBIM mode if you do not require advanced features such as Band Locking or Bridge Mode.
  - Change modes via SSH with the following two commands:
    - `modem_mbim`
    - `modem_qmi`

End of Document