

E2CLink™

Ethernet to Cellular Router

User Manual

NimbeLink Corp

Updated: May 2016



© NimbeLink Corp. 2017. All rights reserved.

NimbeLink Corp. provides this documentation in support of its products for the internal use of its current and prospective customers. The publication of this document does not create any other right or license in any party to use any content contained in or referred to in this document and any modification or redistribution of this document is not permitted.

While efforts are made to ensure accuracy, typographical and other errors may exist in this document. NimbeLink reserves the right to modify or discontinue its products and to modify this and any other product documentation at any time.

All NimbeLink products are sold subject to its published Terms and Conditions, subject to any separate terms agreed with its customers. No warranty of any type is extended by publication of this documentation, including, but not limited to, implied warranties of merchantability, fitness for a particular purpose and non-infringement.

NimbeLink is a registered trademark, and Skywire is a trademark, of NimbeLink Corp. All trademarks, service marks and similar designations referenced in this document are the property of their respective owners.

Table of Contents

Introduction	4
Overview	4
Product Description	4
Orderable Part Numbers	5
Accessories	6
Antennas	6
Power Supplies	6
E2CLink Setup	7
Device Overview	7
Attach Antenna	8
Apply Power	9
Plug in Ethernet Cable	9
Plug in Equipment	10
Get Connected	10
Connect with NimbeLink	11
Activate on your Verizon Account	12
Mounting	13
Adhesive Tape	13
Reusable Strap	14
Default Operation	15
Accessing the Management Console	16
How to Connect to the Management Console	16
Password Configuration	18
Lost Password Reset	18
Steps to Reset a Lost Password	18
Checking the MEID/IMEI/SIM ID	21
Updating the Firmware	21
Accessing the System Log	22
Startup Script	23
Provisioning	24
Manually Configuring the APN	25

Skywire® Initialization Code	27
Custom Startup Code	27
WANWatchdog & Network KeepAlive	27
KeepAlive Script	28
WAN Watchdog	29
Inbound Connectivity	31
Port Forwarding	32
Configure E2CLink Port Forwarding	33
Traffic Rules	34
Configuring Traffic Rules	34
Inbound Connectivity Examples	38
Remotely Accessing the E2CLink's Management Console	38
Step 1: Configuring the Port Forwarding	38
Step 2: Configuring Traffic Rules	39
Step 3: Remotely Connect to the E2CLink	41
Remotely Access a Device Connected to the E2CLink's LAN	43
Step 1: Configure the LAN Side Device to have a Static IP Address	43
Step 2: Configure the Port Forwarding	44
Step 3: Configure the Traffic Rules	45
Step 4: Access the Device	47
Pseudo-Bridge Mode	49
Pseudo-Bridge Mode Configuration	49
Troubleshooting	53
The E2CLink Will Not Connect to the Network	53
Poor Signal Quality	53
Troubleshooting APN Misconfigurations	55
Troubleshooting Cellular Data Plans	55
E2CLink's Management Console Will Not Load	56
Power	56
DHCP Conflicts	56
Browser Caching Error	56
The E2CLink Disconnects from the Network	56
GPL Compliance	57
Federal Regulatory Licensing	57

1. Introduction

1.1 Overview

This document is the user manual for NimbeLink's Ethernet to Cellular Router. Throughout this document the Ethernet to Cellular Router will often be referred to as the 'E2CLink™' or the 'router,' although it may be referred to by its full name.

NimbeLink E2CLink is available with bundled data plans from leading cellular carriers.

Make sure to check the [E2CLink's product page](#) for the most up to date information.

This document documents the operation of the E2CLink using firmware e2c1p-20160321. If your E2CLink is running an earlier firmware version certain features described in this document may not be available. If you would like to update the firmware on your device to the e2c1p-20160321 firmware, please contact NimbeLink's technical support team.

1.2 Product Description

The E2CLink provides a low cost, industrial-grade alternative to cable, DSL, or Wi-Fi internet connections. The E2CLink™ delivers instant cellular connectivity over the Verizon network for any Ethernet enabled device. It is significantly smaller and more affordable than other external cellular routers and can cost significantly less to operate than cable or DSL connections.

NimbeLink's E2CLink router has been tested by Verizon and granted Private Network Certification, which allows it to be used with the Verizon Private Network service. Verizon offers their Private Network service to allow customers to assign private IP addresses from their own private networks, to the E2C Link cellular router. This ensures that the device remains separate and inaccessible from the public internet. Generally, the device is then set up to send data through a hardware Virtual Private Network (VPN) connection between Verizon's core network and the customer's endpoint (application server, edge router, or other private endpoint). For more information about Verizon's Private Network service, please contact a Verizon Wireless business representative, or reach out to NimbeLink to be connected to a representative.

1.3 Orderable Part Numbers

The table below contains a list of orderable part numbers. The retail versions include the Antenna, power supply, and mounting hardware for the E2CLink whereas the non-retail versions are for the OEM device only and do not include any accessories.

Orderable Parts			
Part Number	Description	Carrier	Network Type
NL-R-E2GC R	Ethernet to Cellular Modem 2G 1xRTT Verizon - Retail Version	Verizon	2G 1xRTT CDMA
NL-R-E3GD R	E2CLink – Ethernet to Cellular Modem 3G EVDO with 2G 1XRTT fallback Verizon - Retail Version	Verizon	3G CDMA, 2G 1xRTT CDMA
NL-R-E4GLS R	E2CLink – Ethernet to Cellular Modem 4G LTE Verizon - Retail Version	Verizon	4G LTE CAT 3
NL-R-E2GC	Ethernet to Cellular Modem 2G 1xRTT - Device Only	Verizon	2G CDMA
NL-R-E3GD	Ethernet to Cellular Modem 3G EVDO with 2G 1xRTT fallback - Device Only	Verizon	3G CDMA
NL-R-E4GLS	Ethernet to Cellular Modem 4G LTE - Device Only	Verizon	4G LTE CAT 3
NL-R-EC1G- V	Ethernet to Cellular Modem. LTE CAT1 Ether - Device only	Verizon	4G LTE CAT 1
NL-R-EC1G- VR	Ethernet to Cellular Modem. LTE CAT1 Ether - Retail Version	Verizon	4G LTE CAT 1

1.4 Accessories

1.4.1 Antennas

The E2CLink requires a cellular antenna that supports the underlying cellular technology (2G, 3G, or 4G) that the E2CLink is using. These frequencies will vary between cellular technologies and cellular carriers. The standard antenna shipped with the E2CLink retail kit is a Taoglas TG.30.8113 and supports 2G, 3G and 4G applications. The E2CLink requires a dipole antenna for maximum performance.

Recommended antennas are listed in the table below.

Orderable Parts		
Manufacturer	Part Number	Network Type
Taoglas	TG.30.8113	2G/3G CDMA, 2G GSM, 3G HSPA, 4G LTE
CDW	MAG-212-12-SMA-M	2G/3G CDMA, 2G GSM, 3G HSPA, 4G LTE
Taoglas	TG.35.8113	2G/3G CDMA, 2G GSM, 3G HSPA, 4G LTE
Taoglas	GA.110.101111	2G/3G CDMA, 2G GSM, 3G HSPA, 4G LTE

1.4.2 Power Supplies

The E2CLink requires a 5V DC power supply that can supply at least 1.2A. E2CLink retail kits ship with CUI Inc's SWI6-5-N-P5. The ethernet port on the E2C Link does not support Power Over Ethernet (POE). If POE is required an external power adapter must be used.

2. E2CLink Setup

2.1 Device Overview

The E2CLink™ Ethernet-to-Cellular Router provides a low-cost, industrial-grade alternative to cable, DSL or Wi-Fi internet connections. The E2CLink™ delivers instant cellular connectivity over the Verizon network for any Ethernet enabled device.

Figure 1: Connector Side View of the E2CLink



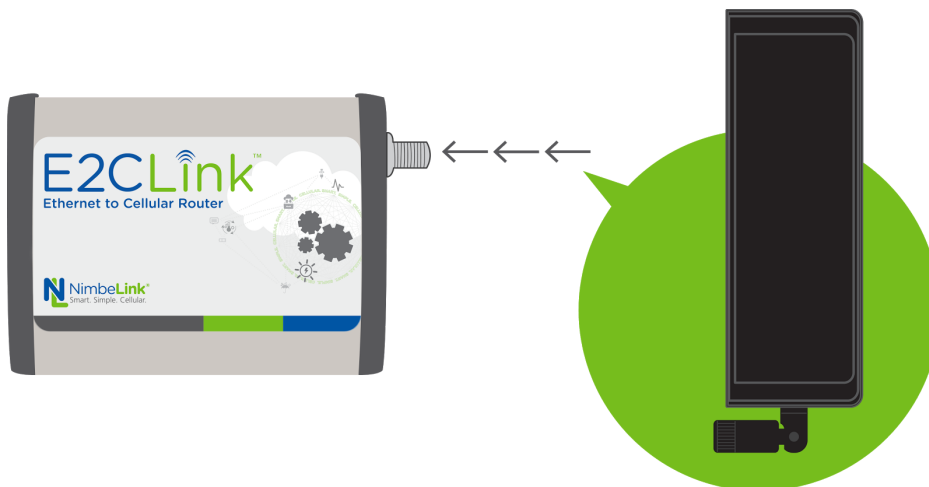


Figure 2: Antenna Side View of the E2CLink

2.2 Attach Antenna

The E2CLink requires an external antenna and provides a standard SMA connector for easy connection. On 2G and 3G devices there is only one antenna port. On 4G devices there are two antenna ports and both antenna ports need an antenna connected to them. If the E2CLink is installed inside of a metal cabinet, a remote antenna should be used.

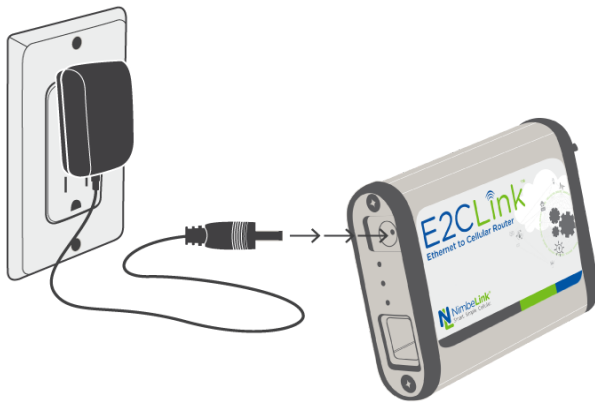
The retail package includes a wide-band blade style antenna that can attach directly to the SMA connector.



2.3 Apply Power

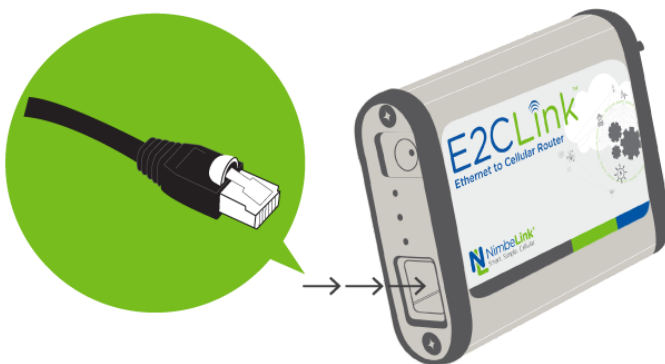
The E2CLink requires a 5V DC power source. The input is a 5.5mm outside diameter, 2.1mm inside diameter barrel jack. The center pin is +5V.

The retail package includes an AC to DC power converter with 6ft cord. Replacement part number: CUI INC. SWI6-5-N-P5



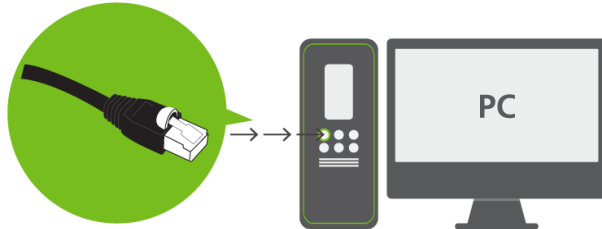
2.4 Plug in Ethernet Cable

The E2CLink connects to equipment with standard CAT 5/CAT 5E Ethernet cables through a RJ45 jack. The Ethernet port on the E2CLink does not support port over Ethernet (POE). If POE is needed an external converter must be used.



2.5 Plug in Equipment

The final step is to plug the other end of the Ethernet cable into a PC or router WAN port.



3. Get Connected

The E2CLink typically does not have an active cellular data plan when it arrives. Once a data plan is active, Verizon devices will automatically provision themselves during first use. While non-Verizon devices may need to have their APNs and or provisioning commands configured. The provisioning process typically takes a few minutes to complete.

Customers using devices on networks other than Verizon will need to contact their cellular data provider to set up a cellular data plan for their device. For Verizon enabled devices there are multiple data plan options available from NimbeLink that will get you connected in minutes or you may contact your Verizon account representative to set up your cellular data plan.

Cellular devices on the Verizon network can be classified as several different device types. On the Verizon Network the E2CLink is classified as a Machine to Machine (M2M) device and needs to be activated on an M2M account. SIM cards that are on consumer plans may not work with the E2CLink because of this classification difference. If your Verizon representative is having difficulties activating a cellular data plan for your E2CLink please have them contact NimbeLink's support team at <https://support.nimbelink.com/>

3.1 Connect with NimbeLink

If you don't have a Verizon M2M Business account, NimbeLink can provide Verizon data plans directly without contract commitments.

The available data plans can be viewed here:

<http://nimbelink.com/skywire-cellular-data-plans/>

To activate service please fill out our online form at <http://go.nimbelink.com>

To activate a line of service you will need to provide the following information for activation and billing purposes:

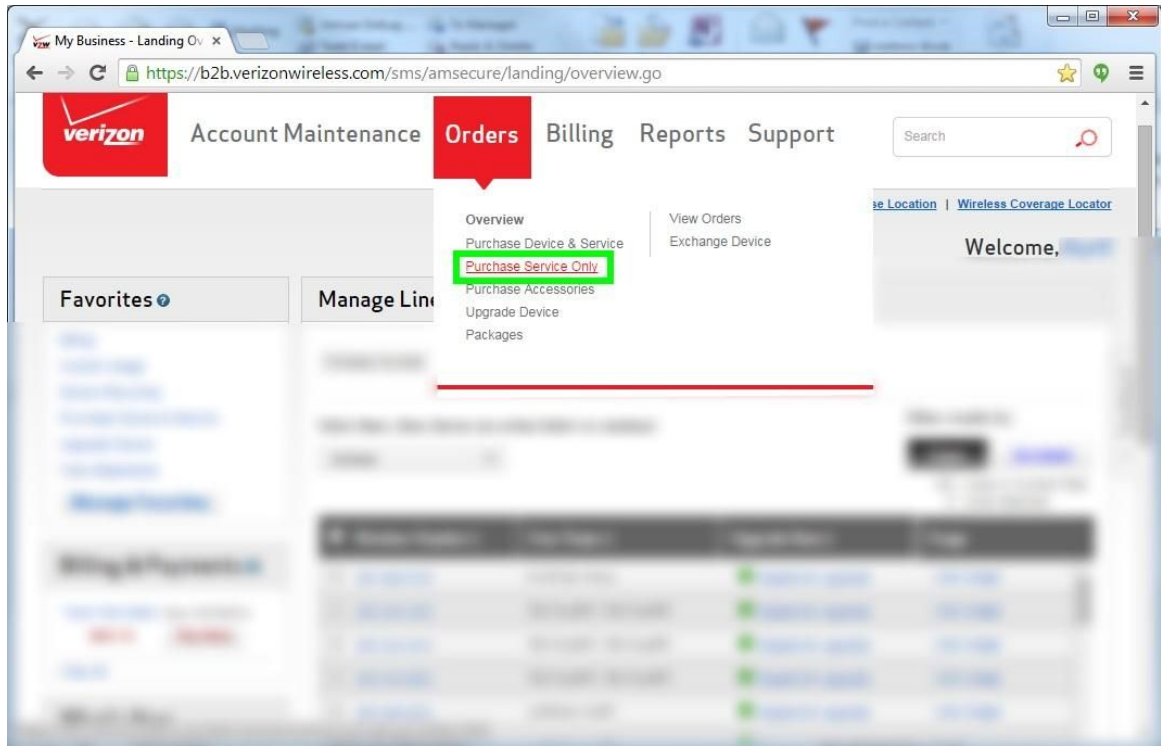
- Name
- Address
- Email
- Phone
- Desired Data Plan
- E2CLink MEID or IMEI & SIM ID number which can be found on the back of the device of the device (examples shown below)



3.2 Activate on your Verizon Account

There are two ways to activate an E2C Link on your existing Verizon account:

- 1) Log into your Verizon My Business Portal account and select Orders -> Purchase Service Only. Follow the onscreen instructions.



- 2) Call your Verizon account representative and tell them you'd like to activate service on your E2CLink. You will need to supply the MEID or IMEI & SIM details which can be found on the bottom of your device. If your Verizon account representative would like the recommended feature codes for activating an E2CLink please have them contact NimbeLink at: <https://support.nimbelink.com/>

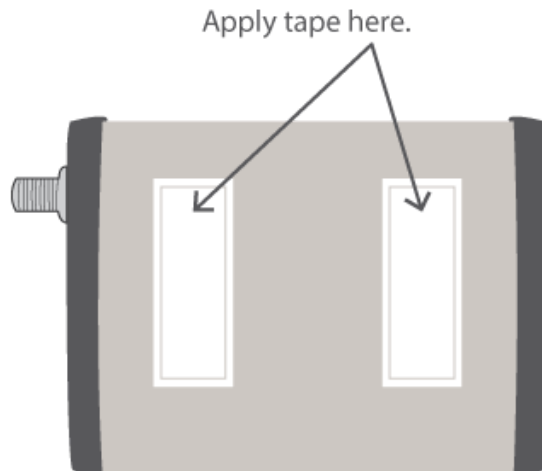
4. Mounting

The E2CLink is a rugged product that can be attached to equipment in numerous ways. The retail packaging includes two methods to adhere the E2CLink in the end application.

4.1 Adhesive Tape

The retail packaged product includes two pieces of weather-resistant, double sided polyurethane foam adhesive which can be applied to the enclosure to adhere the product to a surface. The adhesive attaches well to rigid surfaces.

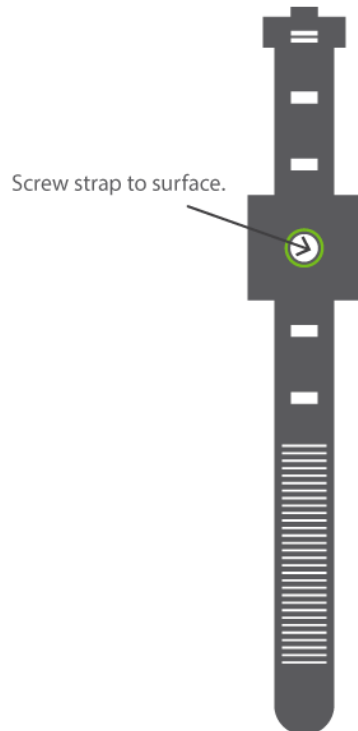
- 1) Wipe dust from the surface of the E2CLink and apply double sided tape as shown. Be sure to copy the MEID or IMEI and ICCID (SIM number) from the bottom label if it will not be visible after installation.
- 2) Wipe dust from surface of the equipment and press the E2CLink firmly for 30 seconds.



4.2 Reusable Strap

The retail package includes one reusable strap that can attach to many surfaces and provide an installation option that allows you to later remove the product if necessary.

- 1) Screw strap to desired surface using screw or bolt appropriate for the surface type.



- 2) Wrap strap around E2CLink and tighten strap to secure the product.



5. Default Operation

When power is applied, the E2CLink will obtain an IP address from the cellular network if the device has a valid cellular data plan. The IP address may be either static or dynamic, and is assigned by your cellular service provider.

By default, the E2CLink acts as a DHCP server and will assign an IP address to any equipment that connects via the Ethernet port. The E2CLink will provide the IP address, subnet mask and default gateway information to the equipment.

If the connected equipment requests or sends data from/to an external IP address, the E2CLink will use the cellular connection to process the request and route the data back to the originating equipment.

The device has 3 states:

Powered-Off: The E2CLink does not have power. This is indicated by the power LED being off and is caused by the device being unplugged or not having any power applied to its input. The ethernet and cellular network are powered down and cannot be detected by the cellular network or any downstream equipment.

Initialization: When power is applied to E2CLink, the power LED will turn on and stay on and the cellular and ethernet Status LEDs will be off. The E2CLink will go through its initialization phase where it will attempt to automatically connect its WAN interface to the cellular network and enable the LAN connection via it's Ethernet port.

The initialization phase may take several minutes to complete.

Powered-On: Once the E2CLink completes its initialization phase it will enter its powered-on mode. This is indicated by the Power LED being on and the Cellular and Ethernet Status LEDs may be on or blinking to indicate connection status and activity.

Once the E2CLink has reached the Power-On state, the connected equipment can get a DHCP address and begin sending/receiving data over the internet. The E2CLink is now connected to the cellular network and is ready to send and receive data.

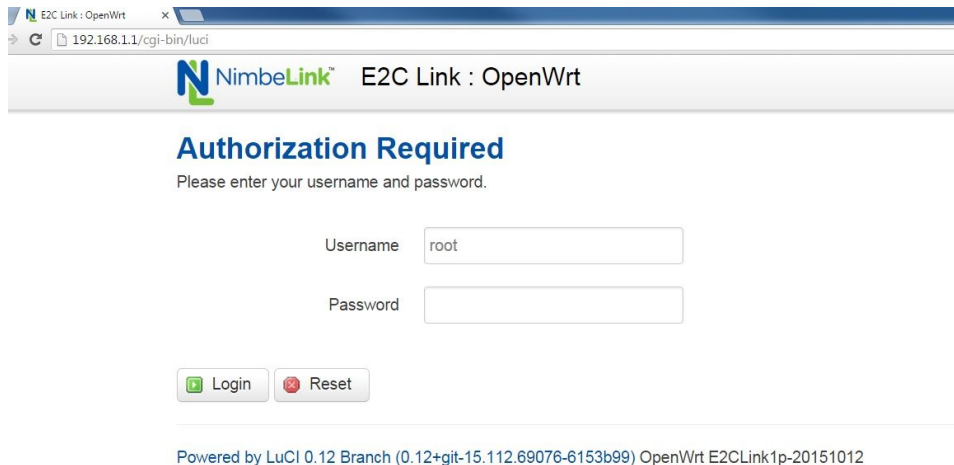
6. Accessing the Management Console

For advanced networking scenarios, the E2CLink configuration can be modified via a web-based management console. The E2CLink is based on the OpenWRT operating system so there is extensive flexibility in how the device can be configured. Typical network use cases may require opening Ports, setting up specific routing rules, or adjusting default Firewall settings.

6.1 How to Connect to the Management Console

- 1) Connect the E2CLink to a PC with an Ethernet cable.
- 2) Configure the PC Ethernet port to get an IP address via DHCP.
- 3) Apply power to the E2CLink and wait one minute. After one minute the E2CLink should be close to completing or will have completed its initialization process and will have assigned an IP address to the PC.
- 4) Using a web browser on the PC, navigate to the web URL: 192.168.1.1

The E2CLink will serve up a web page. The default username is root and password can be left blank until a new username and password are set.



The screenshot shows a web browser window with the address bar displaying "192.168.1.1/cgi-bin/luci". The page title is "NimbeLink™ E2C Link : OpenWrt". The main heading is "Authorization Required" with the instruction "Please enter your username and password." Below this, there are two input fields: "Username" with the value "root" and "Password" which is empty. At the bottom of the form are two buttons: "Login" and "Reset". A footer at the bottom of the page reads "Powered by LuCI 0.12 Branch (0.12+git-15.112.69076-6153b99) OpenWrt E2CLink1p-20151012".

- 5) Once the user has logged into the E2CLink they will be greeted by the Status page where they can view system information of the E2CLink. If the password is not set a yellow warning box will be visible on the top of the page as shown below.

No password set!



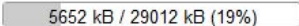

There is no password set on this router. Please configure a root password to protect the web interface and enable SSH.
[Go to password configuration...](#)

Status

System

Hostname	OpenWrt
Model	Nimbelink NL-R-E4GLS
Firmware Version	OpenWrt Nimbelink 20150401a / LuCI 0.12 Branch (0.12+git-15.037.36195-f1e2a26)
Kernel Version	3.10.49
Local Time	Tue May 19 17:20:09 2015
Uptime	1h 38m 8s
Load Average	0.22, 0.06, 0.06

Memory

Total Available	 18572 kB / 29012 kB (64%)
Free	 10916 kB / 29012 kB (37%)
Cached	 5652 kB / 29012 kB (19%)
Buffered	 2004 kB / 29012 kB (6%)

7. Password Configuration

The E2CLink is shipped with “root” as the default user name and no password. The password needs to be configured upon setup to secure the device against unwanted users. The password can be changed under *System>Administration* as indicated by the blue circles in the image below.

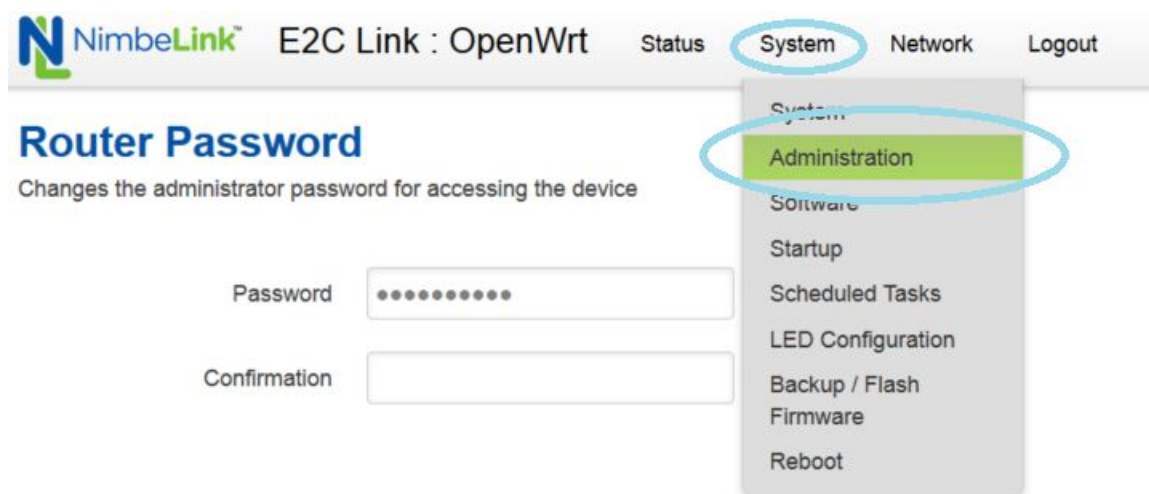


Figure 5

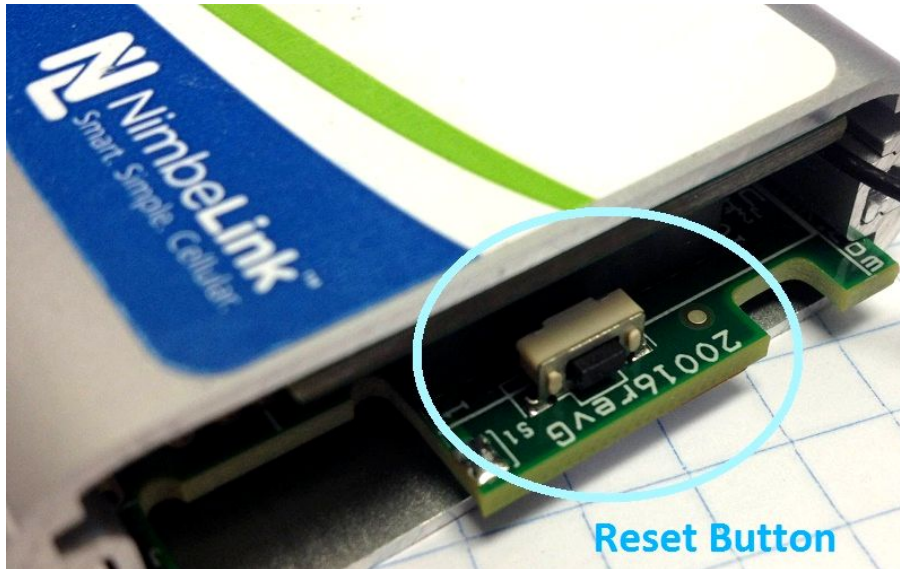
8. Lost Password Reset

If the E2CLink administrative password is lost or the unit has been configured for a static IP address that is now unknown, the unit can be recovered by reflashing the firmware using the boot loader failsafe method. Note that this recovery method does revert the unit to factory settings and the previous unique configuration will be lost. You will need a computer on which you can manually set a static IP address. **DO NOT remove power from the device during the reset process as removing power could damage your device.**

8.1 Steps to Reset a Lost Password

- 1) Obtain the latest version of the E2CLink Firmware by contacting your NimbeLink representative at <https://support.nimbelink.com/>. You will need this firmware image on the computer before you disconnect it from its normal network and connect it only to the E2CLink being recovered.
- 2) Remove power from the E2CLink.
- 3) Connect the computer and the E2CLink together. Make sure they are the only two things connected to this network segment.

- 4) Use a T-9 Torx screwdriver to remove the endplate with the antenna connector(s) attached. Remove both screws and the end plate will come away, revealing a small push button on the PCB in the center of the opening. This small push button is the reset button. Be careful not to pull the end plate and coax cable too far out from the enclosure. The coax cable is fragile.
- 5) Configure the computer for a static IP address of 192.168.1.2
- 6) Press and hold the reset button on the E2CLink.



- 7) Apply power to the E2CLink and carefully watch the LEDs on the other end. As soon as you see four blinks from the two LEDs closest to the Ethernet jack, release the reset button. You should get a burst of fast blinks from the two LEDs. If you do not get the faster blinks, power off the E2CLink and try again.
- 8) Use a browser on the computer to navigate to the management console at 192.168.1.1. You should see the following screen displaying "Firmware Update" in a large font.

FIRMWARE UPDATE

You are going to update **firmware** on the device.
Please, choose file from your local hard drive and click **Update firmware** button.

No file selected.

WARNINGS

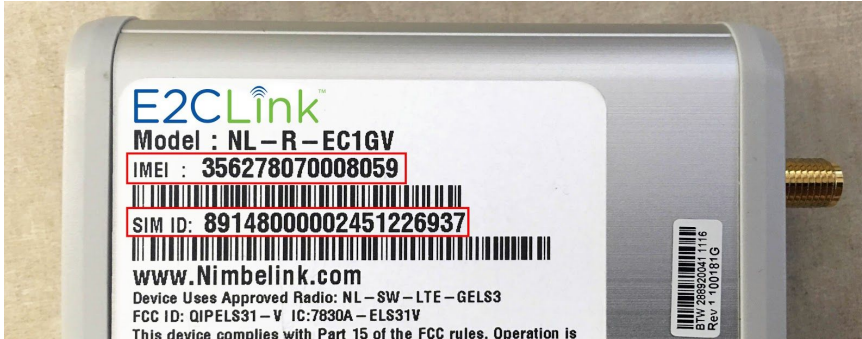
- do not power off the device during update
- if everything goes well, the device will restart
- you can upload whatever you want, so be sure that you choose proper firmware image for your device

You can find more information about this project on [GitHub](#)

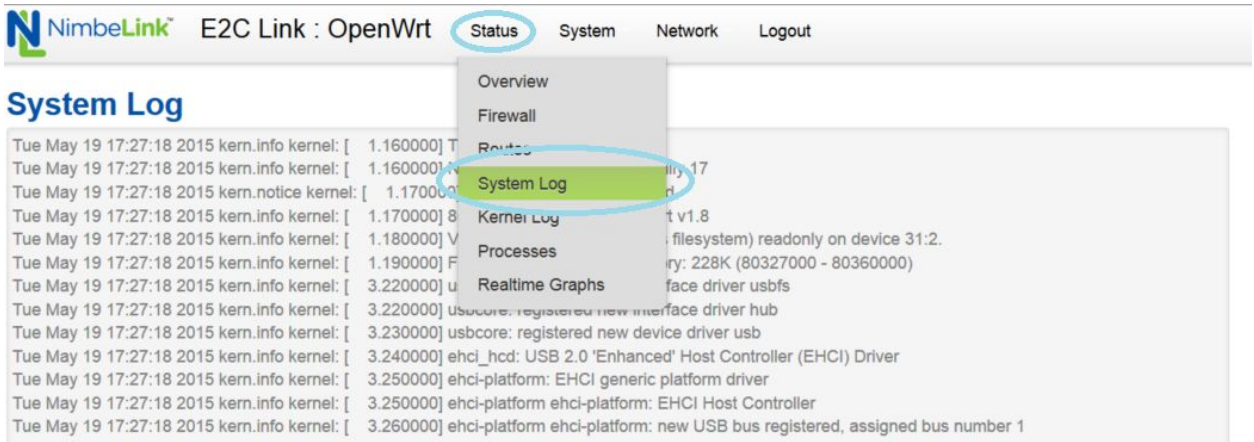
- 9) Click the browse button to select the firmware image provided by NimbeLink.
- 10) Click the *Update Firmware* button to initiate the firmware installation. This will load an update page indicating the firmware update is in progress. **DO NOT remove power from the device during this process as this will brick the device.**
- 11) When this process completes, the E2CLink will be reflashed with fresh firmware and all settings will be reverted to factory default. There will be no administrative password set and you will need to reconfigure any custom settings you had in the router, including the cellular APN if that was previously customized.

9. Checking the MEID/IMEI/SIM ID

The device's MEID/IMEI is a unique identifier for the cellular modem inside of the device. The IMEI can be found in two places. The first is on the back side of the case on the devices label.



The second option is to check the system log where the device's MEID/IMEI, SIM ID, and phone number can be found. To access the system log go to *Status>System log*.



To find the IMEI/MEID, SIM ID, or phone number search the page (ctrl+f in most browsers) for MEID, IMEI, SIM, or phone numbers. The phone number may not be available depending on the firmware version on your E2CLink.

10. Updating the Firmware

The latest version of the E2CLink Firmware is available by contacting your NimbeLink representative at For additional troubleshooting resources, or to ask

any technical questions, please visit: <https://support.nimbelink.com/>. It is recommended to update to the latest firmware version during the device's initial configuration.

To flash the E2CLink's firmware go to *system>Backup/Flash Firmware*. Under the “Flash new firmware image” section click the “choose file” button (3) then navigate to the firmware file provided by NimbeLink and select it.

Make sure the “Keep Settings” option is not selected. Then click the “Flash Image” (4) button to start the firmware update. This will load a new page asking for a confirmation and displaying the MD5 sum of the firmware image. Confirm that the MD5 sum is correct against the MD5 sum provided by NimbeLink for the Firmware image and click continue.

The E2CLink will now flash the new image; DO NOT disconnect power to the device during this process. When the new firmware has been flashed the router will reload the login screen. The user information will revert to its default settings.

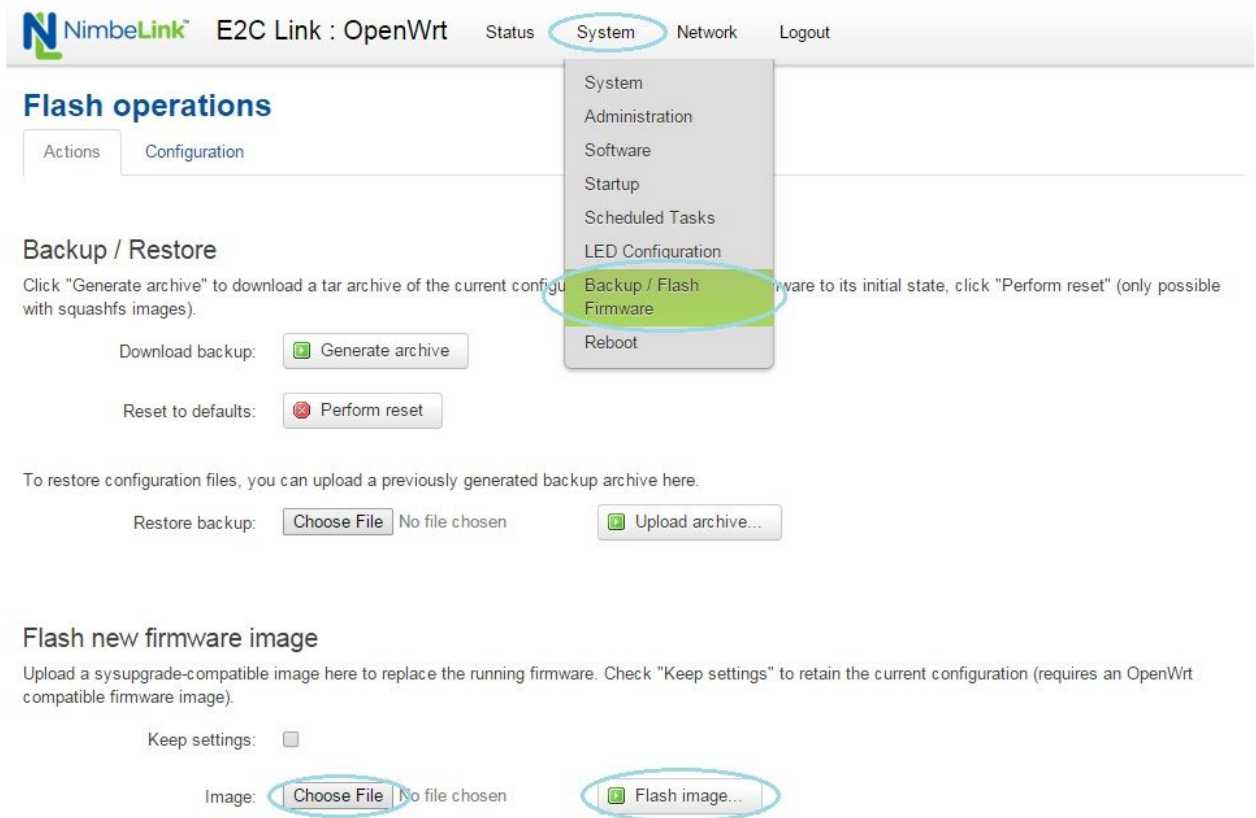
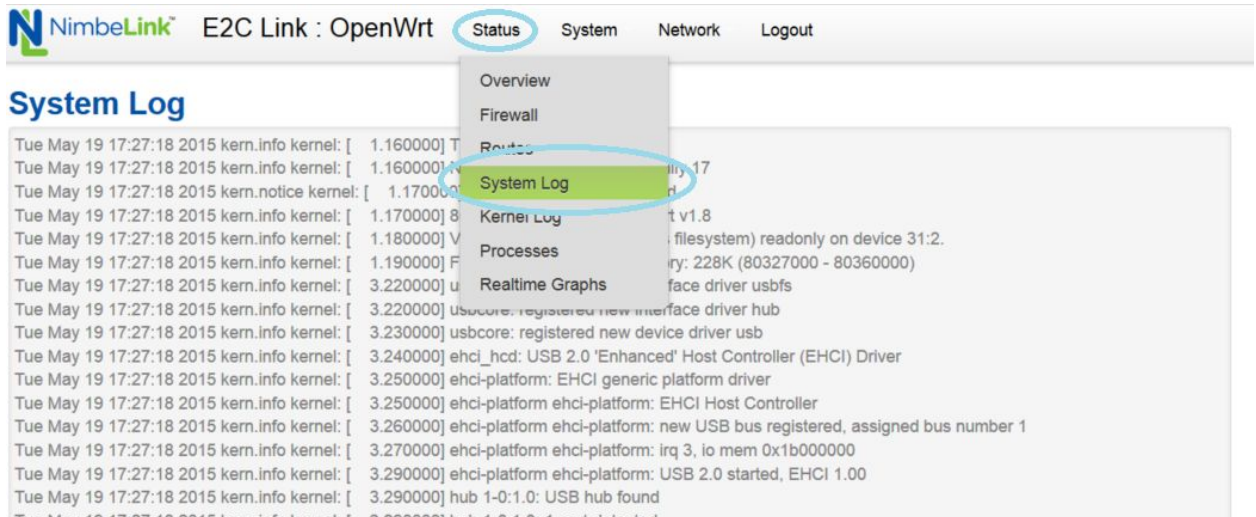


Figure 6

11. Accessing the System Log

The system log is a log files that records systems events. This log file is used to diagnose any issues that may arise when using the E2CLink and a copy may be needed by service technician to diagnose any issues. To view the system log go

to *Status>System Log*. Data in the System Log is constantly being overwritten; startup data may not be available after the system has been running for some time.



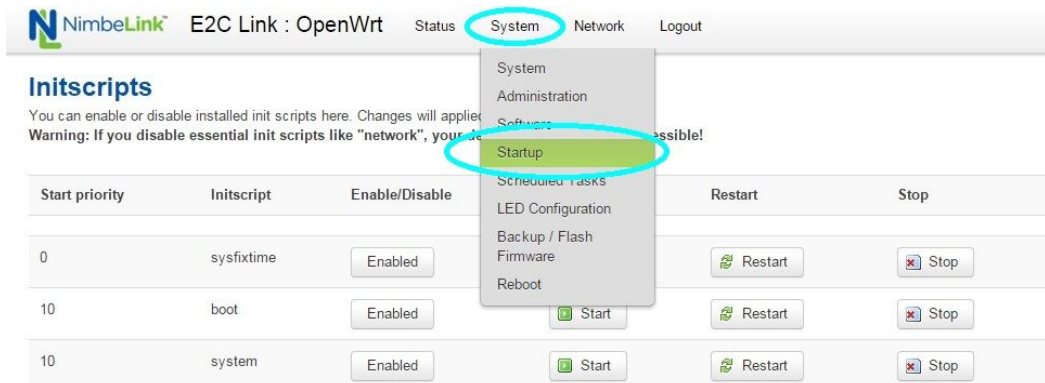
12. Startup Script

Upon boot-up, the E2CLink runs a Local Startup script in addition to any user scripts that may have been configured. The Local Startup script allows to user to

manually provision the modem and manually configure the devices APN (Access Point Name) for applicable devices.

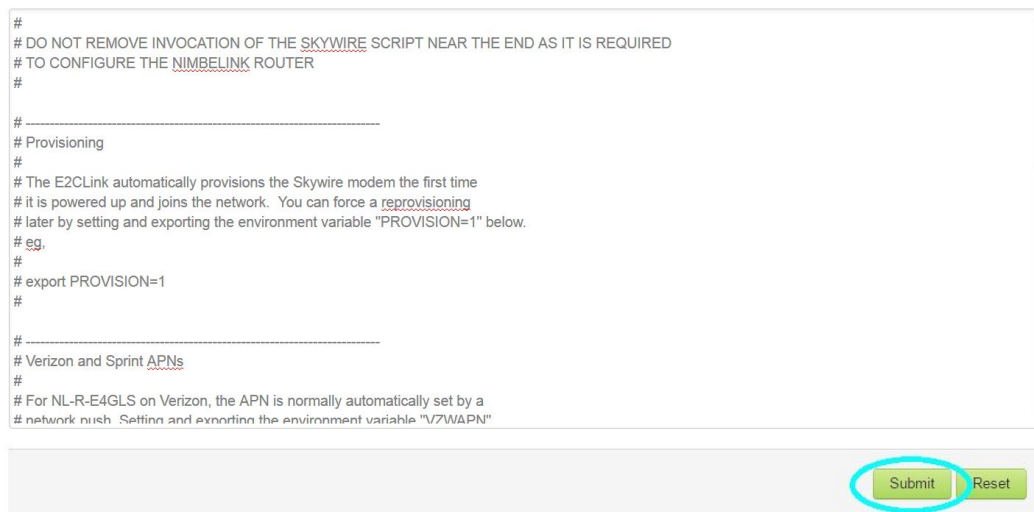
The Local Startup script is divided into five sections: Provisioning, Verizon and Sprint APN configuration, AT&T & T-Mobile APN configuration, Skywire® initialization, and a custom script section.

To access the Local Startup script navigate to *System>Startup* as indicated by the image below. This will load the page where the Local Startup script resides. When the Local Startup scripts configuration is complete click the submit button (2) and then restart the E2CLink by going to *System>Reboot*.



Local Startup

This is the content of /etc/rc.local. Insert your own commands here (in front of 'exit 0') to execute them at the end of the boot process.



12.1 Provisioning

Upon the first initialization of the E2CLink, or when the plan associated with the E2CLink is deactivated and then a new one is activated, the modem will need to be provisioned. This is the initialization process where the cellular modem in the E2CLink becomes a registered device on the cellular carrier's network and receives its phone number and APN (Access Point Name). 4G and GSM devices require an APN for (APN is needed for 4G LTE devices and GSM devices).

The initialization software on the E2CLink automatically provisions the modem upon first initialization. The user may need to force a re-provisioning for future reactivations if any of the following occurs:

- Account changes, such as deactivating and reactivating the modem on a different plan or changing the mobile number
- The APN of the device changes

The E2CLink can be forced to re-provision by issuing an “*export PROVISION=1*” command as directed in the provisioning section of the Local Startup script.

```
# -----  
# Provisioning  
#  
# The E2CLink automatically provisions the Skywire modem the first time  
# it is powered up and joins the network. You can force a re-provisioning  
# later by setting and exporting the environment variable "PROVISION=1" below.  
# eg,  
#  
# export PROVISION=1  
export PROVISION=1
```

By default, a commented out copy of the provisioning command is included in the the Local Startup Script to serve as a reference to the user. When issuing the provisioning command, the user should copy the provisioning command and paste it below the commented version without the # symbol (the # symbol acts to comment out the command).

12.2 Manually Configuring the APN

The E2CLink is configured to automatically set its APN at its first bootup. If the E2CLink is not able to properly configure the APN at bootup the user will need to manually configure the devices APN in order to work on their carrier’s network.

The APN is the name of the gateway that the cellular modem should use when connecting the cellular carrier's network. The APN determines what kind of IP address should be assigned to the device, which security methods that should be used, and if it should be within a customer private network.

APN information can be obtained by contacting your cellular data service provider.

The APN can be manually configured in the Local Startup script and is split into two sections. The first section is where the user can configure the APN for devices on the Verizon or Sprint networks. The second section is where the user can configure the APN for use on AT&T, T-Mobile, and other GSM networks. When manually setting the APN the user must configure the E2CLink to reprovision itself as explained in section 13.1.

Depending on the firmware version your E2CLink is running there might be different instructions inside of the local startup for configuring your APN.

For Verizon and Sprint APNs:

The APN is normally automatically set by a network push. Setting and exporting the environment variable "VZWAPN" to "auto" causes this behavior. You can override this and manually force the APN by setting and exporting the "VZWAPN" variable to your desired APN. eg.

```
export VZWAPN=mv01.VZWSTATIC
```

```
export VZWAPN=NIMBLINK.GW12.VZWENTP
```

```
export VZWAPN=auto
```

For AT&T and T-Mobile APNs:

For NL-R-E3GH and NL-R-E4GLN on AT&T, the default APN is "broadband". If a different APN is required because of the devices IP provisioning, you can manually set it by setting and exporting the environment variable "ATTAPN" below using your desired APN. eg.

```
export ATTAPN="broadband"
```

Once the APN has been manually configured in the Local Startup script, click the *Submit* button (2) to submit the startup script.

Local Startup ⁽¹⁾

This is the content of /etc/rc.local. Insert your own commands here (in front of 'exit 0') to execute them at the end of the boot process.

```
#  
# DO NOT REMOVE INVOCATION OF THE SKYWIRE SCRIPT AS IT IS REQUIRED  
# TO CONFIGURE THE NIMBELINK ROUTER  
#
```

The changes will not be in effect until the modem is rebooted. Go to *System>Reboot* to reboot the modem to make the startup script changes take effect.

12.3 Skywire[®] Initialization Code

The Local Startup script includes a section to initialize the Skywire modem inside of the E2C Link. Do not edit or remove this code, doing so may cause the E2CLink to fail to connect to the cellular network.

12.4 Custom Startup Code

Any custom startup code developed by the user should be included at the end of the Local Startup script before the exit 0 command.

13. WANWatchdog & Network KeepAlive

Devices that are connected to a cellular network can be disconnected by the network due to inactivity or network congestion. The timeout period for network inactivity varies between cellular carriers and network IP types. Please contact your cellular data provider for more information on the network timeout period associated with your cellular data plan. The E2CLink comes equipped with two

features, the KeepAlive and WANWatchdog scripts, which function to keep the E2CLink on the network.

The KeepAlive script will ping a remote host at a specified interval. This ping keeps traffic flowing over the cellular connection in order to avoid a network inactivity disconnect. The WANWatchdog behaves similarly to the KeepAlive script where it will ping a specified host at a set interval, but it has the added feature that it will cycle the WAN interface after it detects that E2CLink has been disconnected from the cellular network.

The WANWatchdog and KeepAlive scripts can be configured by going to *System>Scheduled Tasks*.

The screenshot shows the NimbeLink E2C Link : OpenWrt web interface. The navigation menu includes Status, System, Network, and Logout. The 'System' menu is expanded, showing options like System, Administration, Software, Startup, Scheduled Tasks (highlighted), LED Configuration, Backup / Flash, Firmware, and Reboot. The 'Scheduled Tasks' page contains a text area with the following crontab configuration:

```
#
# KeepAlive - Ping a remote host periodically but do not cycle WAN
#
# example is commented out and therefore disabled. Will ping
# host 8.8.8.8 every hour at :00 and log the pings to systemlog
#
#min hour day month dayofweek command
#0 0-23 * * * /usr/local/sbin/KeepAlive 8.8.8.8
#
```

At the bottom right of the page, there are 'Submit' and 'Reset' buttons, with the 'Submit' button highlighted.

13.1 KeepAlive Script

The KeepAlive Script is controlled by the “`#0 0-23 * * */usr/local/sbin/KeepAlive 8.8.8.8`” command in the Scheduled Tasks window. 8.8.8.8 is the targeted ping destination. “0 0-23 * * *” corresponds to the minute, hours, day, month, and day of the week pinging interval. Depending on the carrier and the IP provisioning of the device, the period will need to be changed to suite.

For example, if you are using a device from Verizon configured with a public static ip address, there is a 20 minute timeout period, so the script should read as follows:

```
20 0-23 * * */usr/local/sbin/KeepAlive 8.8.8.8
```

By default the KeepAlive script is disabled. To enable the KeepAlive script the user needs to be sure to remove the “#” character at the beginning of the line to allow for the line to be read. Once this has been done, click the submit button to save changes.

```
#
# KeepAlive - Ping a remote host periodically but do not cycle WAN
#
# example is commented out and therefore disabled. Will ping
# host 8.8.8.8 every hour and log the pings to systemlog
#
#min hour day month dayofweek command
20 0-23 * * */usr/local/sbin/KeepAlive 8.8.8.8
```

13.2 WAN Watchdog

The WANWatchdog allows the user to configure the E2CLink to ping a remote host at a specified interval. If the WANWatchdog fails to ping the remote host more than the specified amount it will then cycle the WAN interface and reconnect to the cellular network.

The WANWatchdog Script is controlled by the “*/30 * * * *
/usr/local/sbin/WANWatchdog 8.8.8.8 5” command in the Scheduled Tasks window. “*/30 * * * *” corresponds to the minute, hours, day, month, and day of the week pinging interval, by default it configured to 30 minutes. The 8.8.8.8 is the targeted ping destination and the 5 at the end of the line is the number of retry attempts to make before cycling the WAN interface. Depending on the carrier and the IP provisioning of the device, the period will need to be changed to suite.

```
#
# WANWatchdog - Ping a remote host periodically and if more than spec'd
# failures, cycle the WAN interface
#
# example is commented out and therefore disabled. Will ping
# host 8.8.8.8 every 30 mins and if fails 5 times, cycle the WAN interface
#
#min hour day month dayofweek command
*/20 * * * * /usr/local/sbin/WANWatchdog 8.8.8.8 5
```

For example, if you are using a device from Verizon configured with a public static ip address, there is a 20 minute timeout period, so the script should read as follows:

```
*/20 * * * * /usr/local/sbin/WANWatchdog 8.8.8.8 5
```

By default the KeepAlive script is disabled. To enable the KeepAlive script the user needs to be sure to remove the “#” character at the beginning of the line to allow for the line to be read. Once this has been done, click the submit button to save changes.

14. Inbound Connectivity

The E2CLink acts as an embedded firewall/router device that connects a local Ethernet (LAN) to the cellular network and the internet beyond that (WAN). By default, the E2CLink's Firewall Rules block any attempts to remotely access the device or the LAN devices. Remote access to the E2CLink or LAN devices is only possible after modifying the firewall rules to allow specific inbound/outbound connections. Special considerations will need to be made regarding the IP Provisioning of the cellular modem to allow for inbound connectivity.

The E2CLink obtains an IP address from the cellular network according to how the device was provisioned with the cellular provider. These IP addresses may be public IP addresses that are accessible by the open internet or they may be VPN (Virtual Private Network) IP addresses that are protected by the cellular carrier's firewall. There are four types of IP provisioning that the device could have:

- Public Static
- Public Dynamic
- Private Dynamic (VPN)
- Private Static (VPN)

Devices with a dynamic IP type are not suitable for inbound connections as the IP address is dynamically assigned and may change with time. Devices with a static IP type on the public and private networks are suitable for inbound connections as the IP address is statically assigned and will not change with time.

From a security standpoint, devices with a public IP address are assumed to have an IP address that is only protected by the E2CLink's firewall. These devices are accessible by the public internet and all forms of port snooping, DoS (denial of service attacks), and other attacks. The E2CLink's firewalling can secure devices on the LAN against these attacks but the attacks will still be generating cellular data costs because the attackers data is transiting the cellular network to the E2CLink.

Devices using a Private IP address (and the carriers' associated Private Network services) are located on a Virtual LAN (VLAN) within the carrier's network and are additionally protected by the carrier's network firewall. These private devices are then segregated from other private network customers, and from the open internet. Certain types of configurations can allow the devices to access the internet, but in general, devices outside the private network VLAN cannot connect in. Should the need exist for inbound connections using Private IPs, the carriers can work with the customer to establish a hardware VPN (Virtual Private Network), which can connect the customer's private network with the carrier's network. With this VPN in place, traffic can flow from the device to the

customer's network (Mobile Originated), or from the customer's network to the device (Mobile Terminated).

NimbeLink also maintains a special type of private network with Verizon and has data plans available for use with the private network option. The specific NimbeLink-configured private network allows the devices to be assigned Private IP addresses, yet still access the internet to reach public servers (Mobile Originated only). For assistance getting your solution implemented, contact sales@nimbelink.com.

In general, neither Static nor Dynamic Public addresses are ideal because the cellular carrier performs no firewalling on inbound traffic to these addresses and that burden moves to the E2CLink's firewall. Although the E2CLink firewall is robust and can prevent these attacks from reaching the hosts on the LAN behind it, it cannot prevent the consumption of cellular bandwidth and costs due to arbitrary internet traffic hammering on the public IP addresses.

If your device is configured with a public static IP address it is exposed to the public internet and could be subjected to remote access attempts by unknown systems. These attempts will drive up your data usage on your plan and could compromise the security of your device and any connected sub systems. It is recommended that your system dials out to a remote server rather than having a remote service dial in.

The private IP address types provide the best security model since the unfiltered internet will be firewalled at the cellular provider's front door, well before any undesirable traffic makes its way onto the cellular network and to the E2CLink. This eliminates concerns over paying for cellular bandwidth to support internet hackers performing DoS attacks against the E2CLink firewall for example.

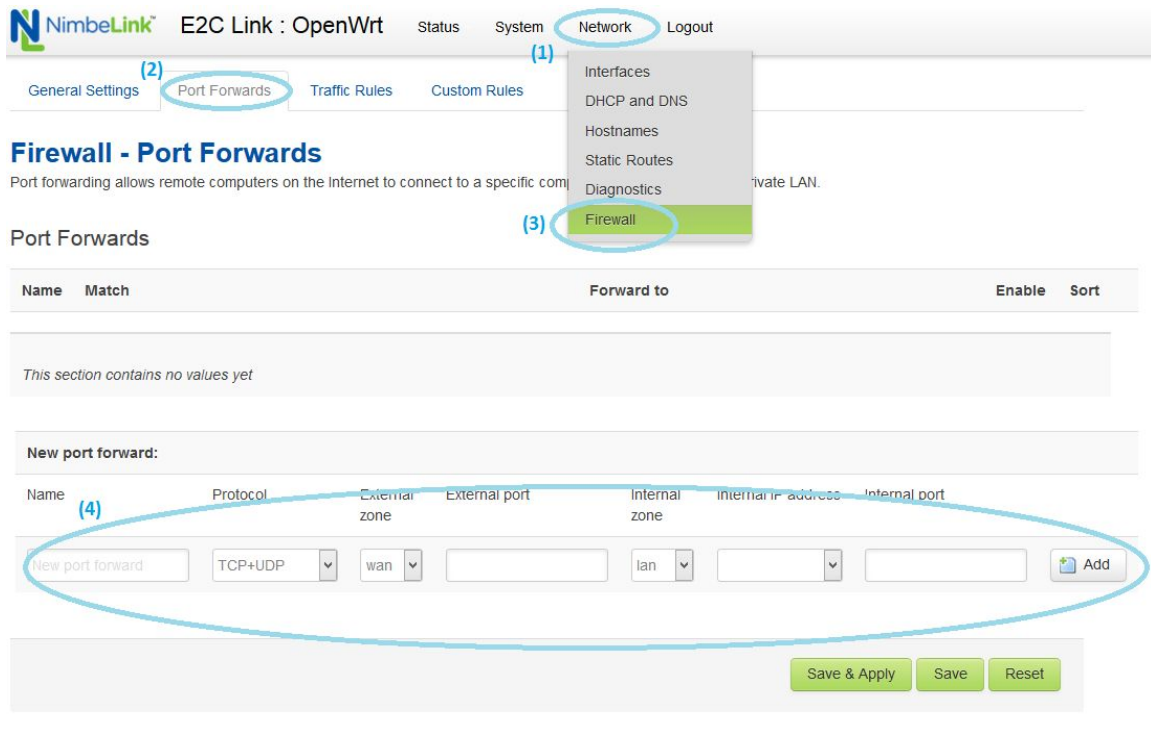
To configure a device to allow inbound connectivity, new port forwarding rules and traffic rules must be configured in the E2CLink's firewall for each port. Please refer to section 14 for instructions on how to configure the E2CLink for inbound connectivity. Example configurations are documented in section 16.

14.1 Port Forwarding

Port forwarding allows the user to direct incoming traffic, from remote computers, to specific IP addresses and ports on the E2CLink's LAN. For a cellular device, Port Forwarding has two components: one is modifying the Port Forwarding rules within the E2CLink and the second is to configure a Public or Private Static IP address, with your cellular data provider (private addresses will require a hardware VPN in order to reach the cellular device from within your network). The following section will detail how to correctly configure Port Forwarding rules on the E2CLink. To change the configuration for your cellular data plan please contact your cellular service provider.

14.1.1 Configure E2CLink Port Forwarding

- 1) Click on the Network tab.
- 2) Click on the Firewall tab.
- 3) Click on the Port Forwards tab.
- 4) Fill out Port Forwarding details and click the Add button.
 - a. Name: The name for the port forwarding rule. For example, "*PLC Remote Access*"
 - b. Protocol: The protocol to use for the port forwarding. For example, "UDP"
 - c. External Zone: WAN (for external connections coming in)
 - d. External Port: The port that will be routed from the WAN to the LAN. For example, "62000"
 - e. Internal Zone: LAN (select LAN if it is a LAN side device)
 - f. Internal IP Address: LAN side IP address of the targeted device. For example, "192.168.1.100"
 - g. Internal Port: Port the targeted device connects through. For example, "62001"
- 5) After the Add button is clicked a new port forwarding rule will appear in the Port Forwards table
- 6) Click the *Save & Apply* to save the changes. To complete the firewall configuration for inbound connections the user will need to configure a traffic rule to open the port on the firewall. Instructions on this are in section 14.2.



14.2 Traffic Rules

To allow inbound traffic the external port needs to be opened in the firewall. This is done in the *Traffic Rules* section. Section 14.2.1 details the steps needed to open an external port.

14.3 Configuring Traffic Rules

- 1) Click on the Network tab.
- 2) Click on the Firewall tab.
- 3) Click on the Traffic Rules tab.
- 4) Scroll down

NimbeLink E2C Link : OpenWrt Status System **Network** Logout

General Settings Port Forwards **Traffic Rules** Custom Rules

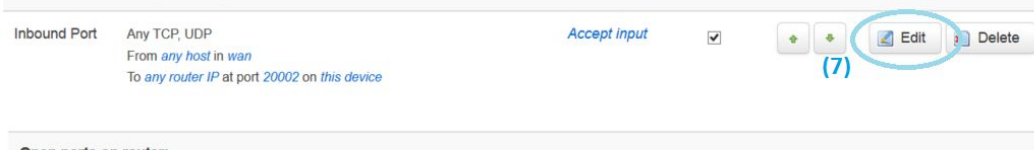
Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example maintain hosts or to open WAN ports on the router.

Traffic Rules

Name	Match	Action	Enable	Sort
Allow-DHCP-Renew	IPv4-UDP From <i>any host</i> in <i>wan</i> To <i>any router IP</i> at port <i>68</i> on <i>this device</i>	Accept input	<input checked="" type="checkbox"/>	+ + Edit Delete
Allow-Ping	IPv4-ICMP with type <i>echo-request</i> From <i>any host</i> in <i>wan</i> To <i>any router IP</i> on <i>this device</i>	Accept input	<input checked="" type="checkbox"/>	+ + Edit Delete
Allow-DHCPv6	IPv6-UDP From IP range <i>FE80:0:0:0:0:0:0:0/10</i> in <i>wan</i> with source port <i>547</i> To IP range <i>FE80:0:0:0:0:0:0:0/10</i> at port <i>546</i> on <i>this device</i>	Accept input	<input checked="" type="checkbox"/>	+ + Edit Delete
Allow-ICMPv6-Input	IPv6-ICMP with types <i>echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type, router-solicitation, neighbour-solicitation, router-advertisement, neighbour-advertisement</i> From <i>any host</i> in <i>wan</i> To <i>any router IP</i> on <i>this device</i>	Accept input and limit to <i>1000</i> pkts. per <i>second</i>	<input checked="" type="checkbox"/>	+ + Edit Delete
Allow-ICMPv6-Forward	IPv6-ICMP with types <i>echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type</i> From <i>any host</i> in <i>wan</i> To <i>any host</i> in <i>any zone</i>	Accept forward and limit to <i>1000</i> pkts. per <i>second</i>	<input checked="" type="checkbox"/>	+ + Edit Delete

- 5) Under the *Open Ports on Router* Section the following fields need to be configured by the user:
 - a. Name: Open Port Rule Name. For example, "PLC Config Port"
 - b. Protocol: Protocols to allow. For example, "UDP"
 - c. External Port: Port to open. For example, "62000"
- 6) Once the Port information is entered click the *Add* Button. This will add the new Open Port rule to the traffic rules.



- 7) The new port rule will be displayed at the bottom of the traffic rules table. There are additional settings that the user needs to configure to enable port forwarding. Click the edit button to continue editing the configuration rules for this port.
- 8) After the edit button has been clicked the editing page for the new traffic rule will load, as shown on the next page. The user needs to define the source port (8) and destination address(9) for the inbound connection in order to correctly route the data. On this page the User can further define the allowed address families, protocols, and the source/destination zone, Source MAC address, IP address, and actions to take for inbound connections. These additional routing options allow the user to select specific IP addresses, MAC addresses, and actions to take when an inbound connection occurs.
- 9) When editing the rule is complete, click on the *Save & Apply* button to save the new Traffic Rule into the firewall.

Firewall - Traffic Rules - Inound Port

This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

Rule is enabled

Name

Restrict to address family

Protocol

Match ICMP type

Source zone

Any zone

lan: lan:

wan: wan:

Source MAC address

Source address

Source port (8)

Destination zone

Device (input)

Any zone (forward)

lan: lan:

wan: wan:

Destination address (9)

Destination port

Action

Extra arguments

Passes additional arguments to iptables. Use with care!

[Back to Overview](#)

[Save & Apply](#)

[Save](#)

[Reset](#)

15. Inbound Connectivity Examples

15.1 Remotely Accessing the E2CLink's Management Console

An E2CLink with a public static IP or a properly configured private static IP address can be configured to allow remote access to the unit's graphical interface. This method does expose the management console to the open internet and may subject the device to intrusion attempts and unwanted data usage. To protect the security of the E2CLink's network users must be sure to properly configure the device's firewall and use a robust password.

This example will walk the user through how to configure the port forwarding and traffics rules to allow for a remote connection into the E2CLink. This example will configure the E2CLink to accept an external connection on port 11000 and then route it to the E2CLink's management console at 192.168.1.1 on port 80. This example assumes the user is using a device with a Public Static IP address.

15.1.1 Step 1: Configuring the Port Forwarding

- 1) Power up the E2CLink and connect a host computer directly to the E2CLink's Ethernet Port. The host computer should not be connected to any other networks during this configuration.
- 2) Login to the management console (the default IP is 192.168.1.1)
- 3) Click on the Network tab.
- 4) Click on the Firewall tab.
- 5) Click on the Port Forwards tab.
- 6) Fill out the *New Port Forward* details then click the Add button.

New port forward:						
Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port
Remote GUI	TCP	wan	11000	lan	192.168.1.1 (O)	80

- a. Name: The name for the port forwarding rule. In this example we will call this Rule "Remote GUI"
- b. Protocol: TCP(HTTP is a TCP protocol)
- c. External Zone: WAN
- d. External Port: 11000
- e. Internal Zone: LAN
- f. Internal IP Address: 192.168.1.1 (default IP address of the E2CLink)

g. Internal Port: 80 (Port 80 is for HTTP traffic)

7) After the Add button is clicked, a new port forwarding rule will appear in the Port Forwards table.

Firewall - Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Port Forwards

Name	Match	Forward to	Enable	Sort
Remote GUI	IPv4-TCP From <i>any host</i> in <i>wan</i> Via <i>any router IP</i> at port <i>11000</i>	IP <i>192.168.1.1</i> , port <i>80</i> in <i>lan</i>	<input checked="" type="checkbox"/>	

8) Click the *Save & Apply Button* to save the changes.

15.1.2 Step 2: Configuring Traffic Rules

- 1) Click on the Network tab.
- 2) Click on the Firewall tab.
- 3) Click on the Traffic Rules tab.
- 4) Scroll down

Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to block access to certain hosts or to open WAN ports on the router.

Name	Match	Action	Enable	Sort
Allow-DHCP-Renew	IPv4-UDP From <i>any host</i> in <i>wan</i> To <i>any router IP</i> at port <i>68</i> on <i>this device</i>	<i>Accept input</i>	<input checked="" type="checkbox"/>	
Allow-Ping	IPv4-ICMP with type <i>echo-request</i> From <i>any host</i> in <i>wan</i> To <i>any router IP</i> on <i>this device</i>	<i>Accept input</i>	<input checked="" type="checkbox"/>	
Allow-DHCPv6	IPv6-UDP From IP range <i>FE80:0:0:0:0:0:0:0/10</i> in <i>wan</i> with source port <i>547</i> To IP range <i>FE80:0:0:0:0:0:0:0/10</i> at port <i>546</i> on <i>this device</i>	<i>Accept input</i>	<input checked="" type="checkbox"/>	
Allow-ICMPv6-Input	IPv6-ICMP with types <i>echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type, router-solicitation, neighbour-solicitation, router-advertisement, neighbour-advertisement</i> From <i>any host</i> in <i>wan</i> To <i>any router IP</i> on <i>this device</i>	<i>Accept input</i> and limit to <i>1000</i> pkts. per <i>second</i>	<input checked="" type="checkbox"/>	
Allow-	IPv6-ICMP with types <i>echo-request, echo-reply, destination-</i>	<i>Accept forward</i>	<input checked="" type="checkbox"/>	





- 5) Under the *Open Ports on Router* Section enter the following:
- a. Name: Remote GUI
 - b. Protocol: TCP
 - c. External Port: 11000

Open ports on router:

Name	Protocol	External port	
Remote Gui	TCP+UDP	11000	

- 6) Once the Port information is entered click the *Add* Button. This will add the new Open Port rule to the traffic rules. Scroll down and click the *Save & Apply* button to save your changes.
- 7) The modem is now configured to allow inbound connections to the GUI over port 11000.

To *any host in any zone*

Remote Gui	Any TCP	Accept input	<input checked="" type="checkbox"/>	   
	From <i>any host in wan</i>			
	To <i>any router IP</i> at port <i>11000</i> on <i>this device</i>			

(8)

- 8) Additional security configurations of the opened external port, such as matched sources and destination hosts, can be configured by clicking the edit button for the *Remote GUI* traffic rule. The edit page will look similar to the image below.

Firewall - Traffic Rules - Remote Gui

This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

Rule is enabled Disable

Name

Restrict to address family

Protocol

Match ICMP type

Source zone Any zone
 lan: lan
 wan: wan

Source MAC address

Source address

Source port

Destination zone Device (input)
 Any zone (forward)
 lan: lan
 wan: wan

Destination address

Destination port

Action

Extra arguments

Passes additional arguments to iptables. Use with care!

- 9) Change the destination address to 192.168.1.1 to only allow connections through port 11000 to access the E2CLink's configuration console. Then click *Save & Apply*.

15.1.3 Step 3: Remotely Connect to the E2CLink

- 1) To remotely connect into the E2CLink you will need to know the public IP address of the device. For devices with a private static IP you will need to contact your network administrator. Devices with a Public Static IP can check their IP address under the *Network* tab (1).
- 2) Under the *Network* tab there is an *Interface Overview* window that displays information on the WAN (cellular) connection (2). This device's WAN IPV4 address is displayed under the *IPV4* section (3). If the device has a public static IP this is the IP address that the device can be accessed from via the public internet. If the device has a private static IP address this is the LAN IP address of this device within its VPN.

Interfaces

Interface Overview

Network	Status	Actions
LAN br-lan	Uptime: 0h 40m 11s MAC-Address: 4E:7F:3A:13:D1:C6 RX: 380 98 KB (3700 Pkts.) TX: 1 12 MB (3180 Pkts.) IPV4: 192.168.1.1/24 IPV6: FD60:A9ED:E9F8:0:0:0:0:1/60	Connect Stop Edit Delete
WAN wwan0	Uptime: 0h 39m 59s MAC-Address: 8A:B3:39:9B:48:27 RX: 23 23 KB (204 Pkts.) TX: 102 0 4 100 (975 Pkts.) IPV4: 166.250.155.87/28	Connect Stop Edit Delete

(1) (2) (3)

Add new interface...

Global network options

IPv6 ULA-Prefix

Save & Apply Save Reset

- 3) The demonstration device has a Public Static IP Address of 166.250.155.087; your device will have a different IP address. Unplug the Ethernet from the E2CLink and the configuration computer then connect the configuration computer to another internet source. To remotely access the E2CLink enter "**your device's IP:11000**" into your web browser and the login screen for the E2CLink's Console will appear.

E2C Link : OpenWrt

192.168.1.1/cgi-bin/luci

NimbeLink E2C Link : OpenWrt

Authorization Required

Please enter your username and password.

Username

Password

Login Reset

Powered by LuCI 0.12 Branch (0.12+git-15.112.69076-6153b99) OpenWrt E2CLink1p-20151012

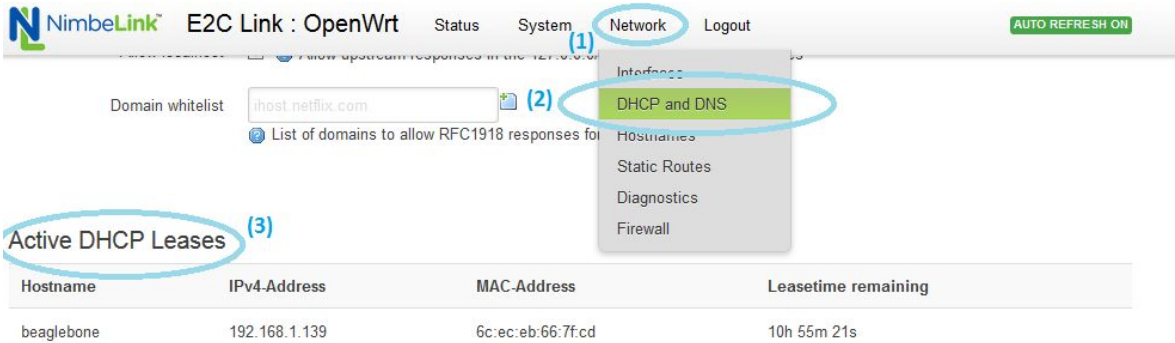
15.2 Remotely Access a Device Connected to the E2CLink's LAN

This example will detail how to remotely connect (SSH) into a device that is connected over Ethernet to the E2CLink. The end device that is being connected to is a BeagleBone Black that is running a Debian Linux distribution. This guide will use the remote connection that was created in section 15.1 to access the management console of the E2CLink. The E2CLink is configured with a public static IP address

This example will guide the user through configuring a device to have a LAN side static IP address based upon the MAC address, configuring the Port Forwarding for the device, and configuring the traffic rules. The first step will configure the LAN side device to have a static IP address. This is needed to ensure that the device stays at a known IP address so the E2CLink can properly forward inbound connections to it. The second step configures the port forwarding rules for the E2CLink to forward connections on the external port into the LAN side device on the appropriate port. The third step is to create a traffic rule to open the external port and configure that port to only connect to the specific LAN side device. The final step details how to SSH into the BeagleBone test device.

15.2.1 Step 1: Configure the LAN Side Device to have a Static IP Address

- 1) Connect your LAN device to the E2CLink's Ethernet port, then power up both devices.
- 2) Log into the management console via the remote connection that was configured in section 15.1. Then navigate to the DHCP and DNS configuration page by going to *Network>DHCP and DNS (1) (2)*.



- 3) Scroll down until the *Active DHCP Leases* window (3) is visible. There will be a DHCP lease for your device showing the host name, IP address, and MAC address of the device. Take note of them, because they will be needed for the next step. In this example the device information is as follows:

- a. Host Name: Beaglebone
- b. IPV4-Address: 192.168.1.139
- c. MAC-Address: 6C:EC:EB:66:7F:CD

- 4) Scroll down to the *Static Leases* section (4) and click the *Add* button (5). A New entry window will appear. In this window you can set your device to have a static IP address on the LAN. Enter in the hostname, MAC address, and IPV4 Address of your device that was shown in the *Active DHCP Leases* section from the previous step.

Static Leases (4)

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served.
Use the *Add* Button to add a new lease entry. The *MAC-Address* identifies the host, the *IPV4-Address* specifies to the fixed address to use and the *Hostname* is assigned as symbolic name to the requesting host.

Hostname	MAC-Address	IPV4-Address	IPV6-Suffix (hex)	
Beaglebone	6c:ec:eb:66:7f:cd (192.168.1.139)	192.168.1.139		Delete
				Delete

(5) Add

Save & Apply Save Reset

- 5) Once the Static IP lease information is entered click the *Save & Apply* button.

15.2.2 Step 2: Configure the Port Forwarding

- 1) In the management console, navigate to *Network>Firewall>Port Forwards*.

The screenshot shows the 'Firewall - Port Forwards' configuration page in the OpenWrt web interface. The 'Network' menu is open, and 'Firewall' is selected. The 'Port Forwards' section displays a table of existing rules:

Name	Match	Forward to	Enable	Sort
Remote GUI	IPv4-TCP From any host in wan Via any router IP at port 11000	IP 192.168.1.1, port 80 in lan	<input checked="" type="checkbox"/>	[Up] [Down] [Edit] [Delete]
BeagleBone	IPv4-TCP, UDP From any host in wan Via any router IP at port 11001	IP 192.168.1.139, port 22 in lan	<input checked="" type="checkbox"/>	[Up] [Down] [Edit] [Delete]

Below the table is the 'New port forward:' form with the following fields:

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port
BeagleBone	TCP+UDP	wan	11001	lan	192.168.1.139	22

At the bottom of the form, there are three buttons: 'Save & Apply', 'Save', and 'Reset'. The 'Add' button is highlighted in the original image.

- 2) Under the *New Port Forward* section enter
 - a. Name: Name of your port forwarding rule, in this example it is "BeagleBone".
 - b. Protocol: TCP+UDP
 - c. External Zone: WAN
 - d. External Port: The port you want to use to connect in through, in this example the port used is 11001.
 - e. Internal Zone: LAN
 - f. Internal IP Address: Assign the Static IP address that you configured in Step 1. In this example it is 192.168.1.139.
 - g. Internal Port: This depends on the protocol you are using to connect to the device. In this case we are SSHing into the Beaglebone so we will use SSH port 22.
- 3) Click the *Add* button to add the Port Forwards Rule to the Firewall. Then click *Save & Apply*.

15.2.3 Step 3: Configure the Traffic Rules

- 1) To open the external port go to *Network>Firewall>Traffic Rules* and then scroll down to the *Open Ports on Router* Section (1).

NimbeLink™ E2C Link : OpenWrt Status System Network Logout

Forward	<i>header-type</i> From <i>any host in wan</i> To <i>any host in any zone</i>	pkts. per <i>second</i>		
Remote Gui	Any TCP From <i>any host in wan</i> To IP <i>192.168.1.1</i> at port <i>11000</i> on <i>this device</i>	<i>Accept input</i>	<input checked="" type="checkbox"/>	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
BeagleBone	Any TCP, UDP From <i>any host in wan</i> To <i>any router IP</i> at port <i>11001</i> on <i>this device</i>	<i>Accept input</i>	<input checked="" type="checkbox"/>	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

(2)

Open ports on router: (1)

Name	Protocol	External port	
<input type="text" value="BeagleBone"/>	<input type="text" value="TCP+UDP"/>	<input type="text" value="11001"/>	<input type="button" value="Add"/>

- 2) Under the *Open Ports on Router* section enter the following information then click the *Add* button (2):
 - a. Name: Name of your Port forwarding rule, in this example is called "BeagleBone".
 - b. Protocol: TCP+UDP
 - c. External Port: The port you want to use to connect in through, in this example the port used is 11001.
- 3) Once the *Add* button has been clicked a new Port Forwarding rule will be created. Click the *Edit* button (3) to further define the traffic rules for this port.
- 4) Scroll down on the Traffic Rules Edit page until the Destination address option is visible (4). Select the Static IP address of the LAN side device that is being connected to. In this example the static LAN IP address is 192.168.1.139. After the IP address is selected click the *Save & Apply* button to apply the new Firewall rule.

(4) Destination address

Destination port

Action

Extra arguments

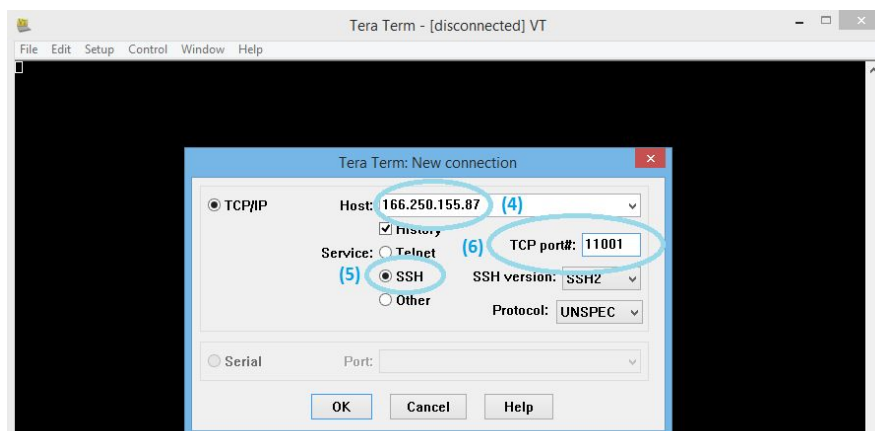
Passes additional arguments to iptables. Use with care!

15.2.4 Step 4: Access the Device

- 1) To access the device you will need the Public IP address of the E2CLink router. To check the IP address of an E2CLink with a public static IP, navigate to the Network interfaces section in the *Network* tab (1). Under the WAN network information section (2) the public IP address (3) of the device is shown in the IPV4 section.

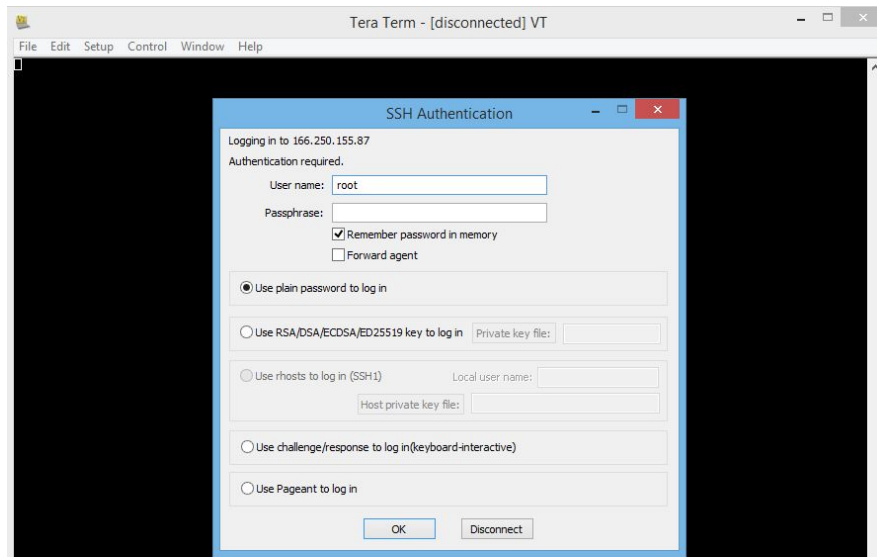
The screenshot shows the NimbeLink E2C Link : OpenWrt Network tab. The 'Network' tab is selected and circled with a blue circle (1). Below the navigation bar, the 'Interfaces' section is titled. Under 'Interface Overview', there are two interface cards: 'LAN' and 'WAN'. The 'WAN' card is circled with a blue circle (2). Within the 'WAN' card, the 'IPV4' section is circled with a blue circle (3), showing the IP address '166.250.155.87/28'. The 'LAN' card shows 'br-lan' and the 'WAN' card shows 'wwan0'. There are 'Connect', 'Stop', 'Edit', and 'Delete' buttons for each interface. An 'Add new interface...' button is at the bottom left.

- 2) Using a terminal program (this example uses Tera Term) establish a SSH connection to the device. Enter in the E2CLink's IP address in the "Host" field (4) and then enter the external port that forwards to the LAN device in the TCP Port field (5) (11001 in this example). Select SSH for the service (6) then click OK.

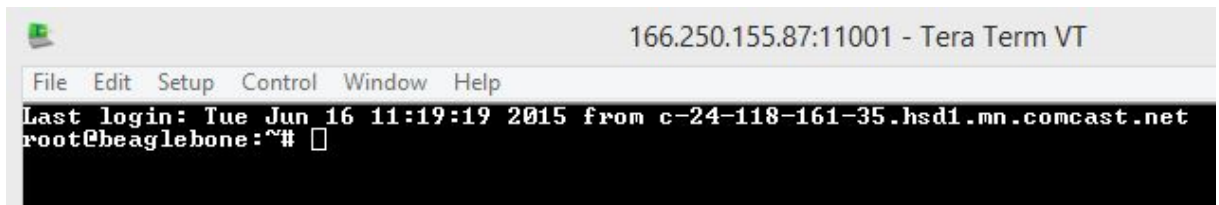


- 3) If the routing is successful an authentication window will pop up asking for login credentials. Enter the appropriate credentials and click OK. If the connection fails review the Firewall rules on the E2CLink and

check to make sure your LAN device supports the attempted kind of connection.



- 4) If the connection and authentication is successful a command prompt will appear and the device is now connected via SSH.



16. Pseudo-Bridge Mode

The E2CLink can be configured for pseudo-bridge mode operation. This mode will route all inbound traffic to the device that is connected to the LAN of the E2CLink. This will bypass the Firewall on the E2CLink so it is imperative that the LAN side device be protected by a local firewall.

The E2CLink does not support IP Pass Through; the pseudo-bridge mode is suggested as an alternative.

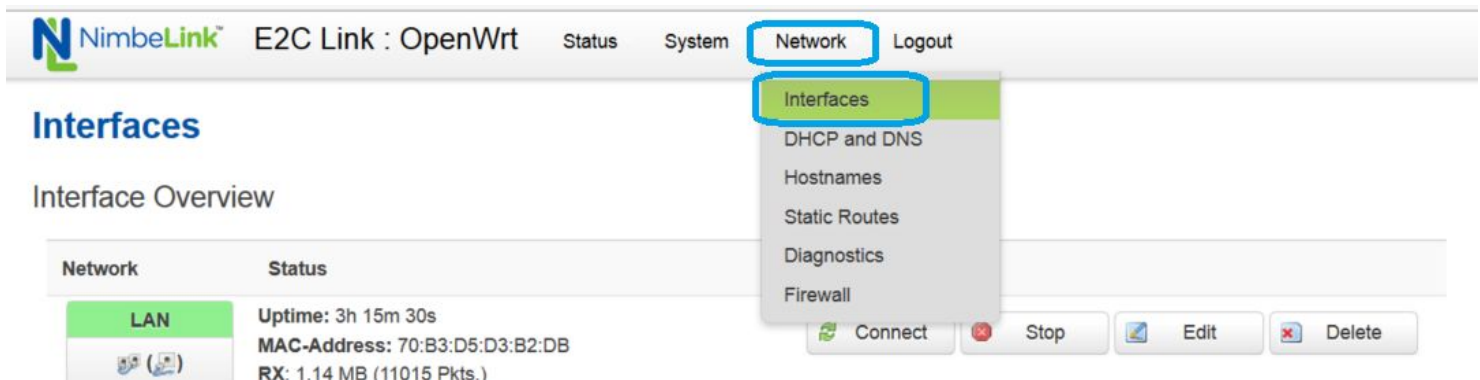
The following example will detail how to set up a pseudo-bridge mode for a single connected device.

16.1 Pseudo-Bridge Mode Configuration


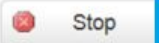


16.1.1 Step 1: Configure the DHCP Service

This step will configure the DHCP on the E2C Link to only have one IP address available, creating a static IP for any device that is connected to the system. This simplifies the firewall rule that will be created in the second step requires a specific IP to route all of the data to. If a new device is connected to the E2CLink the user will need to power cycle the E2CLink.

- 1) Navigate to the Network Interfaces page by clicking *Network>Interfaces*



2) Click the “Edit” button under the LAN interface

Network	Status	Actions
LAN  br-lan	Uptime: 3h 9m 5s MAC-Address: 70:B3:D5:D3:B2:DB RX: 1.05 MB (10271 Pkts.) TX: 914.77 KB (6905 Pkts.) IPv4: 192.168.1.1/24 IPv6: FD82:4A0E:7053:0:0:0:1/60	 Connect  Stop  Edit  Delete

3) Scroll down to the DHCP Server configuration area at the bottom of the page. Change the “Start” field to the address you wish the device to receive (for example, “192.168.1.100”). Then change the “Limit” to “1”. Optional: set the “Leasetime” field to “2m” to have the DHCP lease renew every two minutes to avoid having to power cycle the E2CLink when a new device is connected.

DHCP Server

General Setup **Advanced Settings** IPv6 Settings

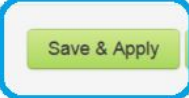


Ignore interface Disable DHCP for this interface.

Start
Lowest leased address as offset from the network address.

Limit
Maximum number of leased addresses.

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

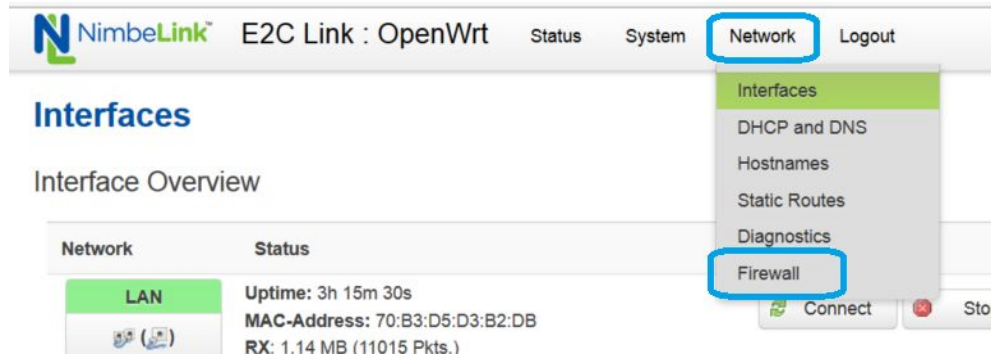
4) Click “Save & Apply” to save your settings.

 Save & Apply  Save  Reset

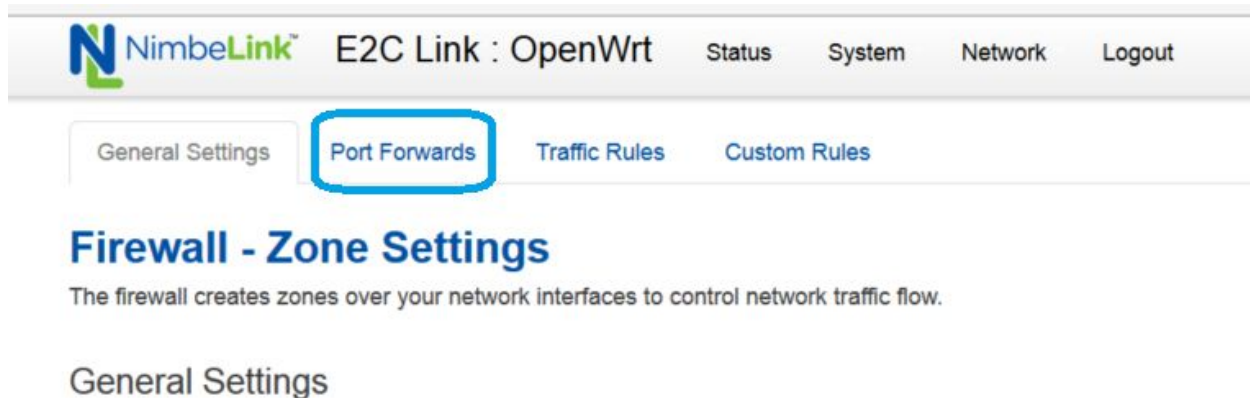
16.1.2 Step 2: Create a DMZ Firewall Rule

This step will configure the E2CLink's firewall to forward all of the inbound traffic to the specified IP address.

5) Navigate to the Network Interfaces page by clicking *Network>Firewall*



6) Click on the “Port Forwards” tab



7) Under the “New port forward” section, fill in the following information and then click the “add button”:

Name = DMZ

Protocol = TCP + UDP

External Zone = WAN

External Port = <leave blank>

Internal Zone = LAN

Internal IP Address = Custom fill in the IP address you configured DHCP service for from above (for example “192.168.1.100”)

Firewall - Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Port Forwards

Name	Match	Forward to	Enable	Sort
SI	IPv4-TCP, UDP From <i>any host</i> in <i>wan</i> Via <i>any router IP</i> at port <i>55056</i>	IP <i>192.168.1.2</i> , port <i>55056</i> in <i>lan</i>	<input checked="" type="checkbox"/>	<input type="button" value="+"/> <input type="button" value="+"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

New port forward:

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port
<input type="text" value="DMZ"/>	<input type="text" value="TCP+UDP"/>	<input type="text" value="wan"/>	<input type="text"/>	<input type="text" value="lan"/>	<input type="text" value="192.168.1.100"/>	<input type="text"/>

8) Click "Save & Apply" to save your settings.

17. Troubleshooting

The following will detail how to diagnose and correct common performance issues that may occur with the E2CLink. During the debug process, users will need to have access the System Log as detailed in section 11.

For additional troubleshooting resources, or to ask any technical questions, please visit: <https://support.nimbelink.com/>

17.1 The E2CLink Will Not Connect to the Network

There are many reasons why an E2CLink might not connect to the network. The most common reasons--poor signal quality, APN misconfiguration (4G LTE and GSM devices), and data plan misconfigurations are detailed in the following sections.

17.1.1 Poor Signal Quality

The E2CLink needs a strong cellular signal in order to provide a robust cellular data connection. There are many factors that will influence the quality of the cellular signal received by the E2CLink, including antenna placement, local network conditions, and network locations. The E2CLink will periodically test the signal strength of the cellular network and report it to the System Log in the E2CLink's Management Console.

To find the signal strength the user can use the search function in your browser to search for "skywire: +CSQ" in the System log. The result of this search will show a line containing the signal strength of the cellular antenna and the bit error rate in percent similar to the output below:

"user.notice skywire: +CSQ: XX,YY"

XX is the reported signal strength of the antenna, and YY is the bit error rate in percent. Typical values are as follows:

Values of XX	Relative to Signal Strength
0-9	Marginal: -113 dBm to -95 dBm
10-14	OK: -93 dBm to -85 dBm
15-19	Good: -83 dBm to -75 dBm
20-30	Excellent: -73 dBm to -51 dBm
31	Excellent: -51 dBm or greater
99	Not Know or not detectable

Values of YY	Bit Error Rate (In Percent)
1	Less than 0.2%
2	0.2% to 0.4%
3	0.4% to 0.8%
4	0.8% to 1.6%
5	1.6% to 3.2%
6	3.2% to 6.4%
7	More than 12.8%
99	Not known or not detectable

Instances where the E2CLink's cellular signal quality is -85dBm and below indicates that there is poor cellular signal at the E2CLink's location. Users should try moving the antenna(s) to a different location and checking the signal again. When a E2CLink is located inside of a building or an electrical box, an external antenna may need to be used to increase the signal quality. Users should take care to mount the E2CLink's antennas away from any large metallic objects, motors, and other equipment that may produce EMI (Electromagnetic Interference).

17.1.2 Troubleshooting APN Misconfigurations

The 4G LTE and GSM E2CLink products require their APN to be configured during their initial network connection. This is a one time process that is handled automatically, unless the user changes the IP provisioning of the cellular data plan associated with the E2CLink. In the event that the E2CLink can not connect to the cellular network the user should verify the APN, which can be found in the System Log. Please note that the System Log will overwrite itself with time. If the APN is not found in the System Log please power cycle your E2CLink to regenerate the initialization data in the System Log.

The APN that is being used can be found by using the search function in your browser to search for 'APN' in the system log. A line similar to the following should be found:

```
Thu May 26 15:21:20 2016 user.notice skywire: VZW auto APN is VZWINTERNET
```

The APN that is in use is located at the end of the line (highlighted in blue), and this APN should match the one provided by your cellular data provider.

If the APN is misconfigured, the system log will contain an output similar to the following:

```
Mon Apr 4 13:30:54 2016 daemon.info qmi[1235]: Starting network vzwintern
```

```
Mon Apr 4 13:30:54 2016 daemon.err qmi[1235]: Unable to connect, check APN and authentication
```

The first line indicates the APN that the E2CLink is attempting to connect with. If it is not successful there will be a line that states “*Unable to connect, check APN and authentication.*” This indicates that the APN is not correctly configured. In the event this error occurs, please check with your cellular data provider that your data plan is active and that the E2CLink is using the correct APN. If the E2CLink is not using the correct APN, the user will need to manually configure the APN. To do so please refer to section 12.2.

17.1.3 Troubleshooting Cellular Data Plans

In rare instances, customers cellular data plan(s) associated with the E2CLink's may be misconfigured and will prevent the E2CLink from connecting to the network. This is the case when the E2CLink can connect to the cellular network, but can not send data out to the public internet. To troubleshoot this issue please contact your cellular data provider and NimbeLink's technical support team. For Verizon enabled devices, NimbeLink can work with your Verizon Representative to verify that the cellular data plan is correctly configured.

17.2 E2CLink's Management Console Will Not Load

The common causes of the E2CLink's Management Console failing to load are detailed below.

17.2.1 Power

If the E2CLink's Management Console will not load please verify that the device is powered. If the E2CLink is powered the LED closest to the barrel jack will be illuminated. If the power LED is not illuminated please verify that the power source is enabled.

17.2.2 DHCP Conflicts

The E2CLink is configured to act as a DHCP server by default. If there are other network connections enabled, DHCP conflicts may occur and prevent the E2CLink's Management Console from being accessed. Please disable any network connections besides the E2CLink's Ethernet connection and attempt to connect again

17.2.3 Browser Caching Error

Browsers will cache data from visited webpages in order to reduce data consumption. In many cases different routers will use the same IP address to access their management consoles (192.168.1.1). If the E2CLink's Management Console will not load please clear your browser's cache or try connecting to the Management Console in a private browsing window.

17.3 The E2CLink Disconnects from the Network

Devices connected to cellular networks are often disconnected to alleviate network congestion after a period of inactivity. If your device is disconnecting from the network after a period of inactivity, please check that the WANWatchdog on the E2CLink is enabled and properly configured. Please refer to section 13.2 in this user manual for instructions on configuring the WANWatchdog.

Devices may also disconnect from the network due to a loss of signal, please refer to section 17.1 to troubleshoot your device's signal strength.

18. GPL Compliance

In compliance with the GPL version 2, we are pleased to provide our modifications to the WRT open source code. Please send an email to licensing@nimbelink.com for more information.

19. Federal Regulatory Licensing

19.1 Export Control Classification Number (ECCN)

ECCNs are five character alpha-numeric designations used on the Commerce Control List (CCL) to identify dual-use items for export control purposes. An ECCN categorizes items based on the nature of the product, i.e. type of commodity, software, or technology and its respective technical parameters.

All Skywire Modems: 5A992.a

19.2 Harmonized Tariff Schedule Code

HTS Code: 8517.62.0010